Key Management and Secure Communications

Secondary Research

Drew Petersen
University of Maryland Global Campus
drew.l.petersen@gmail.com

Executive Summary

One of the fundamental issues facing cybersecurity professionals is organizations not understanding the difficulties of secure communications. Encryption and Key Management are prime examples. Most people think the internet just "works" and give little thought to how and why. Organizational leaders need to have a better understanding of how the systems they rely on every day work so they can provide meaningful support to their information technology and security professionals.

One issue every executive needs to understand is that their IT departments are working with the deck stacked against them. Cybersecurity and defense rely on the process of being "good enough" because attackers always have the advantage. The underlying systems used in encryption and secure communications are fundamentally the same as they were before the internet was a public resource. Meanwhile attackers are utilizing ever-evolving and more sophisticated attacks.

Another main issue leaders need to understand is that no data is truly safe. All communications should be treated as if an unauthorized user has access. Known as the Byzantine Generals problem, it's a known fact that no matter how big or small, someone is trying to listen or steal.

Every year that goes by, this problem becomes harder to handle and the solutions become more complex. The technology behind any computing systems is growing at a rate that makes it impossible for any one person to stay on top of. There needs to be trust in IT departments as a whole and there shouldn't be a single point of failure for any security need.

It is imperative that secure communications and data security not be just a budget item to be raised or lowered but as something integral to the same and effective operation of the company. Anything less can be catastrophic to an organizations public image and its bottom line.

Keywords

Key management, Public Key Infrastructure, Cybersecurity

Introduction

Key Management is a cornerstone of organizational cryptographic security. Much like a safe, if a thief knows the combination, the safe is effectively useless. If the keys for an organization's encryption are known, then the encryption is effectively useless (Barker, Burr, Polk, & Smid, 2012). One of the more common key management systems (KMS) used is the Public Key Infrastructure (PKI) (Benantar, 2001). PKI works by providing digital certificates, proving who those certificates belong to, and ensuring that the certificates can continue to be trusted. PKI is not an encryption method by itself but instead is the concept in which data is encrypted and then verified as authentic (Perlman, 1999). It relies, like much of modern encryption, on the Rivest, Shamir, and Adleman (RSA) algorithm first published in the 1970s (Rivest, Shamir, & Adleman, 1978). PKI consists of four components; the certificate authority, the registration authority, the central directory, and the certificate management system (Perlman, 1999). The fundamental idea behind PKI, and all modern encryption, is to allow secured communications on unsecured networks. Unfortunately, modern encryption is under attack, and with it, key management practices are increasingly less useful and reliable (Wilshusen & Powner, 2009). Key management is plagued by a lack of direction dedicated to its growth and survival, uses inadequate, old, or simply outdated tools, and lacks growing standards and resources dedicated to the field.

First, key management must deal with new threats and new network types, leading to splitting of resources and slowed growth. As an example, the introduction of cloud computing, while great for the end user, has monumentally increased the difficulty in data security (Getov, 2012). Next, key management relies on many of the same tools it has been using for decades. New methods in encryption aren't used or don't become adopted by a wide enough audience to be of much use (Denning & Lewis, 2016). Finally, there has been a lack of resources dedicated to the field of encryption. The answer for many organizations is to hope that their data isn't stolen and if it is, hope the encryption is good enough to protect it. There isn't enough effort made in trying to protect the data in the first place. This puts an enormous strain on the cryptology used to encrypt data (Noor, 2008).

Key Management Threats and Challenges

The fundamental aspects of key management plans are how to exchange keys, how to securely store keys, and the time period to maintain the keys. One of the primary hurdles to implementing a successful key management plan is the ever-evolving threats facing the cyber world. Organizations are constantly under attack from dedicated ransomware attacks, phishing schemes, random accidental malware installation, and the ever-present insider threats. In fact, cyberattacks doubled in the first half of 2017 with more than 200,000 new malware samples being found weekly (Seals, 2017).

