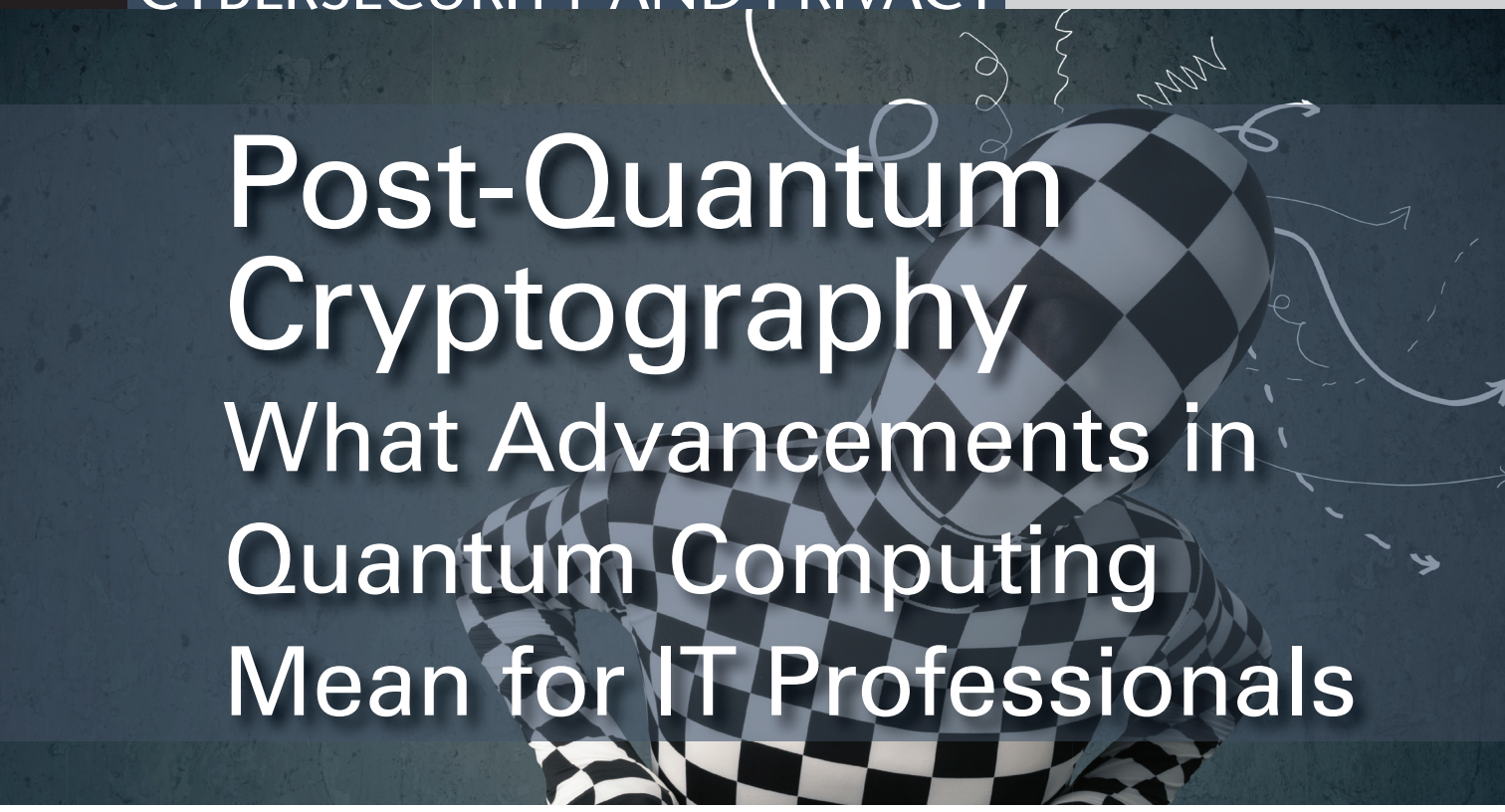

Post-Quantum Cryptography

What Advancements in Quantum Computing Mean for IT Professionals

Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila, *Air Force Institute of Technology, Wright-Patterson Air Force Base*

The impact of quantum computing is a topic of increasing importance to IT practitioners. Thus, the authors present a readily understandable introduction and discussion of post-quantum cryptography, including quantum-resistant algorithms and quantum key distribution.

