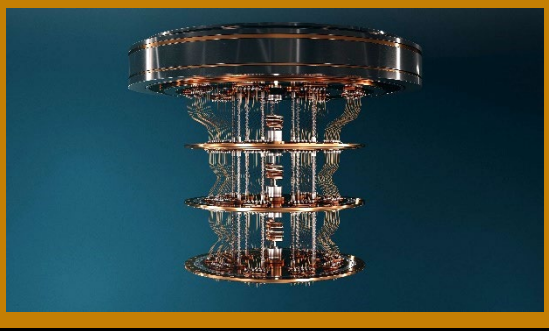
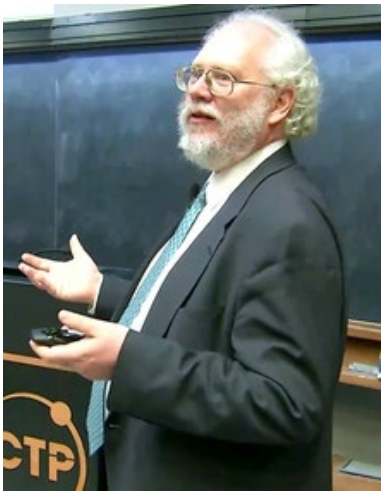
Does Quantum Computing Signal The End of Public-Key Encryption (i.e. The End of Cybersecurity; i.e. The End of the World)



In movie series from “The Matrix” to “The Terminator”, humans are (nearly) exterminated or enslaved by advanced computers with smarter-than-human artificial intelligence (AI). In the case of “Terminator 3: Rise of the Machines”, the villain was an AI-based virus that took over an advanced defense computer known as “Skynet”. While most experts agree that this kind of AI is a LONG way off, we know today that AI can be both helpful in identifying security issues and can be used in malware to beat classical security tools. But what about the “advanced computer” part of the equation?

Nearly all of today’s public-key cryptography systems are based on the idea that it would take years, or even centuries, to perform factorization the product of two large (enough) encryption keys. The highly popular Rivest-Shamir-Adleman (RSA) cryptosystem is an example of this approach. If one has the public key and both of the prime number utilized by the RSA algorithm, the private key can be generated (and hence the cleartext data). So far, the largest RSA key

that has been broken through factorization is an 829-bit RSA number (also known as RSA-250 for the number of decimal bits in the RSA number), which was broken on a very large distributed cluster in 2700 CPU-years. As computing power advanced, RSA stayed ahead of this decryption approach by increasing the size of RSA keys. Today, the National Institute of Standards and Technology recommends utilization of a key of at least 2048 bits (about 617 decimal digits).



Quantum computing, and American mathematician Peter Shor, changed all of this in 1994. In that year, Schor proposed a quantum computer algorithm, now known as "Shor's Algorithm", which solves the factorization problem exponentially faster than can be done on classical computers. This is because the number of parallel operations in a quantum computer that can be computed simultaneously increases exponentially with the number of qubits (quantum bits) in the system. In this way, a single quantum processor can do the work of hundreds, thousands, or even millions of classical processors.

Of course, this only works if one has a quantum computer, or more specifically a quantum computer with a "manageable" error rate. In quantum computers, the error rate (bits that "flip" state) is related to the quantum decoherence time and the number of qubits in the system – the greater the number of qubits, the higher the error rate. This implies both a limit on the size of the problems that can be solved and the time that is available to compute the problem before decoherence "skyrockets" the error rate, and the answer cannot be seen from the noise. Current estimates are that it would take a billionqubits quantum processor to break RSA in a roughly one day. Given that the biggest quantum processor today only has 52 qubits, we are probably a decade (or more) from the point where quantum computing is a real concern.

In the meantime, it is probably better to worry about insiders, human engineering, phishing attacks, and poorly engineered RSA keys, all of which are real issues today for nearly every organization. Like Terminator-style androids or cyborgs, many expected future developments take far longer than science fiction would lead us to believe.

Universities, governments, and a few large technology companies are building quantum computers. The engineering challenges in building a million qubit system today makes this an unlikely challenge to address before the next decade. Meantime, the conspiratorial threat is definitely worthy of conversation and movie themes.

