# CRYPTOGRAPHIC VISIBILITY AND SUPPLY CHAIN COMPROMISE

## Why you need Cryptographic Lifecycle Management

**Prepared by InfoSec Global ("ISG")**

**Ron Williams, CTO, InfoSec Global**

**18 January 2021**

# Table of Contents

# Security Governance and Enterprise Cryptography

Over the past decade, enterprise security practice has become a growing area for attention by the C-Suite. We've seen the maturation of Identity Management and Identity Governance that is able to monitor and manage virtual identities across the enterprise, from creation to retirement. We've seen patch and vulnerability management raised to the level of automated monitoring and remediation. We've seen Threat Management operations increase their ability correlate *business functions* with emerging threats and establish policy-driven governance and processes that addresses the highest risk threats first.

In each of these domains we see the application of *lifecycle management* principles. Each begin with a set of agreed corporate policies that identify the specific monitoring and reporting required of the organization. The governance process is then organized around the collection of relevant status, analysis of that status against corporate policy, and reporting deliverables that identify policy exceptions *and* the set of steps taken to remediate the exception.

## The Cryptographic Visibility Problem

Cryptography is ubiquitous today. It is used to authenticate users and services to one another. It is used to secure data when transmitted between two parties. It its used to conceal stored data on hard drives and other storage media. It is used to conceal our financial transactions from prying eyes when we use our banking apps.

In the SolarWinds supply chain compromise researchers found a key element of the compromise was enabled by weak default cryptographic configuration of the client's Active Directory Kerberos service. This was exploited by attackers to gain administrative privileges in the Active Directory domain to further the objectives of the attack.

## The Policy Problem

Enterprise organizations *may* have operational policies that specify what cryptography algorithms and protocols may be used for this or that purpose. However, more often than not that policy is found as a comment in the code or configuration file that enables it *for a single application* or in spreadsheet used by an operations director for the assets under his or her control.

In general, despite any *central* policies, organizations generally have no way to 1) Identify the cryptographically protocols and algorithms *across* enterprise operations, 2) Evaluate actual deployment status against corporate policy, 3) analyze and prioritize the remediation of policy exceptions or deficiencies, or 4) Consistently be able to identify and report on the status of Cryptographic use - whether on a user's desktop, or on servers housing the corporate *crown jewels*

# Cryptographic Visibility - InfoSec Global's Crypto Analytics

## The Migration Problem- Post Quantum Cryptography and Crypto Agility

Advances in quantum computer processor sizes will continuously and negatively impact the theoretic safety of most currently used public key cryptography algorithms. Migration to Quantum Safe or Post-Quantum cryptography and protocols is inevitable.

Crypto-Agility as a crypto-system and framework decouples cryptographic policy, what algorithms and protocols are acceptable under what conditions, from the application development process and the *application developer*. The framework permits secure, run-time modification of the cryptography deployed to Crypto-Agility enabled client applications, and automated management of cryptography across all Crypto-Agility clients.

Without Crypto-Agility, application clients must either be reconfigured locally (each deployment), re-coded to enable new quantum safe algorithms, or hope the predictions of Post-Quantum vulnerability are significantly *overstated*.

Adoption of and migration to a Crypto-Agility framework provides an organization and the applications they write with a *policy driven* architecture. Future changes, deletion of obsolete cryptography, deployment of new - can be centrally managed. For example, the elimination of a *weak* and to-be-retired cryptographic suite or the update to new Quantum-Safe methods can be effected by a single policy change. Eliminating the future modification of application code to accommodate new quantum-safe techniques.

## Towards Enterprise Cryptographic Lifecycle Management

Lifecycle management is a process whereby managed elements *periodically* evaluated for current status, analyzed against corporate policy, exceptions to policy are identified and process by which they are remediated is documented and auditable. It is a process that *assures* the integrity of the security controls it represents.

Cryptographic Lifecycle Management is therefore the process by which Cryptography and it's elements are managed constantly across the enterprise, and in such a way that potentially business impacting deficiencies can by identified and mitigated *before* they become a target of a major compromise.

As we help our customers address the needs of Cryptographic Governance, Crypto-Analytics is a tool that provides *Discovery* of Cryptography Uses on Network Servers and Hosts, evaluate the discovered crypto against best industry practice and corporate policy, and provide it's users with a complete view with specific recommendations to remediate the exceptions found.

As part of the Cryptographic Lifecycle Management process, ISG Crypto-Analytics provides Discovery, Visibility, Exception Analysis, and specific Remediation Guidance. It enables an organization to establish an inventory of cryptographic assets, their location, status, and use. It enables an organization to design and specify the cryptographic policy by which future scans are compared.

In short, Crypto-Analytics provides visibility into conditions that may be exploited by third parties, and provides the organization with a means to *proactively identify and address cryptographic deficiencies before a mis-configuration or a weak algorithm's use.* Crypto-Analytics enables an organization to *grow into* Cryptographic Lifecycle Management as a standard part of their security operations. It is the critical first element of Cryptographic Lifecycle Management.

# Cryptographic Agility - Decoupling cryptographic policy from development

Some organizations may remember the **Y2K** problem - an entire industry having to modify computers that only used 2 digit date representations. More recently, organizations *continue* to struggle to migrate away from algorithms and protocols based on SHA1. Each migration represents significant time and effort fo organizations that had to re-factor the applications.

Crypto-Agility is a policy-driven cryptographic provider that enables secure run-time modification of the application's cryptography. Migration to the Crypto-Agility API can enable update for all future changes to cryptographic policy in real-time, rather than reconfiguring *each* application individually, or worse, recoding individual apps for each change, Crypto-Agility can establish and *change* the crypto-graphic policy *across the organization*, without rewriting or reconfiguring each deployed application instance.