# The Importance of a Cryptographic Review

## NCC Group Cryptography Services

## Introduction

Cryptography is an underpinning of every organization's data security. It is as simple as the correct deployment of TLS and as complicated as bespoke protocols for software updates. This technology is an integral part of an organization's security infrastructure. With the field constantly evolving, having a dedicated review is becoming increasingly important.

When OWASP released its 2010 Top Ten report of the most critical web application security risks, "Insecure Cryptographic Storage" made the list at #7[i]. Its follow-up report in 2013[ii] ranked the risk at #6 under the expanded umbrella of "Sensitive Data Exposure." The need for cryptographic review is growing as it becomes a higher priority in application security risk assessments. This whitepaper will identify the importance of specialized cryptographic review and the necessary steps for ensuring a successful cryptographic implementation.

## Why Cryptographic Review is Necessary

Cryptography is constantly evolving making it necessary to invest in today's research in order to stay ahead of tomorrow's attacks. Unfortunately, most organizations lack bandwidth for a dedicated cryptographer to stay current with the latest vulnerabilities and research. Someone "learning on the job" does not have the experience or skill required to perform a cryptographic security assessment. It is a complex application security evaluation that requires seasoned and knowledgeable practitioners. Relying on a Bug Bounty program for all application security can also leave an organization vulnerable. While some organizations have crowdsourced forms of application security, they cannot effectively perform white-box assessments of cryptographic implementations.

Safe cryptography requires meticulous development. Most organizations have general-purpose libraries and require their uses to be vetted by internal security teams. Unique uses require a careful planning and design stage, mindful development, thorough positive and negative testing, and a focused and specialized review.

Unlike most parts of application development, if the cryptography is broken then everything will usually still work. For example, if a random number generator produces an encryption key of all zeros, it still encrypts and looks like illegible ciphertext. Unit tests cannot easily confirm that the cryptography is secure—only that it has completed the request. Subtle flaws in the implementation of cryptography, which do not cause any outward indication of fault, can completely break a well-designed cryptographic implementation.

It is well known that cryptosystems are difficult to design correctly and securely. Only by analyzing and breaking similar systems can one hope to design a robust system. A breadth and depth of experience is needed to design, implement, and review complex cryptosystems such as database encryption, software update mechanisms, and secure communication channels.

## The Importance of Correct Methodology

Cryptography is like the steel framework of a building and is critically important to every organization's core business, whether it's realized or not. VPNs, Federated Identity Systems, customer data segmentation—all rely on cryptography. This is why a measured development approach with an expert review is important. It allows second order effects to become apparent and mitigated before any development efforts begin. Common consequences that arise from new cryptographic development can include the following: increased load on servers or embedded devices, inadvertently breaking features such as search or data loss prevention, and increased storage space from lack of de-duplication or compression. To avoid these issues, the most effective approach to a successful implementation is to thoughtfully plan out the stages of design, development, and deployment.

NCC Group Cryptography Services recommends following these phases for an effective implementation:

1. Internal design and discussion with stakeholders across teams
2. Architecture review (commonly with experienced third parties)
3. Revisit design as necessary
4. Application development
5. Test deployment in a development or staging environment
6. Source code review and vulnerability assessment

A poor design will lead to an unstable architecture, making it prone to vulnerabilities. For complicated undertakings, the best time to invest in a cryptographic review is during the internal design phase before any code is written. An organization will lay out what they want to accomplish by deploying cryptography, the intended design, and the different aspects of the system it will touch. Following this phase, an architecture review can point out flaws that would be expensive to fix in deployed systems and call out unanticipated consequences that may affect other components of the environment. It can also provide recommendations for future-proofing and adding in additional defense-in-depth measures.

After application development is tested and deployed, a thorough source code review is essential in order for any security testing to discover cryptographic issues. As detailed earlier, there can be subtle problems when the system appears to be functioning correctly. A capable attacker will perform social engineering, phishing, and even physical attacks to get at embedded crypto keys or other data of value. If an attacker cannot access the data, they will get a hold of the source code (as has been seen with high-profile hacks on both Adobe[iii] and Google[iv]). A source code review is the most effective way to perform a vulnerability assessment, and cryptographic review is generally not something that can be covered in black-box methodologies such as a bug bounty program.

