ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The Necessity of Encryption for Preserving Critical Infrastructure Integrity

Protecting Data At-Rest, In-Transit, and During-Processing with Format Preserving Encryption

June 2017

Authored by James Scott, Sr. Fellow, The Institute for Critical Infrastructure Technology

The Necessity of Encryption for Preserving Critical Infrastructure Integrity

Protecting Data At Rest, In Transit, and During Processing with Format Preserving Encryption

May 2017

Authored by: James Scott, Sr. Fellow, ICIT

Contents

Breaches Result in Loss of Trust

Cybersecurity is rooted in trust. Organizations expend resources purchasing and maintaining the systems and applications that they most trust to be secure against adversarial compromise. Trusted personnel are tasked with maintaining, operating, and improving on these systems and processes. Consumers trust organizations to securely store, process and transmit their data. Lately, consumers have not been able to trust public or private entities to secure their data. Adversaries are irrevocably becoming more sophisticated, capable, and successful in their perpetual attempts to exfiltrate treasure troves of classified information, PII, intellectual property, etc. [1]. There are only two types of networks, those that have been compromised and those that are compromised without the operator's awareness. Attackers launch multi-stage campaigns simultaneously along multiple vectors, and no one solution has proven capable of preventing compromise along all vectors. Over extended periods, threat actors surreptitiously navigate networks in search of access to sensitive systems and data. The risk is compounded by the cultural negligence of vendors that fail to prioritize security throughout the development of the software and hardware upon which other public and private organizations depend. Despite expensive and expansive security suites, Information Security professionals and network operators can never be certain to what information and network segments attackers already have access. What is certain is that unencrypted sensitive information is the easiest and most obvious target for hackers of every categorization of sophistication. If data are valuable to an organization, then it is valuable to an internal or external threat actor. Intentionally leaving data unencrypted is naïve and negligent. It is akin to surrendering to the attacker because they circumvented the perimeter security and then rewarding them with the highest value commodity contained in the network; information which likely describes subjects who may not have even acquiesced to the collection, storage, transmission, or processing of their data. Countless organizations, especially those relying on legacy technologies, are no longer able to repel malicious cyber campaigns. Organizations can no longer confidently assert the security of systems; instead, they must assume systems compromised until sufficient trust can be gained based on security audits, anti-malware detection systems, artificial intelligence defenses, endpoint security, and other bleeding-edge layered defense-grade security solutions.

The government sector is second only to the healthcare sector in system vulnerability and susceptibility to attack, as measured in total records breached. According to HPE CTO Rob Roy, "Whether it is an insider, a contractor, or a nation state, data theft is rising to epidemic levels in government. Even if an agency is not aware of it, chances are high that data has been stolen or misused without their consent." Of the 36.6 million records exposed in 2016, 13.9 million were exfiltrated from government systems. The average breach requires 229 days to detect. Some incidents or the impact of incidents are not discovered until years later; consequently, the number of records exposed in 2016 as the result of government breaches could far exceed current estimations [2]. Between 2010 and 2016, federal and state agencies publicly disclosed 203 breaches. There was a 40% increase in government sector data breaches in 2016, resulting in 72 data breaches. In each and every incident, attackers exfiltrated PII (SSN, names, birthdates, etc.) Intellectual Property, organizational or operational intelligence, and other lucrative information that could be leveraged to impact the public, critical infrastructure, national security, or additional public and private sector organizations. Approximately half of the 2016 government breaches exposed Social Security Numbers [3]. Numerous other incidents exposed even more sensitive information.

The OPM breach and other federal government breaches have eroded the public's confidence in the federal entities' ability to secure sensitive systems and data against adversarial compromise. In June 2015, DHS, FBI, Congress, and the public were informed that the Office of Personnel Management's (OPM) systems were breached by a threat actor believed to be the Chinese sponsored Deep Panda APT in November 2013, March 2014, and October 2014. The breaches of USIS and Keypoint resulted in the loss of the personal information of 27,000 and 48,439 federal employees respectively. The first OPM breach resulted in the loss of network manuals and information that may have allowed the attackers to conduct subsequent USIS, Keypoint, Anthem, and second OPM breaches. The second and third intrusion into OPM's networks resulted in the loss of 4.2 million personal records and 21.5 million SF-86 forms, affecting former and current federal employees and their family members. Additionally, 5.5 million fingerprint files were also exfiltrated from the system. The 127-page forms contain granular information about federal employees, which a nation state could use for a multitude of purposes, such as creating a veritable database of federal employees. As a result, in the future, federal employees can be specifically targeted for espionage and cyber-warfare campaigns. OPM did not follow cyber security best practices. Further, the hyper-exploitable data were not encrypted because according to Former OPM Chief Information Officer Donna Seymour "Some legacy systems may not be capable of being encrypted." Her supposition is not correct. Data can be encrypted on both legacy and modern systems using advanced encryption methodologies such as the Format Preserving Encryption (FPE) derivative of the AES algorithm. Encryption alone does not stop adversaries, and it would not have prevented the exfiltration of data from OPM systems; however, encryption does inhibit the attackers' ability to act on the data, and it would have greatly diminished the proverbial "Sword of Damocles" that will hang over the United States for decades as a result of OPM's failure to encrypt data during storage, transmission, and processing [4].