This leads to increasing complexity and security concerns, which is further compounded by the size of the organization. In a study that interviewed a wide range of CIOs in 2003, a common theme was the increased presence of technology throughout companies and the need for an IT presence throughout multiple departments (Reich & Nelson, 2003). Add in the ubiquity of high-tech devices throughout modern culture and

the problem only continues to increase. That survey of CIOs also demonstrated another issue. The increasing complexity of the job of the IT professional and the more complicated structure of the IT departments, as well as organizations they were part of (Reich & Nelson, 2003). That increase in organizational complexity is a major problem in key management.

Another fundamental threat to the successful implementation of a key management plan is the extensive use of legacy systems (Barker et al., 2012). Legacy systems, whether they are hardware or software related, provide a unique challenge in key management (Alavi & Leidner, 1999). Legacy systems, whether by design, neglect, or a combination of the two, may have trouble interfacing with newer security software or techniques (Zhou, Han, Lin, Perrig, & Gligor, 2013). This requires modern key management plans to be flexible with the systems they interface with. It also increases an entire KMS's vulnerability to an attack. By using legacy systems, the vulnerabilities inherent in those systems likely cannot be solved, leaving the entire system at risk (Zhou et al., 2013).

One final primary threat facing modern key management is the explosion of cloud computing. Cloud computing has revolutionized the way modern organizations can both access and store their data (Zhang, Cheng, Boutaba, 2010). From a security standpoint, users expect 2 functions from cloud computing; secure interaction with cloud services and secure storage of data in those cloud services (Chandramoili, Iorga, & Chokhani, 2014). There are 3 types of cloud computing, Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), and Software-as-a-service (SaaS). While at the core they share similar features and security requirements, they each require a slightly different methodology to accomplish the original 2 goals (Chandramoili et al., 2014). The result is that utilizing cloud computing delegates the key management away from local IT and onto the cloud provider. This adds an additional level of threats to be wary of, particularly insider threats from the cloud provider itself (Chandramoili et al., 2014).

Modern key management plans must account for all the above issues and others not mentioned. They must also satisfy the requirements of the organization for which they are a part of. There is no single solution to these problems but many tools have been created trying to solve the above problems.

The Tools of Key Management

Key management is a complicated business and many tools have been developed to deal with the complexity. It is important to understand why key management exists in the first place in order to understand the need for the tools that have been developed.

Simply put, key management exists because anonymous users on the internet can't be trusted (Parno, Zhou, & Perrig, 2012). Since the end-user can't be trusted or verified, systems have been developed to ensure the authenticity of who the end-user says they are. One of the primary issues facing key management tools is scalability. As security needs rise, the overhead the security tools require also increases. It eventually gets to the point where the security tools become so resource intensive, they make the normal operations of the system difficult (Parno et al., 2012). Researchers have been

looking for solutions to the scalability issue for as long as the internet has been around. One of the primary solutions that has popped up is PKI.

PKI works by allowing principals on the internet, whether they are human, client machine, server, or other, to verify the authenticity of the public key of other principals (Perlman, 1999). Without that verification, principals wouldn't know that their data was sent without being intercepted or modified. This is known as the two generals problem or the Byzantine generals problem (Lamport, Shostak, & Pease, 1982). The foundation of PKI is the certificate authority (CA). The CA functions as a repository for public keys, allowing users to access the CA to verify the trustworthiness of user on the other end of a transmission (Perlman, 1999). PKIs have become widespread on the internet and are particularity prevalent in governmental organizations (Barker et al., 2012). PKIs have their shortcomings however, many of which are shared with all key management techniques.

One of the major problems with PKIs, or any key management program that relies on a central authority, is that you must trust the central authority. If the authority ever becomes untrustworthy, for any reason, the entire system fails (Ellison & Schneier, 2000). Adding to that, it relies heavily on the end-users on either side also being trustworthy, or verified as such. If an end-user can be spoofed, the central authority would have no way of knowing and would show them as trusted (Ellison & Schneier, 2000). Another major issue is who verifies that CA is trustworthy in the first place? Someone must determine trustworthiness and that is a rabbit hole that keeps on going. If you can't trust anyone, how can you make something trustworthy (Ellison & Schneier, 2000)?