Recent developments in quantum computing (QC) show promise to significantly impact the security and privacy of modern cryptography. Although notions of QC were discussed throughout the last quarter of the 20th century, it was only in 1994, when Peter Shor formulated his algorithm for factoring large prime numbers, that QC garnered the attention of the cybersecurity community (security experts, cryptographers, computer scientists, and information theorists). This is because Shor's algorithm places our modern-day public-key infrastructure (PKI) in jeopardy (because PKI is based on the difficulty of factoring large prime numbers using RSA). For example, a 2,048-bit RSA key that is thought to take billions of years to break on a classical computer could be solved in a matter of seconds using a mature QC architecture.[1] Table 1 briefly summarizes how advances in QC directly affect existing and proposed cryptosystems.[2]

Although quantum computers today are experimental systems with small memories and limited processing capability, researchers around the world are racing to develop more powerful, general-purpose quantum computers with large memories, long storage times, and improved processing capability.[3] However, expert predictions of when a practical quantum computer will be available differ drastically from "20 years"

 Published by the IEEE Computer Society

Table 1. Modern cryptosystems and their vulnerability to quantum algorithms.

Cryptosystem	Impact	Comment
RSA	Broken	Shor's algorithm describes an exponential speedup for solving classically difficult number theory problems, such as factoring large prime numbers and solving discrete logarithms.
Diffie-Hellman	Broken	
Elliptical curve	Broken	
Code-based	Not yet broken	These cryptosystems were introduced in the late 1970s, and their security has been well studied. They are not known to be vulnerable to quantum computing (QC) advancements.
Hash-based	Not yet broken	
Lattice-based	Not yet broken	These cryptosystems were introduced in the late 1990s and are believed to be secure against QC advancements.
Multivariate	Not yet broken	
One-time pad (OTP)	Proven unbreakable	Claude Shannon proved the OTP to have perfect secrecy, meaning it is not vulnerable to advancements in QC. Although immune to cryptanalysis, stringent keying requirements limit the OTP's implementation.

to "never."[1] Perhaps the potential of QC is best confirmed by recent purchases from forward-thinking enterprises such as NASA, Google, and the Los Alamos National Laboratory (see www.scientificamerican.com/article/google-nasa-snap-up-quantum-computer-dwave-two and www.dwavesys.com/press-releases/los-alamos-national-laboratory-orders-1000-qubit-d-wave-2x-quantum-computer).

In response to a growing number of advancements in QC, the US National Security Agency (NSA) recently announced a change to its cryptographic Suite B and specified "a transition to quantum-resistant algorithms."[4] This is primarily due to the fact that cryptographers cannot afford to wait and see what happens—sensitive information must be protected for long time periods. For example, the US Department of Defense typically protects sensitive information for a minimum of 25 years. Additionally, it can take many years to fully understand the security and suitability of new cryptosystems, as well as transition them in a thoughtful and cost-effective manner.

In this article, we first provide readily understandable descriptions of unfamiliar QC topics and then highlight practical tradeoffs in proposed post-quantum crypto solutions. More detailed discussions of these topics can be found in the references, particularly in Michael Nielsen and Isaac Chuang's seminal work on QC[5] and in ongoing research at the annual Post-Quantum Crypto Conference (see https://pqcrypto2016.jp/).

A Brief Introduction to Quantum Computing

Although there is no specific date or event, most would agree that the field of QC was born in the 1980s with seminal contributions from the likes of Richard Feynman, David Deutsch, and many others.[6] Over the past three decades, this work has continued through a number of research groups with the goal of understanding and overcoming the challenges associated with building a practical quantum computer.[7] Most notably, David DiVincenzo from the IBM T.J. Watson Research Center established requirements for building a quantum computer that have served the community well.[8] These requirements primarily pertain to a quantum computer's ability to effectively store, manipulate, and read (or measure) information with little or no error. For example, read-write tasks, which are generally considered trivial on a classical computer, are very difficult in the quantum regime, where it is particularly challenging to initialize a quantum system in a known state, perform operations on that state, and ensure that the surrounding environment does not inadvertently impact the system's result.

