HUNTING FOR WEAK CRYPTO

KEEPING OPEN SOURCE CRYPTOGRAPHY SECURE

ABSTRACT

Using open source cryptography can be a double-edged sword - it provides companies with the power to provide core libraries and tools which allow organizations to build SSL, TLS, or other cryptography into their products and projects. But sudden and unpredictable vulnerabilities can put you and your data at substantial risk.

Open source cryptography allows organizations and enterprises of any size to quickly and easily secure their applications and the data they transmit. The choices are almost endless: libsodium, OpenSSL, NaCl, and many others – all make it possible for organizations to build cryptography into their products. But with the wide use and multitude of choices comes risk - poor implementations, abandoned code, and critical flaws can all make an application or service that appears to be secure anything but. How can you guarantee that your infrastructure is using open source cryptography safely and securely? ISG gives you the tools to know everywhere cryptography is used and the power to always keep your own tools, applications, servers, and services up-to-date without re-coding or re-installing.

Open Source Crypto Pain Point #1

POOR OR WEAK IMPLEMENTATION

We ask our IT and security people to be experts at many disciplines... but cryptography requires a level of expertise beyond the general, leading to implemenation errors.

Open Source Crypto Pain Point #2

ABANDONED OR FRAGMENTED CODE

As projects age out or developers move on to new roles, code stops getting updated. If there is cryptography embedded in those projects, the crypto stops getting updates as well.

Open Source Crypto Pain Point #3

CRITICAL FLAWS AND VULNERABILITIES

Flaws and vulnerabilities in cryptography are found regularly. Without knowing where crypto is being used, you put your data and applications at significant risk.

Open Source Crypto Pain Point #4

SUPPLY CHAIN RISKS

Do you rely on third-party vendors to manage cryptography or embed it into the products and services they sell you? Are they updating that crypto regularly?

PAIN POINT #1: POOR IMPLEMENTATION

Today's technology professionals have so much on their plates it just isn't reasonable to ask them to become experts at a whole other discipline. Information security professionals with deep cryptographic knowledge and expertise are exceedingly rare and the same can be said about developers. This isn't because they're unskilled: cryptography is hard to do right, and it is even harder to stay on top of threats, vulnerabilities, or other edge cases that threaten the integrity of an implementation of cryptography. Most open source cryptography solutions contain support for scores of deprecated, vulnerable, weak, or known-broken cipher suites that put your applications and data at risk - and often they're left inside your applications without additional mitigations or protections… if they're known to be there at all (see Figure 1 below). Knowing where these less-than-optimal implementations lie are critical to reducing business risk.