Many other tools have been developed relying on different infrastructures but most do not find widespread use. One of common pitfalls for any cryptography is that users must be using the same system (Parno et al., 2012). A KMS could be spectacular and solve many of the problems of a normal KMS, but if it doesn't fine widespread use, it isn't helpful. That is the largest hurdle to solving not only the problems with PKI, but any key management tool. They rely on being good enough and while the tool itself might evolve (PKI is on version 3), it is still the same tool at its core (Berker et al., 2012). While the internet evolves rapidly, the tools we use to secure it can be 2 decades old or older.

Conclusion

Key management continues to be a field that struggles in the face of modern computing. Cryptography is under attack from many angles and the tools used to manage keys or secure communications are old, outdated, or haven't evolved enough to deal with emerging threats. Compounding these issues is the fact that cybersecurity is underfunded and undermanned. Short-term, this leads to a few organizations unable to protect themselves. Long-term, this situation will lead to attackers having a permanent upper-hand when it comes to intrusion techniques and decryption capabilities. While tools like PKI handle authorization and authenticity today, these tools also struggle keeping up with the ever-changing internet. New tools struggle to adopt widespread usage due to financial limitations or lack of exposure. These are all solvable problems,

but like everything else in cybersecurity, it will take more dedication and more financial backing than is available now.

REFERENCES

Alavi, M., & Leidner, D. E. (1999). Knowledge management systems: issues, challenges, and benefits. *Communications of the AIS*, *1*(2es), 1.

Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. (2012). Recommendation for key management part 1: General (revision 3). *NIST special publication*, *800*(57), 1-147.

Benantar, M. (2001). The Internet public key infrastructure. *IBM Systems Journal*, *40*(3), 648-665.

Chandramouli, R., Iorga, M., & Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In *Secure Cloud Computing* (pp. 1-30). Springer New York.

Denning, P. J., & Lewis, T. G. (2016). Exponential laws of computing growth. *Communications of the ACM*, *60*(1), 54-65.

Ellison, C., & Schneier, B. (2000). Ten risks of PKI: What you're not being told about public key infrastructure. *Comput Secur J*, *16*(1), 1-7.

Getov, V. (2012, July). Security as a service in smart clouds--opportunities and concerns. In *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual*(pp. 373-379). IEEE.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382-401.

Noor, A. (2008, March). Securing the core with an enterprise key management infrastructure (EKMI). In *Proceedings of the 7th symposium on Identity and trust on the Internet* (pp. 98-111). ACM.

Parno, B., Zhou, Z., & Perrig, A. (2012, October). Using trustworthy host-based information in the network. In *Proceedings of the seventh ACM workshop on Scalable trusted computing* (pp. 33-44). ACM.

Perlman, R. (1999). An overview of PKI trust models. *IEEE network*, *13*(6), 38-43.

Reich, B. H., & Nelson, K. M. (2003). In their own words: CIO visions about the future of in-house IT organizations. *ACM SIGMIS Database*, *34*(4), 28-44.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

Seals, T. (2017, August 11). Cyber-attack Volume Doubled in First Half of 2017. Retrieved from https://www.infosecurity-magazine.com/news/cyberattack-volume-doubled-2017/

Wilshusen, G. C., & Powner, D. A. (2009). *Cybersecurity: Continued efforts are needed to protect information systems from evolving threats* (No. GAO-10-230T). GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.

Zhou, Z., Han, J., Lin, Y. H., Perrig, A., & Gligor, V. (2013, June). KISS:"key it simple and secure" corporate key management. In *International Conference on Trust and Trustworthy Computing* (pp. 1-18). Springer, Berlin, Heidelberg.