Phenzi Blasio & Bella Meyer

INFO-I 430

Final Paper- PKI

04 December 2024

Introduction:

This paper aims to report the many possible failures that Public Key Infrastructure (PKI) run into when issuing digital certificates. The first section serves as an overview of the project and the definitions of what PKI, certificate authority or other language used within this report mean. The first page also contains a general guide as to how the paper is structured by page. The second section discusses why this topic was chosen and how we conducted our research when learning about the topic, it also talks about the many different types of failures we encountered, and the causes for those failures, noting the most common ones we found during the conduction of the study. The third section talks about what methods could be taken in order to possibly prevent further issues from occurring, suggestions based on the data we collected and a discussion of what is currently being done. Section 4 reports the conclusion of our study, which ends in a bibliography.

Section 1:

Public Key Infrastructure (PKI) serves as a crucial framework for data encryption. It helps facilitate secure communication over networks. PKI operates through the distribution and management of cryptographic keys within organizations. They are typically overseen by a designated authority known as a Certificate Authority (CA). The problem is that CAs are the

gatekeepers of the internet. They are entities that store, sign, and issue digital certificates. Within PKI, these CAs enable trust between entities throughout the internet, and associated web services, to validate the creation of categorical roles of certificates and identities. There is a standard set of Baseline Requirements that must be met in order to ensure that the application is satisfactory, and that its technological practices are in compliance with the validity of certificates.. We wanted to extend our research further by writing this paper, presenting a project and continuing to gather data over the past few months.Through our investigation, we aim to shed light on these critical inquiries in the realm of PKI. By understanding the factors behind PKI failures, the ongoing tasks vital for certificate validity, and the methods for identifying breach origins on Certificate Authorities, we aspire to contribute valuable insights to bolster the security and resilience of PKI systems for future endeavors.

Section 2:

Our research explores the organizational level of public key infrastructure, specifically focusing on instances where failures arise due to systematic vulnerabilities. These vulnerabilities are not solely rooted in technological shortcomings but often stem from dissonance between business practices, human error being a primary suspect. To investigate this issue, we analyzed Bugzilla Reports from numerous companies using qualitative coding as the primary data analysis method. While we are still in the process of collecting and analyzing data, our findings are expected to offer valuable insights and guidance for organizations to strengthen their cybersecurity measures in the future. The process of qualitative coding we followed was two hours of training to extract the root cause of the reports, then record them in Excel. A list of reports from the year 2021 to the present day was presented to the team each

week to analyze independently. Each Friday, researchers would collaborate for an hour to review each of the reports. Each of the three coders classified the root causes into one of the categories below. The root causes stem from approximately 32 total issues of each Certificate Authorities. The main issues we encountered during the research included: fields in certificates not compliant to BR, Non-BR-Compliant or problematics OSCP responder or CRL, CAA mis-issuance, Possible Issuance of Rouge Certificates, and Other unique cases. We utilized Bugzilla a forum dedicated to tracking PKI security failures across companies. Identified 2021-2022 as years with variant data points that enable an inclusive representation of 100+ certificate events. Every certificate had the root CA and SubCA listed (some CAs are upheld by a different all encompassing or “larger” CA), the issue itself (including but not limited to: BR noncompliance, usage of SHA-1 / MD-5 Hashing, 512/10124 bit keys, miss issuance, audit report failure disclosure), consequences of the failure, the number of certificates affected and the boolean value of whether the report was self reported or not.

Our research has shown that the majority of PKI misconfiguration is due to human error, not faulty software or other internal issues. More than 50% of the issues recorded in the 2021-2022 certificates had at least one error pertaining to the baseline requirements,which in turn leads to malfunctioning on the user’s end. The second leading cause is believed compliance, which in many cases could be an extension of human error. Other major issues that cause PKI failures include weak cryptography practices, especially rogue certificates as well as ineffective warnings, Erroneous/Misleading/Late/Lacking Audit reports, Repeated/Lacking appropriate entropy Serial Numbers, Undisclosed or incorrectly disclosed SubCA, Debian OpenSSL vulnerability, CA/RA/SubCA/Reseller hacked, delayed certificate revocation, self revocation, backdating SHA-1 certificates, certificates for malicious domains charging for compromised certificate revocation, CPS non-compliance, Digital certificate for non-existent domain/bad information of requester, MITM attempt, no BR self-assessment, no

disclosing another CA purchase, no test website for CA, non-acceptable requester validation, not allowed ECC usage, registering competitor trademark, timestamp certificate from root, un-revoking certificates, and certificate lifetime >825 days, false positive/incorrect report, failure to provide a preliminary report within 24 hours, not allowed Hash Function, Inquiry of Explanation, and Insufficient Validation Evidence. In the event that none of these encompass the issue, we left a choice of 'other' to self report or describe. Some PKI failures were only reported to note an audit report, even if there were no failures.

Human error was a driving force behind most failures, but it is not the only cause of such incidents. Multiple causes were identified throughout our research. Most notably software bugs, believed to be compliant/Misinterpretation/Unaware, business model/CA decision/Testing, operational error, non-optimal request check, improper security controls, change in baseline requirements, organizational constraints, and misconfigured software.

