

Quantum Computing and the Future Internet

Data Privacy: De-Identification Techniques

Quantum Cryptology: The Good, the Bad, and the Likely

The Python Programming: Processing NVD Data

# Quantum Cryptography

## Myths, Legends, and Hypothesis

Practical Cryptography and the Quantum Menace

# Table of Contents

## DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

### Feature

#### 14..... **Quantum Cryptography: Myths, Legends, and Hypothesis**

*By Jeff Stapleton – ISSA member, St. Louis Chapter*

Quantum computers offer unprecedented cryptanalysis that will break legacy asymmetric cryptography. Consequently, organizations will need to undergo a cryptographic transition, migrating to post-quantum cryptography (PQC), but the questions are what, when, and how. This article discusses myths, legends, and hypothesis regarding the quantum menace.

#### 19 **Quantum Computing and the Future Internet**

*By Tajdar Jawaid - ISSA member, UK Chapter*

This article discusses quantum computing key concepts, with a special focus on quantum Internet, quantum key distribution, and related challenges.

#### 26 **Data Privacy: De-Identification Techniques**

*By Ulf Mattsson – ISSA member, New York Chapter*

This article discusses emerging data privacy techniques, standards, and examples of applications implementing different use cases of de-identification techniques. We will discuss different attack scenarios and practical balances between privacy requirements and operational requirements.

#### 33 **Quantum Cryptology: The Good, the Bad, and the Likely**

*By Frank Gearhart – ISSA Senior Member – Colorado Springs Chapter*

In this article the author looks at some of the current research in quantum cryptology, some near-term recommendations, and what we might expect from quantum cryptology in the near future.

#### 37 **The Python Programming: Processing NVD Data**

*By Constantinos Doskas – ISSA Senior Member, Northern Virginia Chapter*

This article continues our discussion on database programming by exploring methods of downloading data from websites, loading them on databases, and analyzing them.

### Also in this Issue

#### 3..... **From the President**

#### 5..... **Sabett's Brief**

Does Quantum Computing Mean R.I.P. PKI?

#### 6..... **Women in Cybersecurity**

Disinfecting Our Pandemic and Business Continuity Plans

#### 7..... **The Cryptic Curmudgeon**

Where Do You Buy Your Crypto?

#### 8..... **Open Forum**

Mastering Your Failure in Security

#### 9..... **Privacy**

More Than a Trace of Doubt

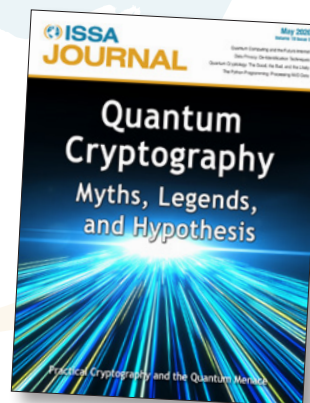
#### 10..... **Security in the News**

#### 11..... **Crypto Corner**

Winning the Red Queen Race

#### 12..... **Association News**

#### 36..... **Career Center**



©2020 Information Systems Security Association, Inc. (ISSA)

The ISSA Journal (1949-0550) is published monthly by  
**Information Systems Security Association**  
1964 Gallows Road, Suite 310, Vienna, VA 22182  
+1 (703) 382-8205 (local/international)



## Hello, ISSA Members and Friends

Candy Alexander, International President



May has come upon us quickly, and like many of you I had hoped that we would begin to see some return back to our “normal” lives and schedules. However, I think it is reasonable to expect that we will be in a social distancing world for the foreseeable future. Like many times throughout my life, that means looking to move the challenging situation into a positive opportunity.

When I stop to reflect upon how much our world has changed, I can choose to focus on the negative: not being able to go to public events such as traveling to attend ISSA events or conferences.

The perceived hardship such as not being able to do activities in the same way things used to be done is really minor. I say perceived because once the new way of doing things had been identified, I have more time to do activities I never had time to do before. For instance traveling—the time to get to an event or client site—took time away from my family or ability to focus on learning.

Rather than spending x amount of time traveling, I can simply open up my virtual conferencing application and participate. With this newfound time I am now able to dive deep into those areas of security that I’m interested in, rather than “have to do.” Things such as catching up on ISSA recorded webinars or trying to liven things up on ISSA’s social link (ISSA members-only portal when you log in to the ISSA website\*). There is some pretty cool stuff going on!

Much like my experience in refocusing my way of “doing things,” the ISSA headquarters support team has been busy in a similar exercise, but on a much bigger scale as you can imagine! Our continued support of the chapters remains a top priority, with several continued efforts such as chapter leader’s meetings, chapter dues payment process refinements to expedite payments back to the chapters, and a few others.

As cybersecurity professionals, we have an extreme need to learn quickly what the best ways are to address the new risk landscapes. To assist our members in this regard, ISSA International has been working on several initiatives to provide you with learning opportunities that are appropriate to the current world we live in, both in program content and delivery methods.

We have been looking to meet the challenge of replacing ISSA in-person events, such as our newly relaunched/re-branded **ISSA Cyber Executive Forum**, to a high-value virtual experience. We are taking our virtual meetings to a whole new level, while providing interaction and collaboration between our members. I encourage all cyber executives to check out our [upcoming program](#) scheduled for mid-May.

ISSA International will be increasing the number of webinars offered with several planned, including those to be hosted by our new International Special Interest Groups (SIGs). The vision for the SIG webinars is to introduce the key issues or talking points that we need to consider and use those in conversations at the local level. We encourage all our members to participate in the webinars and, if you are so inclined, continue the conversation over in the SIG areas in our social link portal.

Like so many others, I choose to remain positive through this crisis. I have faith in our Association, our support team, and most of all you. Together we can overcome the challenges we face by supporting each other and sharing our incredible collective knowledge. Together we can accomplish great things!

Until next time, I wish all of you, your colleagues, friends, and loved ones to stay healthy!

Candy Alexander, CISSP CISM  
ISSA International President  
[Candy.Alexander@ISSA.org](mailto:Candy.Alexander@ISSA.org)

\* Safari users may experience difficulty loading the page; if so, try Chrome or Firefox.

# DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY



## International Board Officers

### President

Candy Alexander  
Distinguished Fellow

### Vice President

Deb Peinert  
CISSP, ISSM

### Secretary/Director of Operations

Shawn Murray, C|CISO, CISSP, CRISC,  
FITSP-A, C|EI, Fellow

### Treasurer/Chief Financial Officer

Pamela Fusco  
Distinguished Fellow

## Board of Directors

Betty Burke, CISSP, CISA

Bill Danigelis, Honor Roll, Senior Member

Mary Ann Davidson  
Distinguished Fellow

Ken Dunham, CISSP, CISM,  
Distinguished Fellow

Alex Grohmann  
CISSP, CISA, CISM, CIPT, Fellow

Rob Martin, CISSP, Senior Member

Lee Neely, CISSP, CISA, CISM

Wayne Proctor, CISSP, CISM, CISA,  
CRISC, Distinguished Fellow

David Vaughn, C|CISO, CISSP, LPT,  
GSNA, Senior Member

## Information Systems Security Association

1964 Gallows Road, Suite 310, Vienna, VA 22182  
+1 (703) 382-8205 (local/international)

The Information Systems Security Association, Inc. (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for security professionals. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial, and government.

The ISSA international board consists of some of the most influential people in the security industry. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as the preeminent trusted global information security community.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

**ISSA**  
**JOURNAL**

Now Indexed with EBSCO

Editor: Thom Barrie

[editor@issa.org](mailto:editor@issa.org)

Advertising: [vendor@issa.org](mailto:vendor@issa.org)

## Editorial Advisory Board

James Adamson

Jack Freund, Senior Member

Michael Grimaila, Fellow

Yvette Johnson

John Jordan, Senior Member

Steve Kirby – Chairman

Joe Malec, Fellow

Abhinav Singh

Kris Tanaka

Joel Weise,  
Distinguished Fellow

Branden Williams,  
Distinguished Fellow

## Services Directory

### Website

[webmaster@issa.org](mailto:webmaster@issa.org)

### Chapter Relations

[chapter@issa.org](mailto:chapter@issa.org)

### Member Relations

[memberservices@issa.org](mailto:memberservices@issa.org)

### Executive Director

[execdir@issa.org](mailto:execdir@issa.org)

## Advertising and Sponsorships

[vendor@issa.org](mailto:vendor@issa.org)

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to

the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect

the official policy of ISSA. Articles may be submitted by members of ISSA. The articles should be within the scope of information systems security, and should be a subject of interest to the members and based on the author's experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent cor-

poration and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see [www.issa.org](http://www.issa.org).

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.

## Does Quantum Computing Mean R.I.P. PKI?

By Randy V. Sabett – ISSA Distinguished Fellow, Northern Virginia Chapter



Several years ago, one of my PKI buddies and I spontaneously started singing a variation on the REM song “It’s The End Of The World As We Know It” after engaging initially in a conversation about the movie *Sneakers* and then extending the underlying concepts in the movie to quantum computing. As you have likely seen, a number of reports (not all of which are necessarily well-founded) have been published over the years stating that quantum computing will make some encryption algorithms obsolete. While a sky-is-falling position may garner eyeballs, the likelihood is slim that complete failure of encryption over the Internet will occur, at least anytime in the near future. A variety of reasons exist as to why this is the case.

First, quantum computing is in its infancy and its power has yet to be even partially tapped. Although the technology is racing ahead, most experts do not think that (a) quantum computers with enough power or (b) specific-use algorithms designed for applying quantum computing to cryptography will be available anytime soon. In one specific example involving cryptography, Shor’s algorithm for factoring integers has the potential for breaking certain types of PKI. Because of how it works, it has garnered the attention of experts in quantum computing. The estimated power needed for Shor’s algorithm to be a serious contender for breaking PKI (as compared to other traditional computing platforms) likely will not be available for at least multiple tens of years. Keep in mind that today’s largest quantum computing platforms have fewer than 100 qubits, with Google (at the time of

this writing) holding the lead with a 72 qubit quantum processor.

Second, efforts have been underway for a while to prepare the cryptographic world for adapting to quantum computing. Most notably, NIST has launched a [Post-Quantum Cryptography](#) project. The project seeks to “solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.” The initial Federal Register Notice requesting submission require-

---

**It’s the end of PKI as we know it.**

**It’s the end of PKI as we know it.**

**It’s the end of PKI as we know it.**

**And the Internet is fine.**

---

ments and evaluation criteria dated [August 2, 2016](#), was followed by a request for nominations of candidate algorithms on [December 20, 2016](#). First round candidates were posted in December of 2017, followed by a down-select to 17 second-round public key encryption candidates on January 30, 2019. Comments are still being accepted, with the most recent set being submitted in April of 2020.

The NIST project means that post-quantum cryptography has already been under intense study for almost four years. The government intends that “the new public-key cryptography standards will specify one or more additional un-

classified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.”

It seems unlikely that quantum computing will pose a serious problem for public key algorithms, at least in the near term. When NIST approves post-quantum public key cryptography algorithms for release; however, the threat of quantum computers to existing standards will need to be re-assessed. It’s entirely possible that the hope for a universal decryptor (think: *Sneakers*) will not actually be realized. Alternatively, all current public key algorithms could be in grave danger.

In any event, the next decade or two will likely bring significant changes to public key algorithms. With post-quantum cryptography, perhaps we’ll all be “Shiny Happy People Holding Hands” (OK, arguably that was a stretch). Have a good May sheltering in place!

### About the Author

Randy V. Sabett, J.D., CISSP, is an attorney with Cooley ([www.cooley.com/rsa-sabett](http://www.cooley.com/rsa-sabett)), a member of the advisory board of the Georgetown Cybersecurity Law Institute and the RSA Selection Committee, a member of the Cyber Leadership Council in the U.S. Chamber of Commerce, and is the former Senior VP of ISSA NOVA. He can be reached at [rsabett@cooley.com](mailto:rsabett@cooley.com).



## Disinfecting Our Pandemic and Business Continuity Plans

By Curtis C. Campbell – ISSA Senior Member, Chattanooga Chapter

*The flattening of the pandemic curve and the jump start of the economy bring hope and anticipation for the health and prosperity of our nations and global society. No doubt we are ready to get moving again to revitalize businesses and propel forward to a more normal time. With that brings a call to action on cybersecurity governance we should not ignore. This article looks at a reality check of reviewing and updating organizational pandemic and business continuity plans.*

The pandemic caught us off guard. Unexpectedly, the world turned off as we all went home to shelter in place without preparation for continuity of work, life, and toilet paper. In cybersecurity one of the key governance activities to support ongoing operations is business continuity management. The objective is to make the organization more resilient to potential threats and allow us to resume or continue operations under adverse or abnormal conditions. In the past, business continuity plans were generally thought of in terms of infrastructure loss or physical location alteration. In best cases these are tested annually. Were our pandemic plans? In the worst of cases, and prior to the COVID-19 pandemic, many pandemic plans may have been stored away, gathering dust in secure portals and shared drives on the network.

Cybersecurity resilience is the ability to adapt to change while protecting the business and its customers from all types of disruptions and disasters. Organizations create IT resiliency with systems of prevention and recovery to deal with potential threats. The goal is to enable

ongoing operations before and during execution of the disaster or crisis. In the past, we may have thought through this in terms of business functions caught off-guard by an incident that took our critical systems off-line. Safe to say, we are now in a different frame of mind. Adapting our business continuity plans to updated pandemic plans is timely as nations prepare to carefully phase organizations and the workforce back in.

By rapid immersion we can now attest to being experienced in a pandemic. What now? It is time to disinfect and wipe off our cybersecurity plans. And as we review our organizational business continuity and pandemic plans, it also makes sense to review our third parties' policies and plans. If our third parties are not prepared, we really aren't either. Below are some tips to keep in mind when reviewing organizational and third-party business continuity plans and pandemic policies.

### Review the plan's purpose

The purpose of the plan should be clearly stated and include descriptive language, identifying the type and what it focuses on. After experiencing the COVID-19 pandemic, we can easily comprehend this on a different level now. Policy language may need revision. For example, the following language is clear but to the point: Unlike many other catastrophic events, a pandemic will not directly affect the physical infrastructure of an organization. While a pandemic will not damage power lines, banks, or computer networks, it will ultimately threaten all critical infrastructures by its impact on human resources by removing essential personnel from the workplace for weeks or months.<sup>1</sup>

Business continuity planning (BCP) provides structure and outlines steps that business operations can continue successfully through a business disruption. Plans can include requirements for HR, food, safety, transportation, security, and manual procedures outlining instructions to employees and service for customers. The following checklist provides components of the plan to include when updating or analyzing your business continuity plan<sup>2</sup>:

- Roles and responsibilities
- Lines of authority, succession of management, and delegation of authority
- Notification roster and call trees for key individuals, employees, partners
- Recovery point objectives and plans
- Detailed procedures, resources, and logistics for processes and systems
- Procedures for any manual alternatives to automated processes
- Testing plans and training exercises
- Schedules, triggers, and any requirements for plan maintenance and updates

### Assess where the plan stands at present

It is important to review your plan to see how it stacks up to today's environment. Does it contain a pandemic plan or crisis management plan? If not, it is important to prepare a checklist as illustrated below.

### Pandemic readiness program

- A corporate annual test of VPN connectivity

Continued on [page 24](#)

<sup>2</sup> EC-Council C|CISO Body of Knowledge.

<sup>1</sup> Sample language from a third-party pandemic plan.



## Where Do You Buy Your Crypto?

By Robert Slade



Oh, come. I already told you that we were not at the quantum cryptocalypse yet. Last May.

The story of Crypto AG has been hitting the mainstream media. For those living under a rock, I will note that internal histories from the German and American intelligence services, and some of those involved, have confirmed a decades-long project to sell weakened encryption systems to those that the intelligence services wanted to spy on.

It's a fascinating story, touching on such historical cryptographic weirdnesses as the fact that, during the second world war, German and American troops used almost identical devices to protect low-level tactical communications during operations. It is interesting that the vulnerability introduced was not a direct backdoor to decryption, but a weakening of the generation of random (or, more properly, **pseudo**-random) data, which is exceptionally difficult to test for ("Are you **sure** that's random data?" "That's the trouble with random: you're never really sure."). The importance of "random" to cryptography can never be over-stressed, and it's also intriguing that an ability to measure randomness is now seen as one of the true tests of quantum computers.

(In fact, quantum may be very good for crypto. Quantum is really, really good as a source of random. But I digress.)

I am sure that most reading the story will take the lesson that governments and intelligence agencies are perfidious and will mess with anybody's security if it helps them extend their surveillance.

But there is another lesson, if you read the story carefully. It points out how ex-

traordinarily difficult it is to install and hide backdoors in crypto, and hide them for a long time, if you are dealing with people who actually understand the technology. I recall the conspiracy theories around DES, the Data Encryption Standard. Since it was from the NSA, lots of people felt (falsely) that the NSA had secretly built a backdoor into DES and could read everything encrypted with it. The NSA didn't help matters given that, when IBM proposed Lucifer, a Feistel cipher, (why do security people always pick names they should **know** are going to be troublesome?) to NIST, the NSA strengthened one aspect and weakened another. Later it was found that what the NSA did actually protected DES from a particular type of attack. When everyone knows the algorithm, and can test it, it just isn't possible to hide a backdoor for decades on end. That's just an extension of Kerckhoff's famous "law": A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

In reading the story, it is somewhat awe-inspiring to note how much effort was put into protecting the fact that the product being sold was deliberately weakened. The ownership of the company was hidden. Sales calls were made to reassure customers who started to get suspicious. Sales people didn't know they were selling weak technology. (Q: What's the difference between a used-car salesman and a computer salesman? A: A used-car salesman knows when he's lying to you.) And when technical people started to suspect the fact that they were not allowed to fix problems they could see, they were shuffled to other areas, put off, read in, or fired.

(Another random oddity from the story: how many astronomers find their way into security. Is this simply a measure of the fact that many, many more people study astronomy than can actually get jobs in the field? It's sort of like the fact that all tech writers are history majors: if you can write a piece in such a way that a totally random event is invested with significance, then you are qualified to point out what is important in operating a system. Or the fact that all HR people have English degrees: if you know so little about the job market that you go out and get a completely useless degree, then you are qualified to tell people how to plan their careers. But I digress.)

One more lesson from the Crypto AG story: it is yet another illustration of the fact that it is much, much more important to have a good sales team (and possibly bribes) than it is to have an actually functioning technical product.

### About the Author

*Rob Slade is both an artificial intelligence program gone horribly wrong and hooked up to various email addresses—and not. At the same time. The only way to tell is to obtain more information than anyone would want to know about him, available at <http://twitter.com/rslade>. It is next to impossible to get him to take profile or "bio" writing seriously, but you can try at [rmslade@shaw.ca](mailto:rmslade@shaw.ca).*



## Mastering Your Failure in Security

By Edgar Vera – ISSA member, Puerto Rico Chapter

Every successful professional or business person has some traits in common. One that stands out is that they teach themselves whatever they need to learn in order to gain an edge. In my case, I taught myself the aspects of the subjects I needed to learn in order to make better decisions, which in turn made me a subject matter expert (SME) in that particular subject.

The reason I became an SME in particular areas was to learn several ways on how NOT to build a system. I failed during several of these processes, which is how I really learned. This requires one to have an open mind. You need to be prepared to fail as many times as you have to in order to learn how *not* to build or create something.

It's easy to have experience in something that you keep repeating over and over, without any repercussion of the consequences. It is difficult to have experience when you take a risk in learning something new that added some form of value and growth for your profession or business.

For example, let's compare how to build a server today versus the 1990s. In the 1990s, which is when the technological boom occurred, we had to build our servers and systems manually. From server acquisition and its required components to the software required to run it, everything was installed and configured manually.

No GUI or fancy UX. If there was any conflict between components, we needed to troubleshoot and figure out what was happening, without "googling" the problem.

This gave me exposure and an edge that many in the industry today don't have or can't conceive or understand. That edge is about learning and understanding how each component worked. From hardware to software, I had to learn how everything within the system worked, which as a consequence made me an SME in that particular area during the time.

Today, building a server is as easy and cheap as buying a VPS host for \$5 a month, installing and configuring it via a GUI wizard with any operating system the particular host offers and you are done.