Many Public-sector security incidents resulted from attempts to secure legacy technology with increasingly inadequate network and endpoint security solutions such as signature driven antimalware, intrusion prevention systems, etc. Legacy technologies are unsustainable and securing such archaic systems is nigh-impossible. For instance, authentication management solutions can secure the Data and Application layers unless an attacker leverages legitimate credentials. Similarly, Firewalls and similar solutions can act as middleware but cannot prevent traffic interception. Encrypted databases and storage could be infected with malware or subject to exfiltration by a malicious insider. Instead, the organization should focus on modernizing their systems and on data-centric security best practices and encryption technologies that "can protect data no matter where it resides, how it is transported, or even how it is used." Sophisticated data-centric encryption solutions do not impede mission performance and are already widely used in the private sector where "render high-value and PII data useless for cybercriminals while supporting legacy systems and enabling compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), and others." Data-centric layered defenses include encryption, tokenization, data masking, and enterprise key management to protect data at all times, everywhere in the network, during all operations [3]. Since agencies and other public entities have habitually failed to secure citizens' data, legislators and regulators must intervene to ensure that local, state, and federal entities possess the resources to secure and eventually modernize their architectures, and they must mandate that organizations secure data at-rest, in-transit, and during-processing to the best of their capabilities, according to available technologies, such as Format Preserving Encryption, and according to established legislation and regulation.

A Public Legacy of Breaches and Exploitation

Government entities have a moral and legal responsibility to act as role-model data custodians by securing data according to its value or potential for harm if compromised and by protecting consumers from malicious exploitation by cyber-adversaries. Agency leaders must prioritize data protection and legislators must ensure not only that they are required to do so, but also that data are holistically and systematically protected at rest, in transit, and during processing on all agency and third-party systems such that even a sophisticated and persistent adversary that gains access to critical system or caches of sensitive information cannot leverage that access to inflict further harm by exploiting it against the public. The OPM breach was the cyber-Pearl Harbor that catalyzes the awakening of an informed, disgruntled, and vengeful public. Now, when breaches occur, consumers, taxpayers, and constituents demand immediate investigations into the accountability of agency heads, IT personnel, and regulators. "Why was that data not encrypted?" is the first question asked following a successful adversarial exfiltration. Failure to take even minimal cybersecurity precautions, such as encrypting data, can serve as the evidence necessary to determine legal liability, can seed decades of cascading incidents and impacts within the public and private sector, and can abruptly terminate otherwise bountiful careers [5].

Government organizations encounter unique impediments when securing sensitive data. Legacy systems are struggling to process their exponentially increasing volumes of data, let alone bear the computational burden of traditional third-party security, that can only indirectly protect data. Most data-protection techniques only shield data in storage. While these methods prove effective for neutralizing lost or stolen storage devices, they do not protect transient data or decrypted volumes. Further, after a decade of embarrassment due to arguably preventable security incidents, government agencies are trying to regain public trust via operational transparency while attempting to combat emerging threats by sharing threat intelligence between relevant stakeholders. As a result, agencies are required to comply with federal standards and regulations that enhance data security and enable data privacy, such as the Cybersecurity Act of 2015, DFARS CUI, and General Data Protection Regulations (GDPR), the

National Institute of Standards and Technology (NIST), and Federal Information Processing Standards (FIPS) [3].