## Side Channel Attacks

When a cryptosystem has not gone through the proper review methodology, its data may be vulnerable to a data breach. The most common of these is a side channel attack. A cryptographic side channel attack is when sensitive information is obtained by accessing extremely subtle pieces of data. That data could be an error returned from a webserver or the amount of time it takes to respond to a request. These simple, and supposedly benign, data points are all it takes to reveal sensitive plaintext or even secret keys.

When Paul Kocher recognized the impact of side channel attacks in the 1990's[v], researchers began discovering potential side channels in nearly every cryptographic algorithm. The most famous example is the CBC padding oracle which allows total plaintext recovery. The CBC padding oracle is based off an error or difference in timing observed from a server, and can be mitigated by adding an authentication mechanism. Another example is the RSA algorithm. It is known to have multiple side channels that are exploitable remotely or locally and can reveal secret keys. A variety of techniques can be used to attack an algorithm from multiple angles depending on the attacker's level of access. These side channel attacks are dependent upon the specific environment the cryptography has been deployed in, implementation details (such as choice of cryptographic library), and how the attacker can provide or modify input to the system.

While many of these data breaches stem from how the cryptography was designed (like the CBC padding oracle), the majority of side channel invasions occur from within the gritty implementation details, buried deep within the code. This makes identifying and remediating these issues an arduous task. Not only is it necessary to know the specifics of an existing side channel in a particular algorithm and published avenues of exploitation, but the entire protocol needs to be looked at from afar to recognize other potential susceptible points.

## Use-Cases

A Whole-Codebase Cryptographic Review: A 5,000 employee SaaS company, with many teams of developers, was in the process of standardizing a single internal crypto library that would be maintained by the internal security team. NCC Group Cryptography Services reviewed the library, as well as performing targeted assessments on internally identified projects that were too large or complex to be cut over to the new library.

NCC Group Findings:

- Weak encryption options in the library that could be inadvertently used by developers
- A complex API was being used and increased the risk of accidental misuse of the library
- In one of the targeted assessments, weak data protection on URL Tokens that could lead to data theft

NCC Group's recommendations enabled the company to greatly simplify how its developers used its internal library; resulting in less work for the internal security review team and a greater confidence in future uses of cryptography. The vulnerability we identified in the URL Tokens helped the organization avoid a potentially devastating breach where any individual would be able to access other customer's data.

Cryptographic Architecture Review: A payment processor was building a new personally-identifiable information vault for storing customer records and passwords. It consisted of multiple HSMs working together, fronted by several services. The Cryptography Services team reviewed the architecture before any code was developed; including the encryption modes in use, how the password hashing would occur, and how the keys would be managed.

NCC Group Findings:

- Weak encryption modes that could allow data substitution or modification
- Over-permissioning of users who were allowed to access the HSMs
- Defense in-depth recommendations for password hashing, that would make an attacker with some level of access be much more limited in the data theft capabilities

The Cryptography Services team were able to identify ways the client could thwart a sophisticated attacker who had gained database access from modifying or swapping the data—a subtle attack that can enable the attacker to view other user's data or log in as an Admin. The team also provided the client with a number of in-depth defense options to limit an attacker's capabilities if they exploited future flaws in various components of the system.

## Conclusion

Specialized cryptographic review is the most effective way to identify deep-seated impactful vulnerabilities in cryptosystems. These vulnerabilities can linger undetected for years, and the impact of their exploitation can be disastrous. NCC Group's Cryptography Services can help an organization tackle these cryptographic challenges and offer the expertise and skills needed in a cryptographic review. If an organization is relying on cryptography to protect extremely sensitive data or building a service offering atop its assurances, a specialized cryptographic review should be part of the development lifecycle to mitigate risk.

[i] The OWASP Foundation, *OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks* (2010), http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf.

[ii] The OWASP Foundation, *OWASP Top 10 – 2013: The Ten Most Critical Web Application Security Risks* (2013), http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf.

[iii] Dan Goodin, "Adobe source code and customer data stolen in sustained network hack," *Ars Technica,* last modified October 3, 2013, http://arstechnica.com/security/2013/10/adobe-source-code-and-customer-data-stolen-in-sustained-network-hack/.

[iv] Wikipedia contributors, "Operation Aurora," *Wikipedia, The Free Encyclopedia,* accessed March 8, 2016, *,* https://en.wikipedia.org/w/index.php?title=Operation_Aurora&oldid=693890498.

[v] Paul C. Kocher*, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems* (San Francisco: 1996), http://www.cryptography.com/timingattack/paper.html.