Currently, state-of-the-art QC experiments realize quantum computers as single-purpose quantum mechanical information processors.[3] These complex devices are designed to execute a single subroutine such as Shor's factoring algorithm or Grover's search algorithm, and require extensive classical computing integration to precisely control the quantum phenomena.[5] Additionally, it is important to note that specialized quantum algorithms must be developed to achieve the desired performance improvements available with quantum computers (see the Quantum Zoo for details, available at http://math.nist.gov/quantum/zoo/). For example, quantum Fourier transforms can be performed exponentially faster with QC than with today's

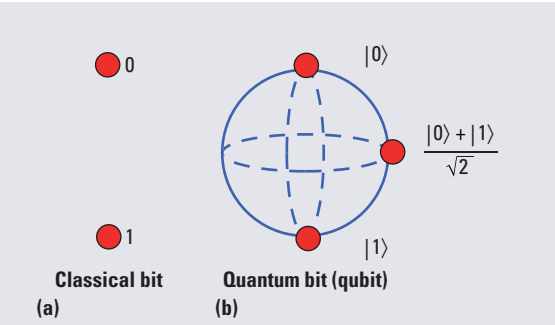

Figure 1. A comparison of (a) a deterministic classical bit and (b) a probabilistic quantum bit (qubit). The classical bit exists in either a 0 or 1 and can be easily read or copied. The qubit exists in a linear combination of states 0 and 1 and cannot be read (or measured) without collapsing its state. For example, the qubit $\alpha|0\rangle + \beta|1\rangle$ must collapse into the state $|0\rangle$ or $|1\rangle$ when measured. Thus, the state of the qubit cannot be perfectly copied without introducing errors.

most powerful supercomputers.[5] This is possible because QC enables multiple calculations to be performed simultaneously on a series of stored values—a behavior that is simply not possible in classical applications.

Figure 1 demonstrates the difference between a classically understood computer bit and a quantum bit (qubit). Classically controlled bits are deterministic—they exist in a known state of 0 or 1. However, qubits are probabilistic in nature, where a qubit's value is determined only after measurement by an observer. A quantum state can exist in a state of $|0\rangle$, $|1\rangle$, or a combination of $|0\rangle$ and $|1\rangle$ known as a "superposition," typically written as $|\psi\rangle$ $\alpha|0\rangle + \beta|1\rangle$. This superposition of states is uniquely quantum mechanical and underlies the power of quantum algorithms (see Table 2 for details).

Additionally, a qubit's state can be entangled with another qubit such that two qubits become directly correlated regardless of the distance between them. This "spooky action at a distance" is the basis of much excitement in both theoretical and experimental quantum information science research and is thought to have tremendous potential for QC to perform instantaneous, error-free quantum teleportation to reduce the effects of environmental noise.[5] Basic descriptions of these unfamiliar quantum mechanical phenomena are provided in Table 2.

Although the challenges of QC are great, a growing community of physicists, computer scientists, information theorists, and engineers are beginning to solve them. For example, quantum error correction codes have been developed to overcome significant QC limitations such as hardware imperfections and decoherence of quantum states to provide more robust solutions.[1] In response to these ongoing advancements, a shift toward post-quantum cryptography is occurring.

Post-Quantum Cryptography

Post-quantum cryptography is a growing research area with the goal of designing efficient cryptosystems that cannot be easily broken using current, proposed, or future QC capabilities (see https://pqcrypto2016.jp/). This includes both solutions that are proven secure (using information theory) and those that are thought to be secure (having demonstrated computational complexity). Of significant interest to the broader security community are encryption algorithms that have been proven secure—they are said to be future proof because they are not vulnerable to cryptanalysis regardless of computational power.