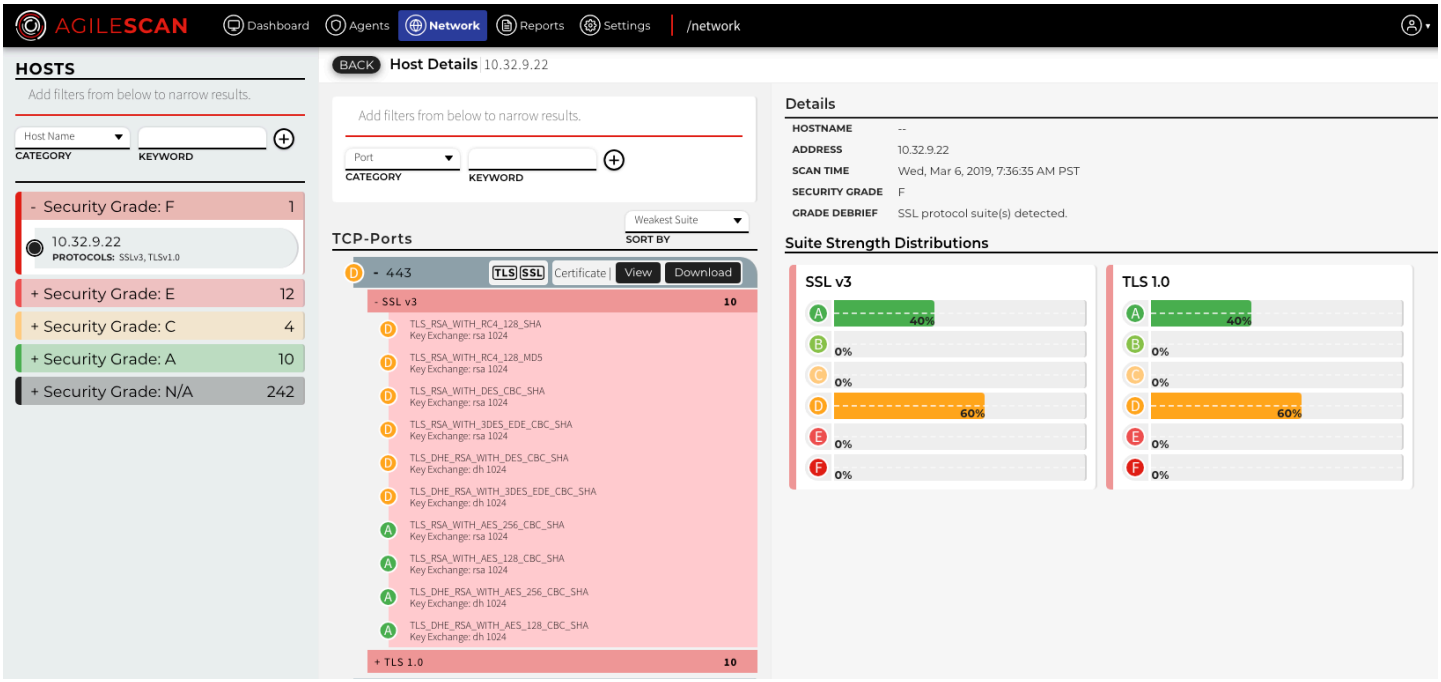

Figure 1: Finding old, weak, or deprecated cryptography with AgileScan.

PAIN POINT #2: ABANDONED AND FRAGMENTED CODE

Developers move on to new projects, to new roles, to new companies… and sometimes their hard work is forgotten or abandoned. Applications parked on a server and have been in some cases running for literally years without updates or patches to their crypto. In other cases, megalithic applications full of fragmented code are running multiple versions of the same cryptography for various purposes. Not having a complete picture of where your encryption exists leaves you with gaping blind spots and puts your regulatory and compliance obligations at real risk. All of these issues leave you exposed to crafty attackers with the ability to exploit those obsolete versions of cryptography.

PAIN POINT #3: CRITICAL FLAWS AND VULNERABILITIES

Perhaps the most famous open source cryptography vulnerability of them all was the Heartbleed bug. The bug left servers running a vulnerable version of OpenSSL exposed to the world - attackers were able to literally grab chunks of memory off servers full of random data… and sometimes that data contained juicy bits of info like usernames, passwords, private keys, or parts of confidential messages. And to make it worse, it was initially almost impossible to detect an attacker taking advantage of the vulnerability. In the years that have followed, there are still tens of thousands of servers exposed to the Internet running Heartbleed-vulnerable OpenSSL… and we can only speculate how many more servers are hidden inside corporate networks.

PAIN POINT #4: THE THIRD-PARTY PROBLEM

How many of us rely on vendors to provide us products and solutions inside our networks? We all do. How many of those vendors allow you to review source to guarantee their products are free from flaws and defects? None of them. We are reliant on these vendors to ship us secure products that are cornerstones of our digital enterprises. In March 2019, the UK's Cyber Security Evaluation Centre found "…serious and systemic defects" in a key supplier of telecommunications infrastructure products. The software that was reviewed used OpenSSL inconsistently: "[I]n the first version of the software, there were 70 full copies of 4 different OpenSSL versions, ranging from 0.9.8 to 1.0.2k… with partial copies of 14 versions, ranging from 0.9.7d to 1.0.2k, those partial copies numbering 304. Fragments of versions, ranging from 0.9.6 to 1.0.2k, were also found across the codebase." Even after being alerted to the issues, and the vendor responding with updates, the UK CSEC found "…code that [was] vulnerable to 10 publicly disclosed OpenSSL vulnerabilities, some dating back to 2006." How many unique versions of open source cryptography are hidden deep inside the third-party products and services you're using inside your infrastructure right now? Could you even find them?

A TWO-PRONGED APPROACH TO FINDING AND SECURING OPEN SOURCE CRYPTOGRAPHY

ISG's unique set of products provides enterprises with the ability to rapidly find and inventory **all** uses of cryptography found in software and systems across your network. It proactively hunts for cryptographic risks and vulnerabilities, providing answers and visibility to how cryptography is used in moments. ***AgileScan*** finds hidden and embedded cryptography and provides an easy-to-understand dashboard that gives you at-a-glance results and analysis of risks using current industry standards and best practices. It detects network protocols used by web applications deployed in both public or private clouds, or inside your internal network. It verifies protocol versions in use, cipher suites available for negotiations, and reports back on potential vulnerabilities, risks, or weaknesses. And if a new threat or vulnerability is found, ISG's cryptography experts quickly add new intelligence, guaranteeing that AgileScan can assess the impact of that new threat by re-scanning your environment and re-assessing your risk and status.

