Internet of Things

Today’s Moderator:

Jason Sabin
Chief Security Officer, DigiCert, Inc.

To ask a question:
Type in your question in the Questions area of your screen.
#ISSAWebConf
Speaker Introduction

Today’s Speakers

**Mark Minnoch**
Technical Account Manager at SafeLogic

**Michele Mosca**
Co-founder and deputy director of the Institute for Quantum Computing at the University of Waterloo

**William Whyte**
Chief Technology Officer, OnBoard Security, Inc.
Speaker Introduction

Mark Minnoch

- Technical Account Manager at SafeLogic
- Has helped technology vendors complete hundreds of successful FIPS 140-2 validations
- Previous roles as FIPS Security Engineer, FIPS Laboratory Director, and Account Manager at the largest FIPS 140-2 testing lab in the world
- Collector of pinball machines
FIPS 140-2 Out of Date?

Mark J. Minnoch, CISSP CISA
SafeLogic Inc.
FIPS 140-2 Fun Facts

- FIPS = Federal Information Processing Standards
- FIPS 140-2 Publication released May 25, 2001
- The Cryptographic Module Validation Program (CMVP) is a joint effort between NIST and CSE
- CMVP validates cryptographic modules to FIPS 140-2 requirements
- FIPS 140-2 is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information

Bottom Line: If crypto is used to protect sensitive info, then it needs to be FIPS 140-2 validated
FIPS 140-2 Out of Date?

YES!

- “Sweet Sixteen” next month
- FIPS 140-3 (or -4) has no published schedule
- ISO 19790:2012 (proposed replacement) turning 5
- Long lead time for NIST to approve algorithms
- FIPS 140-2 validation ≠ Security
NO!

- Record year in 2016 for FIPS 140-2 Certs.
- 34% were software modules
- CMVP reviewing reports quickly
- ROI

Bottom Line: FIPS validations provide value to Vendors (sales) and End Customers (audits)
What Crypto Takes the Heat?

- Crypto is the tool, not the furniture
- Are only NIST Approved algorithms ”good tools”?
- Know your target
- Develop a post quantum strategy

Bottom Line: Different “tools” are required for a post quantum world
Post Quantum FIPS Options

- Follow the herd; do nothing
- Wait for NIST to approve algorithms
- Ask your Product Managers about their roadmap plans
- Ask your Technology Vendors about their roadmap plans
- Implement or seek a “Hybrid Approach”
  - Post quantum crypto and NIST approved crypto
  - Belt and suspenders

**Bottom Line:** FIPS 140-2 and post quantum crypto can coexist today
Mark J. Minnoch, CISSP, CISA
SafeLogic Inc.
mark@safelogic.com
https://www.linkedin.com/in/minnoch/
Dr. Michele Mosca

- Co-founder and deputy director of the Institute for Quantum Computing at the University of Waterloo.
- Founding member of the Perimeter Institute for Theoretical Physics
- Co-founded evolution Q Inc.
- Widely published author in top journals and textbooks
Preparing for the quantum era

Michele Mosca

evolutionQ Inc.

Institute for Quantum Computing, University of Waterloo
Perimeter Institute for Theoretical Physics
What is “quantum”??

Quantum Cryptography
Quantum Computer
Quantum Communication
Quantum Metrology
Quantum Information
...etc...
Quantum gravity
Quantum matter

Quantum framework for physics
New paradigm brings new possibilities

- Designing new materials, drugs, etc.
- Optimizing
- Sensing and measuring
- Secure communication
- What else???
Quantum Cryptography

- Quantum Random Number Generation (QRNG)
- Quantum Key Establishment (QKD)
- Other...

Beijing-Shanghai QKD Backbone
SwissQuantum Network
Tokyo QKD Network
Battelle QKD Network Columbus, Ohio, USA

http://www.idquantique.com/photon-counting/clavis3-qkd-platform/
http://www.uqcc.org/QKDNetwork/
http://www.battelle.org/our-work/national-security/cyber-innovations/quantum-key-distribution

Courtesy of Qiang Zhang, USTC

www.quintessencelabs.com
whitwoodsecurity.com

http://www.quantum-comm.com/index.php/Cate/index/pid/1
Quantum Computer

Full-fledged fault-tolerant quantum computer:
• Known to solve many problems previously thought to be intractable
• Simulating quantum systems (optimizing/designing materials, drugs, chemical processes, etc)
• Optimization (resource allocation, process design, etc.)
• Computational mathematics (including breaking current public-key cryptography)
• and more...