Legacy systems remain ridiculously prevalent in agency IT architectures. These outdated relics demand an estimated three-fourths of the annual IT budget and cost as much as $0.74 per dollar to marginally secure and maintain (compared to $0.15 per dollar for modern system investments) [6]. Practically every breach of an agency in recent years is at least in part due to the compromise of a legacy system and exceedingly few of those exploitable systems had native data encryption implemented at the time of compromise. The common justification that flustered officials spew when attempting to reprehensibly defend their failure to secure sensitive systems and data is some variation of "the outdated architecture did not support foundational defense solutions such as encryption." This hackneyed adage is an empty and baseless excuse. System modernization is inevitable, and the sooner agencies begin to invest in modern systems constructed with security-by-design and in defense-grade solutions, the sooner critical infrastructure systems and the treasure troves of valuable PII, IP, EHRs, etc. will be secured from adversarial exploitation. Transitioning to modernized infrastructure does not occur overnight. Many of the systems in desperate need of revitalization are also essential for the day to day or minute to minute operations of an organization or region. Lives may dynamically depend on the constant uptime of a system or on operators' immediate access to data. In some cases, especially in the case of "Frankensteined" and solutions or applications that were custom tailored over years or decades, redundancy systems necessary to allow an entity to backup or replace a vital unit without interrupting operations, does not exist. Consequently, in lieu of a convenient and immediate security solution, operators sacrifice security in favor of convenience or necessity because they erroneously believe no other options exist. Instead, while intermediary solutions and modernization systems are developed legacy systems can be secured with application "shims" and virtualization clients on the front end, APIs and encryption applications in the middle, and the legacy system on the backend [5].

Legacy systems are attractive targets for hackers because they are static in their form, they are susceptible to novel attack vectors for which defenses did not exist during their construction, and because IT professionals all-too-often fail to secure the systems or protect the data held within, because they convince themselves that "the system cannot support security or encryption" [7]. Some contend that legacy systems are shielded from cyber-adversaries by their outdated programming languages, aged applications, and antique hardware. This rationalization leads to a false sense of security and complacency. Security-through-antiquity or security-by-obscurity is a myth. Legacy systems are complex and expose an organization to considerable risk due to a lack of support, a dearth of updates and patches, technological incompatibilities, and network opaqueness. Based on FISMA reported data from 2012-2015, for every one percent of spending an agency shifts from maintaining a legacy system, it can expect a five percent reduction in the number of security incidents [8]. Other organizations operating legacy architecture eschew encrypting sensitive data out of fear that the cryptographic processes will slow applications, burden IT infrastructure or otherwise sap finite resources. In the past, encryption did contribute to computational overhead and tax memory and processing resources because entire pieces of data had to be decrypted, using whatever key size was originally used for during encryption, in order to read a portion. Each encryption and decryption operation added microseconds to the transaction time. For some sectors, such as finance or healthcare, these minuscule contributions could aggregate into considerable overhead. As a result, these sectors rejected plans to encrypt data at rest, in transit, and during processing, unless mandated to do so. Contemporary cryptographic algorithms and techniques combined with the added processing power and capacity of modern technology mitigate the overhead and impact on performance resultant from holistic encryption solutions. Further, Format Preserving Encryption, field level encryption, and other solutions empower organizations to determine what data or fields to encrypt or decrypt and what non-sensitive information can remain unencrypted to reduce overhead and facilitate operational efficiency.

Select organizations can justify continued reliance on legacy systems. For instance, it is possible that a tailored application required years of customization and that upgrading to the current version would necessitate years of additional resource expenditures to re-modify the application. Patching and updating may be updating or foregone to mitigate the risk of unintentionally disrupting operations or permanently breaking the system. That said, every disregarded update or patch contributes the massive number of accumulated system vulnerabilities. Each vulnerability can be exploited along one or more vectors by cyber-adversaries incalculable. Eventually, the system becomes steeped in technical debt, and it becomes too difficult or expensive to secure. At this stage, when modernization is the most practical, yet also the most difficult solution, encryption is an inexpensive and invaluable tool for delaying compromise, mitigating exploitation and exfiltration, and wasting threat actors' resources. Investments in strong encryption translate to high-yield investments in time that could not otherwise be purchased. Even for systems diligently secured behind comprehensive layers of security solutions, encryption can serve as faux-insurance against security oversights or solution implantation misalignments. A legacy system fortified behind dozens of security applications and defensive measures can be rendered suddenly vulnerable if it is integrated with modern technology, such as the Internet-of-Things and if security professionals lack the resources or foresight to mitigate nascent attack vectors. Encryption also mitigates some of the risk due to malicious insider's illicit access to valuable data-stores. Again, while not a silver-bullet to prevent compromise, encryption does decrease the risk of harmful impacts against the organization and its data subjects. An attacker that exfiltrates properly encrypted data is left with nonsensical fields that can only be decrypted with either the key or a massive investment in computational resources and time [9].