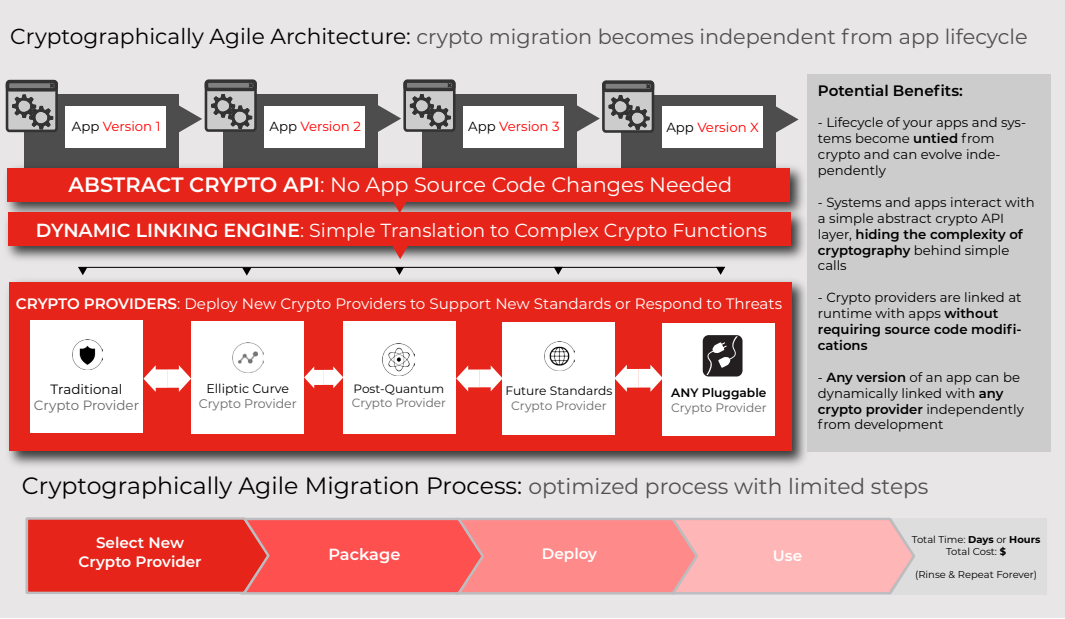

Figure 2: The AgileSec Crypto Agility platform toolkit

Once you've assessed your current cryptographic risk state, **how will you fix it?** For third party products, traditional compensating controls will have to be deployed until vendors can deploy patches and updates. But for your own products, ISG's ***AgileSec Platform*** provides you with the ability to deploy new cryptography to all of your products and applications, *even those already deployed in-field*, giving you the unparalleled power to respond quickly to cryptographic threats and vulnerabilities. We call this *cryptographic agility*, and it allows your systems to easily adopt alternatives to the cryptographic primitives they were originally configured to use. The AgileSec Platform is a unique middleware abstraction layer that delivers **true cryptographic modularization** (see Figure 2 above) and allows real-time modification of cryptography. **All cryptography**. The AgileSec Platform is compatible with almost all major platforms, including Linux (both X86 and ARM), Mac OS (X86), Windows (X86), Android, iOS, and many other major embedded systems platforms. Swap out bad crypto for good crypto in moments once you've integrated the AgileSec Platform into your products.

Infosec Global provides sustainable data protection for a digital world. The company delivers a next generation enterprise grade solution that provides real-time life-cycle management of the cryptography and digital identities for critical systems. The AgileSec Platform manages the entire digital and cryptographic life-cycle from the discovery of threats and vulnerabilities to the updates and fixes of cryptography, keys and certificates. ISG helps governments and enterprises achieve trust through compliance to cryptographic regulations, worldwide.

To learn more, visit **www.infosecglobal.com**

INFOSEC GLOBAL

SAN FRANCISCO
750 Battery St.
San Francisco, CA 94113

TORONTO
2225 Sheppard Avenue East
Suite 1402, Toronto, ON
M2J 5C2 Canada

ZÜRICH
Hardturmstrasse 103
8005, Zürich
Switzerland