Section 3:

Public Key Infrastructure (PKI) failures can have serious implications for security and can disrupt various services relying on cryptographic authentication and encryption. Currently our methods of dealing with PKI failures involve monitoring, incident response, root cause analysis, audit checks, keeping systems up to date, backing up systems for recovery in the event of a severe failure, as well as education. Organizations implement continuous monitoring of their PKI components, including certificate authorities (CAs), registration authorities, and validation services. Monitoring tools can detect anomalies such as unexpected certificate issuance, expiry, or revocation, which might indicate a failure or breach. Once a PKI failure is detected, a predefined incident response plan is activated. This plan typically includes steps to contain the failure, assess the damage, and mitigate any security risks. For instance, if a certificate is compromised, it must be quickly revoked and replaced. Communication protocols are also

important to inform affected stakeholders about the issue and how it's being addressed. After addressing the immediate impacts, a thorough investigation is conducted to determine the root cause of the failure. This analysis helps in understanding whether the failure was due to a technical flaw, operational error, security breach, or other reasons. Regular audits are performed to ensure that the PKI setup adheres to best practices and compliance requirements. Audits can help identify potential vulnerabilities or operational inefficiencies that could lead to failures, but not all of them identify problems within the PKI structure, which is why our research noted audit reports, even in the absence of PKI failure. Based on the findings from incident responses and audits, policies and procedures may be updated to strengthen the PKI environment. This might involve enhancing security protocols, updating software and hardware, or training employees on new processes. Effective backup and recovery strategies are essential to quickly restore PKI operations after a failure. Regular backups of critical PKI components and data ensure that the system can be restored to an operational state with minimal data loss. Ongoing education and training programs for IT and security teams help in recognizing and preventing PKI failures. Awareness about PKI management, security practices, and recent threats can significantly reduce the risk of failures. Implementing redundant systems and ensuring high availability of PKI services can help prevent service disruptions. This includes deploying multiple instances of critical components like CAs across different physical locations. By combining these strategies, organizations can effectively manage and mitigate the impact of PKI failures, maintaining the integrity and reliability of their cryptographic security measures.

The following are a few suggestions that we have come up with based on current tactics as well as our research. The first solution is Root cause analysis, which is conducting a thorough investigation to identify the root cause of the PKI failure. This can involve examining configuration errors, software bugs, or malicious activities. Another method is backup and redundancy; by implementing backup and redundancy measures, critical components of the PKI

infrastructure, including certificate authorities (CAs), key stores, and cryptographic keys ensures continuity of operations in case of failures. Performing regular audits and monitoring of the PKI infrastructure to detect any anomalies or deviations from expected behavior, as well as the implementation of failover mechanisms to automatically switch to backup systems or redundant components in case of PKI failures. It is also integral to keep the PKI software and components up-to-date with the latest patches and security updates to mitigate vulnerabilities that could lead to failures or exploits. In the event of disaster, it is important to develop and maintain a comprehensive disaster recovery plan that outlines procedures for restoring PKI services in the event of catastrophic failures. It is important to test the plan regularly to ensure effectiveness. Providing training to personnel responsible for managing and maintaining the PKI infrastructure to ensure they are knowledgeable about best practices, security protocols, and troubleshooting techniques. If none of these methods work, it may be best to explore alternative encryption mechanisms or cryptographic protocols that can provide security even in the absence of a functioning PKI infrastructure.

In conducting this study we have identified leading causes of PKI failures. The foundational role of PKI is to ensure that secure communication occurs between networks by the distribution and management of the cryptographic keys. Cryptographic keys are predetermined by mathematical algorithms that decide how a public phrase or code can be hidden in a predictable and reversible way. The central conduit for PKI lies with certificate authorities that validate the creation of digital certificates, enabling trust between entities online. Among the most prominent failures that exist, we identified that human error is the leading case behind technical malfunction in public key infrastructure. It is forgotten that human beings create the systems that we utilize for technology. Their errors exist in coding and regulation in the same manner, a lack of overview to the nomenclature of software systems or lack of education on field policy. Which is expected, but certain certificate authorities suffer from these mistakes more so

than others, suggesting that the organizations lack the capability to host domains and subdomains on secure layers of infrastructure.

Nevertheless, this still is still attributed to humans inability to utilize systems as complex as encryption across the internet. The nuances of PKI require technologists to be more than astute at coding and understand the ware of systems. Philosophically, this research has helped us identify that cybersecurity functions like the nodal networks of the human brain. Whereas systems work in parallel with one another such as the development of the hardware in a system using PKI and the software they enable to run their encryption methods sanctioned by NIST. We think that more work to crack down on the dissonant CAs can benefit the security of users across the internet, and enable for more stringent policies to encourage safety on the internet. Additionally, it could disable feelings of distrust between the users of the internet whom have little knowledge of how it functions and put the onus of explicit compliance from the company to the public.

References

Admin, Unknown. “What Is a Certificate Authority?” *GlobalSign*, GMO, 16 Aug. 2023, www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies

Biiswas, Debarati. “What Happens When a Certificate Chain of Trust Breaks?” *AppViewX*, AppViewX, 3 Aug. 2023, www.appviewx.com/blogs/what-happens-when-a-certificate-chain-of-trust-breaks/.

Carl Ellison and Bruce Schneier. “Ten risks of PKI: What you‘re not being told about Public Key Infrastructure”. In: Computer Security Journal 16 (Dec. 2000).

L Jean Camp, Helen Nissenbaum, and Cathleen Mc Grath. “Trust: A collision of paradigms”. In: International Conference on Financial Cryptography. Springer. 2001, pp. 91–105.

R. Anderson. “Why information security is hard an economic perspective”. In: Seventeenth Annual Computer Security Applications Conference. IEEE Comput. Soc.

Serrano, Nicolas and Hadan, Hilda and Camp, L. Jean, A Complete Study of P.K.I. (PKI’s Known Incidents) (July 23, 2019). TPRC47: The 47th Research Conference on Communication, Information and Internet Policy 2019, Available at SSRN: https://ssrn.com/abstract=3425554 or http://dx.doi.org/10.2139/ssrn.3425554