Don't get me wrong, I'm glad we've gotten this far in this aspect.

The problem comes when you start looking for IT or cybersecurity jobs and face the frustration when competing out there with the other professionals. These professionals know what they are doing and they became as good as they are because they did what I'm telling you. They took their time to learn how to build a system from the ground up, then break the system, then build it up again and again.

For example, let say that you built a system using VMware. You created a server and installed a manufacturing production system. We all know that VMware provides a way to automatically restore points based on imaging—and this is a great utility—but not all companies are allowed to use this option based on the complexity of their production business.

Even in the best-planned scenarios based on disaster recovery plan (DRP) exercises, there is always something that won't let you use this option, for which you'll have to troubleshoot the old fashioned way.

In highly regulated companies, such as pharmaceuticals, manufacturing processes are bound to procedures that are

periodically audited. This means that you can't shut down a system just because you think you have to. This has happened to me and many others where the company is in the middle of production and a particular system being used in the process becomes unresponsive or it isn't registering any data and can't be interrupted because if you do then it could cost millions in losses.

What would you do?

The advantage of knowing and understanding the intricacies of how a system operates and works is that you can troubleshoot it without having to incur losses for the company. I mean, that is why you are there, correct?

This is only one of many reasons why you should practice by failing in security or any information technology-related subject. You need to be prepared for anything. You have to understand that you can only achieve this by practicing. In the field of information technology/cybersecurity, the only way you can learn is by experiencing everything yourself. Make sure you have your own IT/cybersecurity lab in place. Experience only comes by practicing.

Knowing where everything is, how it works, and how each part fits together will save you time and also your reputation. The only thing keeping us alive as professionals is our own initiative to keep learning and also practicing everything we learn.

### About the Author

Edgar Vera is experienced in implementing systems and assessing weaknesses in pharmaceutical companies with over 20 years of experience. He currently serves as a consultant for CyberInfoVeritas and is also pursuing a PhD in cybersecurity. He may be reached at [cyberinfoveritas@gmail.com](mailto:cyberinfoveritas@gmail.com).



## More Than a Trace of Doubt

By Karen Martin



The current coronavirus pandemic is the latest crisis to skew the balance between public safety and civil liberties. Proposals to use potentially invasive measures to slow the spread of infection followed hot on the heels of the virus. Unfortunately, during a crisis we have to make important decisions very quickly with imperfect information, which means we are likely to make mistakes. If we *under-react*, lives are unnecessarily lost; if we *over-react*, we risk further erosion of civil liberties.

The electronic contact tracing schemes either proposed or adopted over the last few months all involve some risk to privacy. The good news is that a wide variety of solutions, from voluntary, privacy-centric tracing apps to mandatory comprehensive multi-source data collection, are already in use, so we may be able to see which approaches are most effective. The bad news is that voluntary, privacy-centric solutions may not be as effective as mandatory, privacy-invasive solutions.

Consider four different technical solutions that may help slow the spread of an infectious disease. The first is electronic [quarantine fences](#), which use location-tracking wristbands or cell phone location information to monitor the movements of individuals ordered to stay in quarantine. If the monitoring proves to improve quarantine effectiveness and if it is restricted to high-risk individuals, the public health benefit will likely outweigh the privacy risk.

The second approach uses anonymized, aggregated [location data](#) routinely collected by various apps—with user consent—to track movement trends. This data might help us evaluate the effectiveness of voluntary social distancing or predict the spread of the virus based on the probability of people from different

locations coming into contact with each other. The aggregated data is a relatively low privacy risk, and this approach might be acceptable, if people continue to trust apps to collect location information and if the data actually turns out to help slow the spread of infectious diseases. It is too early to tell whether those two conditions will be met during the next pandemic.

In the third approach, cell phones transmit anonymous ID codes using Bluetooth Low Energy as [proximity beacons](#). If two phones are close enough to hear each other's broadcasts, their users are close enough for one to infect the other. Each device keeps a rolling log of the ID codes it hears. If a user is diagnosed with the infection, the ID codes in its contact log can be added to a centralized exposure list. Every device using the app would periodically check the exposure list to see if any of its own ID codes were detected by someone diagnosed with the disease.

There are several versions of this approach in development or already in use, but most developers are likely to use the approach favored by [Google and Apple](#), who are working together to add privacy-centric exposure notification capability at the operating system level on iPhones and Android phones. Their approach will use temporary ID codes that rotate every 10-20 minutes. The logs will be stored on the devices, unless the user chooses to upload them to an exposure list. Google and Apple will not support mandatory apps; users must choose whether or not to opt-in.

This approach limits privacy risk, but it may not be effective. Experts believe the apps will only help if at least [60 percent of the population](#) use them, but the apps already available are not widely used: reported [adoption rates](#) are six percent in

India, eight percent in Australia, and 20 percent in Singapore. If a US app were available, a recent poll suggests that only [41 percent of Americans](#) would use it.

Secondly, other experts note that a voluntary app with anonymous users is an invitation to abuse, suggesting that some people might lay false trails, hackers could mount denial of service, and "... little Johnny will self-report symptoms to get the whole school sent home."

The fourth approach, used in [South Korea](#), collects cell phone location information, payment card transaction data, and CCTV footage to verify patients' reported movements. The government publishes case information including the patient's age, gender, date of diagnosis, and the places the patient recently visited. This may be an effective way to identify people at risk of infection, but it might also allow armchair sleuths to figure out which 52-year-old male neighbor visited the local love hotel last Tuesday night.

These seem to be the best options currently available for slowing the spread of disease, and, predictably, they all appear to be flawed. Quarantine fences only solve a narrow problem; aggregated location data may or may not be helpful; users may refuse to use voluntary proximity beacons; and many countries may not tolerate comprehensive data collection. Let us hope that we learn which solutions help and decide how much privacy risk we can handle before the next pandemic hits.

### About the Author

Karen Martin is a San Jose based Information Security Engineer. She may be reached at [kjlmartin@gmail.com](mailto:kjlmartin@gmail.com).

## News That You Can Use...

Compiled by Kris Tanaka – ISSA member, Portland Chapter

### Congress Has Now Introduced 32 Crypto and Blockchain Bills

<https://www.forbes.com/sites/jasonbrett/2020/04/28/congress-has-introduced-32-crypto-and-blockchain-bills-for-consideration-in-2019-2020/#6e6cc3661d61>

No longer just for computer science and technology geeks, cryptocurrency and blockchain have gone mainstream. From cryptocurrency regulations to how blockchain technology can be promoted, US legislators have introduced 32 bills for consideration in the 116th Congress.

### Clever Cryptography Could Protect Privacy in Covid-19 Contact-Tracing Apps

<https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/>

Smartphone data surveillance—is it an invasion of privacy? Or is it a possible tracking solution that could help rescue the global economy and save lives? Perhaps it is both. Researchers say that you can develop an app that serves both Covid-19 contact-tracing and preserves user privacy. Several projects are now underway that will allow you to have your cake and eat it too.

### Amazon, IBM And Microsoft Race to Bring Global Access to Quantum Computing

<https://www.cnet.com/news/amazon-ibm-and-microsoft-race-to-bring-global-access-to-quantum-computing/>

Although quantum computing won't replace standard computers, it has the potential to deliver breakthroughs on very specific and complex computational challenges. As the computing revolution moves from theory to reality, there are a growing number of companies who are neck-and-neck in the competition to take the lead in this new space of opportunity. Who will be the first?

### Government VPN Servers Targeted in Zero-Day Attack

<https://threatpost.com/government-vpn-servers-zero-day-attack/154472/>

Sometimes the tools you employ to keep your organization secure can be used against you. In April, at least 200 Chinese government virtual private network (VPN) servers were compromised in a zero-day exploit. Although it is not clear what the criminals were after, researchers suspect the attack may have been executed by DarkHotel, an APT associated with carrying out prior cyberespionage efforts in China, North Korea, Japan, and the United States.

### Microsoft Would Like to Use Your Brainwaves to Mine Cryptocurrency, Please

<https://www.popularmechanics.com/technology/a32318654/microsoft-brainwaves-mine-cryptocurrency/>

Using brainwaves to replace the computation work in mining cryptocurrency sounds like it should belong in a science fiction movie. And for the time being, it remains just an idea. But according to a patent filed by Microsoft in March, this future-forward concept could be put into practice sooner than you think.

### How Covid-19 Is Affecting the Digital Signature Industry

<https://www.biometricupdate.com/202004/how-covid-19-is-affecting-the-digital-signature-industry>

As we navigate the “new normal” created by Covid-19, one thing is clear—digital transformation is no longer optional. Life and business must go on, even in quarantine. But what do you do when you need to sign a contract or an official document? How can you safely and securely confirm the identity of a person or an institution when all your interactions are handled remotely? The digital signature. Although we may shift back to previous business practices after the pandemic subsides, some transformations, like the digital signature, may be permanent.

### Cyber Criminals Are Trying a New Trick to Cash in on Zoom's Popularity

<https://www.zdnet.com/article/cyber-criminals-are-trying-a-new-trick-to-cash-in-on-zooms-popularity/>

With the coronavirus pandemic quickly impacting how we live and work, the bad guys now have new vectors to explore. What's the latest vulnerability? Thanks to the surge in using video conferencing platforms like Zoom, criminals have discovered that they can slide in cryptocurrency-mining malware into legitimate installer programs, allowing them to hijack the processing power of the infected computer without being detected.

### Trump Betting Millions to Lay the Groundwork for Quantum Internet in the US

<https://www.cnn.com/2020/04/27/us-laying-groundwork-for-a-quantum-internet.html>

While other areas of scientific research are experiencing budget cuts, the Trump administration is prioritizing quantum information science by proposing a 20 percent increase in funding for 2021. By helping to accelerate the development of a quantum Internet, the administration is hoping to give researchers the tools to potentially reinvent a variety of fields including cybersecurity and material science.

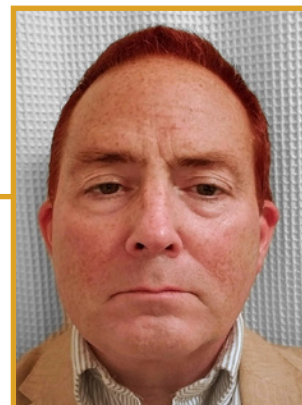
### The Future of Quantum Computing in the Cloud

<https://searchcloudcomputing.techtarget.com/tip/The-future-of-quantum-computing-in-the-cloud>

Even though we are still years away before quantum computing is projected to deliver practical value, cloud service providers are looking to get ahead of the curve by preparing for a time when the two technologies will join forces. Do you think quantum computing in the cloud has the potential to disrupt your organization? Security in the News would like to know if you are getting ready for a quantum revolution. Share your thoughts with editor [Thom Barrie](#).

## Winning the Red Queen Race

By **Luther Martin** – ISSA member, Silicon Valley Chapter



Part of Lewis Carroll's *Through the Looking Glass* can seem distressingly relevant to people working in information security. At one point, Alice notes that she and the Red Queen are running but not making any forward progress. The Red Queen doesn't find this unusual. In her realm, she notes, "it takes all the running you can do, to keep in the same place."

Maybe the Red Queen was the CISO of Wonderland.

The situation where hard work is only enough to break even has become known as a "Red Queen race." Biologists use the term to describe the never-ending evolutionary arms races that end up with no net gain for either competitor. For millions of years, for example, there has been an ongoing battle between plants and herbivores: plants develop defenses like toxins, herbivores develop an immunity to the toxins, plants try another defense mechanism, etc. If we could somehow pull off a *Jurassic Park* and introduce dinosaurs into today's world, they wouldn't do well because they missed out on the last 65 million years of this contest.

A similar Red Queen race between attackers and defenders takes place in cyberspace: attackers invent new attacks, defenders develop new defenses, and the cycle repeats. And just as dinosaurs would be hopelessly outclassed by modern plants, bacteria, and viruses, defenses from only a few years ago would be ineffective against today's attackers. If a hacker from today could time travel back to the year 2000, his more advanced knowledge and tools would easily defeat the state-of-the-art in defensive technology available then.

While plants and animals have no control over how they will evolve, we are smart enough to be able to analyze our

situation and learn how to do it better. Applying proven systems engineering principles may be what we need to do this.

[Systems engineering](#) is an interdisciplinary field that draws inspiration from many technical and non-technical disciplines to help create successful systems. You can't build complex systems like spacecraft without it. If you replace the word "successful" with the word "secure" in that definition, you have a good summary of information security, so it shouldn't be too surprising that the two fields are closely related, even though they require very different thought processes (systems engineers that I've talked to insist that this is a very important and under appreciated difference). Being secure is just one aspect of a successful system, so it seems reasonable to assume that information security should be a subset of systems engineering.

But the two differ dramatically in practice. The biggest difference may be that systems engineering practices are applied throughout the complete life cycle of a system, but security is too often added after systems are designed, sometimes even after they're implemented. This might suggest that the Titan [Epimetheus](#) ("afterthought") from Greek mythology should be the patron god of information security. Epimetheus was a bit of a clown who didn't take his job too seriously. We probably shouldn't use him as a role model or look to him for guidance.

As a team of researchers from RAND [noted](#), "Poor systems security engineering is very difficult to mitigate by overlaying security controls, whereas security controls overlaid on a sound, secure design can be quite effective." So it's possible to greatly improve the security of systems, but this has to be an

integral part of their complete life cycle. If you design a system well and use secure principles to guide its implementation, then you may achieve the best possible result. But if you wait until after a system is designed and then try to make it secure, you are probably doomed to fail. Instead of a system that is reasonably secure, you will end up with something that may essentially be *impossible* to make reasonably secure.

On the other hand, systems engineering isn't cheap, which seems to limit its use. Its popularity seems proportional to the cost of the project where it's used. It's commonly used in big government projects like spacecraft and major military systems where the right functionality is of the utmost importance and other factors like cost are less critical. It's almost never seen at Silicon Valley startups. We probably can't change what happens at these two extremes, but we might be able to use ideas from it to affect what happens in between them.

Systems engineers tell me that if we used their approach, it would make our jobs much easier. They might be at least partially right. Maybe using their ideas can give us a way to reduce that never-ending stream of patches and updates that we suffer. If it can do that, it's worth looking at. It can't be worse than our current Red Queen race, can it?

### About the Author

*Luther Martin has survived over 30 years in the information security industry, during which time he has probably been responsible for most of the failed attempts at humor in the ISSA Journal. You can reach him at [lwmarti@gmail.com](mailto:lwmarti@gmail.com).*

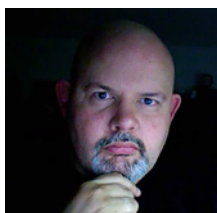


## News from the Foundation

### The George “Chip” Meadows Memorial Scholarship

**T**he Alamo ISSA Chapter has announced they have memorialized one of their scholarships in honor of a past chapter president and active member of the San Antonio information security community: the George “Chip” Meadows Memorial Scholarship. He passed away at the age of 57 on September 23.

Meadows was an ISSA Distinguished Fellow and a volunteer who organized various information security functions and gave presentations and talks on technical topics in his field. He designed and delivered cyber exercises for the Center for Infrastructure Assurance and Security as a project technical lead and traveled across the nation assisting state and local governments in protecting their infrastructure from cyber attacks.



**George “Chip” Meadows**  
Photo Credit: University of Texas, San Antonio

He is known within the DefCon community and the FBI Citizens Academy. An active member of the San Antonio B-sides community, Alamo ISSA, ISACA, and InfraGard chapters, Meadows was also an elder within his congregation at Baruch Eloheinu. In addition to being an advocate for information security, most remember him as being a genuine friend with a kind soul. He leaves behind his wife, Anna Meadows, and son Matthew.

### 2020 Cybersecurity Scholarships

The application period for the 2020 ISSA Education Foundation scholarships, which opened April 2, will continue through June 15, 2020. The application form is available on our website, [ISSAEF.org](https://www.issaef.org), with the following eight scholarships available:

- **Howard Schmidt Memorial Scholarship**  
for undergraduates - \$3,500
- **E. Eugene Schultz, Jr. Memorial Scholarship**  
for graduates - \$3,500
- **Shon Harris WIS Memorial Scholarship**  
for women in security - \$2,000
- **Metro Atlanta ISSA Chapter scholarships**  
three \$1,000 for local universities
- **Alamo Chapter scholarships: George “Chip” Meadows Memorial Scholarship** (\$1,500) and one \$500 scholarship for local universities

Help spread the word about these great opportunities to your friends and family **at no cost to you**—just use Amazon Smile while shopping online and automatically. With absolutely no

cost to shoppers, **0.5 percent** of eligible purchases will be donated by Amazon to our scholarship fund! It’s simple: start the purchase on <https://smile.amazon.com>, select “[ISSA Education and Research Foundation Inc](https://www.issaef.org)” (needs to be done only the first time) and shop as usual. Do not forget to tell your family/friends to do the same.

Done with all your shopping? ISSAEF is a 501(c)3 public foundation—you can make an individual, tax-deductible donation to our scholarship program through our website <https://www.issaef.org/donate>.

**SEEKING VOLUNTEERS** to participate in short-term projects, scholarship publicity, fundraising, and governance of the Foundation. Those interested in joining a truly dedicated and enthusiastic group, please send an email with your background to [volunteer@issaef.org](mailto:volunteer@issaef.org).

Like us on [Facebook](#) and [LinkedIn](#).

## ISSA International Awards

*Congratulations to the 2019 international award winners. We have offered the recipients an opportunity to reflect upon receiving their awards and the state of information security.*



### ISSA Hall of Fame Dan Geer

**What do you consider to be your most significant accomplishment as an information security professional?**

I’ll nominate a group accomplishment rather than an individual

one, but the most significant is surely to have made the practice of information security a quantitative endeavor. No one of us can take the credit alone, but the group that made it happen cannot number more than fifty and is probably less than half that. I’ll claim one of those slots.

### What is the most important issue facing the industry?

There is no one issue in the technical sense, but the meta issue in the policy sense is whether we steer by mean time between failure (driving MTBF to infinity) or mean time to repair (driving MTTR to zero). Yes, one can just mix the two up, doing a little of the one and a little of the other. The question is, however, which is optimal and why.

Choosing MTBF as the core driver is built on the assumption that vulnerabilities are sparse, not dense. If they are sparse, then the treasure spent finding them is indeed well spent so long as we are not deploying new vulnerabilities faster than we are eliminating old ones. If they are dense, then any treasure spent finding them is more than wasted, it is disinform-

**You have not picked a profession, you have joined a crusade.**

mative. The question then for you is whether you think you can get rid of a big enough fraction of your vulnerabilities to meaningfully achieve a vulnerability-free state, one which does not require a playbook for emergencies.

If we cannot answer whether vulnerabilities are sparse or dense, then should we not default to choosing instant recovery, which is to say a

mean time to repair of zero? If we do choose fast recovery, which is, one would note, consistent with planning for maximal damage scenarios rather than planning for most probable scenarios, we make our paramount security engineering design goal that of no silent failure (not no failure, but no silent failure). The choice here effectively restates the accountant's doctrine of prudence—that of anticipating possible future losses but not future gains.

#### **What is the biggest challenge currently consuming your time and energy?**

The biggest challenge is to see clearly, a challenge not unique to information security though I consider the practice of information security to be the most intellectually difficult vocation on the planet.

We know that optimality and efficiency work counter to robustness and resil-

ience. We know that complexity hides interdependence, and unacknowledged interdependence is the source of black swan events. We know that the benefits of digitalization are not transitive, but the risks are (transitive). We know that because single points of failure (like cable landing points) require militarization wherever they underlie gross societal dependencies; frank minimization of the number of such single points of failure is a national security obligation. Because we know that cascade failure ignited by random faults is quenched by redundancy whereas cascade failure ignited by sentient opponents is exacerbated by redundancy, we therefore know that preservation of uncorrelated operational mechanisms is likewise a national security obligation – those uncorrelated operational mechanisms are the analog alternative, and only government action can preserve them against the onslaught of “progress.” And I know from the teachings of my career that information security is fundamentally conservative expressly because the conservative understands that ordered liberty depends on putting a speed limit to irrevocable change. Making choices such as these clear to decision makers up and down the ladder will consume the remainder of my career.

