The Quantum Threat to PKI Infrastructure for Financial Services

Introduction

Dr. Alison Vincent,
Former Group Chief Information Security Officer at HSBC and Chief Technology Officer at Cisco

Cryptography doesn't have to be complicated. Unfortunately, the existing Public Key Infrastructure (PKI) used in our Financial Institutions has become very complex and in turn open to attack. The proliferation of edge devices, evolving standards and the growing quantum threat are highlighting an imperative to act now.

This paper highlights how financial institutions need to have an alternative to legacy PKI and a solution that is also secure against quantum attack in future. Symmetric key encryption is a great solution. It is already well understood, simple, 'secure by design', and incorporated into most networking software systems.

Read on to understand that simpler encryption is stronger encryption and Arqit has the solution.

The threats to existing infrastructure

Financial institutions were quick to seize on the opportunity of the communications boom enabled by the Internet. In doing so Public Key Infrastructure (PKI), the standard cryptographic security mechanisms for the Internet, were adopted at scale despite the Internet not being initially designed with security in mind. PKI was only adopted because it could be overlayed into an untrusted environment. Yet it comes with a great deal of complexity, creating a very large attack surface for cyber-security adversaries and huge headaches for financial institutions.

Recent years have seen a proliferation of attacks on financial systems reliant on PKI and the management burden is viewed as increasingly unscalable. And things are set to become worse as quantum technologies advance, including quantum computation, which will sound the death knell for current forms of PKI.

This oncoming crisis is causing people and organisations to rethink the security of the Internet. However, it also represents an opportunity to redesign security for the 21st Century Internet, replacing problematic PKI methods with stronger, simpler encryption.

Where are the risks today?

With such a dependency on outdated PKI, its flaws threaten the availability, integrity and confidentiality of our financial services and systems. For financial institutions, they face the possibility of fiscal loss, reputational damage among customers or wasted investment at best; at worst, organisational and possible systemic failure.

Financial institutions make use of public key cryptography across their IT and enterprise systems, for both the confidentiality and authentication of data in several ways. All of these protect information of significantly greater economic value than the typical Internet transaction. But where exactly are the risks?

SWIFT transaction services

SWIFT is the target of choice for adversaries who can bring Nation State-level resources to bear, with millions of dollars stolen through compromising access to SWIFTNet[1]. As users harden the remotely exploitable vulnerabilities, adversaries turn to PKI vulnerabilities; it's unclear how up to date SWIFTNet's encryption posture is. Case in point, their certificate page still recommends checking their root certificate and other signing certificates with the SHA1 hash function, which has been deprecated since 2011[2]. SWIFT systems are and will remain, high-profile targets for all threat actors operating with financial motivations. Regardless of the implementation of standard or advanced security controls, there is still a high risk these systems have flaws that will be identified, targeted and exploited by persistent threat actors. This is a consequence of the complex nature of the infrastructure deployed within financial institutions.

Payment Services

PKI is also used to secure payment services, such as the European Banking Internet Communications Standard (EBICS) that is used throughout the Single European Payment Area (SEPA). Data elements are sent using the Transport Layer Security Protocol and routed with PKI certificates. The European Payments Council has been lax in keeping up to date with advice on public keys. The 2021 version of their recommendations document still permits the use of 1024-bit keys where the National Institute of Standards and Technology (NIST) has been recommending a minimum of 2048-bit keys since 2015[3].

ATM

The exploitation of communication between ATMs and host processing allows not just the compromise of financial transactions, but the deployment of malware too. An example of this was demonstrated through The Scrooge and Dillinger rootkits, with Dillinger being deployed remotely from network traffic. As a result of this, it was recommended ATM services used both VPNs and TLS to harden this traffic[4].

However, known vulnerabilities to PKI can re-open this attack vector and ATMs owners are asked to regularly inspect this traffic for questionable PKI usage[5].

Internet banking

Internet banking, specifically mobile banking and payment apps has become the default choice for many banking customers. As of 2021, there are an estimated 169.3 million mobile banking users in the United States, of whom nearly 80% said that mobile banking was their preferred way to access their accounts[6]. And it's likely this number will continue to rise as we navigate our way through the pandemic, with more people preferring remote access to their bank as opposed to entering a physical branch. As of 2020, as many as 1.9 billion individuals worldwide actively used online banking services with that the number forecast to reach 2.5 billion by 2024[7].

