PKI in a Hyperconnected World

PKI in a Hyperconnected World
An overview

Public Key Infrastructure (PKI) is the most ubiquitous network security technology in use today. But industry professionals have been raising concerns over its safety for many years, with a number of high-profile disasters in the last decade highlighting the fragility of PKI. As our networks change and become more dynamic, with services moving into the cloud and enterprise embracing IoT, it is time to rethink one of the pillars of network security.

In this report we will look at PKI through a critical lens and explore some of the big issues that enterprise faces today. As cybercrime continues to rise and attacks at nation-state level are becoming more sophisticated and commonplace[1], this is more relevant than ever. The job of the CISO or IT Director needs to be focused on security outcomes, but too often time is wasted trying to manage unwieldy security infrastructure that was not designed for the job as it exists today.

We will also discuss an alternative to PKI: symmetric key infrastructure. Symmetric keys have many advantages over the public or private keys used in PKI. By combining them with a cloud-based service we are able to overcome many of the drawbacks of PKI in modern enterprise. This solution allows companies to implement security uniformly, safely, and at scale, without the burden of costly certificate and key management.

This technical paper is aimed at CISOs, IT Directors, and security leaders responsible for protecting data and networks, anticipating future threats, and implementing security policy.

[1] Bulletproof Annual Cybersecurity Report. (2021). Bulletproof. https://www.bulletproof.co.uk/industry-reports/2021-report.pdf

What is PKI?

When the building blocks of the Public Key Infrastructure (PKI) system were created in the 70s and matured through the 80s and 90s, it had all the attributes needed to flourish. We lived in a world where, although computers could communicate on the same network, there was no 'internet' to speak of. However, as appetite for this network grew on a global scale and the World Wide Web was born, the need for authentication and security became more pressing.

But the ability to scale services was difficult and internet bandwidth was expensive, so most processes were offline and asynchronous. In response to this, a decentralised and disconnected infrastructure was created within the design of PKI. It had a federated trust model that could work on a global scale where endpoints could share information in brief windows of connectivity, then do their identity validation offline.

Authenticity is provided using public certificates, signed by a trusted third party, which an owner can prove belongs only to them. It is due to this design that sites like Google can provide secure services to around four billion people, globally. So, for example, when a browser connects to google.com it needs to be sure that the site it is talking to is owned and operated by Google, and not a malicious third party. This is done by checking the site's certificate, a digital asset that proves that the site is authentic and belongs to Google. Of course, Google are not able to assert this for themselves, they need a trusted third party to issue their certificate and attest to its authenticity (in this case, Google's certificate is issued by GlobalSign). This authentication is used in communication protocols like TLS (Transport Layer Security) which encrypt the traffic between the browser and the website. It is now used in the vast majority of web traffic, with usage being over 90% on most platforms.[2]

Today, PKI is broadly concerned with three aspects of data security:

Confidentiality

Ensuring information is sent encrypted, so that it can only be read by the intended recipient.

Integrity

Confirmation that the information has not changed in transit.

Authenticity

Assurance that the device that is being connected to is legitimate and owners can prove who they are.

Beyond the public internet, PKI has been adopted into most enterprises as a way to manage authentication and encryption within their own networks. Companies become their own authority and issue certificates to devices rather than relying on a trusted third party. Although this is appealing because it brings control within the enterprise's domain, it also means inheriting many of the issues and drawbacks of PKI. In fact, a slew of high-profile security failures in the last decade can be directly attributed to the improper implementation or management of PKI in enterprise.

[2] Google. (2021). HTTPS encryption on the web. https://transparencyreport.google.com/https/overview

The problems with PKI

While PKI has enjoyed incredible success as a method for authenticating and managing encryption across the vast majority of the internet, it is not without criticism. In this section we will break down the most important problems that companies face with PKI today.

The management burden

As the use of PKI has proliferated through enterprises, key management has become a major issue. The management of certificates is becoming a multi-million-dollar cost for companies, with high profile outages from some of the biggest online companies such as Microsoft[3], Spotify[4] and Ericsson[5]. In a 2020 report[6] , 73% of respondents admitted that mismanaged digital identities had led to downtime in their organisation, with 55% saying they had experienced four or more outages in the last two years alone. Many of the reasons for these outages are as trivial as a forgotten certificate expiry or inadvertent revocation. The same report estimated that, on average, 16% of an IT department's budget is spent on PKI, amounting to $3m per year.

One problem stems from the fact that PKI is managed in a separate layer to the network and business systems that run above it. Software that often relies upon the correct setup of certificates to function, has no interaction or integration with that layer. This means that not only does it increase the cost and complexity of deploying the software, but when the certificates do not work – or with the case of revocation and expiry the certificates just stop working – there can be significant system downtime. Furthermore, it can be extremely hard to diagnose, especially in today's scalable architectures.