#### **What would you like to say to your peers?**

You have not picked a profession, you have joined a crusade.

## **Wisconsin Chapter Patch Tuesday Presentation**

TUESDAY, MAY 12, 2020 • 3:00 PM CENTRAL TIME

### **Starring Lance Spitzner of SANS & The HoneyNet Project** **Also featuring other notable industry leaders**

Lance Spitzner, SANS Institute's Director of Research and Community, is well known as founder of The HoneyNet Project. He will speak on “Leading Change: Build a Security Culture of Protect, Detect, and Respond.”

Learn how to become a far more effective security leader by leveraging the principles of organizational change and embedding security throughout your workforce. Key things you will learn include: How we are driving attackers to target humans; Why so many security initiatives fail at the human level; and What is a strong security culture and two key elements to creating one.

**ONLINE REGISTRATION AVAILABLE UNTIL 5/12/2020: [CLICK HERE](#)**

#### **A few milestones of Dan Geer's illustrious career:**

*The X Window System and Kerberos (1988), the first information security consulting firm on Wall Street (1992), convenor of the first academic conference on mobile computing (1993) and on electronic commerce (1995), the "Risk Management Is Where the Money Is" speech that changed the focus of security (1998), principal author of and spokesman for "Cyberinsecurity: The Cost of Monopoly" (2003), co-founder of SecurityMetrics.Org (2004), author of Economics & Strategies of Data Security (2008), and author of Cybersecurity & National Policy (2010). Creator of the Index of Cyber Security (2011) and the Cyber Security Decision Market (2012). Lifetime Achievement Award, USENIX Association, (2011). Expert for NSA Science of Security award (2013-present).*

## **ISSA.org => Events**

### **WEB CONFERENCE**

[Empowering the Modern SOC – Force Multiplying Analysts by Orchestrating Threat Intelligence](#)  
May 6 @ 1:00 pm - 2:00 pm EDT (US)

### **CHAPTER EVENT, WEB CONFERENCE**

Wisconsin Chapter  
[Starring Lance Spitzner of SANS & The HoneyNet Project](#)  
May 12 @ 4:00 pm - 7:00 pm EDT (US)

### **WEB CONFERENCE**

[Trends and Statistics for Mobile Phishing in the Enterprise](#)  
May 13 @ 1:00 pm - 2:00 pm EDT (US)

### **CYBER EXECUTIVE FORUM**

[May Virtual Cyber Executive Forum 2020](#)  
May 15 @ 9:50 am - 6:00 pm EDT (US)

### **WEB CONFERENCE**

[Current Landscape of Mid-Market Threat Intelligence](#)  
May 20 @ 1:00 pm - 2:00 pm EDT (US)

### **WEB CONFERENCE**

[Threat Reports Undone](#)  
May 26 @ 12:00 pm - 2:00 pm EDT (US)

### **ISSA INTERNATIONAL EVENT**

[CCPA Enforcement: What to Expect after July 1st](#)  
June 3 @ 1:00 pm - 2:00 pm EDT (US)

# Quantum Cryptography

## Myths, Legends, and Hypothesis

By Jeff Stapleton – ISSA member, St. Louis Chapter



**Quantum computers offer unprecedented cryptanalysis that will break legacy asymmetric cryptography. Consequently, organizations will need to undergo a cryptographic transition, migrating to post-quantum cryptography (PQC), but the questions are what, when, and how. This article discusses myths, legends, and hypothesis regarding the quantum menace.**

Quantum computers use quantum bits (qubits) to encode linear algebraic equations that can solve *hard* mathematical problems that are *infeasible* on classical computers. The adjective *infeasible* is chosen carefully, meaning: not possible to do easily or conveniently, that is, something that is impracticable, but not necessarily impossible. Given enough resources such as time, money, and computing power, whether it be a massive supercomputer or a million regular computers, almost any mathematical problem can be solved. After all, we all know the answer is *forty two*. Seriously, there is much research in the development of quantum computers, for example:

- IBM offers its Q Network [4]
- Google is researching quantum processors and algorithms [3]
- Microsoft is developing quantum solutions [10]
- D-Wave is exploring quantum systems [2]

Qubits encode two bits of information using superposition versus classical computers that can only encode one bit. Thus  $N$ -qubits can encode  $2^N$  data bits, an exponential increase. Qubits also share information amongst themselves using

quantum entanglement, where separate particles mirror each other's characteristics. Entanglement has been used as a key management method called Quantum Key Distribution (QKD) for many years. However, if you do not understand quantum mechanics, it's not necessary to understand the risks. The physicist Richard P. Feynman once said: *If you think you understand quantum mechanics, you don't understand quantum mechanics* [13]. So what do you need to know to understand the quantum menace?

Two well-known *hard* mathematical problems are (1) determining discrete logarithms and (2) factoring numbers. For large enough numbers, solving either problem is infeasible by classical computers. This means the amount of computer power is too high, too expensive, or the length of time necessary, many thousands of hours, to solve these problems is too much. When quantum computers are sufficiently stable with enough qubits at low error rates, they will be able to solve these and other problems literally in seconds. Many business problems unsolvable today will be tractable tomorrow. But the question is: how can this computational potential affects today's modern cryptography?



Three well-known asymmetric algorithms will be at risk. Recall that asymmetric algorithms use a key pair, namely a public key and a private key. The private key cannot be determined from the public, based on the infeasibility of hard mathematical problems, namely factorization and discrete logs.

- The RSA public key  $N$  is the product of two prime numbers, called  $P$  and  $Q$ . The RSA private key is computed using  $P$  and  $Q$ . But since factoring large values of  $N$ —today we use 2048-bit numbers (about 618 digits)—is infeasible,  $P$  and  $Q$  cannot be determined. But a quantum computer will be able to factor  $N$  and reveal  $P$  or  $Q$ , and thus computing the private key using a classical computer is relatively easy, since the private key is based on the simple product  $(P-1)$  and  $(Q-1)$ .
- The Diffie-Hellman (DH) public key is the exponentiation of an agreed upon domain parameter, call it  $G$ , raised to a random number, call it  $X$ , so the public key is  $G^X$  with modular arithmetic. Finding the private key from the public key is determining the discrete log. So knowing  $G$  and  $G^X$  the hard problem is to find  $\text{Log}_G(G^X)$ . But likewise, a quantum computer will be able to compute the private key  $X$  from the public key  $G^X$  by a discrete log.
- The Elliptic Curve analog of Diffie-Hellman (ECDH) is the same as Diffie-Hellman using Elliptic Curve Cryptography (ECC) mathematics. Similarly, a quantum computer will be able to compute the ECDH private key from the public key.

All three of these cryptographic algorithms are used to establish symmetric keys. RSA is used for key transport, and both DH and ECDH are used for key agreement. Specifically,

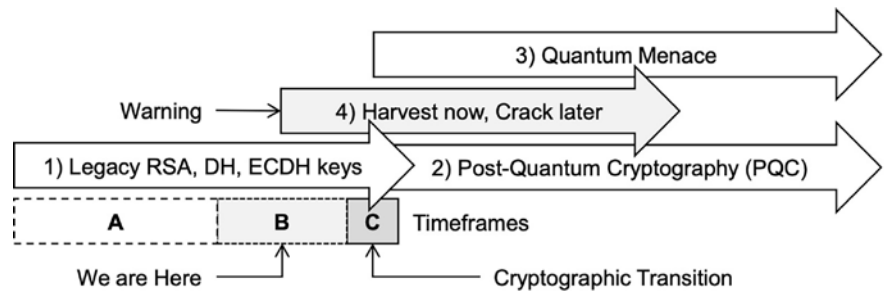


Figure 1 – Arrows of time

the cryptographic protocol Transport Layer Security (TLS) uses RSA, DH, or ECDH to establish two session keys, such as AES-256 for data encryption, and another used as a keyed-hash message authentication code (HMAC) with a hash algorithm such as SHA-256. When a reliable quantum computer becomes available for cryptanalysis, the public key encapsulated within a digital certificate for the TLS protocol can be reversed to determine the private key, so what affect will this inevitable capability have on TLS and other security protocols?

For this next discussion, refer to figure 1. Four arrows, numbered 1, 2, 3 and 4, are mapped to three time frames labeled A, B, and C.

Herein lies the problems:

#### Arrow 1 – the legacy

This arrow represents the current use of legacy asymmetric algorithms (e.g., RSA, DH, or ECDH) for key establishment with TLS. The first time frame (A) was the happy zone when hard math problems were infeasible.

- White Diffie and Martin Hellman published their groundbreaking paper “New Directions in Cryptog-



### Members Join ISSA to:

- Earn CPEs through Conferences and Education
- Network with Industry Leaders
- Advance their Careers
- Attend Chapter Events to Meet Local Colleagues
- Become part of Special Interest Groups (SIGs) that focus on particular topics

**Join Today: [www.issa.org/join](http://www.issa.org/join)**

**Regular Membership \$95\***

(+ Chapter Dues: \$0-\$35\*)

**CISO Executive Membership \$995**

(Includes Quarterly Forums)

\*US Dollars/Year

raphy” in 1976 introducing asymmetric cryptography using discrete logarithms.

- Shortly thereafter, Ron Rivest, Adi Shamir, and Leonard Adleman published their paper “A Method for Obtaining Digital Signatures and Public-Key Cryptosystem” in 1978, expanding asymmetric cryptography using factorization.
- Victor Miller published his paper “Use of Elliptic Curves in Cryptography” in 1985 and independently Neal Koblitz published his paper “Elliptic Curve Cryptosystems” in 1987, both researchers extending asymmetric cryptography with elliptic curve algebra.

**ISSA International Web  
CONFERENCE**

**ISSA Thought Leadership Series**



## Empowering the Modern SOC – Force Multiplying Analysts by Orchestrating Threat Intelligence

**60-minute Live Event: Wednesday, May 6, 2020**

10 a.m. US-Pacific/1 p.m. US-Eastern/6 p.m. London

It's harder than ever before for analysts to keep up. The nature of today's operating environment has resulted in an ever-increasing volume of alerts paired with a growing complexity and scale of subsequent investigations. In this talk we will be discussing in depth what this means in the daily life of analysts, and how imperative it is to force multiply them to enable quicker and more effective response. We will explore the key role of operationalized threat intelligence, and why (and how) orchestrating it alongside SOC processes and technology can enable organizations to be more effective when detecting and responding to threats.

**Moderator:** Alex Grohmann, Founder, Sicher Consulting

**Speakers:** Sean Ennis, Product Manager, RSA & Iain Davison, Security Architect & Technical Director of Strategic Alliances & OEM, ThreatConnect

Generously co-supported by

**RSA** NETWITNESS  
PLATFORM

**ThreatConnect**

Click [HERE TO REGISTER](#).

For more information on these or other webinars:

[ISSA.org=>Events=>Web Conferences](https://issa.org=>Events=>Web%20Conferences)

### Arrow 2 – PQC

This arrow represents the future use of post-quantum cryptography (PQC) algorithms. The National Institute of Standards and Technology (NIST) is currently managing yet another cryptographic transition. Ralph Poore and Jeff Stapleton published their paper “Cryptographic Transition” [14] in 2006. Previously, NIST has facilitated the replacement of DES with AES, the replacement of SHA1 with SHA2, and the alternative SHA3 algorithms. The good news is that NIST is pretty good at such transitions. The NIST Post-Quantum Cryptography (PQC) [11] program is selecting the algorithms that will run on classical computers but are designed to be resistant to quantum computer cryptanalysis.

### Arrow 3 – the quantum menace

This arrow represents the quantum menace, basically cryptanalysis using quantum computers. The Peter Shor paper, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” proposed using quantum computers in 1997. This paper explained how a quantum computer might be used for solving the two hard mathematical problems, factorization for breaking RSA, and discrete logs for breaking DH and ECDH. The third time frame (C) is when the cryptographic transition from legacy asymmetric cryptography to PQC algorithms occurs. When this happens and how long it will take, are of course some of the big questions. Information security professionals are told that quantum computers are inevitable, the theoretical issues have been resolved, and it is just an engineering problem.

### Arrow 4 – the hidden threat

This arrow represents the hidden threat, when bad actors are harvesting TLS sessions during the second time frame (B) that is now; *we are here*. The recordings capture the exchange of public keys, possibly including ephemeral keys that are still safe because the private key cannot be determined from the public keys. Ephemeral keys are additional asymmetric keys used once per session so that if the static private keys are compromised, the attacker cannot replay the TLS key handshake because the ephemeral keys are unavailable. However, the quantum menace equally applies to both static and ephemeral keys. Thus, when the third time frame (c) arrives, the bad actors can determine the private keys, derive the session keys, and access the encrypted data.

Ephemeral keys have been available for Diffie-Hellman (DHE) since SSL v3.0 in 1996 and introduced with Elliptic Curve Diffie-Hellman (ECDHE) for TLS v1.1 specifications in 2006. TLS v1.3 [5] published in 2018 deprecated RSA key transport (RSA digital signatures remained valid) and mandated the use of ephemeral keys. As noted, the security concept being that if the server private key was compromised, bad actors who had recorded the TLS session could not replay the negotiation because the ephemeral keys are unavailable. But, ephemeral keys will be vulnerable to the quantum menace.

## Hypothesis

The hypothesis is about when the cryptographic transition needs to occur. Michele Mosca [12] provided an inequality equation  $D + T \geq Q_c$  where  $D$  is the amount of time needed to secure data,  $T$  is the time for the cryptographic transition, and  $Q_c$  is the time for the quantum menace. Called Mosca's Inequality, but sometimes expressed as  $X + Y > Z$ , consider when  $D$  is three years,  $T$  is estimated for five, ten, fifteen, and twenty years, and  $Q_c$  is assumed to be twelve years. See figure 2 for a graphical representation using these parameters.

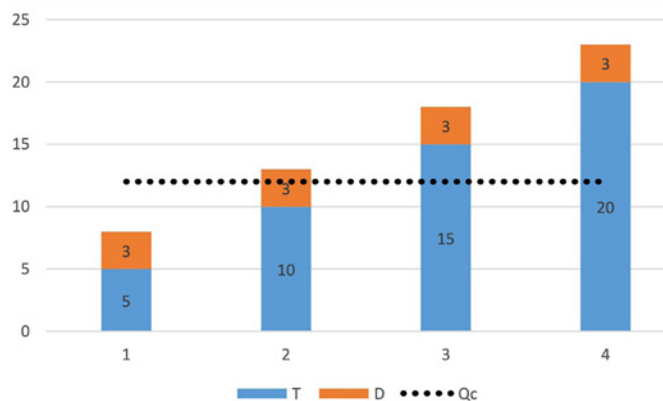


Figure 2 – Mosca's Inequality

For the first estimate when the transition is five years but  $Q_c$  is twelve years, the transition can be completed in time at low risk. But for the second estimate when the transition is ten years, the 3-year data is at medium risk because quantum computers are available. However, when the transition takes fifteen or more years the data is at high risk due to quantum cryptanalysis. So, there is a race to transition from legacy asymmetric cryptography to PQC. Clearly, adjusting the 3-year data protection parameter or the 12-year quantum computer parameter will change the inequality, so each organization needs to manage its own risk regarding PQC migration.

## Legends

The legends are about choosing the PQC algorithms. The PQC algorithms have not yet been selected or standardized by NIST. Per the NIST PQC program, sixty-nine Round 1 candidates were announced in December 2017, with twenty-six Round 2 candidates announced in August 2019, with Round 3 planned sometime in 2020 or 2021 with draft standards in 2022 to 2024. Characteristically, before manufacturers implement technologies into their products, the industry standards are published. Thus, transitions are often delayed waiting on standardization.

As noted, this is not the first NIST time has helped facilitate a cryptographic transition. In 1973 the National Bureau of Standards (NBS, later renamed NIST) called for a new industry cryptographic algorithm. NBS selected the IBM submission called Lucifer, the algorithm was selected, adjusted, and the Data Encryption Standard (DES) was published in 1976.

Fast forward to 1997, NIST called for the replacement of DES. NIST selected Rijndael, an algorithm submitted by two Belgian cryptographers (Joan Daemen and Vincent Rijmen) and the Advanced Encryption Standard (AES) was published in 2001. In 2007 NIST called for an alternate to SHA2. NIST selected Keccak, designed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche, and SHA3 was published in 2015.

## Myths

The myths are about the cryptographic transitions at the industry level. As an example, before AES was published in 2001 the financial industry needed to migrate away from DES. DES was used to protect personal identification numbers (PIN) associated with payment cards: debit cards used at the point of sale (POS) and credits cards used for cash advance at automated teller machines (ATM). DES was also used to protect the payment cards themselves.

- PIN encryption:** the PIN is encrypted at the point of sale at the merchant location or at the ATM at the bank, merchant, or other locations. The enciphered PIN is transmitted to the card issuer for verification. When the enciphered PIN moves from one system or network to another, the PIN is translated from one key to another key. PIN translation happens within secure cryptographic devices (SCD). The SCD imports the enciphered PIN, decrypts the PIN using one key, re-encrypts using another key, and exports the translated PIN. The PIN and the two keys are never exposed outside the SCD.
- PIN verification:** when the PIN is originally chosen by the cardholder, a PIN token is generated by the issuer using another key different than PIN encryption. The issuer stores the PIN token for subsequent verification, but not the actual PIN. When the card issuer receives the enciphered PIN from a payment network, the PIN is decrypted, the PIN token is regenerated, and if the newly generated token matches the stored token, the PIN verifies. PIN verification algorithms are vendor proprietary, many originating from the early days of ATM processing.
- CVV verification:** when a payment card is created, a card verification value (CVV) is generated using another key different than PIN encryption and PIN verification. The CVV algorithm is brand proprietary despite having different names: JCB uses Card Authentication Value (CAV), MasterCard uses Card Validation Code (CVC), Visa and Discover use Card Verification Value (CVV), and American Express uses Card Security Code (CSC). When the card issuer receives the CVV as part of the card transaction, the 16-digit card number, the 4-digit card expiration date (MMYY) and the 3-digit card type are used to regenerate the CVV, and if the newly generated CVV matches the stored CVV, the card is verified.

The Accredited Standards Committee X9, accredited by the American National Standards Institute (ANSI) for developing standards for the financial service industry, published



two Triple Data Encryption Standards (TDES) in 1998 as an interim solution to replace DES before AES was available. PIN encryption systems were converted from DES to TDES many years ago, and are now being converted to AES. However, since PIN verification algorithms are vendor proprietary, they have not been migrated from DES. X9 is developing an AES-based PIN verification standard, but at this time this is still work in progress. While the CVV algorithm has been converted from DES to TDES, since the CVV algorithm is brand proprietary, it has not yet been converted to AES. Accordingly, TDES has been available since 1998 but the replacement of DES within the financial service industry is incomplete in two decades.

Hence, we can conclude that cryptographic transitions might take many years, upwards of twenty years or more. Thus the Mosca Inequality is looking more like the fourth estimate in figure 2, which has a high risk for the quantum menace. This implies that organizations need to begin making plans for PQC migration much sooner rather than later. The good news is that industry participants are already taking action. The International Telecommunication Union (ITU) Standards [8] has updated X.509 "Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks" [9] with extensions for alternate public keys and signatures, including PQC signatures and key management algorithms. ASC X9 has undertaken several proactive initiatives:

- Established the X9F Quantum Computing Risk (QRC) Study Group [1] and published both a white paper and technical report on quantum computing risks
- Established the X9F PKI Study Group and restored its X9F5 Financial PKI workgroup [15] to focus on developing further standards and liaison with the ISO TC68/SC2/WG8 workgroup
- Approved a new work item to develop a new standard for quantum-safe TLS handshake

Other industry announcements include Futurex [6] and Thales, which partners with ISARA and ID Quantique [7] to combat the future security threats of quantum computing.

## Conclusion

In summary, the *menace* is the inevitable cryptanalysis of legacy asymmetric algorithms using quantum computers. The *hypothesis* is when quantum computers are available, maybe sometime in the next ten to fifteen years. The *legend* is the development and selection of post-quantum cryptographic (PQC) algorithms to replace the legacy asymmetric algorithms. The *myth* is how long the cryptographic transitions might take, possibly anywhere from five to twenty years. Organizations need to take the quantum menace seriously and begin to prepare for the inevitable transition.