Non-fault-tolerant quantum devices:
• Not a known threat to cryptography
• Can they capture some of the power of quantum computation (and bypass some/all the cost of fault-tolerance)?
• Can they simulate themselves or similar systems faster/cheaper than conventional computers?
• Can they solve useful problems better than conventional devices?

©2017 M. Mosca
How secure will our current crypto algorithms be?

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key Length</th>
<th>Security level (Conventional Computer)</th>
<th>Security level (Quantum Computer)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>1024 bits</td>
<td>80 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>2048 bits</td>
<td>112 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>ECC-256</td>
<td>256 bits</td>
<td>128 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>ECC-384</td>
<td>384 bits</td>
<td>192 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>AES-128</td>
<td>128 bits</td>
<td>128 bits</td>
<td>~64 bits</td>
</tr>
<tr>
<td>AES-256</td>
<td>256 bits</td>
<td>256 bits</td>
<td>~128 bits</td>
</tr>
</tbody>
</table>

©2017 M. Mosca
What will be affected?

Products, services, business functions that rely on security products will either stop functioning or not provide the expected levels of security.

- Clouding computing
- Payment systems
- Internet
- IoT
- eHealth
- etc.

Secure Web Browsing - TLS/SSL
Auto-Updates – Digital Signatures
VPN - IPSec
Secure email - S/MIME
PKI

RSA, DSA, DH, ECDH, ECDSA, ...

AES, 3-DES, SHA, ...

©2017 M. Mosca
How large of a quantum computer is needed?

https://qsoft.iqc.uwaterloo.ca/
(Quantum Compiler tools, Quantum Computer Simulator – Quantum++, etc.)
How close are we to having sufficient quantum resources?

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret and R. J. Schoelkopf

Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stage, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored via error correction, for a time substantially longer than the decoherence time of its physical qubit components.
What is ‘z’?

Mosca:
[NIST April 2015, ISACA September 2015]:
“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”

Microsoft Research [October 2015]: Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade. ...Use of a quantum computer enables much larger and more accurate simulations than with any known classical algorithm, and will allow many open questions in quantum materials to be resolved once a small quantum computer with around one hundred logical qubits becomes available.
Quantum-safe cryptographic tool-chest

conventional quantum-safe cryptography + quantum cryptography

a.k.a. Quantum Resistant Algorithms (QRA) or Post-Quantum Cryptography

- Deployable without quantum technologies
- Believed/hoped to be secure against quantum computer attacks of the future
- Requires some quantum technologies (less than a large-scale quantum computer)
- Typically no computational assumptions and thus known to be cryptographically secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem

©2017 M. Mosca
Do we need to worry now?

Depends on:
• $X =$ security shelf-life
• $Y =$ migration time
• $Z =$ collapse time

“Theorem”: If $X + Y > Z$, then worry.

©2017 M. Mosca
Fact: If \( X+Y>Z \), then you will not be able to provide the required \( X \) years of security.

Fact: If \( Y>Z \) then cyber systems will collapse in \( Z \) years with no quick fix.

Prediction: In the next 6-24 months, organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan.
Quantum Risk Assessment

Phase 1- Identify and document assets, and their current cryptographic protection.

Phase 2- Research the state of emerging quantum technologies, and the timelines for availability of quantum computers.

Phase 3- Identify and document threat actors, and estimate their time to access quantum technology “z”.

Phase 4- Identify the lifetime of your assets “x”, and the time required to migrate the organizations technical infrastructure to a quantum-safe state “y”.

Phase 5- Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. \((x + y > z?)\)

Phase 6- Identify and prioritize the activities required to maintain awareness, and to migrate the organization’s technology to a quantum-safe state.

http://www.evolutionq.com/methodology-for-qra.html

©2017 M. Mosca
Testing new tools

openquantumsafe.org
Security is a choice

Problematic choices:

- “Do nothing: my vendors will take care of this for me”
- “Do nothing until NIST standardization is done”
- “Get it over with”
Historic opportunity
The choice is ours

Embrace quantum technologies that will help humanity and live in a safer cyber-enhanced world?

☑️ Yes
☐ No
Thank you!!
Comments, questions and feedback are very welcome.

michele.mosca@uwaterloo.ca
michele.mosca@evolutionQ.com

QUESTIONS?

Homework: Ask “what is (y)our quantum plan”?
Dr. William Whyte

- Chief Technology Officer at OnBoard Security, Inc.