Figure 2 describes the field of post-quantum cryptography in two distinct areas: quantum-resistant algorithms and quantum cryptography (also known as quantum key distribution, or QKD). In general, quantum-resistant algorithms fit well into the existing IT infrastructure and are believed to be secure against advancements in QC. Alternatively, quantum cryptography considers solutions that exploit the laws of quantum mechanics to distribute (or grow) private shared secret keying material, which can be used with the one-time pad (OTP) encryption algorithm—the only known technique to achieve perfect secrecy.[9]

Quantum-Resistant Algorithms

The development of quantum-resistant algorithms is a maturing research area that explores secure alternatives to conventional public-key cryptosystems.[10] Of note, the US National Institute of Standards and Technology (NIST) recently started a post-quantum crypto project and held its first workshop in 2015 to discuss new public-key cryptography solutions (see http://csrc.nist.gov/groups/ST/postquantum-crypto/).

Assuming the proposed quantum-resistant algorithm is sufficiently secure against QC attacks, suitability is primarily assessed in three ways: required key length, private-key lifetime, and computational speed.[11] However, the most important

Table 2. Basic descriptions of quantum computing terminology.

Quantum phenomenon	Description
Qubit	The fundamental unit of quantum information. Typically described by two states labeled $\|0\rangle$ and $\|1\rangle$.
Superposition	A linear combination of quantum states typically written as $\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$, where the probability of observing state $\|0\rangle$ is $\|\alpha\|^2$, the probability of observing state $\|1\rangle$ is $\|\beta\|^2$, and $\|\alpha\|^2+\|\beta\|^2 = 1$. The quantum system $\|\psi\rangle$ is said to be written in the orthonormal basis $\{\|0\rangle, \|1\rangle\}$.
Entanglement	The quantum mechanical phenomenon in which the state of a combined system of qubits is known, but the state of the individual qubits cannot be known independently. This can give rise to paradoxical physical phenomenon. For example, if two qubits A and B are entangled, and qubit A is measured, then qubit B instantaneously collapses to a state determined by the properties of the combined system regardless of the distance between the individual qubits.
Measurement	Observation of a quantum state. Before measurement, the quantum system's state is not precisely known—it is in a superposition of states. The act of measurement forces the qubit to collapse to an Eigen vector of the measurement system (for example, horizontal or vertical).
Decoherence	Loss of information due to interaction with the environment (noise).
No-cloning theorem	States that it is not possible to perfectly copy an unknown quantum state (ambiguity between states is unavoidable). In contrast, it is easy to copy or recopy a classical bit as many times as necessary.
Multivariate	Not yet broken
One-time pad (OTP)	Proven unbreakable

consideration is, perhaps, how well the proposed solution fits into the existing IT infrastructure. Thus, proposed solutions are often directly compared to RSA's security and performance. For example, replacing a reusable 1,024-bit private key with a single-use 1-Mbit key directly impacts a device's memory, processing, and communication requirements. Moreover, it could potentially slow down the user's overall experience.

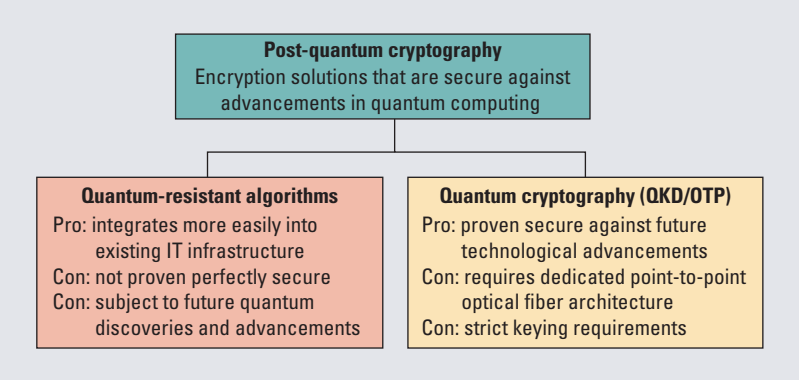

Figure 2. A depiction of cryptographic solution areas considered secure against advancements in quantum computing. The NSA has publically announced a transition toward quantum-resistant algorithms, while quantum key distribution (QKD) systems paired with one-time pad (OTP) encryption provide proven, future-proof solutions.

Although there are many types of public-key quantum-resistant algorithms being developed, promising candidates include error correction codes, lattice-based matrices, and hash-based digital signatures.[2,11] Other approaches of note include multivariate cryptosystems; however, successful implementations have been elusive thus far. Each solution uses unique mathematical structures to make them secure (or safe) against QC attacks. In general, these solutions depend on the computational complexity of NP-hard problems (problems that cannot be solved in polynomial time but may be checked in polynomial time).