## References

1. ASC, "ASC X9 Publishes White Paper and Technical Report on Quantum Computing Risks," Accredited Standards Committee X9 (March 2019) – <https://x9.org/asc-x9-publishes-white-paper-and-technical-report-on-quantum-computing-risks/>.
2. D-Wave, "Quantum Computing," D-Wave – <https://www.dwavesys.com/quantum-computing>.
3. Google Research, "Quantum," Google – <https://research.google/teams/applied-science/quantum/>.
4. IBM, "Quantum Starts Here, IBM – <https://www.ibm.com/quantum-computing/>.
5. IETF, "RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3," Internet Engineering Task Force (August 2018) – <https://tools.ietf.org/pdf/rfc8446.pdf>.
6. Isara, "Futurex Announces Post-Quantum Hybrid Certificate Authority Solution," ISARA (February 2020) – <https://www.isara.com/company/newsroom/futurex-isara-announcement-post-quantum.html>.
7. Isara, "Thales Partners with ISARA and ID Quantique to Combat the Future Security Threats of Quantum Computing," ISARA (August 2019) – <https://www.isara.com/company/newsroom/thales-partner-isara-idquantique.html>.
8. ITU, "Telecommunication Standardization Sector," ITU – <https://www.itu.int/en/ITU-T/Pages/default.aspx>.
9. ITU-T, "X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks, ITU – <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14033>.
10. Microsoft, "...Experience Quantum Impact Today," Microsoft – <https://www.microsoft.com/en-us/quantum>.
11. NIST, "Post-Quantum Cryptography," NIST – <https://csrc.nist.gov/projects/post-quantum-cryptography>.
12. Sagar, Ram. "Mosca's Inequality and Its Effect on Quantum Cryptography, Analytics," Analytics India Magazine, January 2019 – <https://analyticsindiamag.com/moscas-inequality-and-its-effect-on-quantum-cryptography/>.
13. Sosayweall, "On the Shoulders of Science," Blog – <https://ontheshouldersofscience.blogspot.com/2013/01/if-you-think-you-understand-quantum.html>.
14. Stapleton, Jeff and Ralph Poore, "Cryptographic Transitions," IEEE Region 5 Conference (April 2006) – <https://ieeexplore.ieee.org/document/5507465>.
15. X9, "X9 Subcommittees and Work Groups," Accredited Standards Committee X9 – <https://x9.org/x9-boardsubcommittees/>.

## About the Author

Jeff Stapleton has been an ISSA member and participated in X9 standards since 1989; he has contributed to the development of more than three dozen X9 and ISO security standards, and has been the chair of the X9F4 Cybersecurity and Cryptographic Solutions workgroup since 1998. He can be reached at [jj578023@yahoo.com](mailto:jj578023@yahoo.com).



# Quantum Computing and the Future Internet

By Tajdar Jawaid - ISSA member, UK Chapter



**This article discusses quantum computing key concepts, with a special focus on quantum Internet, quantum key distribution, and related challenges.**

## Abstract

One of the biggest concerns among cybersecurity professionals these days is the hype around quantum computing, its incomprehensible power, and its implications. The advancement in quantum computing has the potential to revolutionize our daily lives, but it can also completely break down the Internet as we know it. Mathematicians and physicists have developed algorithms based on quantum computing, which can change the Internet security paradigm. This article discusses quantum computing key concepts, with a special focus on quantum Internet, quantum key distribution, and related challenges.

Classical computing has done an amazing job, revolutionized our daily lives, and has a global impact. From television, the Internet to mobile phones, from booking train and air travels to satellite navigation, everything involves classical computing. In general, we see around us the wonders of classical computing, but we rarely discuss or are aware of the limitations of classical computing such as solving exponential problems. For instance, classical computing has the following limitations or is not very good at finding optimal solutions, to say the least, in the following scenarios:

- **Optimization:** Finding the optimal combination of N numbers of given inputs. One example is the famous “Traveling Salesman Problem,” which is to find the shortest path while traveling between N number of cities. The problem gets quickly exponential with N number of routes of different lengths.
- **Chemistry:** Simulating a molecule on classical computing to find out the reaction rates, synthesis, etc., for instance,

simulating molecules like ammonia ( $\text{NH}_3$ ) is computationally intractable on classical computing.

- **Factorization:** Finding the prime factor of a large composite number is almost impossible using classical computing, due to the exponential complexity. This limitation of classical computing is the basis of Internet cryptographic solutions, now under threat by quantum computing.

## Quantum mechanics

Quantum mechanics is the field of quantum physics that relates to the study of elementary particle motion, energy, and properties. These elementary or subatomic particles are photons, electrons, the nucleus of an atom, etc. Quantum mechanics describes the interactions, motions, and energies of these sub-atomic particles mathematically and reveals key properties of particles at the quantum level. Characteristics like *quantum superposition* and *quantum entanglement* are the foundation of quantum computing. These key concepts of quantum mechanics and characteristics of quantum particles have been developed throughout the 19th and 20th centuries.

However, the application of quantum mechanics in the computing world was first envisioned in 1980 by Russian-German mathematician Yuri Manin. In his paper, “Computable and uncomputable,” Manin discusses the limitations of classical computing and the exponential power of quantum computing due to the nature of superposition and entanglement principles of the quantum world [20]. In 1981 Richard Feynman refined the idea and showed that it is impossible to simulate the quantum system with the use of classical computing [7]. Since the 1980s there have been breakthroughs and developments that have shifted quantum computing from the theoretical realm to the physical world.

Various companies are developing the first wave of experimental quantum computers. Figure 1 shows the IBM Q [13] and the Google quantum computer [15]. IBM has even made quantum computing available to the public in the cloud for free hands-on experience through IBMQ System One.

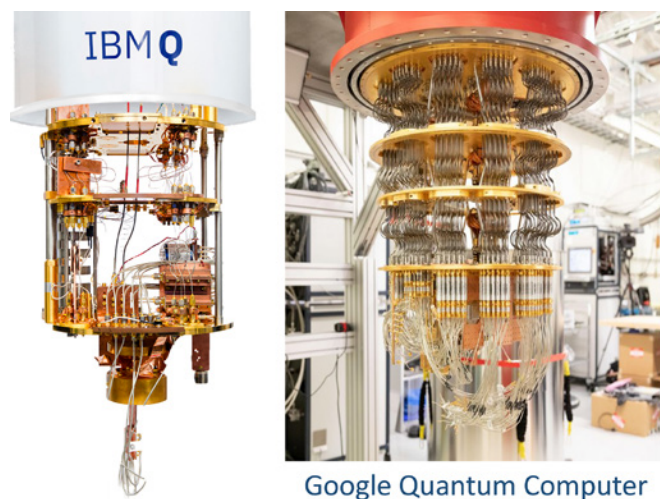


Figure 1 – IBM Q and Google Quantum Computers

## Quantum computing

See sidebar "Quantum Mechanics Pioneers" for original papers describing quantum mechanics.

**Quantum superposition:** Superposition is based on Heisenberg's uncertainty principle, which states that the position and momentum of a particle cannot be correctly measured simultaneously. This is due to the characteristic of a quantum particle to be in any or all-states before it is measured.

**Quantum entanglement:** Quantum entanglement states that if any pair of particles generated in a way that they interact with each other, their properties (such as position, spin, momentum, etc.) get appropriately correlated or entangled. They will have exactly opposite but correlated quantum properties in the entanglement state. Once they are entangled no matter how far they are from each other, this correlation remains intact.

**Quantum bits (qubits):** Quantum computers work on quantum bits or qubits. Qubits work on the state of elementary particles like electron, neutron, photons, etc. These elementary particles have internal angular momentum or spins. The states 1 and 0 describe the particle's spin—clockwise/anti-clockwise or up/down—at the point of measurement when there is no surrounding noise. Unlike classical bits, which can have a definitive state of 0 or 1, a qubit can exist anywhere

between 0 and 1 simultaneously due to the superposition principle.

For instance, two classical bits can have four possible state combinations (i.e., 00,01,10,11). But at any given state it will only have two bits of information, and to access all four possible states of combinations, the classical computer has to do at least four operations. Whereas two qubits can exist in all four possible states at once, it will require a single operation for quantum computers to access all four states of information stored in two qubits. This quantum advantage increases exponentially with additional qubits. For instance, 4-qubit quantum computers can process 16 bits of information in a single operation and so on. It is thus possible in theory that a 2500 qubits quantum computer can process information that is more than the total number of particles in the observable universe.

## Application of quantum computing

Quantum computing is arguably the most exciting technology of this century, and we are just starting to scratch the surface of it. Quantum computing has the potential to revolutionize the field of medicine by simulating molecules to build new drugs that may help find the cure for diseases and viruses more quickly.

Physicist and mathematicians can solve difficult physical and mathematical problems that have puzzled them for decades. It can help businesses and financial industries to make better forecasts, increase profitability, and achieve sustainable growth. The optimization problems can be solved by simultaneously sampling the whole dataset through the power of quantum superposition to find the optimal results. Quantum computing can also help in adjacent fields like logistics, operations, research, decision making, pattern recognition, machine learning, and quantum simulation of complex material properties and molecular functions.

However, from the infosec point of view, the real threat is breaking of the hardness of factorization. A quantum computer can factor numbers exponentially faster than classical computers as shown by Shor's algorithm [17]. The Internet is currently dependent on public-key cryptographic schemes such as RSA signatures (RSA), the Diffie-Hellman key agreement protocol, elliptic curve digital signature algorithms (ECDSA), etc. These cryptographic schemes are based on the hardness of integer factorization or the discrete logarithm problem. Shor's algorithm shows that a quantum computer with 4099 perfectly stable qubits can break RSA 2048 encryption in just 100 seconds, which would otherwise take billions of years through classical computing.

## Quantum Mechanics Pioneers

**Niels Bohr:** "[On the Constitution of Atoms and Molecules](#)" (1913) and "[The Structure of the Atom](#)" (1922)

**Werner Heisenberg:** "[The Development of Quantum Mechanics](#)" (1933)

**Einstein, Podolsky, and Rosen:** "[Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?](#)" (1935)

**Erwin Schrödinger:** "[The Present Situation in Quantum Mechanics: A Translation of Schrödinger's 'Cat Paradox' Paper](#)" (1935)



## Post-quantum Internet and cryptography

To secure the Internet in the quantum world, quantum key distribution (QKD) algorithms and communication standards need to be developed. To address the threat posed by the advancement in quantum computing, American and European governments have initiated dedicated projects and workshops. The US National Institute of Standards (NIST) has started the “Post-Quantum Crypto Project” [14] to develop a quantum-resistant suite of protocols. Similarly, the European Telecommunication Standards Institute (ETSI), which is one of the three European standards organizations, has started “ETSI-IQC Workshops on Quantum-Safe Cryptography” [6]. Both these standards organizations are pulling scientists together around the globe to address and develop a suite of cryptographic protocols and standards for a quantum Internet.

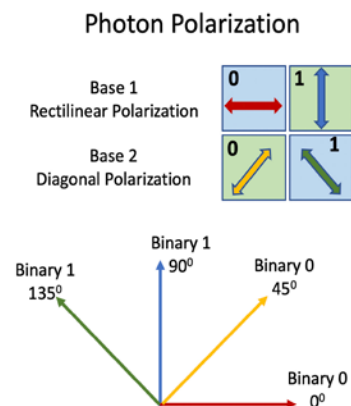
### Quantum key distribution basics

The first quantum key distribution protocol was developed by Charles Benett and Gilles Brassard in 1984, also known as BB84. The BB84 protocol was developed on the basis of the Heisenberg uncertainty principle. The QKD protocols so far developed fall in the following two categories:

- Protocols based on the Heisenberg uncertainty principle (e.g., BB84) [2]
- Protocols based on quantum entanglement (e.g., E91) [5]

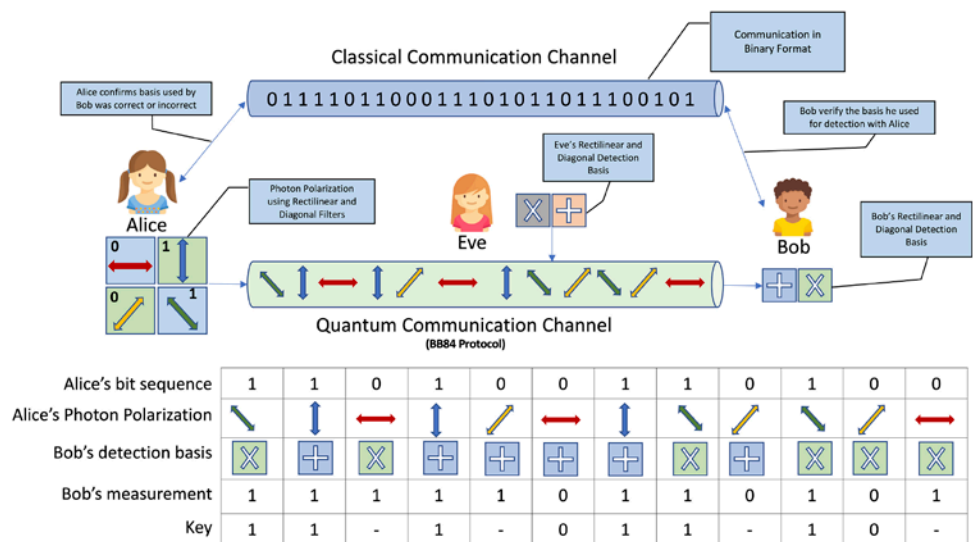
### BB84 Heisenberg uncertainty principle-based Protocol

The BB84 protocol shows particles such as polarized photons can be used to develop and distribute cryptographic keys. Figure 2 describes how bits can be encoded with the polarization of the photon state in BB84. The binary 1 can be encoded using  $90^\circ$  or  $135^\circ$  photon polarization and similarly the binary 0 can be encoded using  $45^\circ$  or  $0^\circ$  photon polarization. The base 1 uses a rectilinear basis for photon polarization, while base 2 uses a diagonal basis for photon polarization for encoding. Figure 2 and 3 illustrated BB84 visually.



**Figure 2 – Photon polarization in BB84**

In Figure 3 Alice and Bob decided to establish a secure communication channel using both



**Figure 3 –BB84 quantum key distribution**

quantum and classical communication channels. To start the process Alice will use a photon polarization filter to encode binary 1 and 0 using photons polarization states. Alice will send a random bit sequence of 0 or 1 using both polarization bases randomly.

Bob will use a rectilinear or diagonal basis to decode the values without knowing which sequence of basis Alice used to encode the data. Through this Bob will create two tables of bits, one for each basis (i.e., rectilinear and diagonal). Due to the random mix of bits, there is a risk eavesdropper Eve could intercept Alice's bits, decode and resend the bits back to Bob. This will create roughly 50 percent disagreement between Alice and Bob where they think their sequence of the basis used for encoding and decoding should coincide. This is due to the fact that Eve will destroy the information as soon as she reads it to decode. Bob's information will further be reduced due to the photons lost in transmission due to noisy channels.

Once the quantum communication phase has ended, Alice and Bob will use the classical channel to verify the communication through a process called *sifting*. They will identify which photons were received successfully, and the sequence of the bases used for encoding and decoding. If the quantum communication did not have any interference, Alice and Bob agree on the bits encoded/decoded using the sequence of the bases used.

In the case of eavesdropping, the encoding and decoding will produce different results on the sequence where they think their results should match. They will discard all those bits where they use the same sequence but have different results. Where comparison agrees they will use those bits as a one-time pad to send communication over the classical channel. Once this one-time pad is used up, this protocol is repeated to generate a new one-time pad over the quantum channel for subsequent information.

In 1992 Charles Bennett proposed a simplified version of BB84 referred to as BB92. BB92 describes that it is not nec-

essary to use four polarization states: the 0 and 1 can be encoded using just two polarization states. 0 can be encoded at  $0^\circ$  rectilinear bases, whereas 1 can be encoded at  $45^\circ$  diagonal bases without compromising the security [3].

### E91 entanglement-based Protocol

In 1991 Artur Ekert reported the application of Bell's theorem in the quantum key distribution process. The basic premise of Ekert's paper [5] is the fact that entanglement is inherently secure. The entangled qubit properties cannot be copied or reproduced within the known laws of nature. Hence, this property should be applied to quantum key distribution. Applying the Alice and Bobs example to the E91 protocol, Alice and Bob both will receive the entangled photons from the same source. These entangled photons are the exact opposite

of each other due to the entanglement principle discussed above. Alice and Bob can agree on a key basis as in BB84 and can invert their keys to reveal the secret key.

### QKD security concerns

QKD protocols promise the highest possible level of security due to the known laws of quantum physics that cannot be violated. However, QKD protocols are still susceptible to attacks due to imperfect communication channels.

**Man-in-the-middle attack** (eavesdropping) or due to **noisy imperfect transmission channels**. It is not easy to differentiate the two errors; hence, both are assumed to be eavesdropping. To mitigate these errors there are two techniques (Information Reconciliation and Privacy Amplification) proposed in 1992 by Bennett and Brassard with their colleagues [4].

1. *Information reconciliation* is the process to remove the errors caused by noisy channels.
2. *Privacy amplification* is the process of reducing or eliminating Eve's partial information about Alice and Bob's key.

**Photon number splitting attack** is another kind of attack in addition to a man-in-the-middle attack. Due to noise in the quantum channel, it is impractical to produce and detect a single photon. In practice a laser pulse is used to produce a small number of photons. In the case of Alice and Bob transmitting the photons through a laser, Eve can split off the single or small number of photons to measure, allowing the rest of the photons to still be transmitted to Bob. This will help Eve have the secret key information without disturbing the whole communication and, hence, without being noticed. To mitigate this, a solution has been developed by Lo et al, using decoy signals randomly in a way that Eve cannot differentiate between the decoy and non-decoy photon pulses [12].

### Quantum communication protocol for quantum Internet

By using quantum entanglement capabilities scientists are researching to develop quantum communication for the future Internet. As we know, entangled particles can have information regardless of how far apart they are. However, the entanglement itself is very fragile; it doesn't hold after a certain distance. As particles cannot be copied (no cloning theorem) and cannot maintain the status for long, they quickly lose their entangled status [19]. Scientists are working on quantum repeaters that will be used to extend the transmission of entangled particles over large distances through a technique called entanglement swapping to achieve quantum teleportation [1].

### Quantum computing challenges

As quantum computing is still in its infancy, there are many problems that have to be overcome. The following are some of the key challenges faced by quantum computing.

### Quality of qubits

The quality of qubits refers to error correction rates and stability of quantum properties or states held by the qubits, also

ISSA International Web  
CONFERENCE

### ISSA Thought Leadership Series



## Trends and Statistics for Mobile Phishing in the Enterprise

**60-minute Live Event: Wednesday, May 13, 2020**

10 a.m. US-Pacific/1 p.m. US-Eastern/6 p.m. London

Your employees work differently now, often using their own devices to access enterprise data from home, airports, shopping malls, and the local coffee shop. Employees working outside of their corporate perimeters, coupled with the shift to cloud-based services, opens a whole new door of vulnerabilities that organizations need to consider. Namely, phishing threats.

Learn how evolving phishing threats can leave your corporate data unprotected, and how to address this common yet largely undetected issue. Attendees will learn why phishing is a bigger problem on mobile.

**Speaker:** Chris Hazelton – Director, Product Marketing, Lookout

Generously supported by



Lookout

Click [HERE TO REGISTER](#).

For more information on these or other webinars:

[ISSA.org => Events => Web Conferences](#)

known as their coherence time. Figure 4 shows the coherence time visually in which a qubit holds its state information. Generally, qubit coherence time is between 50 to 90 milliseconds in trapped-ion systems.

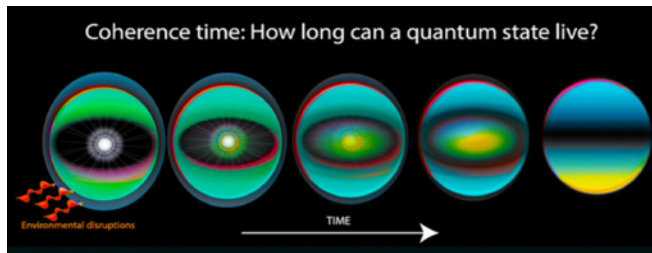


Figure 4 – Coherence Time [11]

There are research and experiments that show that environments can be created where the state of qubits endures from 10 to 39 minutes [18] [16]. This opens up new research opportunities for developing this technology further.