- Previously served as Chief Scientist at Security Innovation and CTO for NTRU Cryptosystems and Senior Cryptographer with Baltimore Technologies in Dublin, Ireland

- Currently the chair of the IEEE 1363 Working Group for new standards in public key cryptography

- Holds a PHD from Oxford University on Statistical Mechanics of Neural Networks
Evolution to post-quantum cryptography

William Whyte, Onboard Security

2017-04-25
Comparing Post-Quantum Asymmetric Crypto Algorithms

- Additional data needed for post-quantum crypto algorithms
  - NTRU needs 600 additional bytes.
  - R-LWE needs 1100 bytes.
  - McEliece needs 1 Mbyte.

- NTRU: Lattice-based encryption algorithm, invented in 1996, standardized since 2008

- R-LWE is a new algorithm that has been around in various forms since 2005
  - Lattice-based cryptographic algorithm like NTRU
  - Attractive provable security properties but pays the price in lower performance and larger keys.

- McEliece is based on coding theory and has been around since 1978
  - Enormous key and very large minimum ciphertext size make it impractical for most applications.
  - Has been available for scrutiny for quite a while but it is not clear it has received quality scrutiny.
NTRU:

- \( \frac{g}{f} = 71 \mod 124 \)
- \( g \) and \( f \) are both “small”
- Find \( g \) and \( f \).

- Easy in one dimension
- But we can define “division” of multi-dimensional objects
  - Work in a “polynomial ring”
- As dimension goes into the hundreds, this problem becomes very hard to solve
NTRUEncrypt – Performance

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key Generation</th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTRU (439)</td>
<td>2588</td>
<td>128</td>
<td>204</td>
</tr>
<tr>
<td>rsa3072</td>
<td>1313224</td>
<td>9280</td>
<td>18382</td>
</tr>
<tr>
<td>curve25519</td>
<td>230</td>
<td>219</td>
<td>219</td>
</tr>
<tr>
<td>ecfp256q</td>
<td>92</td>
<td>301</td>
<td>301</td>
</tr>
<tr>
<td>nistp256</td>
<td>485</td>
<td>1672</td>
<td>1672</td>
</tr>
</tbody>
</table>

- Security level = 128
- Benchmarked on SUPERCOP: [http://bench.cryp.to/supercop.html](http://bench.cryp.to/supercop.html)
- Units: k cycles. 1 second = 2.7 × 10⁹ cycles with a 2.7 GHz CPU
- Security arguments and how to derive the parameters: [https://eprint.iacr.org/2015/708](https://eprint.iacr.org/2015/708)
Comparing Post-Quantum Signature Algorithms

- **pqNTRUsign-563** (128 bit strength)
  - 1056 bytes key and signature sizes.
  - Implementation exists. Ready for standardization.

- **BLISS signature** – a scheme instantiated over NTRU lattices
  - 630 bytes key and signature sizes.
  - Did not provide parameters for quantum security
  - Implementation from academia. Unclear about standardization process.

- **XMSS** – a stateful hash based signature scheme
  - Large signature size, 8400 bytes.
  - Undergoing standardization process.

- **SPHINCS** – a stateless hash based signature scheme
  - Large key size, 1000 bytes, and even large signature size, 41,000 bytes.
Getting there from here
Possible solutions

1. Define a quantum-safe ciphersuite
   - Solves the problem!
   - but...
     - No community consensus on a quantum-safe encryption algorithm
     - Not clear there’s appetite to roll out a whole new set of algorithms given that the ECC discussion is still going on
     - No good quantum-safe signatures

2. “Quantum-safe” existing ciphersuites
QSH = Classic handshake + QS-KEM

- Use a classic handshake (e.g. ECDH) to transport a premaster secret \( pms1 := Y^a | B^x \)
- Use a quantum-safe key encapsulation mechanism to transport another premaster secret \( pms2 := q \)
  - Plug-and-play for most existing quantum-safe encryption algorithms
- Derive the final master secret as \( ms := KDF(pms1 | pms2) \)
An over-simplified qsh-key exchange

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientHello:</td>
<td>HelloReply:</td>
</tr>
<tr>
<td><em>Do you speak ECDH or DH?</em></td>
<td><em>Yes I speak ECDH</em></td>
</tr>
<tr>
<td>ClientKeyShare:</td>
<td>ServerKeyShare:</td>
</tr>
<tr>
<td><em>Here is my public key A and my cert for A</em></td>
<td><em>Here is my public key B and my cert for B</em></td>
</tr>
<tr>
<td><em>Here is my key share X = g^x</em></td>
<td><em>Here is my key share Y = g^y</em></td>
</tr>
<tr>
<td>{Finished}</td>
<td>{Finished}</td>
</tr>
<tr>
<td>Session key = KDF(Y^a</td>
<td>B^x)</td>
</tr>
</tbody>
</table>
An over-simplified qsh-key exchange

