Panel Discussion
PQC Considerations for DNSSEC

NIST Third PQC Standardization Conference

June 7-9, 2021

Panelists and Introductions

Moderator: Haya Shulman, Fraunhofer Institute for Secure Information Technology

Panelists:

- Jim Goodman, Crypto4a Technologies Inc.
- Russ Housley, Vigil Security LLC
- Burt Kaliski, Verisign
- Victoria Risk, Internet Systems Consortium
- Douglas Stebila, University of Waterloo
- Roland van Rijswijk-Deij, University of Twente and NLnet Labs

DNSSEC – A Critical Use Case for PQC Algorithms

Panel Goal: Exploration of DNSSEC-related considerations for PQC digital signature algorithm selection with intent to spur further consideration in concert with parties who define and implement DNS and DNSSEC-related standards

(1) DNSSEC is one of the use cases for PQC called out by NIST, but has been relatively less studied than others such as TLS

(2) Given the broad dependence on UDP for DNS exchanges, DNSSEC is not currently favorable to typical sizes of signatures and keys for PQC signature algorithms

(3) DNSSEC function as critical internet infrastructure and with long deployment cycles makes algorithm stability especially important

What is the practical impact of a quantum compromise of DNSSEC?

- Root key compromise
- To TLDs
- Relative to X.509 compromise
- Authentication looking forward versus non-repudiation or confidentiality looking back

What characteristics should DNSSEC have in a PQC world?

- Rollover considerations
- Key management considerations
- Signature size versus key size
- DNSSEC signing considerations
- Transport considerations
- Viability and stability considerations

What are the implications for PQC algorithm selection?

- Complexity of transition, implementation, and operation
- Impact on existing usage and operational models
- Ecosystem viability
- What are the preferred trade-offs?

How should we move forward to address the PQ challenge for DNSSEC (who, what, when, how)?

- Who will be at the table – NIST, IETF, IRTF, ICANN, ITU, resolver operators, registry operators, cryptographic library vendors, device manufacturers, open source community?
- What are the next steps?

Q&A

Appendix – Participant Biographies

Jim Goodman, Crypto4a Technologies Inc.

Jim is the Principal Security Architect at Crypto4A, overseeing all security-related aspects of the company's products, as well as investigating and assessing promising new technologies. He has more than 25 years of experience developing software, firmware, and hardware for a wide variety of security-related products, ranging from next generation gaming consoles, to high assurance HSMs. Jim holds a Ph.D. from the Massachusetts Institute of Technology (MIT), where his research focused on cryptographic algorithm design and implementation.

Russ Housley, Vigil Security LLC

Russ Housley is an expert in security protocols, system engineering and system security architectures, and he has authored many Internet standards. He has over 30 years of communications and computer security experience, and he is the Founder of Vigil Security, LLC. He served as Chair of the Internet Engineering Task Force (IETF) from 2007 to 2013, and as Chair of the Internet Architecture Board (IAB) from 2013 to 2015. He was an IETF Security Area Director from 2003 to 2007, and has also served in leadership positions of the Institute of Electrical and Electronics Engineers (IEEE), including the IEEE 802 Executive Committee in the early 1990s.

Burt Kaliski, Verisign

Dr. Burt Kaliski Jr., Senior Vice President and Chief Technology Officer (CTO), leads Verisign's long-term research program, an ongoing series of innovation initiatives that explore emerging technologies, assess their application to the company's business and recommend new strategies and solutions. He is also responsible for the company's industry standards engagements, university collaborations and technical community programs.

Prior to joining Verisign in 2011, Kaliski served as the founding director of the EMC Innovation Network, the global collaboration among EMC's research and advanced technology groups and its university partners. He joined EMC from RSA Security, where he served as Vice President of Research and Chief Scientist. Kaliski started his career at RSA in 1989, where, as the founding scientist of RSA Laboratories, his contributions included the development of the Public-Key Cryptography Standards (PKCS), now widely deployed in internet security.

Victoria Risk, Internet Systems Consortium

Victoria (Vicky) is the Product Manager for ISC's open source: BIND, Kea and ISC DHCP and Director of Marketing for ISC. Previously she served for 15 years as a Product Line Manager for CISCO with a focus on emerging technologies and integration of acquired product lines.

Haya Shulman, Fraunhofer Institute for Secure Information Technology SIT in Darnstadt

Dr. Haya Shulman is the Director of Cybersecurity Analytics and Defences department at the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt, and Scientific Leader of the Fraunhofer Project Center for Cybersecurity at the Hebrew University of Jerusalem in Israel. She is also the head of the Analytics Based Cybersecurity Mission in ATHENE German National Research Center and is a representative for Fraunhofer SIT in ATHENE Board. Dr Shulman established and is the leader of the Hessian-Israeli Partnership Accelerator program in Darmstadt and Jerusalem. Dr. Shulman obtained her PhD in Computer Science in 2014. Her research is focused on the applied aspects of cybersecurity, identifying weaknesses in networks and critical infrastructures and devising practical and effective countermeasures. Dr. Shulman received various awards for her work, including the German IT Sicherheitspreis and the IETF/IRTF Applied Networking Research Award.

Douglas Stebila, University of Waterloo

Douglas is an Associate Professor of Cryptography in the Department of Combinatorics & Optimization at the University of Waterloo in Waterloo, Ontario, Canada. His research focuses on improving the security of Internet cryptography protocols such as SSL/TLS, SSH, PKI and developing practical quantum-resistant cryptosystems. He is a co-founder of the Open Quantum Safe project. He is an author on a number of research publications on the topic of Internet security with a focus on cryptographic algorithms and protocols including post-quantum algorithms. He is a co-author on two IETF RFCs related to PKI for SSH. He is one of the inventors for the FrodoKEM key encapsulation mechanism which is a third-round alternate in the NIST PQC KEM algorithm selection process.

Roland van Rijswijk-Deij, University of Twente and NLnet Labs

Roland is a Professor of Computer Network Security in the Design and Analysis of Communication Systems (DACS) group at the Faculty of Electrical Engineering, Maths and Computer Science (EEMCS) at the University of Twente. He is also Principal Scientist at NLnet Labs, a not-for-profit foundation dedicated to research into and open-source software for the core protocols of the Internet. His network security research has focused on DNS and RPKI and he is an author on a number of publications related to the topic of DNS security. He is an active participant within the IETF with a focus on DNS privacy and DNSSEC and is a coauthor on an IETF draft for DNS privacy.