### Quantum error correction (QEC)

Computation is required to have error detection and error correction mechanisms and algorithms in place to do the precise calculations. Physicists have developed some very efficient techniques to do large-scale quantum error correction on a two-dimensional qubit grid with about one percent error tolerance [8].

This means that to break classical 2048-bit RSA encryption a total of 220 million physical qubits are required, and it would take around 26.7 hours to break the encryption by finding the factors [8]. This was further refined by Craig Gidney and Martin Eker in 2019 when they demonstrated that it would require eight hours with 20 million noisy qubits to break 2048 RSA encryption [9].

### Cryogenic cooling

Quantum particles vibrate and fluctuate continuously due to Heisenberg's uncertainty principles. This vibration of quantum particles or atoms is dependent on their mass: the lighter the atom, the more it vibrates. To work with vibrating quantum particles, a state of near zero-point motion energy needs to be achieved. Supercooling to very low temperatures is required to propel the quantum particles to the state of extremely low energy levels so that they can be easily controlled.

Figure 5 visualizes atoms at room temperature and at near absolute zero. The cryogenic temperature ranges from  $-150^{\circ}\text{C}$  ( $-238^{\circ}\text{F}$ ) to absolute zero ( $-273^{\circ}\text{C}$  or  $-460^{\circ}\text{F}$ ). IBM's quantum computer, for instance, uses 15 millikelvin to cool down its quantum computer, which is colder than the temperature of outer space [10]. Working with these low temperatures is not very easy and could be an obstacle to produce commercial quantum computers. But there are breakthroughs in molecule-sized and atom-sized transistors that once matured enough may help overcome this challenge.

### No-cloning theorem

A quantum state cannot be copied—no cloning theorem—due to the conservation of quantum information law [19].

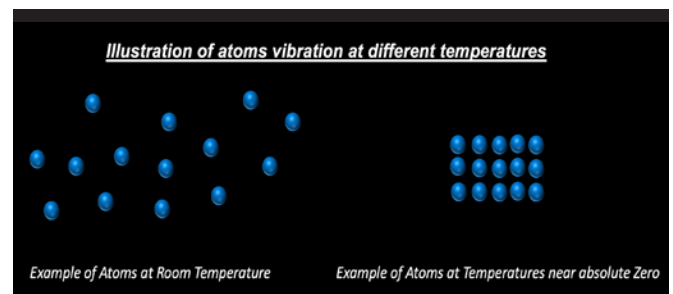


Figure 5 – Atom vibrations at different temperatures

This represents a challenge while transmitting, storing, and processing the information through quantum computing without the ability of copying and duplicating the qubits. Special algorithms, techniques, and technologies need to be developed to overcome this challenge.

## Conclusion

Quantum computing is a promising and emerging field that has great prospects to revolutionize our daily lives. But there are challenges in quantum computing, though these challenges can be categorized as a “teething” problem instead of limitations. There are recent breakthroughs and advancements in technology, new research, and development in this field that will make the quantum revolution possible in the foreseeable future. Unlike the hype, it is safe to assume that there is no immediate threat to the current public-key infrastructure through quantum computers, as it still requires a quantum computer with millions of qubits to break current cryptography. The parallel research and advancement in the field of quantum cryptography algorithms like NIST “Post-Quantum Crypto Project” and ETSI “Workshops on Quantum-Safe Cryptography” will help develop a secure quantum Internet. The practical impact of this technology on our daily lives may be a few decades away, but there is no doubt that once this technology is matured enough, the future of humanity will be very different.

## References

1. Azuma, K; Tamaki, K; Hoi-Kwong, L. “All-Photonic Quantum Repeaters,” Nature Communications by Nature.com (2015, April 15) – <https://www.nature.com/articles/ncomms7787>.
2. Bennett, C. H.; Brassard, G. “Quantum Cryptography: Public Key Distribution and Coin Tossing,” Theoretical Computer Science, Volum 560, Part 1, 4 December 2014, Pages 7-11 – <https://www.sciencedirect.com/science/article/pii/S0304397514004241?via%3Dihub>.
3. Bennett, C. “Quantum Cryptography Using Any Two Non-orthogonal States,” APS, Rev. Lett. 68, 1992, pp. 3121-3124 – [http://prola.aps.org/pdf/PRL/v68/i21/p3121\\_1](http://prola.aps.org/pdf/PRL/v68/i21/p3121_1).
4. Bennett C. H., et al. “Experimental Quantum Cryptography,” University of Colorado (1984, September) – <http://cs.uccs.edu/~cs691/crypto/BBBSS92.pdf>.
5. Ekert, A. K. “Quantum Cryptography Based on Bell’s Theorem,” American Physical Society, Lett.67, 661 (1991, April



- 18) – <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661>
6. ETSI, “ETSI/IQC Quantum Safe Cryptography Workshop 2019,” European Telecommunication Standard Institute – <https://www.etsi.org/events/1609-etsi-iqc-quantum-safe-cryptography-technical-track#pane-1/>.
  7. Feynman, P. R. “There’s Plenty of Room at the Bottom,” Caltech Engineering and Science, Volume 23:4, February 1960, pp22-36 – <http://www.zyvex.com/nanotech/feynman.html>.
  8. Fowler, Austin G. et al. “Surface Codes: Towards practical Large-Scale Quantum Computation,” American Physical Society (2012, September) – <https://link.aps.org/doi/10.1103/PhysRevA.86.032324>.
  9. Gidney, C. and Eker, M. “How to Factor 2048-bit RSA Integers in 8 Hours Using 20 million Noisy Qubits,” arXiv.org Cornell University (2019, December 6) – <https://arxiv.org/pdf/1905.09749.pdf>.
  10. IBM, “Look Inside a Quantum Computer,” IBM – <https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/>.
  11. JQI, “Coherence Time: Survival of a Quantum State,” Joint Quantum Institute (Nov 25, 2013) <https://jqj.umd.edu/news/quantum-bit/2013/11/25/coherence-time-survival-quantum-state>.
  12. Lo, H., et al. “Decoy State Quantum Key Distribution,” Cornell University (1995, May 12) – <http://arxiv.org/pdf/quant-ph/0411004>.
  13. Manglaviti, A. “Quantum Information Science Effort Expands at Brookhaven Lab,” Brookhaven National Laboratory (2019, February 19) – <https://www.bnl.gov/newsroom/news.php?a=213134>.
  14. NIST, “Post-Quantum Cryptography Project,” National Institute of Standards – <https://csrc.nist.gov/projects/post-quantum-crypto.gaphy>.
  15. Shankland, S. “Google Quantum Computer,” CNet (2019 October, 23) – <https://www.cnet.com/pictures/take-a-look-at-googles-quantum-computing-technology/>.
  16. Saeedi, K., et al. “Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28,” Science Magazine (2013, November 15) – <https://science.sciencemag.org/content/342/6160/830>.
  17. Shor, W.P. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” IEEE Computer Society (1996, January 25) – <https://arxiv.org/pdf/quant-ph/9508027.pdf>.
  18. Wang, Y., Um, M., Zhang. “Single-Qubit Quantum Memory Exceeding Ten-Minute Coherence Time,” Nature Photon 11, 646–650 (2017) – <https://doi.org/10.1038/s41566-017-0007-1>.
  19. Wootters W.K. and Zurek, W.H. “The No-Cloning Theorem,” Physics Today 62, 2, 76 (2009) – <https://physicstoday.scitation.org/doi/abs/10.1063/1.3086114?journalCode=pto>.
  20. Yu, Manin. “Computable and Uncomputable” (in Russian), Sovetskoye Radio, Moscow (1980).

### About the Author

Tajdar Jawaid, PMP, MS Cybersecurity from University of Dallas, TX, is a security architect working for Telefonica UK. He has around 18 years of experience in security architecture and design. He may be reached at [tjawaid@udallas.edu](mailto:tjawaid@udallas.edu).



## Disinfecting Our Pandemic and Business Continuity Plans

Continued from [page 6](#)

- An annual review by department managers that allows them to document and review their staffing issues and designate backup staff for critical business functions
- An annual eLearning session for all employees that reviews the concepts of the pandemic plan
- An annual review of all technology equipment needed for all employees working offsite during the pandemic plan

### Business continuity committee oversight

- Conduct an annual review of contingency plans
- Contingency plan development
- Plan corporate tests and exercises with management
- Initiate and facilitate corporate tests and exercises
- Identify risks
- Review audit and exam recommendations
- Report to the board

- Review critical vendor relationships
- Monitor CDC and WHO websites as needed for pandemics

### Update strategies for implementation

While an event is fresh on our minds, updating our organization’s business continuity strategy is time well spent. During past weeks, I reviewed multiple third-party providers’ business continuity and pandemic plans for assessing risks in these areas. I found a lot of variations in depth and scope in these plans, but for the most part good efforts were made in trying to envision plans for dealing with unprecedented times. For example, one third-party provider’s pandemic policy (dated 2017) outlined the promotion of social distancing with three feet of spatial separation. It also included primary strategies for treating the pandemic “influenza” the same as seasonal influenza with a vaccination, flu shots, antiviral medications, and the use of infection control measures. From current experience we know that this information is inaccurate.

rate for the type of pandemic such as COVID-19 and could not be currently accepted or available. Obviously, a spatial distance of six feet is mandated for the COVID-19 virus, which cannot be treated the same as the flu.

Another third-party's pandemic plan listed specific steps to include a pandemic kit to be maintained by the location or the facilities manager and checked periodically for expiration dates with additional supplies replenished as needed. This plan further advised managers to ensure these supplies were available to employees when outbreaks occurred in that region. This plan was thorough in describing what the kits included: Supply of gloves in medium and large sizes, disposable thermometers, disinfectant wipes, nuisance dust masks, and hand sanitizer. Of course, we know now a particular type of N95 mask and hand sanitizers with 60 percent or more alcohol base are more effective as well as plastic face shields. But, the third-party's pandemic kit was well-thought out, and the plan detailing what to do and what to prepare was explained in a much more granular level.

### Crisis management and BCP

True crisis management is a critical component of the continuity strategy. The good news is that continuity planning is flexible, customizable, and easily adaptable before we get to the crisis stage. Organizations should tailor their plan to address unique concerns and document information that is necessary to support things after a business disruption. Lastly, making the plan available and readily distributed to personnel in the event of emergency guarantees quick response and a workable action plan.

### Conclusion

Before March 2020, it would have been a safe bet that many of us filed these plans electronically very neatly on the back burner of our secure portals. Today, revisiting and updating these policies and procedures will be an important first step. As we enter the world again, add the business continuity and pandemic plans to the list of things you are disinfecting and wiping off to use, and treat them with new priority. As cybersecurity leaders, we are tasked with defining and directing our programs but also reviewing and assessing them. This includes updating and annually reviewing policies and practices to maintain adequacy. Hopefully soon, the COVID-19 pandemic will be behind us. But since our organizations cannot simply don a mask to stay protected, the time to plan is now.

### About the Author

Dr. Curtis C. Campbell is VP of Atlantic Capital Bank in Atlanta, GA, and president of ISSA Chattanooga Chapter. She is a cybersecurity author with 25 years experience in information security, compliance, procurements, and third-party risk in the enterprise. Curtis holds a PhD in Organizational Leadership in Information Systems Technology. She serves on the advisory board of University of TN-Chattanooga, a National Center for Academic Excellence for Cyber-Defense studies. Connect with Curtis via [curtis@mprotechnologies.com](mailto:curtis@mprotechnologies.com).



## ISSA Journal 2020 Calendar

Past Issues – digital versions: click the download link: [↓](#)

### JANUARY

Best of 2019

### FEBRUARY

Regulation, Public Policy, and the Law

### MARCH

Preparing the Next Generation Security Professional

### APRIL

Corporate and Nation-State Cybersecurity: Attack and Defense

### MAY

Practical Cryptography and the Quantum Menace

### JUNE

The Infosec Toolbox: Basics to the Bleeding Edge  
Editorial Deadline 5/1/20

### JULY

Security vs Privacy Tug of War  
Editorial Deadline 6/1/20

### AUGUST

Disruptive Technologies  
Editorial Deadline 7/1/20

### SEPTEMBER

Shifting Security Paradigms in the Cloud  
Editorial Deadline 8/1/20

### OCTOBER

The Business Side of Security  
Editorial Deadline 9/1/20

### NOVEMBER

Big Data/Machine Learning/Adaptive Systems  
Editorial Deadline 10/1/20

### DECEMBER

Looking toward the Future of Infosec  
Editorial Deadline 11/1/20

For theme descriptions, visit  
[www.members.issa.org/page/CallforArticles](http://www.members.issa.org/page/CallforArticles).

EDITOR@ISSA.ORG • WWW.ISSA.ORG

# Data Privacy: De-Identification Techniques

By **Ulf Mattsson** – ISSA member, New York Chapter



**This article discusses emerging data privacy techniques, standards, and examples of applications implementing different use cases of de-identification techniques. We will discuss different attack scenarios and practical balances between privacy requirements and operational requirements.**

## Abstract

The data privacy landscape is changing. There is a need for privacy models in the current landscape of the increasing numbers of privacy regulations and privacy breaches. Privacy methods use models and it is important to have a common language when defining privacy rules. This article will discuss practical recommendations to find the right practical balance between compliance, security, privacy, and operational requirements for each type of data and business use case.

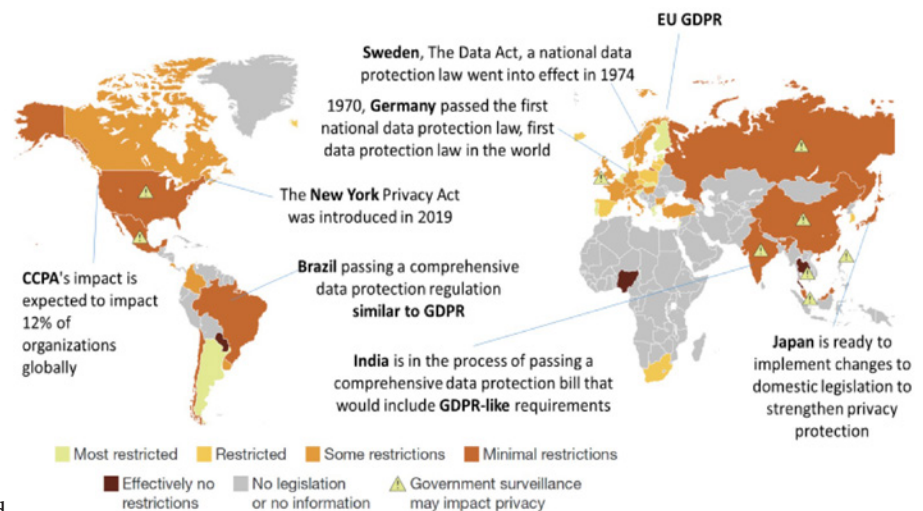


Figure 1 – Forrester's global map of privacy rights and regulations [4]

**S**ensitive data can be exposed to internal users, partners, and attackers. Different data protection techniques can provide a balance between protection and transparency to business processes. The requirements are different for systems that are operational, analytical, or test/development as illustrated by some practical examples in this article.

We will discuss different aspects of various data privacy techniques, including data truthfulness, applicability to different types of attributes, and if the techniques can reduce the risk of data singling out, linking, or inference. We will also illustrate the significant differences in applicability of pseudonymization, cryptographic tools, suppression, generalization, and noise addition.

## Many countries have local privacy regulations

Besides the GDPR, many EU countries and other countries have local privacy regulations (figure 1). For instance, the

California Customer Privacy Act (CCPA) is a wake-up call, addressing identification of individuals via data inference through a broader range of PII attributes. CCPA defines personal information as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household such as a real name, alias, postal address, and unique personal identifier [1].

## Privacy fines

In 2019, Facebook settled with the US Federal Trade Commission (FTC) over privacy violations, a settlement that required the social network to pay US\$5 billion. British Airways was fined £183 million by the UK Information Commissioner's Office (ICO) for a series of data breaches in 2018, followed by a £99 million fine against the Marriott International hotel chain. French data protection regulator Commission Natio-



nale de l'informatique et des Libertés (CNIL) fined Google €50 million in 2019.

## Privacy and security are not the same

Privacy and security are two sides of a complete data protection solution. Privacy has to do with an individual's right to own the data generated by his or her life and activities, and to restrict the outward flow of that data [15]. Data privacy, or information privacy, is the aspect of information technology (IT) that deals with the ability to share data with third parties [10].

Many organizations forget to do risk management before selecting privacy tools. The NIST “Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management” [9] can drive better privacy engineering and help organizations protect individual privacy through enterprise risk management. Figure 2 illustrates how NIST considers the overlap and differences between cybersecurity and privacy risks.

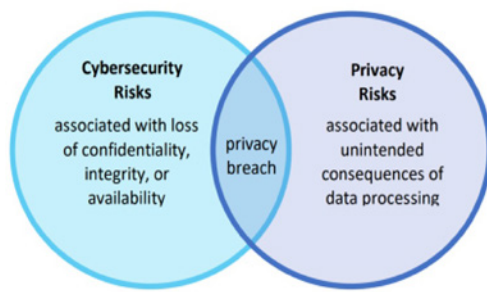


Figure 2 – Overlap and differences between cybersecurity and privacy risks [9]

## Privacy suffers if you don't know your data

You must start with knowing your data before selecting your tools. Defining your data via data discovery and classification is the first part of a three-part framework that Forrester calls the “Data Security and Control Framework” [11]. This framework breaks down data protection into three key areas:

1. Defining the data
2. Dissecting and analyzing the data
3. Defending the data

## Privacy standards

ISO standards provide a broad international platform, and frequently the standards are based on mature security and privacy standards developed by US ANSI X9 for the financial industry. ISO published an international standard to use as a reference for selecting PII (personally identifiable information) protection controls within cloud computing systems [7]. The classification of attributes reflects the difference between singling out a data principal in a dataset and identifying a data principal within a specific operational context:

- **Identifier:** a set of attributes in a dataset (collection of data) that enables unique identification of a data principal within a specific operational context.

- **Direct identifier:** an attribute that alone enables unique identification of a data principal within a specific operational context.
- **Indirect identifier:** an attribute that when considered in conjunction with other attributes enables unique identification. Indirect identifiers need to be removed from the dataset by selectively applying generalization, randomization, suppression, or encryption-based de-identification techniques to the remaining attributes.
- **Local identifier:** a set of attributes that together single out a data principal in the dataset. For example, each record may be comprised of a set of attributes. Each record carries information about a data principal and each attribute carries a known meaning.
  - **Unique identifier:** an attribute that alone singles out a data principal in the dataset.
  - **Quasi-identifier:** an attribute that when considered in conjunction with other attributes in the dataset singles out a data principal.

Figure 3 depicts the relationship between the various types of identifiers described above. Any attribute that is equal to or part of one of the types of identifiers defined above is deemed to be an identifying attribute. In figure 3 *Dataset* refers to the dataset to which de-identification techniques are to be applied, and *context* refers to the information derived from the operational context of the dataset.

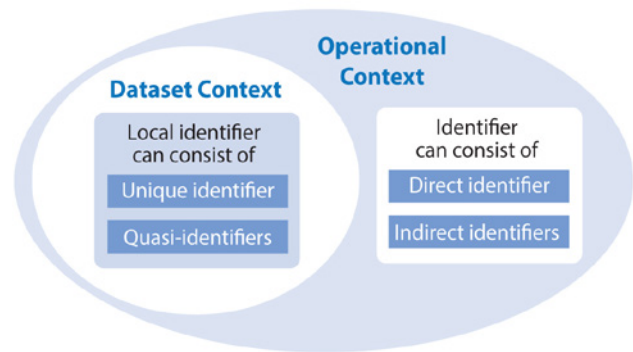


Figure 3 — Types of identifiers

## De-identification of data

Interest in technical capabilities for anonymizing data expanded as the GDPR came into force. This is because, with truly anonymized data, data protection authorities no longer consider it personally identifiable information and it falls outside of scope for the regulation.