The private sector IT refresh cycle ranges three to five years; meanwhile, the age of most state system is more accurately measured in decades. State and local governments are especially reliant on antiquated and ill-maintained technologies due to a lack of resources or qualified professionals [10]. To efficiently combat the overwhelming threat landscape surrounding state and local government systems, many have adopted the Federal Information Processing Standard (FIPS) for cybersecurity acquisitions. FIPS 140-2 is the gold standard of encryption solutions. HPE is the first company to receive FIPS 140-2 certification for its SecureData format-preserving encryption package. The solution was the first validated by NIST to meet the strict standards that the federal government now relies on when buying technology from vendors. It also preserves the relationship between encrypted fields of data, and it works with third-party software [11]. FPE facilitates collaboration between stakeholders, the use of big-data analytics, and the adoption of new technologies such as cloud, Hadoop, or IoT solutions while diminishing the risk of data leakage or exfiltration of IP, PII, classified intelligence, and other information [3].

When cloud, modernization, and encryption solutions began to emerge, agencies initially refused to upgrade antiquated systems and applications out of concern that PII and other sensitive information would not be secure or that critical systems might cease functioning. Many of their concerns were founded in false pretenses concerning encryption. Some wrongly believe that encryption will break applications or render legacy applications inoperable because the operation of algorithmically securing the data would alter the format of the information. Rob Roy contends, “The argument that we can't protect legacy systems is no longer the case. NIST validated a new AES method last year that supports protecting legacy systems - this new Format Preserving Encryption (FPE) is data centric, meaning the protection follows the data whether at rest, in use, and in motion, and has the added ability of supporting data sharing and analytics without decryption.” In 2016, NIST standardized “Format Preserving Encryption.” FPE is a form of Advanced Encryption Standard (AES), which encrypts data in the same format. The only difference is that each value is encrypted and that a portion of the values may be disclosed for use or analysis while the remainder of the data remains encrypted. Similarly, identity-based encryption within cloud solutions enhances security because no one organization “holds the keys” to the data. Instead, each organization holds its own root key and individuals authorized to access specific datasets can access those data as needed [5].

Data Integrity Can be Preserved through Encryption

In 2016, NIST published SP 800-38G, establishing standards for Format Preserving Encryption. Their FF1 AES encryption standard enabled government agencies and contractors to use FPE to protect sensitive data-at-rest, data-in-motion, and data-in-use while preserving data formats [3]. Format-preserving encryption (FPE) enables users to encrypt data in a way that mimics its initial format. For example, a nine digit Social Security number encrypted with FPE would become a nine-digit string with different characters from the original, and it could be used in any process that does not require the number to be decrypted. State and local government legacy systems are the most likely to rely on legacy systems requiring rigid input parameters and whose operations could be disrupted by the employment of any encryption algorithm that altered the format of the original value (i.e. expressing a 9-digit SSN as 9 letters) [11]. Older AES methodologies transformed data into long strings that did not match the original data format, could not be used for analytics without decryption, and could not be transmitted to other databases or applications that did not expect the unfamiliar format. Previous NIST standards were only applicable to binary data and it was technologically infeasible to encrypt decimal values while also allowing computers to read the number in its original format. FPE makes it easier and more effective for organizations to encrypt data at-rest, in-motion, and in-use, while preserving its utility and format. It can be sued to render long strings indecipherable in binary and decimal formats. Even if a system is compromised, FPE encrypted data are worthless to attackers. However, analysts can still identify patterns in the encrypted data, run queries, and transmit it to systems around the world without breaking other databases. FPE can leave a small portion of the data deciphered so that it can be used for identification and processing, but it cannot be used to compromise the user. A familiar example of this is being able to see the last four digits of the SSN or credit card number in private sector transactions. The government sector can similarly de-identify sensitive information without necessarily overhauling existing infrastructure.

FPE Reduces Regulatory Investments

Regulatory and legislative compliance is a critical cornerstone of Information Security because mandatory adherence to cybersecurity and cyber-hygiene best practices in the public and private sectors reduces the overall risk of loss, theft, manipulation, or unauthorized dissemination of important data. Non-compliance often results in fines, sanctions, and other penalties, which can amount to millions of dollars annually. An estimated 93% of organizations report challenges meeting compliance requirements. Approximately 49% of organizations reported receiving fines or sanctions for regulatory non-compliance in recent years due to their inability to meet the demands of the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act (FISMA), the Federal Risk and Authorization Management Program (FedRAMP), IRS Publication 1075, Controlled Unclassified Information (CUI), General Data Protection Regulation (GDPR), National Institute of Standards and Technology (NIST standards), and a multitude of other audit standards, all at once because they lack the necessary resources to fulfill all requirements pertinent to their operations. Since encryption and due diligence protection of data is part of practically every regulation, organizations that adopt FPE solutions and accompanying technologies can maximize their investment towards simultaneously meeting portions of all relevant regulations [1].