However, banking apps are like any other app in that they are well-known for flaws. In 2017[8] a report from the University of Birmingham in 2017 highlighted issues with the application of PKI in apps from several banks. The vulnerabilities were fixed promptly but it demonstrates the complexity of securing mobile applications, especially those created by an applications team sitting outside of the central security team, or indeed outside of the organisation itself.

When new PKI vulnerabilities are exposed, the proof-of-concept of choice is to typically highlight how the vulnerability can be used to spoof an Internet banking website. However, these attacks are not limited to theory. In 2017 a Brazilian bank's[9] entire web presence was hijacked for six hours.

As more Internet traffic moves towards mobile applications, it's clear a new platform and a chance for fresh PKI implementation has not resulted in more secure transactions[10]. One study found that 77% of financial apps have at least one serious vulnerability that could lead to a data breach[11]. Cryptographic issues pose one of the most pervasive and serious threats, with 88% of analysed apps failing one or more cryptographic tests. Nearly half (49%) of the payment apps tested are vulnerable to encryption key extraction.

[1]SWIFTNet PKI Evolution | SWIFT - The global provider of secure financial messaging services
[2]Threat analysis (f-secure.com)
[3]EPC Document (europeanpaymentscouncil.eu)
[4]Check Point ATM Security Solution Brief and ATM Encryption (SSL/TLS) | CSF International (CSFi)
[5]Common SSL Attacks: SSL & TLS Key Vulnerability | Venafi p
[6]Insider Intelligence, March 2021
[7]Statista Research Department, Oct 19, 2021
[8]University of Birmingham
[9]An Unprecedented Heist Hijacked a Brazilian Bank's Entire Online Operation | WIRED
[10]SSL Vulnerabilities in Your Mobile Apps: What Could Possibly Go Wrong? (venafi.com)
[11]Most mobile finance apps vulnerable to data breaches (Helpnetsecurity.com, June 2021)

High-availability infrastructure

Financial institutions move vast quantities of sensitive transactional and market data around inside internal networks. The links between nodes within the bank's high availability infrastructure carry most of this data and represent the most valuable targets for cybercriminals. Protecting these links needs to be of highest concern to any financial institution, but often the methods used are outdated and the keys used to secure the data are refreshed only very rarely, often involving very manual processes.

Private and public cloud

Cloud adoption remains a sore point in many financial institutions: many see the advantages of the cloud but are locked out due to privacy and security concerns, particularly those stipulated by regulators. This has improved in recent years, particularly in private cloud (BCG say most banks now have "mature private cloud capabilities"[12] but public cloud adoption remains woefully low (EY say 80% of UK banks have migrated less than 10% of their business to public cloud[13]). Finding efficient and secure ways to give employees access to always-on, distributed, and collaborative cloud services should remain a high priority if institutions want to retain a competitive edge.

Why is PKI so prone to vulnerabilities?

Complexity is the enemy of security. And it's the complexity of highly mathematical PKI methods that have led to the bad security properties we see in financial systems today. This includes:

- An immature understanding of what constitutes a hard problem and how hard that problem is, leading to a need to constantly update parameters and keys sizes. Legacy parameters are all too easily revisited.
- Subtle mathematical structure leads to subtle ways systems can be made vulnerable.
- Emphasis on unmanaged transfer of trust leads to multiple abuses of trust.
- Complex mathematics leads to sprawling code bases. These are much harder to scrutinise and mean implementation errors are much more serious in security code than in other circumstances.

The fact is that simpler encryption is stronger encryption.

Why is the problem going to get worse?

The secure-access service edge

Distributed workforces, workloads, devices and burgeoning IoT environments means the network perimeter as we once knew it is gone for good. Now organisations are adopting new approaches to suit this paradigm. Gartner coined the term SASE (secure access service edge) to describe a new package of networking technologies with the ability to identity sensitive data or malware and the ability to decrypt content at line speed, with continuous monitoring of sessions for risk and trust levels.

As the trend of fluid network edges driving SASE becomes more widespread, it becomes harder to trust devices. PKI has been adopted for this use case, with digitally signed certificates from trusted authorities authenticating the user. This is far from the zero-trust approach organisations need: it outsources trust to a certificate authority and the user must decide what authorities to trust.

Device proliferation

The number of devices and connections in the corporate environment has increased rapidly and shows no sign of stopping any time soon. As mentioned in the point above, devices need to be authenticated and the sheer number of devices increase the risks faced by organisations using PKI.