A second issue is a lack of proper understanding and expertise within the organisation. PKI needs to be adapted as networks become larger and more complicated, and many companies lack the specialisms required to create and properly implement a PKI strategy.

In response, an entire key management industry has sprung up around these problems, with companies that exist solely to support other companies with their PKI burden. Some are even emerging as holistic key-management-as-a-service solutions. This certainly helps customers offload their management burden, but as networks become more complex and the management burden grows, this naturally leads to additional cost and fails to solve the underlying issues when things go wrong.

16% of an IT department's budget is spent on PKI, amounting to $3m per year.

Security

As use of PKI has proliferated it has become increasingly maligned by the cryptographic community[7,8], partly down to the number of high-profile (and extremely damaging) security breaches that have occurred over the last decade.

[3] Warren, T. (2020). Microsoft Teams goes down after Microsoft forgot to renew a certificate. The Verge. https://www.theverge.com/2020/2/3/21120248/microsoft-teams-down-outage-certificate-issue-status

[4] Shorter, T. (2020). Lessons Learned: Spotify Certificate Outage. Security Boulevard. https://securityboulevard.com/2020/08/lessons-learned-spotify-certificate-outage-keyfactor/

[5] Porter, J. (2018). Millions of smartphones were taken offline by an expired certificate. The Verge. https://www.theverge.com/2018/12/7/18130323/ericsson-software-certificate-o2-softbank-uk-japan-smartphone-4g-network-outage

[6] The Impact of Unsecured Digital Identities. (2020). The Ponemon Institute.

[7] Serrano, N., Hadan, H. and Camp, L. J. (2019). A Complete Study of P.K.I. (PKI's Known Incidents). TPRC47: The 47th Research Conference on Communication, Information and Internet Policy 2019. http://dx.doi.org/10.2139/ssrn.3425554

[8] Grimm, J. (2016). PKI: crumbling under the pressure. Network Security, 2016(5), 5–7. https://doi.org/10.1016/S1353-4858(16)30046-0

Heartbleed - disclosed in 2014. This software bug in the OpenSSL code (the most commonly used PKI code in websites), was perhaps the most famous TLS vulnerability. Malicious users could cause a buffer overread making the targeted computer provide data from parts of its memory which the attacker should not have been allowed to access. Overreads in other code are usually exploited in combination with other vulnerabilities, but in the case of Heartbleed just the overread alone meant that valuable data could be revealed including passwords, cookies, and even private keys. If these keys are disclosed, all connections to the website can be easily read by an attacker.

Curveball - disclosed in 2020. Disclosed by NSA researchers in 2020, the CurveBall vulnerability follows from incomplete validation of the full set of parameters necessary for the elliptic curve digital signature algorithm. Websites could be certified using a standardised curve, with a securely generated and handled private key. Yet by modifying a single parameter, an attacker could masquerade as that website to anyone accessing Windows 10 and either Microsoft Edge or Google Chrome. The vulnerability also allowed man-in-the-middle attacks and fake signatures for executable code.

Flame - disclosed in 2012. The disclosed in 2012. The FLAME malware family was detected in 2012, running on arounda thousand computers using Microsoft Windows across the Middle East. The malicious code was signed with a PKI certificate making it appear to have originated from Microsoft. This had been achieved via a cryptographic attack on the MD5 message digest (hash) function. Two certificates with the same MD5 fingerprint were produced using techniques dating from 2008: one certificate was benign, but the other could act as a delegated signing authority for Microsoft. An automated Licensing Service was used to sign the benign certificate and the signature was transferred to the malicious certificate.

None of these issues were with PKI in a theoretical sense, rather they were caused by mistakes in the implementation. However, these are inevitable since the surface area of PKI is large, with many different implementations available, different actors involved, and many different elements to PKI itself. This surface area will only continue to grow as networks become larger and more complex.

Trust

Trust is a central issue in security. Ideally, an organisation should not trust external people or technology. This is not only to protect it from those who might intentionally try to harm it, but also isolate it from other companies' mistakes.

To communicate with an external network there must be an element of trust that the system being communicated with is authentic. There's no scalable way to do that across an anonymous public network like the internet without trusting someone else to certify who everyone is. In PKI this is done by certificate authorities (CAs), organisations which certify the identity of endpoints on the network. When using PKI, trust is placed in the CA that it has gone to the correct lengths to identify the owner of the endpoint.

This reliance on external or even internal sources of trust both erodes security and increases management burden. It also creates single points of failure that can have devastating consequences for businesses should they become compromised.

Evolving network architecture

As enterprises evolve, so do their networks. In the cloud era, companies want to take more advantage of cloud-based services like Office 365 and Salesforce to run business operations. These always on, globally accessible, and full-service solutions have increased productivity for companies and reduced the overhead of managing on-premises hardware.

In addition, the number of devices that companies have to manage is increasing. Servers and workstations are now dwarfed by the numbers of laptops, tablets, and company phones that organisations need to keep secure. This job is made more difficult as more devices are used outside of the traditional local area networks (LAN), either at home or on the move.

