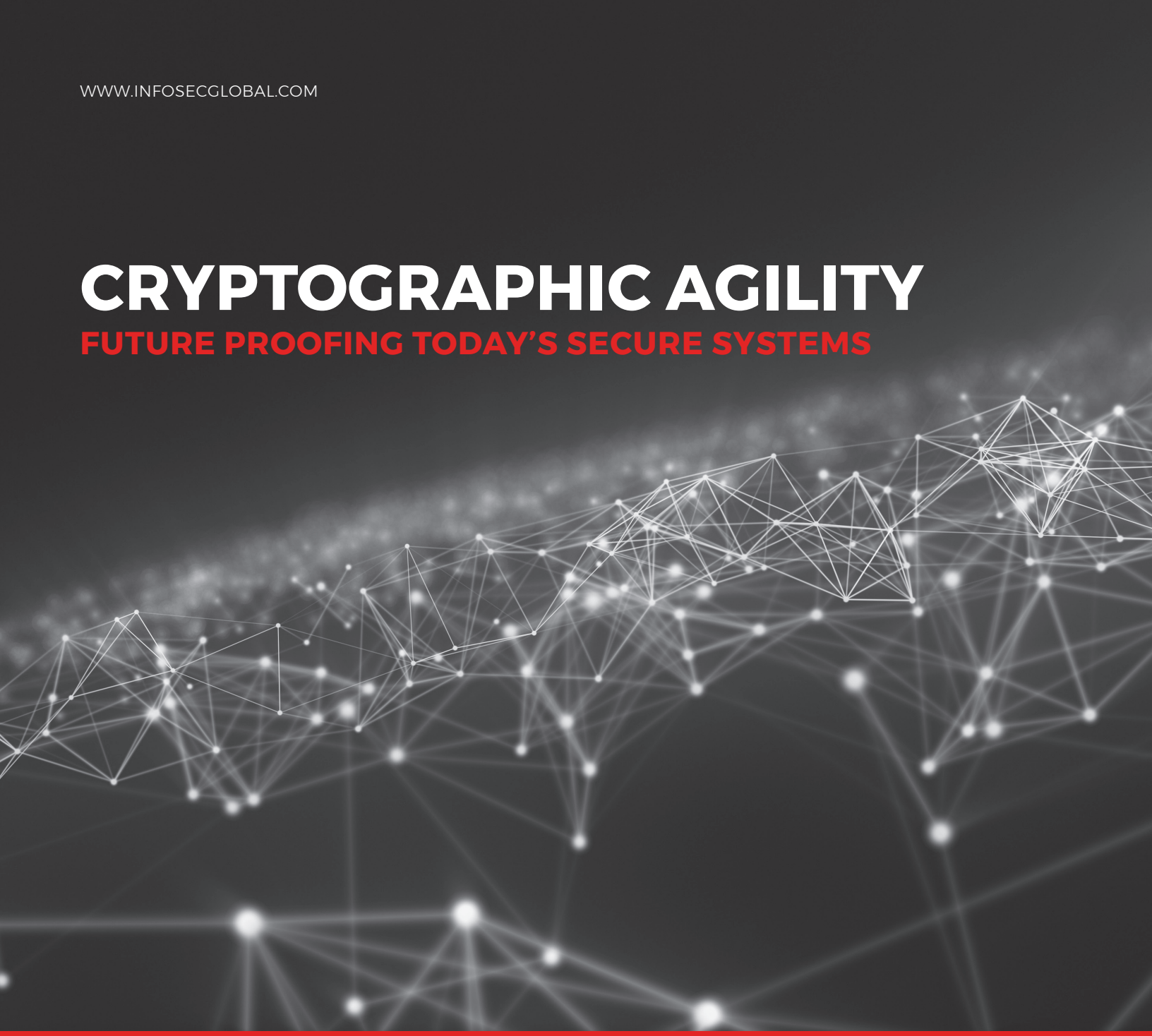
WWW.INFOSECGLOBAL.COM

CRYPTOGRAPHIC AGILITY

FUTURE PROOFING TODAY'S SECURE SYSTEMS



INFOSEC GLOBAL
FEDERAL

CONTENTS

CRYPTOGRAPHIC AGILITY:
FUTURE PROOFING TODAY'S SECURE SYSTEMS

Cryptography is a fundamental building block of secure system design that security architects use as part of a layered approach to keep information private, and protect systems against fake communications. Potential attacks against networks and systems can be achieved by subverting communications and introducing havoc using specially constructed false messages. These types of attacks are safeguarded against when using proper modern cryptography to check the authenticity of messages and guard their privacy.

Commercial systems that use encryption methods typically use only a handful of cryptographic algorithms that are well studied by mathematicians who are responsible for designing the ciphers and trying to break them. Outside of mathematics, cipher design is often viewed as a black art, and it is difficult to discern the security merits of one algorithm from the next in an objective way. Security designers therefore rely on a very small number of standards groups and governments to specify cryptographic algorithms and the resulting standards tend to be rigid and long lived.