Mandatory Encryption Can Restore Trust in the Public Sector

Encryption is an organization's last hope when all other defenses have failed to deter an attacker. It is not a panacea. Rather, it is a tool to be used in conjunction with defense-grade layered defense solutions such as anti-malware, whitelisted firewalls, UEBA, etc. Encryption, especially Format Preserving Encryption, is universally possible on legacy and modern systems and no responsible organization can justify failing to protect their data at-rest, in-transit, and during-processing by encrypting the data. Encryption is unique in that it is the only solution that definitely impedes an adversary's ability to exploit exfiltrated data because, in order to profit from or leverage the data in future attacks, the adversary must first expend significant resources breaking the complex encryption securing the data. It is a foundational operation. For the sake of consumers, critical infrastructure, and national security, public and private organizations must at least encrypt their data; even if legislators and regulators have to mandate encryption requirements. Rob Roy explains, “It's really not rocket science, all they need is a mandate to protect the data entrusted to them by US citizens. All data has a lifecycle, and the process to managing it is simple - define what data you need to protect (e.g. PII, PHI, high value data, state secrets), discover it in file shares, databases or content managers, classify it and then apply your policy and protection around it.”

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

[1] "Addressing Compliance With HPE Security". *HPE*. N.p., 2017. Web. 5 June 2017. https://www.hpe.com/h20195/V2/getpdf.aspx/4AA6-8876ENW.pdf

[2] Scott, James and Drew Spaniel. "The ICIT Ransomware Report: 2016 Will Be The Year Ransomware Holds America Hostage". ICIT. N.p., 2017. Web. 7 Mar. 2017. http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf

[3] “Protect High Value Government Data” HPE. N.p., 2017. Web. 5 June 2017.

[4] James, Scott, and Spaniel Drew. "Handing Over The Keys To The Castle: OPM Demonstrated That Antiquated Security Practices Harm National Security". ICIT. N.p., 2015. Web. 5 June 2017.

[5] Roy, Rob. "The 5 Myths Of Encryption - Carahsoft :: Community Trends". Carahsoft.com. N.p., 2017. Web. 5 June 2017. http://www.carahsoft.com/community/the-5-myths-of-encryption

[6] Scott, Tony. "Improving And Modernizing Federal Cybersecurity". whitehouse.gov. N.p., 2016. Web. 1 June 2017. https://obamawhitehouse.archives.gov/blog/2016/04/08/improving-and-modernizing-federal-cybersecurity

[7] Loeb, Larry. "OPM Breach Offers Tough Lessons For Cios - Informationweek". *InformationWeek*. N.p., 2015. Web. 5 June 2017. http://www.informationweek.com/software/opm-breach-offers-tough-lessons-for-cios/a/d-id/1320898

[8] Waterman, Shaun. "Legacy IT Makes Federal Agencies Less Secure, Study Says - Cyberscoop". *Cyberscoop*. N.p., 2017. Web. 5 June 2017. https://www.cyberscoop.com/study-legacy-makes-agencies-less-secure/

[9] Korolov, Maria. "Forgotten Risks Hide In Legacy Systems". *CSO Online*. N.p., 2014. Web. 5 June 2017. http://www.csoonline.com/article/2139382/data-protection/forgotten-risks-hide-in-legacy-systems.html

[10] Miller, Ben. "Federal Certification For Encryption Software Could Help Government Use Legacy System Data, HPE Says". *Govtech.com*. N.p., 2017. Web. 5 June 2017. http://www.govtech.com/biz/Federal-Certification-for-Encryption-Software-Could-Help-Government-Use-Legacy-System-Data-HPE-Says.html

[11] Miller, Ben. "Federal Certification For Encryption Software Could Help Government Use Legacy System Data, HPE Says". *Govtech.com*. N.p., 2017. Web. 5 June 2017. http://www.govtech.com/biz/Federal-Certification-for-Encryption-Software-Could-Help-Government-Use-Legacy-System-Data-HPE-Says.html