With PKI, there's no need to know the sender/receiver in advance as public keys can be shared on demand. While this has been suitable for large networks of untrusted nodes like the internet, the burden to manage keys and certificates on corporate networks become ever greater. Misconfigured or expired certificates are a prime route for attackers to access systems, as seen in the 2017 Equifax breach[14].

[12]Financial Institutions Need to Pursue Their Own Path to the Cloud | BCG
[13]UK banking public cloud adoption: banks must think big to transform
[14]7 Data Breaches Caused by Human Error: Did Encryption Play a Role? | Venafi 2020

Evolving standards

In 2018, the Internet Engineering Task Force (IETF) updated TLS, one of the most important security protocols for the internet, to version 1.3. In IETF's words, it is a 'major revision designed for the modern Internet with major improvements in the areas of security, performance, and privacy'.

However, the update doesn't address some of the major issues with other versions. The first is the challenging nature of transitioning from an earlier standard. Three years after TLS 1.3 was launched, TLS 1.2 is still the most widely used version of the SSL/TLS protocol despite several high-profile vulnerabilities which exploited optional parts of the protocol and outdated algorithms. Second, certificate refresh timeframes are still too long. One certificate authority concedes in its best practice guide that "renewing certificates at least annually would be good"[15].

The quantum threat

Banking systems of record are the legacy bedrock for all other systems, which means they are a high value target for a quantum adversary and make all existing systems of data encryption redundant. And while predictions vary as to when quantum computers will enter mainstream usage, financial institutions must prepare now to ensure they're protected against the threat of quantum attack.
Two of the most widely used current cryptographic methods are RSA and Diffie-Hellman. RSA is typically used in identity certificates – cryptographically signed digital assets which prove the identity of an endpoint or device – although it's used widely in e-mail encryption. Diffie-Hellman is the most commonly used public key-exchange method, used in almost all encrypted web sessions to establish a shared key between the client and server.

Both methods rely on one-way or "trapdoor" mathematical functions: easy to compute in one direction, but hard to reverse. They are also examples of asymmetric cryptography, where one key is used to encrypt data (the public key) and another key is used to decrypt it (the private key), related by the trapdoor function. The encryption key can be made public because the trapdoor function makes it extremely difficult to compute the private key from the information revealed in the public key. However, quantum computers can efficiently reverse the trapdoor function for both RSA and Diffie-Hellman, turning it into a revolving door computable in both directions.

Information encrypted with either of these methods can be decrypted easily with a quantum computer. Usually, the data itself is not encrypted using asymmetric keys directly, rather this is used to transfer symmetric keys between the two parties, a process called key encapsulation. In symmetric encryption, methods like AES and ChaCha, both parties have the same key, and it employs functions that are, by design, easily computable in both directions.

These keys are known to be safe against quantum attack. But while the data itself is encrypted with a secure symmetric key, the data is still insecure because the key was encapsulated for exchange using an asymmetric method.

Quantum speed up

NIST, the US agency given the task of leading the global response to the threat, has urged all parties to begin work urgently to migrate to new protections. While the timetable of quantum computing attack is uncertain, what is certain is that PKI is already failing us and total network upgrade cycles take a long time.

However, we can start to put more data around the timing of quantum attack. Enormous advances in quantum computing have occurred and there is a vast investment being poured into the race for Universal quantum computing. Basic architecture, error correction and algorithm improvement have all resulted in a dramatic increase in the efficiency of quantum computing. Physical qubit numbers are not the only determinant of the schedule and with an increase in the ratio of logical to physical qubits, the timetable is accelerating. The vast resources and talent pouring into this area means the innovation will only intensify.

Looking at the rate of growth in physical qubits over the last few years, it's clear that the huge volume of investment is starting to result in impressive leaps in capability. Several companies (Google, Rigetti, IBM) already quote physical qubits of more than 100 qubits, and our analysis shows a rapid doubling of qubit numbers across the sector. IBM are themselves targeting an increase from around 100 qubits today to around 1000 by the end of 2023[16], which roughly means a doubling every 7–8 months. Honeywell is also on target to double their computing power every 6 months[17]. By that measure, it seems likely that quantum computers with qubit numbers on the order of 10,000 qubits will appear within the next 5–10 years. If PsiQuantum is able to meet its own aspirations, we could even see a 1-million-qubit machine by then[18]. The opinion that quantum computing will advance faster than the 2019 consensus suggests it is neither rare nor limited to marginal commentators. Sundar Pichai, CEO of Google, announced at the World Economic Forum in 2020 that quantum computing could end the usefulness of PKI encryption by 2025[19]. Research by the Global Risk Institute in 2020[20] surveyed 44 deep experts in quantum computing and the majority thought that there was a probability to break encryption before 2030.

