Discovery of Quantum Vulnerable Cryptography and Migration to Post-Quantum Cryptography

Dr. Vladimir Soukharev
Principal Cryptographic Technologist
and Chief Post-Quantum Researcher

InfoSec Global, Canada
Common Cryptographic Pitfalls

Lack of Crypto Visibility
Organizations do not know which cryptographic algorithms are used to protect critical information

Vulnerable Crypto Implementation
Organizations implementing their own specific cryptography with lack of skills

In-Secure Crypto and Key Usage
Incorrect usage of cryptography parameters due to lack of crypto knowledge

Outdated Crypto Algorithms
Previously safe algorithms becoming in-secure without knowing it

Quantum Computer Vulnerable Crypto
Long-life data protect by crypto scheme not ready for quantum computer era

Complex Crypto Update Process
Costs and efforts required to manually update cryptography across several systems and apps
## Diversity of Crypto Options

<table>
<thead>
<tr>
<th>Traditional Cryptography</th>
<th>Lightweight Cryptography</th>
<th>National Cryptography</th>
<th>Post-Quantum Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>CLEFIA</td>
<td>USA Suite A</td>
<td>Code-Based</td>
</tr>
<tr>
<td>ECC</td>
<td>PRESENT</td>
<td>GER ECGDSA</td>
<td>Hash-Based</td>
</tr>
<tr>
<td>AES</td>
<td>PHOTON</td>
<td>RU GOST</td>
<td>Isogeny-Based</td>
</tr>
<tr>
<td>Serpent</td>
<td>SPONGENT</td>
<td>KOR KCDSA</td>
<td>Lattice-Based</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>Multivariate-Based</td>
</tr>
</tbody>
</table>
Crypto Threat Management

Crypto Focused Assessment

- Check inventory of crypto
- Check crypto vulnerabilities
- Check compliance
- Check security profiles
- Define remediations actions

Server
Cloud
Storage
Devices
Applications
Network

Threat Database
Crypto Analytics
Cryptographic Risk Assessment

Inventory, assess and report
- Certificates
- Cryptographic Algorithms
- Cryptographic Protocols
- Cryptographic Libraries
Cryptographic agility is the ability of a system to easily adopt alternatives to the cryptographic primitives it was originally designed to use.
# Need for Cryptographic Agility

<table>
<thead>
<tr>
<th>Modern Cryptography</th>
<th>Platform Optimized Cryptography</th>
<th>FIPS Certified Crypto</th>
<th>Custom Crypto Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use modern, resilient and clean crypto implementation</td>
<td>Implement dedicated algorithms, counter measures or optimizations</td>
<td>Certify specific platform for use in government</td>
<td>Allow end-user to select crypto to use in their systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Post-Quantum Readiness</th>
<th>In Field Crypto Update</th>
<th>Sovereign Crypto Program</th>
<th>Future Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swap to post-quantum crypto standards as soon as available</td>
<td>Update crypto foundation of systems running in the field</td>
<td>Deploy National Crypto Program</td>
<td>Prepare systems for future standards</td>
</tr>
</tbody>
</table>
Agile Cryptography
Crypto Agile Architecture

Applications

Abstract Crypto API  Protocol API

Dynamic Linking Engine

Cryptographic providers | Application Independent

- Standard Crypto Provider
- FIPS Crypto Provider
- Post-Quantum Crypto Provider
- Plugin Architecture
Prepare for the Quantum Computer

1. Create a Crypto Inventory
   - Know your vulnerabilities

2. Move to a Crypto Agile System
   - Do the effort once
   - Use standard crypto for now

3. Move to NIST standards
   - NIST published its standards

4. Move to PQC
   - Use today’s PQC algorithms

5. Monitor Crypto Threats
   - Ready for future crypto challenges

---

Today: Quantum Computer Risk
Dr. Vladimir Soukharev
Principal Cryptographic Technologist
and Chief Post-Quantum Researcher

Vladimir.Soukharev@infosecglobal.com

InfoSec Global, Canada