13 Types of Endpoint Security
Not a Menu to Pick and Choose From -
Effective Endpoint Security Means Doing Them All

1) Internet of Things (IoT) Security – Reliance on a strong firewall for an organization's endpoint security is not enough, especially for companies that have most employees working remotely. Every device used by employees represents risk.
    - Install an EDR system to manage, monitor, and scan for vulnerabilities.
    - Remove outdated devices, install next gen solutions.
    - Monitor all app and device access.
    - Encrypt communications and segment your network to isolate problems.
2) Antivirus Solutions – A popular and well-recognized type of endpoint security, but limited against more advanced cyber threats. Unfortunately, many companies rely on this as their only security measure.
    - Includes anti-malware capabilities; can scan files for malicious threats against threat intelligence databases.
    - Enterprises can install directly onto endpoints to identify unknown signatures.
3) Endpoint Detection and Response - Continuously monitor all files and apps entering your enterprise endpoints.
    - EDR can offer granular visibility, threat investigations, and detection of fileless malware and ransomware.
    - Provides alerts for easy potential threat identification and remediation.
4) Forensic analysis- Works in conjunction with EDR by monitoring all endpoint activity.
    - Creates a digital footprint of all incidents.
    - All info surrounding an attack, including what happened, who is responsible, and the resulting consequences, is collected and analyzed to prevent future incidents.
5) URL Filtering – Restricts web traffic to trusted websites.
    - Prevents users from accessing malicious websites and websites with harmful content.

Provides organizations with control over what gets downloaded, where it gets downloaded, and who downloads it, to prevent surreptitious downloads.

6) Application Control – Controls applications permissions

Uses whitelisting, blacklisting, and gray-listing to prevent malicious applications from running and compromised applications from running in dangerous ways.

7) Network Access Control – Network access control overlaps with identity and access management.

Primary focus is on securing access to network nodes.

Limits user access to specific devices and access to network infrastructure.

Emphasizes firewalls and data limitations

8) Browser Isolation - Browsing sessions kept separate from valuable digital assets.

Destroys web browser codes after user finishes browsing.

9) Quarantine Protection – Separating dangerous files to prevent harm to devices and networks.

Allows valuable files to be cleaned rather than discarded. (CITE2)

Can isolate systems or databases that you believe carry a high level of risk.

10) Cloud Perimeter Security - form a protective perimeter around your cloud environments and databases. Cloud providers are not responsible for your enterprise cybersecurity.

11) Endpoint Encryption – Encrypts data stored on endpoints by coding and scrambling data to protect it even if captured in a breach.

Prevents issues such as data leaks (whether intentional or not) via data transfer by fully encrypting that data.

Functions like a virtual private network client (VPN) and is responsible for encrypting all web traffic that leaves your systems.

12) Secure Email Gateways - Secure email gateways monitor incoming and outgoing messages for suspicious behavior, preventing them from being delivered.

Hackers favors using email to deliver malware into your enterprise.

Emails can be sent according to IT infrastructure to prevent phishing attacks.

All email gateways should include virus and malware blocking, content filtering, and email archiving.

13) Sandboxing - A “sandbox” serves as an isolated and secure digital environment which replicates your typical end-user operating system.

Can contain potential threats for observation before allowing them into the network.

Can help contain zero-day threats and works well against zero-day attacks.

Frank Dimina

splunk>

"Embrace the chaos" to extract value from data. This might sound like a motto for 2020 generally, or even the coronavirus, but instead is the mantra or approach of Frank Dimina, Vice President for public sector at Splunk. Splunk is a software platform used in every branch of government, all 15 cabinet-level departments, 43 states, half of the largest 25 cities, and at 750 institutions of higher education. Dimina helps customers leverage data for intelligent decision-making.

COVID-19 brought chaos and a relentless deluge of data, testing agency continuity of operations from capacity and security to an exponential increase in the demand for digital services. One major takeaway – agencies gained a new perspective on software as a service:

"Cloud ensured they had no interruption of services. They didn't have to refactor their tools or processes just to complete their day-to-day work streams. They were also able to scale up as these increases in digital demands and users working from home required more capacity, these cloud-based approaches allowed them to increase scaling in just a few clicks. They didn't have to wait on hardware procurement or data center space. There is a lot more value potentially in the way we look at these cloud SaaS based offerings. Cloud benefits are not always about cost. It's about agility, redundancy, resiliency and scalability."

> *"Machine data to us is the digital exhaust that comes from any computing device, whether it's a computer, a server, a router, your mobile phone, your laptop, an application, or even a door sensor. All of that is generating information constantly, and our mission is to make machine data accessible, usable and valuable to everyone."*
> Frank Dimina, WashingtonExec.

Interestingly, in May 2019, Dimina was espousing this era of data chaos and the need to make critical decisions quickly. He employs a 4 step strategy to leverage mass data for critical decision making – 1) investigate, 2) monitor, 3) analyze, and 4) act. Optimize work by recognizing patterns and trends, automating repetitive tasks, leaving optimal brain capacity for higher-level strategic decisions and planning. 2020 brought the chaos and results.