[15]SSL/TLS Best Practices for 2021 | ssl.com, 2021
[16]New Scientist, November 2021
[17]The Quantum Daily
[18]PsiQuantum
[19]https://www.telegraph.co.uk/technology/2020/01/22/googles-sundar-pichai-quantum-computing-could-end-encryption/
[20]Quantum Threat Timeline Report 2020

Reducing the number of required qubits

Experts in this area know that it's not just about physical qubits, but logical qubits, which are the error-corrected collection of physical qubits that results in a single, robust, and usable quantum bit.

For example, Google's approach to quantum computing results in only 1 logical qubit for every 1000 physical qubits, but IBM's work[21] is leading them towards 1 in 100 or perhaps even 1 in 10 in the next few years, and the rate of improvement appears to be exponential. There are also emerging technologies to create physical qubits which are inherently robust to errors[22] and could lead to an order-of-magnitude reduction in the error rate in a single bound. The most exciting advances announced in recent months have been around error-correction. This drastically reduces the resources to run a quantum algorithm and crucially, this is rarely considered when assessing the qubit numbers required to break encryption. A recent article from Häner et al[23] showed that RSA-2048 could be broken with as few as 2,000 logical qubits, which would mean only 20,000 physical qubits with better error correction. This is compared with an estimated 20 million physical qubits from a paper published only last year[24] and this estimate itself had dropped from 1 billion in 2012 by tailoring the algorithm to the quantum hardware being used.

This rapid change demonstrates just how far we can reduce the numbers of qubits once error correction improves. There are also interesting advances in quantum memory. Whilst it's not a technology suitable for operations at distance, using entanglement-based quantum memories we can potentially network quantum computers together in the same location, generating rapid scale up in capability.

Innovation continuing at pace

Improvements in error correction and the implementation of Shor's algorithm means that the number of qubits will be reduced to perhaps only 20,000 within the same period. The number of physical qubits per machine are increasing at around 2x every six months, meaning we're likely to see a 10,000-qubit quantum computer between 2025–2030.

Taken together, these threads of research activity and volume of investment make it likely that we'll see a quantum computer able to break encryption within a decade, and perhaps in only five years.

It's only with this holistic view that we can start to form a realistic picture of when the threat will emerge. Given the possibility that it could happen within five years, there's no reason for enterprise or governments to delay migration to quantum-secure technology.

The imperative to act now

It took nearly two decades for us to deploy public key infrastructure. The April 2021 NIST cybersecurity whitepaper states "experience has shown that, in the best case, 5 to 15 or more years following the publication of cryptographic standards will elapse before a full implementation of those standards is completed"[25]. The replacement of algorithms generally requires changing or replacing cryptographic libraries, implementing validation tools, developing hardware that implements or accelerates algorithm performance, modifying dependent operating system and application code, changing communications devices and protocols, and user and administrative procedures. Security standards, procedures, and best practice documentation also needs to be changed or replaced, as do installation, configuration, and administration processes and documentation. And this work only begins once a candidate is chosen, which may take another 2–4 years.

Solving the quantum quandary

The limits of post-quantum algorithms

Post-quantum algorithms (PQA) are being touted as a solution to increase resistance to quantum attack.. PQAs are a set of mathematical algorithms and protocols using asymmetric keys. But while they offer the same advantages as existing asymmetric algorithms, with additional resistance against quantum attack, there are significant challenges with its use.

PQA is also not a drop-in replacement to today's cryptography. Not only does it introduce new attack vectors, but it brings significant disruption to upgrade to these new algorithms; potentially up to a decade[26] to implement at vast cost. Additionally, there are computational complexity challenges, particularly on endpoint devices as their 1400x complexity increase creates unmanageable latency.

[21]Science Magazine
[22]IEEE
[23]Häner et al
[24]Gidney & Ekera
[25]NIST
[26]Migration to Post Quantum Cryptography | NIST
[27]Status Update on the 3rd Round | NIST

Worryingly, PQAs that have failed within the NIST process have failed due to attacks that do not require quantum resources. There is a distinct lack of quantum analysis of these algorithms. Furthermore, these even more complex mathematical structures will lead to more vulnerable corner cases. Additionally, authentication processes using PQA are a particular challenge, with NIST likely to issue another call for signature algorithms after the process has changed[27].