- **Anonymization:** A method of de-identification that removes all personally identifiable information from a dataset to the extent that makes the possibility of re-identification of the data negligible. Anonymization requires an approach that might combine different elements, such as technology, oversight, and legal agreements with third parties [12].

- **Pseudonymization:** A method of de-identification that replaces personally identifiable information with false identifiers, which facilitates data analysis while maintaining strong data protection [12] (figure 4).

De-identification			
	Pseudonymization		Anonymization
	Basic	Strong	
Approach	Replaces basic identifiers	Replaces basic and indirect identifiers	Removes permanently all personal identifiable information
Regulatory obligations	Regulatory requirements apply, but it contributes to significantly mitigate some risks.	No regulatory requirements are lifted. Additional measures are required for compliance purposes.	When business processes and other legal and organizational remedies are appropriately aligned, it significantly reduces the scope of compliance.

Figure 4 – Pseudonymization and Anonymization

## De-identification techniques

Some techniques are performed on the original dataset and others are performed on a copy of the dataset that you may share with users or organizations that should not have access to the original data. We are discussing these aspects below and the consideration that you may lose data granularity when applying some techniques, including data generalization. It can partially reduce the risk of linking and partially reduces the risk of inference if the group identifies a sufficiently large group of individuals. Selection of group sizes needs to consider if the result will be skewed if the data is used for statistical analysis, for example in population census reporting.

### Sampling

Data sampling is a statistical analysis technique that selects a representative subset of a larger dataset in order to analyze and recognize patterns in the original dataset. To reduce the risk of re-identification, sampling is performed on data principals [7].

Sampling provides data truthfulness (factual data that has not been accidentally or deliberately distorted) at record level and partially reduces the risk of singling out. It partially reduces the risk of linking and partially reduces the risk of inference.

### Aggregation

Aggregation is an approach where attribute values or related attributes provide information at a broader level than at which detailed observations are taken [7].

- Aggregation of attribute values includes the set of broadly used statistical functions that, when applied to an attribute in microdata, produce results that represent all the records in the original dataset.
- Aggregation of related attributes includes attributes within a common branch of a hierarchy, or statistical functions that produce results that represent all the attribute values of the related attributes in any individual record.

## Pseudonyms independent of identifying attributes

Pseudonym values are typically independent of the replaced attributes' original values via generation of random values. Data tokens may or may not be derived from original values. Tokens were covered in an earlier article [8]. When pseudonyms are generated independently of the attributes, a table containing the mappings (or assignments) of the original identifier(s) to the corresponding pseudonym can be created. For security reasons, appropriate technical and organizational security measures need to be applied to limit and/or control access to such a table, in accordance with the organization's objectives and re-identification risk assessment [7] (figure 5).

Technique	Definition	
Differential privacy	The purposeful addition of noise to a data set, allowing for analysis while still preserving the privacy of individuals	Age: 47 years → Age: 40 to 50 years
Synthetic data	Completely replacing a data set with artificial data points, while maintaining the statistical properties and structure of the original data set	Original data → Synthetic data
Tokenization	Replacing direct or indirect identifiers with a unique but nonsensical symbol	1 PII → 85T78C

Figure 5 - Examples of de-identification techniques

### Generalization

Generalization techniques reduce the granularity of information contained in a selected attribute or in a set of related attributes in a dataset. Generalization techniques preserve data truthfulness at the record level. The output of generalization is microdata.

### Rounding

Rounding may involve a rounding base for a selected attribute and then rounding each value up or down to the nearest multiple of the rounding base. Whether to round up or down is decided probabilistically, based on how close the observation is to the nearest multiple of a rounding base. Rounding provides data truthfulness at record level and is applicable to identifying attributes. It partially reduces the risk of linking and partially reduces the risk of inference.

### Top and bottom coding

This technique sets a threshold on the largest (or smallest) value that a given attribute can take. Values that are above (or below) the threshold are replaced with a single value indicating the top (or bottom) category. Top/bottom coding provides data truthfulness at record level and is applicable to identifying attributes. It partially reduces the risk of linking and partially reduces the risk of inference.

### Randomization

Randomization is a category of de-identification techniques in which values of an attribute are modified so that their new values differ from their true values in a random way. Ran-

domization techniques do not preserve data truthfulness at the record level. To achieve the chosen objectives, an effective randomization process resulting in useful data needs to be tailored on a case-by-case basis [7]. Randomization reduces the risk of singling out identifying attributes. The output of randomization is microdata.

### Noise addition

Noise addition modifies a dataset by adding random values—noise—to the values of a selected attribute with continuous values, while as much as possible retaining the original statistical properties of the attribute across all records in the dataset. Such statistical properties include distribution, mean, variance, standard deviation, covariance, and correlation of the attribute. Noise addition does not provide data truthfulness. It is applicable to identifying attributes and partially reduces the risk of singling out. It partially reduces the risk of linking and partially reduces the risk of inference.

### Synthetic data

Synthetic data is based on generating microdata artificially to represent a predefined statistical data model (figure 5). By definition, a synthetic dataset does not contain any data collected from or about existing data principals but looks realistic for the intended purposes. Synthetic data fitting the original data too closely can reveal information about genuine data principals, such as their personal data. Privacy guarantees of synthetic data can be evaluated using the differential privacy model.

## Privacy measurement models

### Differential privacy

Differential privacy is a model that provides mathematical guarantees that the probability distribution of the output of this analysis differs by a factor no greater than a specified parameter regardless of whether any particular data principal is included in the input dataset [6] (figure 5). Differential privacy basically “guarantees that the probability that any data principal suffers privacy loss exceeding is bounded by a defined factor” [2].

### K-anonymity model

The k-anonymity model ensures that groups smaller than  $k$  individuals cannot be identified. Queries will return at least  $k$  number of records. K-anonymity is a formal privacy measurement model that ensures that “for each identifier there is a corresponding equivalence class containing at least  $K$  records” [6].

K-anonymity can thwart the ability to link field-structured databases but a typical problem statement could be the following, illustrated by figure 6: Given person-specific field-structured data, produce a release of the data with scientific guarantees that the individuals who are the subjects of the data cannot be re-identified while the data remain practically useful. Description of a potential solution: A release

provides k-anonymity if the data for each person cannot be distinguished from at least  $k-1$  individuals whose data also appears in the release [14]:

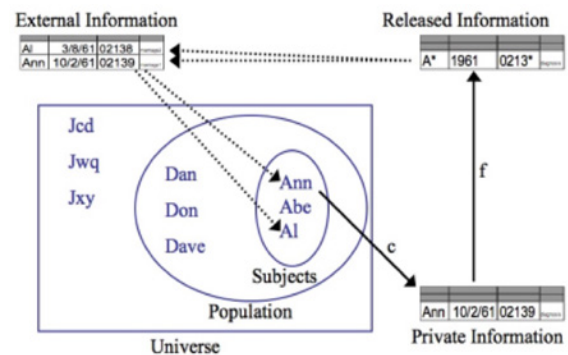


Figure 6 – K-anonymity example

## General principles for application of de-identification techniques

ISO 25237:2017 offers detailed guidelines for the selection of de-identification techniques for the health care industry [5].



**ISSA Thought Leadership Series**



**Threat Reports Undone**

**60-minute Live Event: Wednesday, May 26, 2020**  
10 a.m. US-Pacific/1 p.m. US-Eastern/6 p.m. London

It's everyone's favorite time of year. What will we learn from this year's breach reports? Join us as we review the latest data, look for lessons and trends, and help you understand what it all means. Our panel of experts will focus on how security professionals can learn from the data, and hopefully avoid becoming a statistic for next year's report

Generously supported by



Click [HERE TO REGISTER](#).

For more information on these or other webinars:  
[ISSA.org => Events => Web Conferences](#)



Technique name		Use Case / User Story	Data protected in			Data truthfulness at record level	Applicable to types of attributes	Reduces the risk of		
			Transit	Use	Storage			Singling out	Linking	Inference
Pseudonymization	Tokenization	Protects the data flow from attacks	Yes	Yes	Yes	Yes	Direct identifiers	No	Partially	No
Cryptographic tools	Deterministic encryption	Protects the data when not used in processing operations	Yes	No	Yes	Yes	All attributes	No	Partially	No
	Order-preserving encryption	Protects the data from attacks	Partially	Partially	Partially	Yes	All attributes	No	Partially	No
	Homomorphic encryption	Protects the data also when used in processing operations	Yes	Yes	Yes	Yes	All attributes	No	No	No
Suppression	Masking	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Local identifiers	Yes	Partially	No
	Local suppression	Protects the data in analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	Partially	Partially	Partially
	Record suppression	Removes the data from the data set	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Sampling	Exposes only a subset of the data for analytical applications	Partially	Partially	Partially	Yes	Yes	Partially	Partially	Partially
Generalization	Generalization	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	Partially	Partially	Partially
	Rounding	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	No	Partially	Partially
	Top/bottom coding	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	Yes	Identifying attributes	No	Partially	Partially
Noise addition	Noise addition	Protects the data in dev/test and analytical applications	Yes	Yes	Yes	No	Identifying attributes	Partially	Partially	Partially

Figure 7 – Examples of applicability of different data protection techniques

### Handling of direct identifiers

Common ways of dealing with direct identifiers are either removing them from the dataset (using masking) or replacing their values with pseudonyms (using pseudonymization). Unlike masking, pseudonymization preserves the ability of linking records belonging to the same data principal even after the data is de-identified.

### Handling of remaining attributes

Indirect identifiers and sensitive attributes should be removed from the dataset by “selectively applying generalization, randomization, suppression, or encryption-based de-identification techniques to the remaining attributes” [7]. Record suppression provides data truthfulness at record level. Local suppression provides data truthfulness at record level and is applicable to identifying attributes and partially reduces the risk of singling out. It partially reduces the risk of linking and partially reduces the risk of inference.

### Re-identification attacks

Re-identification is an ongoing process that needs to reevaluate attack scenarios each time additional data becomes available from different sources. Carnegie Mellon University researchers discovered that it was possible to identify 87 percent of the US population from the 1990 census with only ZIP code, gender, and date of birth [13].

A re-identification attack is an action performed on de-identified data by an attacker with the purpose of re-identification. Typically, a re-identification attack involves the creation of an “observation” dataset representing some or all of the

data principals from the original dataset. Exact disclosure occurs when an attacker determines the exact value of an attribute for a data principal [13]. Statistical disclosure occurs when aggregated data enables an attacker to obtain a better estimate of an attribute value than is possible without it.

An attacker can be an entity that has access to the de-identified data, in the form dictated by the design of the de-identification technique (e.g., by retrieving the de-identified dataset or through de-identified responses to data queries), as well as access to any additional reasonably available data external to the de-identified data.

Known approaches used in re-identification attacks include, but are not limited to:

- **Singling out:** isolating some or all records belonging to a data principal in the dataset by observing a set of characteristics known to uniquely identify this data principal.
- **Linking:** associating records concerning the same data principal or a group of data principals across separate datasets.
- **Inference:** deducing with non-negligible probability the value of an attribute from the values of a set of other attributes.

### Summary of applicability and risk reduction

Since sensitive data can be exposed to internal users, partners, and attackers, different data protection techniques can provide a balance between protection and transparency to business processes. The requirements are different for systems that are operational, analytical, or test/development as

illustrated by some practical examples and use cases in figure 7. The figure also illustrates the significant differences in applicability of pseudonymization, cryptographic tools, suppression, generalization and noise addition.

We discussed different aspects of these data privacy techniques in this article. The aspects include data truthfulness, applicability to different types of attributes, and if the techniques can reduce the risk of singling out, linking, or inference. I covered different cryptographic tools, including masking and tokens in my earlier article [8].

### Implementation aspects

The privacy policy is the heart of a privacy solution where you can define models, formats, and parameters for the privacy techniques that are used for different data objects. Implementing a secure private cloud can provide a convenient model for hosting your privacy policy, encryption, and tokenization system. The centrally managed policy can define security and privacy rules and formats for access control, masking, tokenization, and other controls. The policy can be cached locally on each system to meet operational requirements for latency and availability.

Figure 8 gives examples of applications that are using techniques described above. For example, a cloud access security broker (CASB) could use pseudonymization (tokens) to protect data that is processed and stored by a SaaS application. Tokenization is also used by applications for payments, call centers, and data warehouses (analytics).

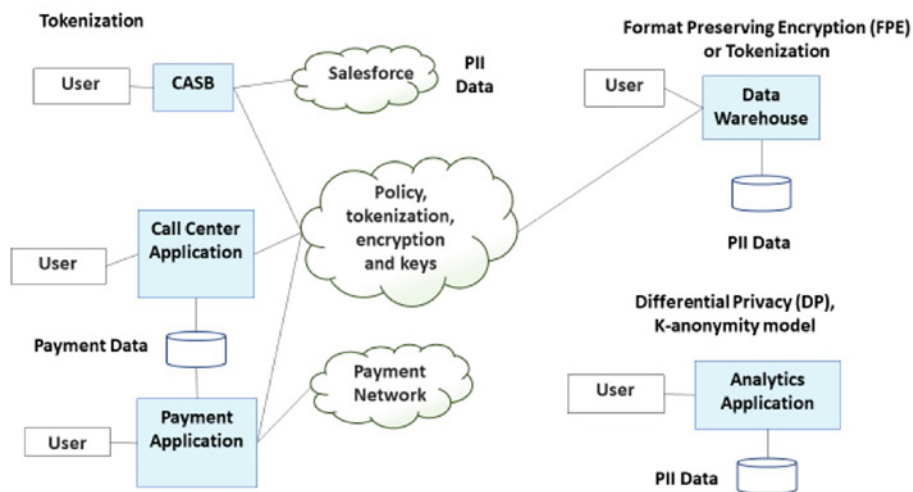


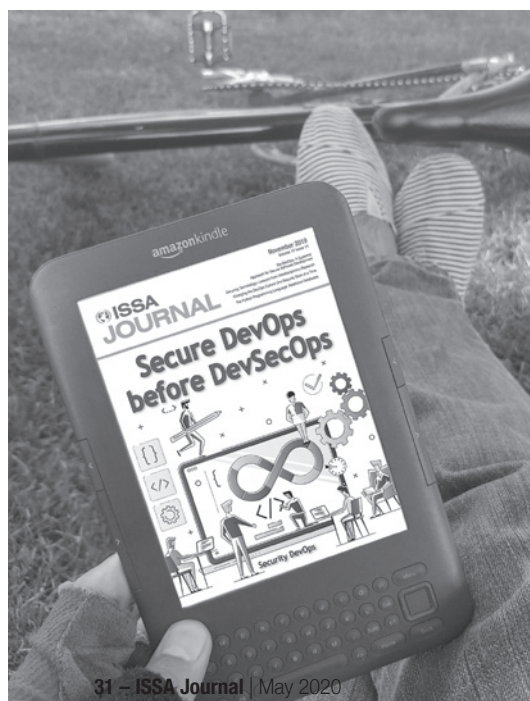
Figure 8 – Examples of applications implementing different use cases of privacy protection models

### Practical recommendations

You need to consider when to create multiple versions of some datasets, since some of these techniques are performed on the original dataset and others are performed on a copy of the dataset. The de-identified copy may be shared with users or organizations that should not have access to the original data. Keeping the original dataset, though, may also introduce liability, additional attack surface, and issues with regulatory requirements if not properly protected.

You may consider the business consequences of losing data granularity when applying some techniques, including data generalization, differential privacy, and k-anonymity.

Organizations should implement a common privacy framework based on the most stringent rules in the regions that



## The ISSA Journal on the Go!

### Have you explored the versions for phones and tablets?

Go to the [Journal home page](#) and choose "ePub" or "Mobi."

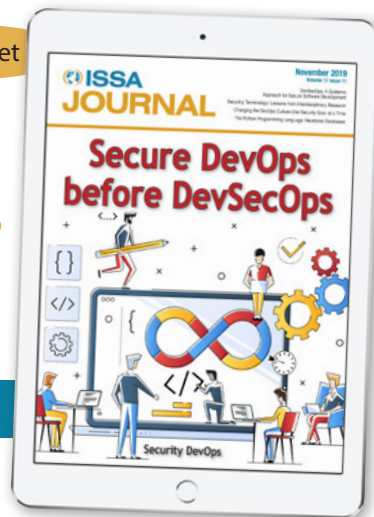
#### Mobile Device ePubs

- ePubs are scalable to any size device: iPad/tablet provide an excellent user experience
- You'll need an ePub reader such as iBooks for iOS devices



iPad/tablet

iPhone



**NOTE:** choose ePub for Android & iOS; Mobi for Kindles

**Take them with you and read  
anywhere, anytime...**

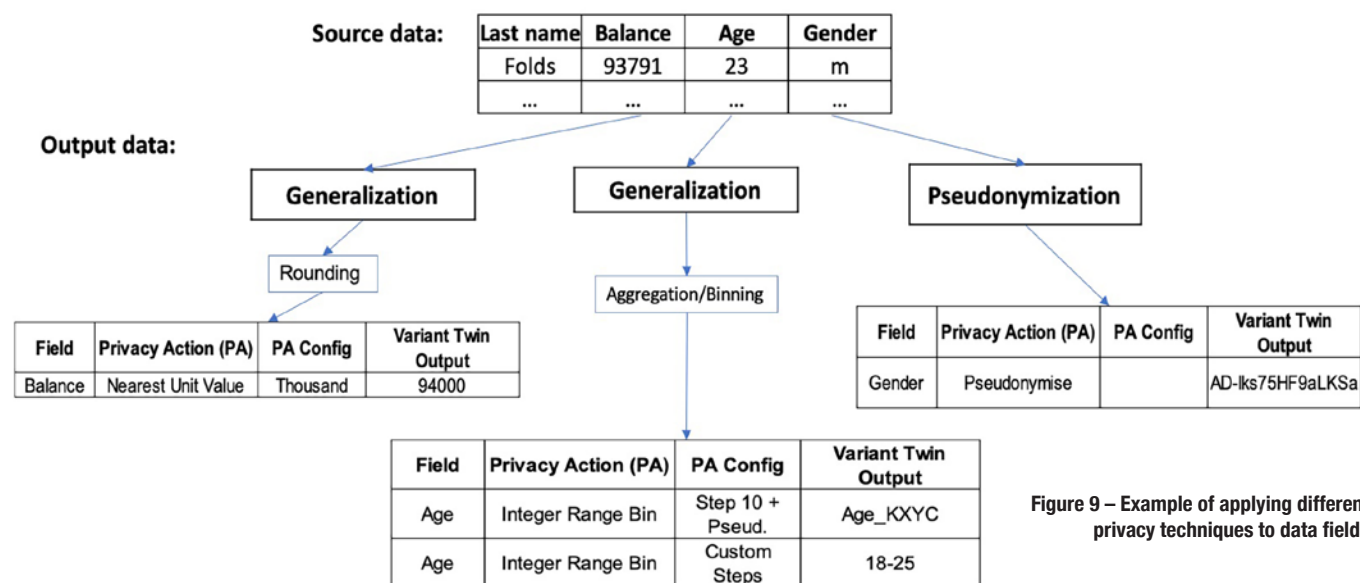


Figure 9 – Example of applying different privacy techniques to data fields

they are operating in and data that they are collecting. This can be done by selecting the most stringent rule in each regulation and implement corresponding controls. It can be a significant effort in the short term, but it will pay off in the long term by reducing fines and administration efforts.

Some organizations forget to do risk management before selecting privacy techniques and tools. Protecting PII data is now becoming increasingly critical and standards from ISO and NIST provide comprehensive definitions and a common language when discussing privacy techniques.

Figures 9 and 10 are examples of applying different privacy techniques to data fields based on ENISA guidance [3].

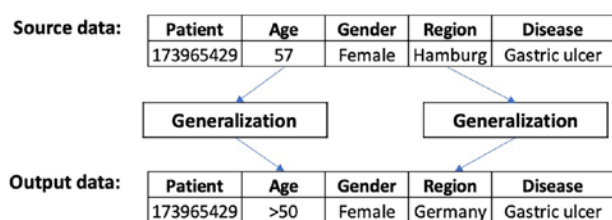


Figure 10 – Example of applying generalization to data fields

## Conclusion

We need privacy models that can mathematically be evaluated when discussing data security and privacy in an informed effort. The use of attack scenarios when evaluating different privacy models and techniques can help in understanding what we are defending against. Most privacy protection techniques can be used on identifiers and preserve data truthfulness at the record level. Only a few privacy protection techniques can reduce the risk of linking.