A unique challenge of encryption standards is having to deal with future proofing their effectiveness over time. While other types of technology standards tend to become outdated as new and better technology takes its place, in the case of cryptography, the mathematics becomes less secure over time by the virtue of researchers and cryptanalysts who are constantly discovering new mathematical methods to solve problems faster, the types of problems on which cryptography derives its security, and effectively breaking the cryptographic methods. In other words, cryptography becomes weaker over time because mathematicians learn to be smarter.

This highlights a recurring problem in the security field in that security breaches occur very often and need to be addressed over time. Security designers take a layered approach in dealing with the high likelihood of a future breach and include safeguards, mechanisms and controls to recover and repair the security posture of a system once a break has occurred. For instance, many systems have a secure bootstrap mechanism that uses cryptograph - ic keys stored in hardware to authenticate new software that is installed into the system. In the event that a system is compromised, a new and preferably fixed version of the system software can be installed to recover the overall system security. Using cryptography permits these types of upgradable systems to be fixed when a security hole is discovered. But what happens to a system if the cryptography primitive is the broken component that needs to be upgraded?

Even the strongest modern cryptographic algorithms are not designed to be unbreakable. Instead they are de - signed to balance effectively strong security with convenience and manageability. As a counter example, the cipher that is best known to be resilient to breaking is called the one-time-pad, which is very strong, and also extremely difficult to use. One-time-pad requires keys that are as long as the message attempting to be sent, making the scheme completely impractical for modern encrypted communications.

Modern ciphers are designed to strike a balance between convenience and security. Once a cipher has been well studied and accepted by the cryptographic community, it can be proposed for use in cryptographic and protocol standards where the algorithm's parameters are narrowed and documented. At this point, the standard will define the security levels by specifying the required minimum key sizes to be used during encryption operations. Standards will also anticipate that security levels of ciphers will diminish over time, and so key sizes are specified that allow for programmers and product vendors to tune the security level of the cipher higher as computational and cryptanalytic methods improve over time. Higher level security standards, for instance protocol standards like TLS, will also build in support for a number of ciphers which can be used optionally or interchangeably. However, in order to control the number of permutations by designers that implement the standard, algorithm support still tends to be rigid in the sense that deviating from the handful of specified algorithms and key sizes is either difficult or impossible.

As standards proliferate and gain acceptance, application software and vendor products adopt the protocol stan - dard and often narrow the cryptographic options even further in order to limit implementation complexity, and reduce time-to-market as well as support and maintenance headaches.

In effect, this creates a value chain where cryptography standards are adopted by higher level protocol standards for integration into application software and devices. Product vendors tend to further narrow cryptographic op - tions during their development cycle in order to limit complexity. In the short term, limited complexity is good for security because less errors tend to be made, however, the long term security posture of end products becomes limited with respect to features that allow cryptographic ciphers and implementations to be changed over time.

THE AGING ENTRENCHMENT PROBLEM

Cryptographic algorithms have a shelf life, they do not maintain their security level over time, instead they get weaker as time passes. Contrast this with the tendency for important secure systems to become more rigid and entrenched over time. For instance, financial industry payment systems are well known for implementing two-fac- tor authentication schemes, like chip and pin payment cards, however, once implemented and deployed to tens of thousands of customers it becomes extremely difficult to change the cards which could be in a customer's hands for five years or longer.

Similarly, in the Industrial Internet of Things use case, where an autonomous sensor could be installed in a remote location and expected to operate with secure communications over a period of 10+ years. While a single device might be easy to retrieve and replace, it is much harder to upgrade thousands of devices spread over a large geographic area.

These types of long lived and highly distributed secure devices will often outlive the usefulness of the cryptography that is built into them, and for security purposes will need to be replaced or upgraded. Security architects often use protocol standards to justify their cryptography choices, because choices are limited. Designers should be choosing ciphers that are robust enough for the lifecycle of their long lived applications and systems, or imple - ment a design that can accommodate future security updates to protocols and cryptography as they age.

THE TRUSTED ORIGINATOR PROBLEM

Cryptography and security protocol standards are created by national and international standards bodies, however, they are sometimes perceived to be influenced by governments. Some governments are wary of foreign influence on the security found in commercial international standards, and for certain use cases, a wary government might mandate the use of a custom cryptographic algorithm for domestic use. Often this may involve starting with a well-known standards based algorithm and making parameter changes, or making slight alterations to the structure of the cipher. Regardless, the new resulting custom algorithm is much like a new language in that it is not compatible with broad-based standard ciphers.

CHALLENGES OF NEW ENCRYPTION

New cipher introduction creates a number of challenges for many types of businesses that rely on cryptography for privacy and authentication.