Symmetric keys with quantum key distribution

Symmetric keys are already used by the financial services industry for the most important use cases because of their inherent security advantages. However, these keys are typically distributed manually to ensure against interception. Until now there has not been a secure way to deliver them at the scale needed for global enterprise.

Quantum key distribution (QKD) is a new way to create a pair of symmetric keys between two parties (traditionally called Alice and Bob). This is a fundamentally different approach to key sharing. Rather than hiding the symmetric key behind difficult mathematics as in PQA, the key is shared in the open using quantum bits. This means data is encoded into the quantum mechanical properties, like polarisation, of individual particles.

QKD has been proven over relatively short distances on fibre networks[28]. Arqit delivers symmetric key distribution on a hyper scale through software, fulfilled from the cloud, automatically creates keys in infinite volumes at minimal cost.

Embrace the 'secure by design' quantum opportunity

Transformation and change are nothing new to financial services institutions. Often considered 'leaders' in embracing technology change to deliver better business outcomes, the quantum threat should be considered a quantum opportunity. The rise of quantum computers will bring huge benefits to financial institutions and society in general, yet we must be prepared for all eventualities.

Quantum technology contains the promise of a cyber-security technique of its own, allowing secrets to be transmitted as quantum information that cannot be copied or interfered with by an adversary without alerting the sender. This allows the transmission of data securely through fibre optic cables or via satellites. Arqit has embraced this technology.

QuantumCloud™, our Platform-as-a-Service (PaaS) enables secure user authentication and encryption layers. Deployed through novel quantum secure cloud infrastructure globally in a scalable low-cost manner, it enables financial services institutions to adapt their infrastructure to be simpler and safer for a post-quantum world.

It is safe against attacks on PKI today and definitive against quantum attack tomorrow, and it is globally scalable, with a lightweight, low-cost agent. Additionally, it is incorporated within existing standardised AES256. There is no fundamental software re-architecture needed. And it enables innovation in areas like blockchain to now be viable for the long term.

QuantumCloud™ promises a simple upgrade path, automating all key handling and potentially replacing several other products too, making it easier to obtain IT budget.

Financial institutions now have an alternative to increasingly problematic legacy PKI. One that is also secure against quantum attack in future, but without the uncertainty and complexity of the unsatisfactory and unpredictable developments of PQA. Symmetric key encryption is already well understood, simple, 'secure by design', and incorporated into most networking software systems which greatly minimises the disruption of moving to QuantumCloud™.

To find out how Arqit can help your organisation, contact us at **contactus@arqit.uk**

[28]Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas | Nature, 2021

ARQIT

References

1. SWIFTNet PKI Evolution | SWIFT - The global provider of secure financial messaging services
2. Threat analysis (f-secure.com)
3. EPC Document (europeanpaymentscouncil.eu)
4. Check Point ATM Security Solution Brief and ATM Encryption (SSL/TLS) | CSF International (CSFi)
5. Common SSL Attacks: SSL & TLS Key Vulnerability | Venafi p
6. Insider Intelligence, March 2021
7. University of Birmingham
8. An Unprecedented Heist Hijacked a Brazilian Bank's Entire Online Operation | WIRED
9. SSL Vulnerabilities in Your Mobile Apps: What Could Possibly Go Wrong? (venafi.com)
10. Most mobile finance apps vulnerable to data breaches (Helpnetsecurity.com, June 2021)
11. Financial Institutions Need to Pursue Their Own Path to the Cloud | BCG
12. UK banking public cloud adoption: banks must think big to transform
13. 7 Data Breaches Caused by Human Error: Did Encryption Play a Role? | Venafi 2020
14. SSL/TLS Best Practices for 2021 | ssl.com, 2021
15. New Scientist, November 2021
16. The Quantum Daily
17. PsiQuantum
18. Science Magazine
19. IEEE Spectrum
20. Haner et al
21. Gidney & Ekera
22. Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms | NIST
23. P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," Society for Industrial & Applied Mathematics (SIAM), p. 1484–1509, 1997.
24. How Quantum Computers Break Encryption | Shor's Algorithm Explained
25. Quantum computers and the Bitcoin blockchain
26. Post-Quantum Cryptography, NIST March 2021
27. Migration to Post Quantum Cryptography | NIST
28. Status Update on the 3rd Round | NIST
29. Twin-field quantum key distribution over a 511km optical fibre linking two distant metropolitan areas | Nature, 2021