Many organizations are ignoring the fact that re-evaluating the privacy of de-identified data should be an ongoing process that needs to reevaluate the attack scenarios each time additional data becomes available from different sources. CCPA gives us a wake-up call about the issue of identifying

individuals via data inference. I hope that other regulations will follow these requirements.

## References

- Bigmanager, "PI Vs PII: How CCPA Redefines What Is Personal Data," BigId (Nov 4, 2019) – <https://bigid.com/ccpa-redefines-pii/>.
- Dwork C., et al. "Our Data, Ourselves: Privacy via Distributed Noise Generation," Proceedings of Eurocrypt 2006, Lecture Notes in Computer Science vol. 4004, Springer-Verlag (2006), pp.486-503 – <https://www.iacr.org/archive/eurocrypt2006/40040493/40040493.pdf>.
- ENISA. "Pseudonymisation Techniques and Best Practices," ENISAS (Dec 3, 2019) – <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>.
- Iannopollo, Enza et al. "Forrester's Global Map of Privacy Rights and Regulations," Forrester (June 24, 2019) – <https://www.forrester.com/report/Forrester+Global+Map+Of+Privacy+Rights+And+Regulations+2019/-/E-RES141638>.
- ISO 25237:2017 "Health informatics — Pseudonymization," ISO – <https://www.iso.org/standard/63553.html>.
- ISO, ISO/IEC 20889 "Privacy Enhancing Data De-identification Terminology and Classification of Techniques," ISO – [https://webstore.iec.ch/preview/info\\_isoiec20889%7Bed1.0%7Den.pdf](https://webstore.iec.ch/preview/info_isoiec20889%7Bed1.0%7Den.pdf).
- ISO/IEC 20889:2018 "Privacy Enhancing Data De-Identification Terminology and Classification of Techniques," ISO – [https://webstore.ansi.org/Standards/ISO/ISOIEC208892018?gclid=EAJaIQobChMIvI-k3sXd5gIVw-56zCh0Y0QeeEAAYASAAEgLVKfD\\_BwE](https://webstore.ansi.org/Standards/ISO/ISOIEC208892018?gclid=EAJaIQobChMIvI-k3sXd5gIVw-56zCh0Y0QeeEAAYASAAEgLVKfD_BwE).
- Mattsson, Ulf. "Data Security: On Premise or in the Cloud," ISSA Journal, December 2019 – <https://www.issa.org/journal/december-2019/>.
- NIST. "Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management," NIST – <https://>

Continued on [page 41](#)



# Quantum Cryptology: The Good, the Bad, and the Likely

By Frank Gearhart – ISSA Senior Member – Colorado Springs Chapter



In this article the author looks at some of the current research in quantum cryptology, some near-term recommendations, and what we might expect from quantum cryptology in the near future.

**“The greatest obstacle to discovery is not ignorance—it is the illusion of knowledge.”**

*~ Daniel J. Boorstin, Librarian of the US Congress*

## Abstract

Practical quantum computing—assuming it is achieved—will have tremendous impacts on our global information society and could help solve currently intractable problems. Quantum cryptology could break the encryption algorithms that protect our financial, commercial, industrial, defense, and individual data systems. But quantum cryptology depends on capable and stable quantum computing, which currently faces significant challenges. In this article I will look at some of the current research in quantum cryptology, some near-term recommendations, and what we might expect from quantum cryptology in the near future.

As cybersecurity practitioners, our primary concern is “How can I protect my data?” With quantum cryptology, this translates to “Will my encryption tools remain effective?” and “Will my encrypted data stay secure?” If we do nothing and quantum computing lives up to its promises, the answers are “No” and “No.”

According to the US National Institute of Standards and Technology (NIST) the arrival of quantum computing is expected to impact commonly used algorithms in the following ways [10]:

- AES will need to increase the key size used
- SHA-2 and SHA-3 will need to output larger hashes
- RSA will no longer be secure
- Elliptic Curve Cryptography-based algorithms such as ECDSA and ECDH will no longer be secure

- The Digital Signature Algorithm (DSA) will no longer be secure

However, quantum computing and cryptology is not assured. While there is significant research being done, there are also significant challenges, and these challenges may prevent a practical quantum computer from ever being developed.

## QKD and quantum cryptography

A side note on terminology: Quantum key distribution (QKD) is not quantum cryptography, although popular articles often equate the two. QKD uses quantum effects such as photon spin to detect if an eavesdropper is attempting to read the key as it is being transmitted between authorized parties [15]. QKD ensures that only bits that have not been seen by an eavesdropper are used in the key. Once a key has been securely shared, traditional encryption algorithms are used. China has demonstrated the practical use of QKD across four thousand miles using fiber-optic cabling and low earth orbit satellites [8]. Unfortunately, it is not likely that QKD will soon be coming to a laptop or a mobile phone near you.

## Quantum hardware and programming

Like traditional computing, quantum computing depends on reliable hardware and software. There are four logical structures that make up the hardware of a quantum computer:

- The quantum data plane, which includes the physical qubits and supporting structures
- The control processor plane, which manages the operations and measurements needed to run the algorithm as well as any quantum error correction algorithms

- The control and measurement plane, which carries out operations and measurements on the qubits and translates between the control processor's digital signals and data plane's analog signals
- The host processor, a traditional computer that handles access to networks, external storage, user interfaces, etc. [9]

This is not the same architecture used in traditional computers. In fact, a quantum computer could be thought of as a specialized component in a hybrid system—part traditional computer and part quantum. From a security viewpoint, since the host processor is a traditional computer, it is a target for traditional classical cyber attacks and requires appropriate protections.

Programming a quantum computer is new. There is no *Quantum Programming for Dummies* book on bookstore shelves. We have decades of practice in programming for traditional hardware, which all use the von Neumann architecture [6]. While quantum programming is far from mature, there are several quantum programming languages in use or in development [5]. Quantum Computing Language (QCL) is an open-source quantum programming language with a C-like syntax. LanQ also has a C-like syntax and supports both tra-

ditional and quantum instructions. Q# (Q-sharp) was developed by Microsoft, which released version 2 of Q# in 2018. Other quantum programming languages include QML and Quipper. Additionally, quantum programming libraries for Python and C/C++ are available. To run quantum programs, IBM currently makes 5-qubit and 16-qubit quantum computers available online via their IBM Q project, with over 80,000 users currently accessing IBM Q [5].

### How many qubits is enough?

In traditional computing, more CPU cores generally equates to a more powerful computer. In quantum computing, more qubits equate to more computing power. There is no single answer to how many qubits is enough to run useful programs. Some research puts a lower bound of between 90 and 360 qubits for a quantum computer that can solve specific types of problems that are too difficult for traditional computers to solve [3]. Implementing Shor's algorithm could require thousands of stable qubits [2].

These numbers are far from what is currently available. Google recently announced a 78-qubit computer, while IBM reports they will soon have a 52-qubit computer available for customers [13].

The number of computing qubits available is not the only challenge. Qubits are notoriously unstable and require specialized hardware to input and output data as well as keep the qubits as isolated from external influences as possible in order to maintain quantum stability. Traditional computer hardware is far more robust, running reliably in environments from interplanetary space to vehicle engine bays and industrial machinery. Secondly, quantum computers theoretically require at least five error-correcting qubits for every computing qubit. Without these error-correcting qubits, quantum processors can have error rates that reach five percent or higher [2].

There is one more item to keep in mind regarding quantum computing. Because the quantum mechanics underpinning quantum computing is probabilistic, quantum algorithms are probabilistic, that is, the answers they give have a certain probability of being the correct answer, but that probability is not one hundred percent. This may require new approaches to computing, such as running the same quantum program with the same parameters and inputs multiple times to determine confidence levels in the output. In other words, if asked "What is 35 divided by 5?" a quantum algorithm may respond with "I'm 95% certain the answer is 7."

### Quantum cryptanalysis

There are two quantum algorithms that currently pose the greatest threats to current cryptosystems: Shor's algorithm and Grover's algorithm. Shor's algorithm poses a threat to the security of the two most widely used asymmetric algorithms: RSA and Diffie-Hellman-Merkle (also known as Diffie-Hellman or DH).

## ISSA CYBER EXECUTIVE FORUM



The unique strength of the Cyber Executive Forum is that members can feel free to share concerns, successes, and feedback in a peer-only environment.

### May Virtual Cyber Executive Forum

May 14 and May 15, 2020

### August Cyber Executive Forum

Las Vegas, NV – August 2 - 3, 2020

Concurrent with Black Hat USA

### October Cyber Executive Forum

Washington DC – October 22 - 23, 2020

For information or to register: [Click Here](#)

RSA is based on the idea that it is easy to multiply two very large prime numbers, but very difficult to take the product of those two primes and determine which two prime numbers are its divisors. Diffie-Hellman-Merkle is based on the difficulty of the discrete log problem. Shor's algorithm (published in 1994 by Peter Shor) can find the RSA and DH factors exponentially faster than traditional methods, even when using current supercomputers [14]. However, estimates are that a quantum computer running Shor's algorithm may require hundreds or thousands of computational qubits. A new quantum algorithm called variational quantum factoring (VQF) may be more efficient than Shor's algorithm, but VQF is still theoretical [2].

Grover's algorithm poses a less severe but still significant threat to the security of symmetric encryption algorithms such as AES. Grover's algorithm (published in 1996 by Lov Grover) is a general search algorithm that provides a significant speed increase over traditional algorithms when searching through a random collection of items (such as a list of all possible decryption keys for an encrypted file). Grover's algorithm reduces the time it would take to search a list of  $N$  number of items from  $N$  to  $\sqrt{N}$  [14]. As an example, if it would take a traditional computer one year to find a decryption key, it would take a quantum computer running Grover's algorithm nineteen days (on average).

### Quantum cryptography

The news from the quantum world isn't all bad. Since 2017, NIST has overseen a public search for quantum-resistant algorithms to replace those that are susceptible to quantum-based attacks. First let's look at asymmetric algorithms.

NIST is testing twenty-six post-quantum cryptography algorithms with the goal of finding quantum-resistant digital signature and public-key algorithms [11]. The PQC algorithms selected can be used in TLS, SSH, IKE, IPSec, and DNSSEC protocols. Three classes of algorithms showing the most promise as quantum-resistant asymmetric encryption algorithms are lattice-based, code-based, and multivariate [1]. Of these, lattice-based algorithms appear to offer the best likelihood for providing a quantum-resistant asymmetric (public-key) cryptosystem, but there are challenges in finding accurate methods of verifying their cryptographic strength [7].

For symmetric encryption, increasing the size of the keys used can defend against Grover's algorithm. Moving from a 128-bit key to a 256-bit key increases the key space by a factor of  $2^{128}$ . This would cause Grover's algorithm to take (on average)  $2^{63}$  times as long to find a 256-bit key as it would to find a 128-bit key – equivalent to going from one year to far longer than the estimated age of the universe, which is ~13.7 billion years.

### A quantum computing future

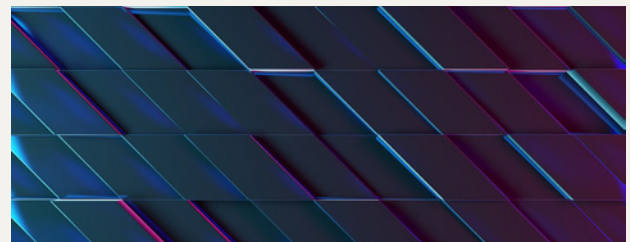
Most experts believe a general-purpose quantum computer may be available within the next ten to thirty years—a remarkably wide range that reinforces just how little knowledge

we have about many aspects of quantum computing [2]. In September 2019 Dario Gil, the IBM Research Director, said “We define QA [quantum advantage] as when we will have systems that are powerful enough and, of course, programmable that would allow us to solve problems that matter, something of relevance to your business or science that we couldn't do before. So my best estimate is that we're still years away” [13].

At least one expert thinks that quantum computers may never exist. In a 2019 article, quantum physicist Mikhail Dyakonov wrote that practical quantum computers are unlikely to be built in the foreseeable future [4]. Dyakonov argues that



### ISSA Thought Leadership Series



## Current Landscape of Mid-Market Threat Intelligence

**60-minute Live Event: Wednesday, May 20, 2020**

10 a.m. US-Pacific/1 p.m. US-Eastern/6 p.m. London

The global threat landscape is changing. Mid-market enterprises are facing the same threats as larger ones. Attackers are no longer exclusively focused on high-value intellectual property assets of billion-dollar corporations. Any organization handling sensitive information has become an inviting target for hackers to exploit.

This interactive web conference will cover:

- Current cyber attacks most threatening to mid-market enterprises
- Getting cutting-edge expertise in-house without hiring
- Assessing and training your employees
- Developing and testing an emergency response plan
- How can you fund these efforts?
- Getting started with your updated cybersecurity plan

**Speakers:** Chris Schreiber, Cybersecurity Platform Strategist, FireEye & Steve Cobb, CISO, One Source

Generously supported by



Click [HERE TO REGISTER](#).

For more information on these or other webinars:

[ISSA.org => Events => Web Conferences](#)



a general-purpose quantum computer would require between 1,000 and 100,000 stable qubits. This means that between  $2^{1,000}$  and  $2^{100,000}$  parameters that describe the state of the quantum computer would need to be continuously managed. That lower number –  $2^{1,000}$  – is larger than the number of subatomic particles in the known universe. If Dyakonov's arguments are correct, it may be impossible to create a quantum computer large enough to be of any use.

### Until PQC arrives

Until quantum-resistant cryptographic algorithms are available, the US National Security Agency (NSA) has the following recommendations to remain secure [12]:

### ISSA CAREER CENTER

The ISSA [Career Center](#) offers a listing of current job openings. Among the current job listings [5/1/2020] are the following:

- **Global IT Audit Senior** – Newmont, Greenwood Village, CO
- **Penetration Tester** – State Farm Mutual Automobile Insurance Company, Richardson, TX
- **Cyber Security Analyst/IA Specialist** – VASTEC, Tampa, FL
- **System Administrator / System Security Instructor - 2 positions** – Northeast Wisconsin Technical College, Green Bay, WI
- **Senior Cybersecurity Analyst** – EMF, Rocklin, CA
- **Assistant Vice President of IT@UC, Office of Information Security** – University of Cincinnati, Cincinnati, OH
- **Information Security - SOX Analyst** – Motorola Solutions, Krakow, Poland
- **Senior Information Security Analyst** – KOHLS, Milpitas, CA
- **Information Security Engineer** – Federal Reserve Bank of Chicago, Chicago, IL
- **Business Information Security Consultant** – Northwestern Mutual, Milwaukee Corporate, WI
- **Travel Senior Information Security Analyst / Lead Security Control Assessor** – Motorola Solutions, Maryland
- **Information Security Engineer I - Federal SOC** – CenturyLink, Broomfield, CO
- **Information Security Architect** – Centene, Rancho Cordova, CA
- **Information Security Manager** – Raytheon Technologies, Arlington, VA
- **Mid-Level Information Security Manager** – Raytheon Technologies, Arlington, VA

- Use 256-bit keys with the Advanced Encryption Standard (AES-256)
- Use 384-bit Elliptic Curve Cryptography (ECDH P-384 and ECDHA P-384)
- Use 384-bit digital signatures (SHA-384)
- Use 3,072-bit modulus for Diffie-Hellman key exchange

If possible, organizations should adjust their encryption settings to implement these recommendations. Keep in mind that some of these adjustments could noticeably impact a system's performance. As we know, security is often a tradeoff.

### Near-term risk

Given the current state of quantum computing, I believe the cybersecurity risk over the next five to ten years is low. Over the next two to three decades, if (1) the promise of quantum computing is fulfilled and (2) Grover's and Shor's algorithms (or similar algorithms) can be effectively implemented, then I see the longer term risk as follows:

- Any data stored using AES-128 or similarly strong symmetric encryption may be stolen, stored, and read within weeks or months.
- Any data transmitted using RSA or similar asymmetric encryption algorithms may be captured and read very soon after capture.

One way to reduce the risk to stored data is to decrypt those data stores and re-encrypt them with quantum-resistant algorithms once those algorithms are available.

### Conclusion

It is likely the first practical quantum computers will be extremely expensive, with programming and computing time a limited and very valuable resource, and therefore tightly controlled. As a result, I believe the first quantum computing threats to cybersecurity will likely come from large, technically advanced nation-states that have the resources to develop and maintain this technology. China and the United States are currently considered the front-runners in developing quantum computing and related technologies, but there may be unknown projects out there. As practitioners we should continue to do what we have always done: guide our organizations through waves of attacks and defend while keeping an eye on the horizon so that we can prepare for the coming storms.

### References

1. Bernstein, Daniel J., and Tanja Lange. 2017. "Post-Quantum Cryptography." *Nature* (Macmillan Publishers) 549: 188-194 – <https://www.nature.com/articles/nature23461?draft=collection>.
2. Brooks, Michael. 2019. "Before the Quantum Revolution." *Nature* 574 (7776): 19-21.
3. Dalzell, Alexander M., Aram W. Harrow, Dax Enshan Koh, and Rolando L. La Placa. 2018. "How Many Qubits Are

Continued on [page 41](#)

# The Python Programming: Processing NVD Data

By **Constantinos Doskas** – ISSA Senior Member, Northern Virginia Chapter



**This article continues our discussion on database programming by exploring methods of downloading data from web sites, loading them on databases, and analyzing them.**

This article continues our discussion on database programming by exploring methods of downloading data from websites, loading them on databases, and analyzing them. In past articles we had an overview of NVD database data as it is distributed in JSON files, downloaded the HTML code of the NVD website, and developed a method to identify the names of the JSON-zipped files that comprise the NVD database. In this article we will be downloading the JSON files and start processing them.

## The scenario of this article

In continuation of the work we have done in the previous articles, we are going to download the National Vulnerability Database (NVD) zipped JSON files. Once we have the files in our local storage, we will decompress them and process their data. While we are processing the data, we will create database tables and load them with NVD data. Note that there are many ways to design such a database; we will avoid following strict database design rules in order to enable everybody to understand the basic process. As mentioned in the past, while we are processing data, we may encounter errors and our program must be able to handle them and either continue processing or terminate with a useful message to the operator.

## Start with the flowchart

Before we start developing a computer program, we create a graphical representation of it. That step comes after a step that produces an analysis document. Let's consider that we do have an analysis document that will guide us, providing the inputs, outputs, and other data that was collected in the form of requirements, etc. Now that we have that information and before we start producing any code, we take pencil and paper, or a drawing app, and draw the skeleton of the program to

be developed. This drawing is very useful since we can easily share it with others and go through a process of refinement, adjusting it until we are confident of its completeness. Then, we start the effort of developing, testing, and debugging the code until it is ready to go to production.

Development shops are using various types of graphs, depending on their procedures. We will use a traditional flowchart. To make the flowchart simple, readable, and appropriate for a short article, we will divide it into a number of charts.

In figure 1 we view the overall process.

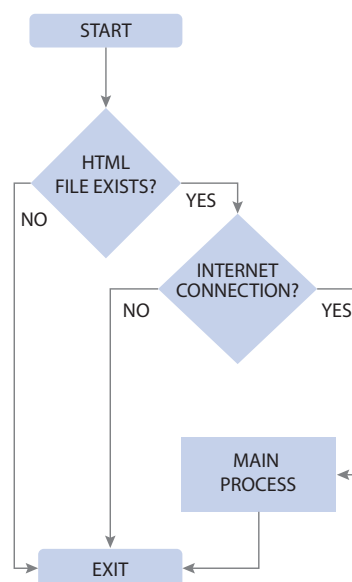


Figure 1

Next, in figure 2 we focus on the code before the main process.