16 Big Players in Cybersecurity Products and Services Globally

1) Splunk – Software platform relying on machine data analytics, used by every branch of government, all 15 cabinet-level departments, 43 states, many of the largest cities and 750 institutions of high education.

2) Cyren – Cloud security solutions for 1.3B users with automated early detection and remediation with major clients including Google, Microsoft, Dell, T-Mobile, and Intel.

3) Proofpoint – Cybersecurity platform that protects workers and data from threats targeting email, social media, and mobile devices used by over 27k companies.

4) NortonLifeLock – Cybersecurity software and services for nearly 50M consumers helps secure devices, identities, and online privacy.

5) Rapid7 – Provides cybersecurity analytics and automation and consulting services using an active, analytics-driven approach.

6) Radware – Cybersecurity and application delivery systems for physical, cloud, and software defined data centers for over 12k enterprise and carrier customers.

7) Mimecast – Comprehensive email security, service continuity, and archiving using cloud architecture for over 36k customers.

8) Crowdstrike – Software, agent-based sensor that can be installed on Windows, Mac, or Linux that relies on a cloud-hosted SaaS Solution, to manage and respond to threats.

9) Fortinet – Security fabric architecture, Fortinet ranks first in shipping security appliances worldwide and has over 450k customers.

10) Check Point Software Technologies - Multinational provider of software and combined hardware and software products for IT security, including network security, endpoint security, cloud security, mobile security, data security and security management.

11) CyberArk - Provides centralized audit records for all privileged access activities utilized primarily in the financial services, energy, retail, healthcare and government markets.

12) F5 - Specializes in application services and application delivery networking including the availability of computing, storage, and network resources.

13) Akamai - Global content delivery network, cybersecurity, and cloud service company, providing web and Internet security services.

14) Palo Alto Networks - Its core products are a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security.

15) FireEye - Provides hardware, software, and services to investigate cybersecurity attacks, protect against malicious software, and analyze IT security risks.

16) Zscaler - Provides Internet security, web security, firewalls, sandboxing, SSL inspection, antivirus, vulnerability management and granular control of user activity in cloud computing, mobile and Internet of things environments.

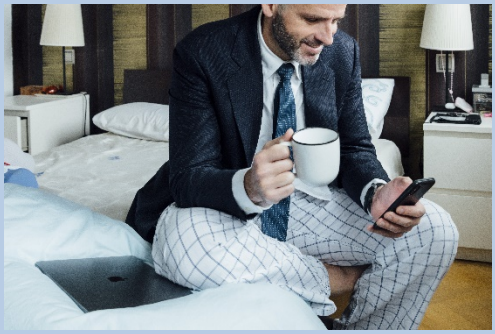
G2M Research Webinar, Tues, August 25 at 9am

Gen4 PCIe SSDs, SmartSSDs, and ESDFF –

Where Do SSDs Go Next?

KIOXIA

Upcoming 2020 Endpoint Security Events - All Virtual



SANS San Francisco, August 24-29

SANS Virginia Beach, August 24-29

Gartner Security & Risk Management Summit, September 14-17

Phoenix Virtual Cybersecurity Conference, September 17

GSX+, September 21-25

Virtual Cybersecurity & Fraud Summit: Toronto, September 22

G2M Research Webinars for the Rest of 2020

As our industry continues to be virtual, webinars can be a good way to stay up to date and get your message out. G2M has several webinars scheduled for this year on hot topics in our industry. Interested in attending our webinars? Register by clicking on the dates of interest. Interested in Sponsoring a webinar? Contact **G2M** for a prospectus.

Our July webinar "AI, Self-Driving Cars, and Advanced Storage" was sponsored by NVIDIA, Weka, and b-plus. View the recording and/or download a PDF of the slides here.

G2M RESEARCH

Aug 25*:*	**Advanced SSDs- PCIe Gen4, New Form Factors, and Smart SSDs**
Sept 15:	Edge Computing/Storage – Get (& Keep) Your Data Off Of My Cloud
Oct 20:	AI and Storage Use Cases in Healthcare
Nov 17:	NVMe-oF™ - Using Telemetry to Improve Network Latency

Check back for additional 2020 company-specific, conference, and other webinars (to be posted soon).

Let us know if there are any endpoint security and/or enterrise storage topics you would like to see covered this year or next.

Our first quarter 2021 webinar schedule will be released soon.