The job of managing and securing the entire wide area network (WAN) is becoming more difficult as it grows. An emerging model, first recognised by Gartner, is the Secure Access Service Edge (SASE). This describes a dynamic network architecture where devices such as routers, switches, and laptops (and even services like public cloud) all sit at the edge of the corporate domain. Ensuring security across these different devices and services means integrating technologies for the differing communication channels, whether that be through internal network infrastructure, private tunnels like VPN, or via the internet. This is something that PKI is not designed to accommodate.

The quantum threat

As the name implies, PKI relies on the use of public keys. These keys have a private counterpart, and if information is encrypted with the public key, then only the private key is able to decrypt it. This property is what allows us to be sure that a certificate actually belongs to someone because if we encrypt something with a public key, only the owner of the certificate (and the private key) is able to decrypt it.

This asymmetry is possible because of a special type of mathematical function, sometimes called a one-way function, which is easy to compute in one direction but very hard to reverse. Take multiplication: it is easy to take two numbers and multiply them together, but much more difficult to take the output and work out which two numbers were initially multiplied together. This is called the "factorisation problem" and its difficulty underpins RSA, one of the most ubiquitous technologies used in PKI.

All public key cryptography used commercially today relies on the difficulty of reversing one-way functions, but there is a new technology on the horizon which is able to reverse these functions much more easily – a quantum computer. By taking advantage of quantum phenomena that emerges at very low temperatures and distances (e.g. the size of an atom) a quantum computer can efficiently solve problems that a traditional computer can not. This speedup can be dramatic:
a calculation that might take a traditional computer several millennia to solve, can be computed in days or even hours on a quantum computer.

Efforts are currently underway in many countries to produce a quantum computer, both in research institutes and in companies like Google[9]. Once these devices are able to reach a certain scale, the impact to PKI will be devastating and will render all public key cryptography vulnerable to attack.

Predictions vary on how long it might take to reach the "cryptopocalypse" as some have dubbed it, but many sources believe it might be within the next ten years[10]. This might seem far enough away not to worry about but given the speed of adoption of technology in this industry, we need to begin our transition away from public key cryptography today if we want to safeguard our information now, and into the future. There is already evidence that malicious actors are currently harvesting data with the intent of decrypting it later once the encryption can be broken.

[9] Arute, F., Arya, K., Babbush, R. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510. https://doi.org/10.1038/s41586-019-1666-5

[10] Mosca, M. (2016). A quantum of prevention for our cybersecurity. Global Risk Institute. https://globalriskinstitute.org/download/a-quantum-of-prevention-for-our-cybersecurity-1-pdf/

Symmetric key infrastructure

Is there an alternative to PKI? Considering the problems we have discussed, a good solution would include the following:

- A SaaS-based platform where encryption and identity management are delivered as a service, removing the burden for customers and reducing the possibility of implementation errors.
- An ability to rotate security keys more often, removing the issue of long-lived certificates that can remain valid for months or even years.
- A trust-free architecture where the final security keys are only known to the communicating parties, not to a central authority.
- A pay-as-you-go service where companies only pay for the keys and services that they use.
- Security against the quantum threat.

Arqit delivers this solution with QuantumCloud™, a SaaS platform that enables connected devices to negotiate secure, quantum-safe connections using symmetric keys (such as standard AES-256).

Key management and device authentication is managed in the cloud using a web interface, allowing system administrators to focus on security outcomes rather than key and certificate management. The final security keys are never known by QuantumCloud™, because of the use of novel key exchange algorithms. Symmetric keys are also robust against the quantum threat, generated in the moment from high-quality quantum, random sources and agreed between end points using Arqit's lightweight software agent, ensuring the highest levels of security. Since QuantumCloud™ is a SaaS platform over traditional TCP/IP there is no requirement for specialist infrastructure, meaning it scales easily over existing networks.

	QuantumCloud™	PKI
Trust-free architecture	✓	✗
Cloud-based policy management	✓	Available from some vendors
Secure against quantum attack	✓	✗
Easy to scale	✓	✗
Supports both point-to-point and group keys	✓	✗
Scope	Private & public networks	Public & private networks

Conclusion

PKI has been the solution for network security for decades, but its time is coming to an end. The need for the world to adopt a more dynamic network model, together with the technical shortcomings of PKI, means security professionals need to look beyond PKI and explore other solutions.

QuantumCloud™ is a drop-in alternative for network security that addresses the shortcomings of PKI, and delivers a host of new benefits to customers today, as well as protection against the quantum attack of the next few years. Our cloud-based symmetric key platform is easy to scale and allows customers to concentrate on security outcomes, instead of managing certificates and storing keys. It applies to all and any connected devices in the world, with equal simplicity, efficiency and security.

Get in touch today to find out more.