Government/industry regulators that do not trust standards based cryptography may have a desire to mandate ciphers that were created domestically in order to avoid foreign influence and potential back-doors. However, industry still needs commercial security tools and products in order for the regulated companies to adopt and use the new ciphers in networks and systems. If commercial off the shelf technology products do not support the custom ciphers, then companies need to augment products with long and expensive custom development projects.

Governments tend to be the first to define and use custom ciphers, and they rely on government integrators to add the custom ciphers to information security systems. This is often done for the purposes of national security related projects where secrecy is of the utmost importance and requires that the custom ciphers remain a guarded secret that is only known to cleared national citizens. In this case, the dilemma is how to separate product procurement from state secret cipher integration? Products are typically imported and stringently evaluated against security criteria. If custom secret ciphers need to be integrated into the product, special care must be taken to ensure that foreign nationals supplying security products are not privy to the implementation details of the custom secret ciphers.

Software and hardware product vendors are also at a disadvantage when multiple customers request slightly dif - ferent variants of their products to support their custom cryptographic needs. Product variants can cause product inventory headaches and complicate ongoing support and maintenance of products over the long term, adding additional expenses to the bottom line.

IMPLEMENTING CRYPTOGRAPHIC AGILITY

Cryptographic Agility is a design technique for allowing products, systems and protocols to replace the cryp - tographic implementations over time. This can be accomplished in a variety of ways, but like any other system, security systems are built using a variety of sub-components working together, and all sub-components in the system need to be crypto agile.

Many low level security protocols have cryptographic agility built in, for instance, the popular web security proto - col TLS/SSL allows for cipher suites to be changed, and X.509 digital certificates can support new cryptographic algorithms.

If a system needs to simply be “future proofed” to allow new cryptography to be substituted at some time in the future, then there are many solid security framework choices that product makers and system designers can use to ensure cryptographic agility using manual re-configuration. Although manual re-configuration is often not practical in today’s communication systems.

Much more sophistication and care is required when dealing with cryptographic reconfiguration in an automated fashion. For instance, in cases like payment card systems or Internet of Things, there is typically a very large deploy - ment of autonomous end-points, and visiting each device to reconfigure cryptographic subsystems in a secure way is very impractical.

AUTOMATED CRYPTOGRAPHIC CONFIGURATION AND MANAGEMENT

InfoSec Global's AgileSec Multi-Crypto is an example of a platform security system that is designed to automate the distribution and management of custom cryptographic implementations across a diverse set of remote software and devices.

The product consists of a cryptographic toolkit that is built into end points, and a management server infrastruc - ture that remotely deploys and sets policy for cryptography usage. On the end-point products, the toolkit includes a software agent that can receive, authenticate and securely store custom cipher implementations. The toolkit is also responsible for dynamically linking cryptographic code into applications at runtime, in accordance with cryptographic policies that are provided remotely by the cryptographic management service.

In the case of the Aging Entrenchment Problem, a solution like AgileSec Multi-Crypto allows large scale deploy-ments of devices that are geographically spread out to stay current with industry security requirements that change over time in systems that are intended to be long lived. These long lived systems tend to become more expensive to support over time, if such a system is intended to last 15+ years, crypto that is current today tends to become antiquated within 5-10 years, AgileSec Multi-Crypto introduces managed cryptographic agility into long lived applications to keep their security posture strong over time.

In the case of the Trusted Originator problem, a solution like AgileSec Multi-Crypto allows large scale solutions to be developed and tested using standards based cryptography, and subsequently permit customers with their own secret cryptography, to reconfigure the final system with their own ciphers, after the system has been deployed on their own home soil. This permits non-nationals to develop secure systems without the need for them to be privy to the internal national secrets of their customers.

AgileSec Crypto, Network Protection and Cyber Assurance products and services are designed to meet cyber security needs today and in to the future. AgileSec solutions meet the demands of highly complex regulatory requirements for government and enterprise.

CRYPTO MARKET

AgileSec Cryptography

Multi-Cryptography Framework

Modern Cryptography – Suite B

Custom algorithms at run-time

Source Code review

NETWORK MARKET

VPN and Link Encryptor

Based on AgileSec Crypto

Control Internet Traffic Routing

Support for Custom Crypto

ASSURANCE MARKET

Technology Compliance Lab

Vulnerability Assessment

Localized Deployment

Run by Local Experts

FOR MORE INFORMATION

For more information about AgileSec cyber security products, or to discuss how InfoSec Global can help your organization, contact us at info@infosecglobal.com.

INFOSEC GLOBAL
FEDERAL

SWITZERLAND
Hardturmstrasse 103
8005, Zürich
Switzerland

UNITED STATES
Tel: +1 416-492-3333
2225 Sheppard Avenue East
San Francisco

CANADA
TORONTO
Tel: +1 416-492-3333
2225 Sheppard Avenue East
Suite 1402, Toronto, ON
M2J 5C2 Canada

OTTAWA
403-270 Albert Street
Ottawa, ON K1P 6N7
Canada

WWW.INFOSECGLOBAL.COM
info@infosecglobal.com