Code-based (error correction). Code-based cryptosystems such as McEliece use error correction codes to generate public keys from private matrices with purposefully injected errors. Code-based schemes have appealing security features and are relatively fast because of the algorithm's low complexity in encryption/decryption.[2] However, the suitability of code-based cryptosystems is hindered by relatively large key sizes, with public keys requiring millions of bits.[11] Despite this shortcoming, McEliece with hidden Groppa codes was recently recommended by Europe's Post-Quantum Crypto Project because it "has been studied since 1978 and has withstood attacks very well."[12]

Lattice-based. Lattice-based encryption depends on the difficulty of solving complex mathematical problems, much like RSA. For example, given an n-dimensional vector space, finding the closest vector to an arbitrary point in the lattice is difficult.[10] In general, lattice-based schemes offer promising security and performance while fitting nicely within the existing IT infrastructure.[2] Among the various lattice-based variants being explored, NTRU schemes are generally thought to be the most practical because they have relatively small public- and private-key sizes (kilobits), are NP-hard computationally, and offer performance gains over conventional methods such as RSA.[11]

Hash-based. Introduced in the 1970s, the security and performance of hashing schemes such as those proposed by Ralph Merkle, Leslie Lamport, and Whitfield Diffie have been well studied.[11] In today's cryptographic infrastructure, digital signatures are commonly used for identification and authentication purposes such as verifying email correspondence. In general, these methods are relatively fast, and their security relies on the irreversibility of one-way functions, independent of number theory problems.[2] Unique to hash-based schemes, the one-way function's ability to avoid collisions (matching digital signatures) determines the minimum security requirement for the cryptosystem. For example, a secure scheme should not generate matching message hashes from user-defined input messages. Although very appealing, the overall suitability of hash-based cryptosystems is less than ideal because established schemes generally require single-use private keys or limit their reuse.[11]

Quantum Cryptography

Quantum cryptography exploits quantum mechanical properties to perform cryptographic tasks such as quantum commitment, oblivious transfer, secure multiparty computation, and QKD. As the most mature application of quantum cryptography, QKD has already been commercialized by several vendors. Utilizing the postulates of quantum mechanics, these systems provide the means for two geographically separated parties to grow unlimited amounts of secure symmetric keying material for use in OTP applications. In this way, QKD uniquely enables the only known future-proof post-quantum solution.

However, QKD systems have several technical limitations and barriers to acceptance. For example, to properly employ the OTP encryption technique, QKD systems must follow strict keying requirements to achieve the advertised level of data security. Specifically, the QKD-generated symmetric key must be as long as the message to be encrypted, can never be reused, and must be truly random.[9] Moreover, QKD is a point-to-point solution with relatively slow key-generation rates, and commercial offerings do not undergo formal security certification.[9] Despite these shortfalls, QKD has appeal as a post-quantum crypto solution for some high-security niche markets such as banking, government, and military.

Despite several difficult engineering challenges, recent advancements in QC are showing promise toward the viability of quantum computers. Although much work remains, these developments are already forcing a change to the existing cryptographic infrastructure. So what do these QC advances mean for IT professionals?

- The need to transition away from classical encryption methods is a balance between the user's security requirements and cost. Ultimately, the question to ask is, "How long does your data need to be secure?" If the answer is 30 years or more, you are already behind the power curve. However, if you have relatively short-lived security requirements, you can wait.
- As QC technologies continue to mature, expect to see an increasing emphasis on transitioning away from RSA public-key encryption because of its vulnerability to Shor's algorithm. Changes in security standards and policies are sure to follow.
- Researchers will continue to improve the security, efficiency, and suitability of post-quantum cryptosystems. Thus, in the not-too-distant future, practitioners will be responsible for installing, operating, and maintaining a new generation of crypto solutions.
- Although it is impossible to predict the future, most experts agree that a universal quantum computer will be built in the near future (perhaps by 2050[13]). However, this does not mean desktop computers will be replaced with quantum computers. More realistically, we can

expect to see highly specialized quantum computers only in top research centers.