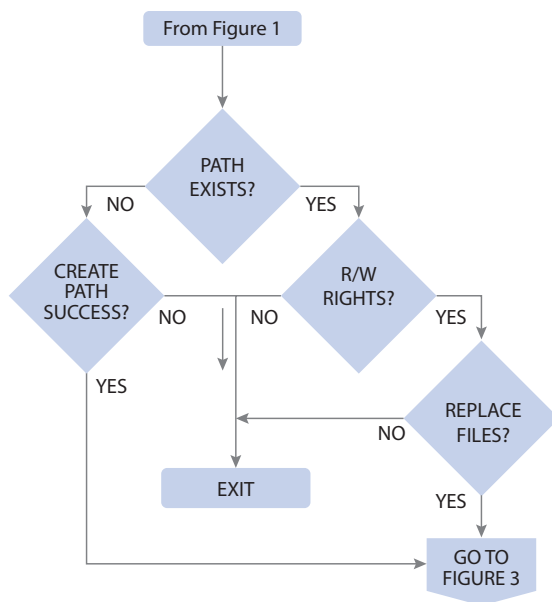


Figure 2

Finally, in figure 3 we flowchart the main process, the download of JSON files.

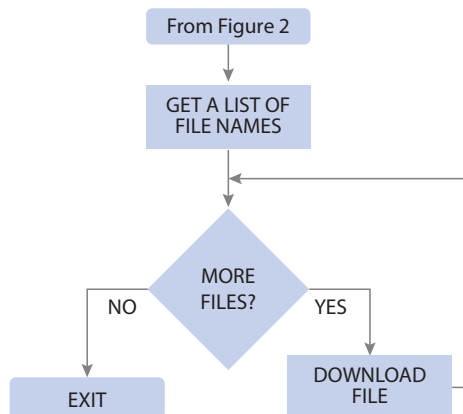


Figure 3

Now that we have the program flowchart, let us examine some of the code. A big part of the code was posted in the last article. In this article we will add some error handling code. There are two basic methods of handling errors. One is to handle the error right where it takes place, the other to have code down the line that handles it.

In the following snippet, the function *checkInternetConnection()* tests for Internet connection and passes to the main program a 'Y' if there is Internet connection and 'N' otherwise. If there is no Internet connection the program prints a message and terminates.

This was the first method of managing a condition/error. The next function in the snippet, *is\_html\_downloaded(htmlfile)*, takes input from an argument, *htmlfile*, which carries the name of the file that contains the NVD HTML code. If that file was previously downloaded and placed in the current directory, the function allows processing to continue; otherwise it terminates the program.

```

import requests
import socket
import os
import sys
.....
def checkInternetConnection():
    try:
        socket.create_connection(("nvd.nist.gov",80),20)
        return 'Y'
    except OSError:
        print("OSError. Connection failed")
        return 'N'
def is_html_downloaded(htmlfile):
    try:
        os.listdir(htmlfile)
    except FileNotFoundError:
        print('Error - No such file or directory: '+htmlfile)
        print('Download the file and re-run the program')
        sys.exit('Process terminating')
# - Main program -----
if 'N' in checkInternetConnection():
    print('No internet connection. \
        Connect to internet and re-run the program')
    sys.exit('Process terminating')
  
```

Here is a quick note regarding the above code: The socket module that was imported in the program provides low-level connectivity functions. The format of the *socket.create\_connection* method takes several arguments. We are currently using the following:

```
socket.create_connection((url,port),timeout)
```

(url,port) is a tuple and timeout is time to wait for a connection in seconds.

Next, there are a few conditional statements that are used to determine if the directory, which we will use to store the downloaded files, exists and if the files, if they exist, should be overwritten (see figure 2). We will not present the code here, but it will be available to download.

In the previous article we created a loop that searched the NVD webpage and extracted the links and names of files to be downloaded. Here are a few of those links and file names:

#### Links (in a List that we named refs):

```

https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-
modified.json.zip
https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-
recent.json.zip
https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-2020.
json.zip
https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-2019.
json.zip
https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-2018.
json.zip
  
```

#### Files (in a List that we named files):



```

nvdCVE-1.1-modified.json.zip
nvdCVE-1.1-recent.json.zip
nvdCVE-1.1-2020.json.zip
nvdCVE-1.1-2019.json.zip
nvdCVE-1.1-2018.json.zip

```

Using a loop, we will download these files to the directory in our local storage.

```

for i in range(len(refs)):
    nvdfile=requests.get(refs[i],stream=True)
    # -- Once the file is downloaded use a "with"
    loop to save it on disk
    # -- Note that the file is saved chunk by chunk.
    with open('CVE_FILES/'+files[i],'wb') as fh:
        for achunk in nvdfile:
            fh.write(achunk)

```

Once the files are downloaded, we may start processing them. In this study we will first create database tables and load the data. Note that as we have stated before, each of these JSON files organizes the data in a complex directory. Imagine the data stored in an onion-type structure. Let's take the outer layer and load it on a table. This layer offers a description of the contents of the file. We will leave just one element unprocessed. That element contains all the vulnerabilities of the year that the JSON file was created. Our first table will have the following fields.

```

year_id, data_type, data_format, data_version,
number_cves, time_stamp,file

```

The field file contains the name of the JSON file itself. Let's see the code that creates that table.

```

import zipfile
import os
import json
import sqlite3
# -- Create or open a database
dbase=sqlite3.connect('nvd_data.db')
mydbCursor=dbase.cursor()
# -- Drop table if exists
mydbCursor.execute("DROP TABLE IF EXISTS {}".
    format('nvd_master'))
# -- Create tables
mydbCursor.execute('CREATE TABLE IF NOT EXISTS\
    nvd_master(year_id TEXT PRIMARY KEY, data_type
    TEXT,
    data_format TEXT, data_version TEXT, number_cves
    INTEGER,
    time_stamp TEXT, file TEXT)')
for afile in os.listdir('CVE_FILES/'):
    if afile.count('20')>0:
        year=afile[afile.index('20'):afile.index('.json')]
        print('\nYear:' ,year)
        print('Processing File: ',afile) # - file to
        process
        zf=zipfile.ZipFile('CVE_FILES/'+afile,'r')
        j=zf.open(zf.namelist()[0]) # -- open unzipped in
        read mode

```

```

cved=json.loads(j.read()) # -- Loading json
data on a Python Directory
j.close() # -- close unzipped file (in memory)
nvdMasterValues=""+"year+"
jdkeys=cved.keys()
print('Master Dictionary, keys: ',len(jdkeys))
for k in jdkeys:
    if k.lower().count("items") == 0:
        print('Key:value Pair
            ',k,':',cved[k])
        if cved[k].isnumeric():
            nvdMasterValues=nvdMasterValues+" "+cved[k]
        else:

```



[Click here for On-Demand Conferences](#)

### Breaking Down Zero Trust: What Does it Actually Mean?

Recorded Live: April 28, 2020

### Proofpoint State of the Phish 2020

Recorded Live: Wednesday, April 8, 2020

### Dissecting Ransomware to Defeat Threat Actors

Recorded Live: March 11, 2020

### Supply Chain Security – Shifting Left

Recorded Live: March 3, 2020

### Combating Business Email Compromise and Email Account Compromise

Recorded Live: February 19, 2020

### 2019: A Year in Review

Recorded Live: January 28, 2020

### The Asset Management Resurgence

Recorded Live: January 22, 2020

### Software-Defined Segmentation Solving the Challenges of Today's Accelerated Enterprise

Recorded Live: December 11, 2019

### Building a People-Centric Cybersecurity Strategy for Health Care

Recorded Live: December 4, 2019

### The Persistent Pernicious Myths and Hidden Truths of Cybersecurity

Recorded Live: November 6, 2019

### Cloud Data Security: Own Your Data Encryption Keys

Recorded Live: Wednesday, November 13, 2019

### Attack of the Botnets – Internet of Terror IoT II


Recorded Live: October 22, 2019

### Top Five Ways to Identify Automated Attacks to Your Website and Mobile Apps

Recorded Live: October 16, 2019

### The Seven Deadly Sins of Insiders and How to Defend

Recorded Live: October 9, 2019

Table:  nvd\_master

	year_id	data_type	data_format	data_version	number_cves	time_stamp	file
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	2020	CVE	MITRE	4.0	740	2020-02-09T08:00Z	nvdCVE-1.1-2020.json.zip
2	2019	CVE	MITRE	4.0	14271	2020-02-09T08:00Z	nvdCVE-1.1-2019.json.zip
3	2018	CVE	MITRE	4.0	16035	2020-02-08T08:29Z	nvdCVE-1.1-2018.json.zip
4	2017	CVE	MITRE	4.0	15952	2020-02-08T08:52Z	nvdCVE-1.1-2017.json.zip
5	2016	CVE	MITRE	4.0	10252	2020-02-09T08:29Z	nvdCVE-1.1-2016.json.zip
6	2015	CVE	MITRE	4.0	8445	2020-02-09T08:38Z	nvdCVE-1.1-2015.json.zip

Figure 4 – nvd\_master table

```

nvdMasterValues=nvdMasterValues+"," +cved[k]+"
    else:
        print(k,' key was found, skipped. This
is the key of the CVE records')

nvdMasterValues=nvdMasterValues+"," +afile+"
    print(' -- Creating table entry using
the following SQL statement')
    mydbCursor.execute("INSERT INTO nvd_master\
VALUES({}).format(nvdMasterValues))
    dbase.commit()
    dbase.close()

```

The table that was created by the above code is shown in figure 4.

In the following articles we will be creating additional tables and visualizations based on the data. Figure 5 is an example.

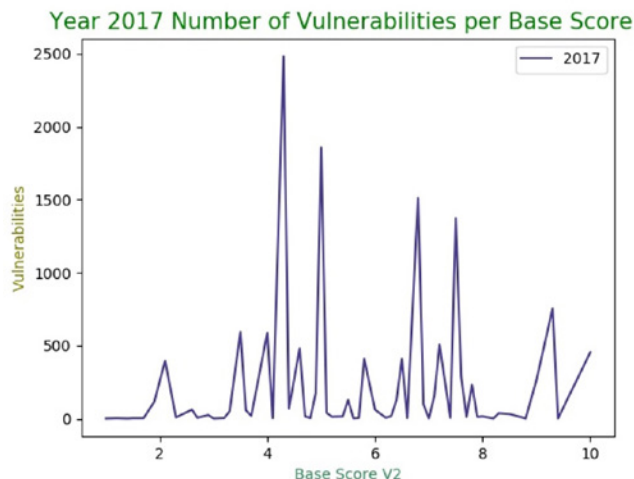


Figure 5 – Year 2017, number of vulnerabilities per base score

## Review and conclusion

This article is part of a series of articles that aim in helping cybersecurity professionals understand how information is acquired, organized, stored, and processed. The topic of the current article is how data from the NVD website may be downloaded, extracted, and prepared for analysis. The article presented ways to handle errors and respond to user requests.

Future articles will present ways to analyze the downloaded data and discuss the risk management framework.

I hope that you enjoyed the article and you will find ways to apply the presented concepts to your daily tasks. I am moving slow on these concepts giving you time to run the code and experiment. ISSA International makes available the code on its [website](#).


You are always welcome to email me with any questions you may have. I wish you well and will be pleased to “see” you through the next article.

## About the Author

Constantinos Doskas is head of the IT and Security Department of Olympus. He has been involved in information systems management and development for over 30 years. He is currently involved in mentoring graduate students and ISSA members in Northern Virginia. He may be reached at [cdoskas@ofcorp.com](mailto:cdoskas@ofcorp.com).



## 2019 Journal – Past Issues

Past Issues – digital versions: click the download link: 

-  Best of 2018    Legal & Public Policy
-  Cloud    Infosec Basics
-  Cryptography    Privacy
-  Internet of Things    The Toolbox
-  Information Security Standards
-  The Business Side of Security
-  Security DevOps    Looking Forward

## Quantum Cryptology: The Good, the Bad, and the Likely

Continued from [page 36](#)

- Needed for Quantum Computational Supremacy?" arXiv. org. September 18 – <https://arxiv.org/abs/1805.05224>.
4. Dyakonov, Mikhail. 2019. "The Case Against: Quantum Computing." IEEE Spectrum (IEEE) 56 (3): 24-29 – <https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing>.
  5. Garhwal, Sunita, Maryam Ghorani, and Amir Ahmad. 2019. "Quantum Programming Language: A Systematic Review of Research Topic and Top Cited Languages." Archives of Computational Methods in Engineering: State of the Art Reviews (Springer Netherlands) 1-22. Accessed April 10, 2020. doi:10.1007/s11831-019-09372-6.
  6. Hennessy, John L., and David A. Patterson. 2003. *Computer Architecture: A Quantitative Approach*. 3rd. San Francisco, CA: Morgan Kaufmann. Accessed April 10, 2020.
  7. Hsu, Jeremy. 2019. "How the United States Is Developing Post-Quantum Cryptography." IEEE Spectrum. September 6 – <https://spectrum.ieee.org/tech-talk/telecom/security/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy>.
  8. Khan, Imran, Bettina Heim, Andreas Neuzner, and Christoph Marquardt. 2018. "Satellite-Based QKD," February – [https://www.osa-opn.org/home/articles/volume\\_29/february\\_2018/features/satellite-based\\_qkd/](https://www.osa-opn.org/home/articles/volume_29/february_2018/features/satellite-based_qkd/).
  9. National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects (2019)*. Edited by Emily Grumbling and Mark Horowitz. Washington, D.C.: The National Academies Press – doi:10.17226/25196.
  10. NIST. 2016. "Report on Post-Quantum Cryptography." CSRC. April – doi:10.6028/NIST.IR.8105.
  11. NIST. 2019. "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process." NIST Computer Security Resource Center. January 30. Accessed April 13, 2020. doi:10.6028/NIST.IR.8240.
  12. NSA. "Commercial National Security Algorithm Suite." NSA/CSS. August 19, 2015 – <https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm>.
  13. Russell, John. "IBM Opens Quantum Computing Center; Announces 53-Qubit Machine," HPC Wire, September 19, 2019 – <https://www.hpcwire.com/2019/09/19/ibm-opens-quantum-computing-center-announces-53-qubit-machine/>.
  14. Shrivastava, Prakhara, Kapil Kumar Soni, and Akhtar Rasool. "Evolution of Quantum Computing Based on Grover's Search Algorithm." 2019 10th International Conference on Computing, Communication and Networking Technologies. Kanpur: IEEE. 1-6 – doi:10.1109/IC-CCNT45670.2019.8944676.

15. Yuen, Horace. 2014. "Some Physics and System Issues in the Security Analysis of Quantum Key Distribution Protocols," Quantum Information Processing (Springer Nature) 13 (10): 2241-2254 – doi:10.1007/s11128-014-0756-4.

### About the Author

Frank Gearhart is a lead cybersecurity engineer (contractor) at DoD Missile Defense Agency, Colorado Springs, CO. He is a past president of Colorado Springs Chapter and ISSA Volunteer of the Year – 2017. He has ten years of cybersecurity experience, served in the US Coast Guard, is a PhD candidate at North Central University, and may be reached at [frank.gearhart@outlook.com](mailto:frank.gearhart@outlook.com).



## Data Privacy: De-Identification Techniques

Continued from [page 32](#)

- [www.nist.gov/system/files/documents/2019/09/09/nist\\_privacy\\_framework\\_preliminary\\_draft.pdf](http://www.nist.gov/system/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf).
10. Rouse, Margaret. Data Privacy (Information Privacy)," TechTarget – <https://searchcio.techtarget.com/definition/data-privacy-information-privacy>.
  11. Shey, Heidi et al. "Rethinking Data Discovery And Classification Strategies," Forrester (July 10, 2018) – <https://www.forrester.com/report/Rethinking+Data+Discovery+And+Classification+Strategies/-/E-RES85842>.
  12. Shey, Heidi et al. "Demystifying De-Identification, Anonymization, And Pseudonymization," Forrester (Nov 7, 2019) – <https://www.forrester.com/report/Demystifying+DeIdentification+Anonymization+And+Pseudonymization/-/E-RES158075>.
  13. Sweeney, Latanya. "Simple Demographics Often Identify People Uniquely," Carnegie Mellon University (2000) – <https://dataprivacylab.org/projects/identifiability/index.html>.
  14. Sweeney, Latanya. "Database Security: k-anonymity" – <http://latanyasweeney.org/work/kanonymity.html>.
  15. Techopedia, What is the Difference between Security and Privacy, <https://www.techopedia.com/7/29722/security/what-is-the-difference-between-security-and-privacy>.

### About the Author

Ulf Mattsson has participated in the development of standards in ANSI X9 and PCI DSS for more than fifteen years. He has more than 70 issued US patents and has been developing products and services for robotics, applications, data encryption and tokenization, data discovery, cloud application security brokers, and web application firewalls. Ulf may be reached at [ulf@ulfmattsson.com](mailto:ulf@ulfmattsson.com).





## ISSA Cyber Executive Membership Program

The role of information security executive continues to be defined and redefined as the integration of business and technology as it evolves. While these new positions gain more authority and responsibility, peers must form a collaborative environment to foster knowledge and influence that will shape the profession.

The Information Systems Security Association (ISSA) recognizes this need and created the exclusive Cyber Executive Membership program to give executives an environment to achieve mutual success. Connecting professionals to a large network of peers, valuable information, and top industry experts the program is a functional resource for members to advance personal and industry understanding of critical issues in information security.

### Membership Benefits

- Free registration at four Executive Forums per year, including lodging for one night and all meals at each Forum
- Extensive networking opportunities with peers and experts on an on-going basis
- Privileged access to online community
- Direct access to top subject matter experts through educational seminars
- An effective forum for understanding and influencing relevant standards and legislation
- A unified voice to influence industry vendors
- Automatic CPE submission

**Visit [ISSA.org](http://ISSA.org) => Cyber Executive Forum for more information or to register for the Forum.**

## ISSA Chapters around the Globe

### Asia Pacific

Bangladesh  
Chennai  
Dehradun  
India  
Philippines

### Canada

Alberta  
Ottawa  
Quebec City  
Vancouver

### Europe

Brussels European  
France  
Germany  
Italy  
Netherlands  
Poland  
Romania  
Spain  
Switzerland  
Turkey  
UK  
Ukraine

### Latin America

Argentina  
Barbados

Bolivia  
Brasil  
British Virgin Islands  
Chile  
Colombia  
Ecuador  
Peru

### Middle East

Bahrain  
Egypt  
Iran  
Israel  
Kazakhstan  
Kuwait  
Qatar  
Saudi Arabia

### USA

Alamo San Antonio  
Blue Ridge  
Boise  
Buffalo Niagara  
Capitol Of Texas  
Central Alabama  
Central Florida  
Central Indiana  
Central Maryland  
Central New York

Central Ohio  
Central Plains  
Central Texas  
Central Virginia  
Charleston  
Charlotte Metro  
Chattanooga  
Chicago  
Colorado Springs  
Columbus  
Connecticut  
Dayton  
Delaware Valley  
Denver  
Des Moines  
East Tennessee  
Eastern Idaho  
Fayetteville/Fort Bragg  
Fort Worth  
Grand Rapids  
Grand Traverse  
Greater Augusta  
Greater Cincinnati  
Greater Spokane  
Hampton Roads  
Hawaii  
Inland Empire  
Kansas City

Kentuckiana  
Kern County  
Lansing  
Las Vegas  
Los Angeles  
Metro Atlanta  
Middle Tennessee  
Milwaukee  
Minnesota  
Montana  
Motor City  
National Capital  
New England  
New Hampshire  
New Jersey  
New York Metro  
North Alabama  
North Dakota  
North Oakland  
North Texas  
Northeast Florida  
Northeast Indiana  
Northeast Ohio  
Northern Colorado  
Northern Virginia  
Northwest Arkansas  
Northwest Ohio  
Oklahoma

Oklahoma City  
Orange County  
Phoenix  
Pittsburgh  
Portland  
Puerto Rico  
Puget Sound (Seattle)  
Quantico  
Rainier  
Raleigh  
Rochester, NY  
Sacramento Valley  
San Diego  
San Francisco  
San Jose  
SC Upstate SC  
Silicon Valley  
South Florida  
South Texas  
Southeast Arizona  
Tampa Bay  
Tech Valley Of New York  
Texas Gulf Coast  
Triad of NC  
Utah  
Ventura County  
West Texas  
Wyoming  
Yorktown