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
</table>
| **ClientHello:**  
*Do you speak ECDH or DH?*  
*Do you also speak NTRU or R-LWE?*  
------> | **HelloReply:**  
*Yes I speak ECDH and NTRU*  
<------ |
| **ClientKeyShare:**  
*Here is my public key A and my cert for A*  
*Here is my key share X = g^x*  
*And here is my NTRU public key NPK*  
------> | **ServerKeyShare:**  
*Here is my public key B and my cert for B*  
*Here is my key share Y = g^y*  
*And NTRU cipher C = Enc_NPK(q)*  
<------  
*{Finished}* |
| *{Finished}*  
<------> | *Session key = KDF(Y^a | B^x | q | NPK)*  
<------> |
| *Session key = KDF(A^y | X^b | q | NPK)* |
QSH is secure

- At least does no harm
- pms1 is (classically) authenticated
- pms2 is quantum-safe
- $ms := \text{KDF}(pms1 \| pms2)$ is both authenticated and quantum-safe

- Defeat harvest-then-decrypt attack with low cost
- Inherit classical authentication
- Lack of quantum-safe authentication
  - Authenticity can wait, privacy can’t...
QSH incurs minimum cost

- Extra work: a public key generation, an encryption and a decryption
- More load on clients, less on servers
- Packet size increase is significant for all known quantum-safe algorithms though
Quantum-safe devices running in FIPS Approved mode

- NIST has stated that hybrid mode is Approvable.
- Other Info can be obtained using non-Approved security mechanisms; FIPS-approved devices, running in FIPS Approved Mode, can carry out QSH.
- Five years (?): NIST approves quantum-safe algorithms; FIPS-approved devices can be in FIPS mode while only running quantum-safe algorithms.
QSH summary

- QSH for TLS1.2 and TLS1.3

- Selecting QS crypto for QSH
  - [http://www.ietf.org/id/draft-whyte-select-pkc-qsh-00.txt](http://www.ietf.org/id/draft-whyte-select-pkc-qsh-00.txt)

- Working code with WolfSSL
  - [https://github.com/wolfSSL/wolfssl](https://github.com/wolfSSL/wolfssl)

- qstor code:
  - Requires a patch to fix cell size issue
  - [https://github.com/NTRUOpenSourceProject/ntru-tor](https://github.com/NTRUOpenSourceProject/ntru-tor)

- Security proof:
  - [https://eprint.iacr.org/2015/287.pdf](https://eprint.iacr.org/2015/287.pdf)
Building a Quantum Risk Mgmt. Plan

Deliver Phase 1 - Quantum Risk Management Plan as an RFP Response

Deliver Phase 2 - Quantum-Safe Solutions:
• Quantum-safe TLS to combat data vaulting threat
• Quantum-safe code signing
• Quantum-safe symmetric keys

Deliver Phase 3 – Complete Quantum-Safety
• Quantum-Safe Standardized PKI
• Quantum-Safe Authentication, Key Management, etc.

Probability of general purpose QC doing crypto breaking is very real after 2022 – it could occur sooner...

Template for a “Quantum Risk Management Plan” (QRMP)
Open Discussion & Q&A

• Jason Sabin - Moderator
• Mark Minnoch
• Michele Mosca
• William Whyte

To ask a question:
Type in your question in the Questions area of your screen.

You may need to click on the double arrows to open this function.

#ISSAWebConf
May - Breach Report Analysis

2-Hour Live Event: Tuesday, May 23rd, 2017
Start Time: 9:00 a.m. US-Pacific/ 12:00 noon US-Eastern/ 5:00 p.m. London

Overview:

Once again, the new data breach reports are published. Are we, as security professionals, succeeding in protecting our assets? This session will review the latest breach reports, provide insight into current trends, and evaluate potential solutions.
A recording of the conference and a link to the survey to get CPE credit for attending the April ISSA International Web Conference will soon be available at: https://www.issa.org/page/April2017 and check out previous web conferences at https://www.issa.org/?OnDemandWebConf

If you or your company are interested in becoming a sponsor for the monthly ISSA International Web Conferences, please visit: https://www.issa.org/?page=BecomeASponsor
Webinar attendees can join ISSA at a 15% discount by using the code **WEBCON42** during the checkout process.

The discount is available for all memberships except Students, and can also be used to renew your membership.