Lastly, it is worth noting that IT professionals are needed to help transition QC research efforts out of the laboratory and into practical applications, by supporting advanced QC security configurations and designing new QC communication interfaces. QC has arrived, and we need to understand how this new technology impacts our profession. IT

Acknowledgments

This work was supported by the Laboratory for Telecommunication Sciences (grant number 5743400-304-6448). The views expressed in this article are those of the authors and do not reflect the official policy or position of the US Air Force, the Department of Defense, or the US government.

References

1. R. Van Meter and C. Horsman, "A Blueprint for Building a Quantum Computer," *Comm. ACM*, vol. 56, no. 10, 2013, pp. 84–93.
2. D.J. Bernstein, *Post-Quantum Cryptography*, Springer, 2009.
3. T. Monz et al., "Realization of a Scalable Shor Algorithm," *Science*, vol. 351, no. 6277, 2016, pp. 1068–1070.
4. "Cryptography Today," National Security Agency, 11 July2016;https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm.
5. M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2010.
6. M. Steffen et al., "Quantum Computing: An IBM Perspective," *IBM J. Research and Development*, vol. 55, no. 5, 2011, pp. 13:1–13:11.
7. T.D. Ladd et al., "Quantum Computers," *Nature*, vol. 464, no. 7285, 2010, pp. 45–53.
8. D.P. DiVincenzo, "The Physical Implementation of Quantum Computation," *Fortschritte der Physik*, vol. 48, nos. 9–11, 2000, pp. 771–783.
9. L.O. Mailloux et al., "Performance Evaluations of Quantum Key Distribution System Architectures," *IEEE Security & Privacy*, vol. 13, no. 1, 2015, pp. 30–40.
10. "Q&A with Post-Quantum Computing Cryptography Researcher Jintai Ding," *IEEE Spectrum*, 1 Nov. 2008; http://spectrum.ieee.org/computing/networks/qa-with-postquantum-computing-cryptography-researcher-jintai-ding.
11. R.A. Perlner and D.A. Cooper, "Quantum Resistant Public Key Cryptography: A Survey," *Proc. 8th Symp. Identity and Trust on the Internet*, 2009, pp. 85–93.
12. *Initial Recommendations of Long-Term Secure Post-Quantum Systems*, Commission of the European Communities, Horizon 2020 program, project no. 645622, 2015.
13. N.D. Mermin, *Quantum Computer Science: An Introduction*, Cambridge Univ. Press, 2007.

Logan O. Mailloux *is commissioned as a computer developmental engineer in the US Air Force and is an assistant professor of systems engineering at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio. His research interests include system security engineering, complex information communication and technology implementations, and quantum key distribution systems. Mailloux is a Certified Information Systems Security Professional and a Certified Systems Engineering Professional. He received a PhD in systems engineering from AFIT and is a member of Tau Beta Pi, Eta Kappa Nu, the International Council on Systems Engineering, ACM, and IEEE. Contact him at Logan.Mailloux@afit.edu.*

Charlton D. Lewis II *is commissioned as a physicist in the US Air Force and is an assistant professor of physics at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio. His research interests include atomic and molecular collisions, hypersonics and plasmas, counter-WMD technologies, first-principle high-power microwave effects on electronics, and astrostatistics. Lewis received a PhD in theoretical physics from AFIT. Contact him at charlton.lewis@me.com.*

Casey Riggs *is commissioned as a cyberspace operator in the US Air Force and is a fulltime master's student in systems engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include quantum algorithms, quantum cryptography, and cybersecurity. Riggs received a BS in aeronautical engineering from the US Air Force Academy. Contact him at Casey.Riggs@afit.edu.*

Michael R. Grimaila *is a professor of systems engineering, head of the Department of Systems Engineering and Management, and member of the Center for Cyberspace Research at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management and security, and systems engineering. Grimaila is a Certified Information Security Manager and Certified Information Systems Security Professional. He is a member of Tau Beta Pi, Eta Kappa Nu, and ACM; a senior member of IEEE; and a fellow of the Information Systems Security Association. Contact him at Michael.Grimaila@afit.edu.*