SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE WHITE PAPER

Strengthening Information Security with Strong Key Management

October 2021

Secure Technology Alliance
4680 S Downing St.
Englewood, CO 80113

www.securetechalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce, and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Strengthening Information Security with Strong Key Management

Information security risk is an omnipresent concern, impacting both the public and private sectors. To underscore the importance of protecting the U.S. Federal Government's computer systems, the White House issued an Executive Order (EO) on improving the nation's cybersecurity in May 2021.[1] The EO dictates that federal agencies must adopt data encryption to the maximum extent consistent with federal and other applicable laws.

While legislative requirements have a far-reaching impact, it is important not to overlook how the coronavirus pandemic caught the world by surprise. The workforce and employers, including the U.S. Federal Government, were forced to rapidly adopt new behaviors. One of the most obvious impacts on how we work is the dramatic increase in employees working remotely.

A recent McKinsey publication "The future of work after COVID-19" indicates that 20 to 25 percent of the workforces in advanced economies could work remotely between three to five days a week without a loss of productivity.[2] This finding suggests that there could be four to five times more remote employees than before the pandemic.

As working from home has become the new normal, organizations including the federal government are accelerating their digital transformation, with information security becoming an opportunity and concern all at once. Since most employees have been forced to work remotely, this strain has become a stress test on the information security infrastructure.

Unsurprisingly, Wi-Fi networks for residential use may not provide the same level of cybersecurity protection as the traditional office Wi-Fi environment. Furthermore, home networks are likely easier for hackers to penetrate. The increase in remote work calls for urgent implementation of an information security framework based on zero trust. Meanwhile, information security leaders undergoing digital transformation recognize that protecting customer privacy data and enabling a digital workforce are the biggest stakes ahead. The following critical actions will define an effective information security blueprint. To mitigate the potential impact of a compromise, it is crucial to minimize intruder access to data and sensitive information on disk. Now more than ever, organizations must lead with a zero-trust strategy for the protection of their data and assets, especially in the wake of COVID-19.

A zero-trust implementation is designed to protect data where it resides, practice a minimalistic access approach, and require access to resources to be granted in advance and to be continuously authenticated. Most importantly, access to the zero-trust network is considered hostile until proven otherwise.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] https://www.mckinsey.com/business-functions/organization/our-insights/grabbing-hold-of-the-new-future-of-work

It is crucial to consider hardware security even before the server is manufactured and to choose a computer hardware manufacturer with a strong security commitment, from sourcing raw materials to secure recycling of storage devices and until data server sunsetting.[3]

Developing an end-to-end information security plan is a team sport. Since the best zero-trust plan probably cannot stop insider threats or system attacks via a compromised account, IT security must monitor data sources, such as network flow data and database server activities. By correlating network activities with the abnormalities at the application and user account level, IT would be in a much better position to detect incidents of compromised user credentials or hijacked devices. IT should also periodically assess how access permission is granted, managed, and monitored to mitigate accidental misuse and intentional exploitation across the information security landscape.

Data breach could not only interrupt daily business operations in the public and private sectors, but also leaves organizations vulnerable to legal liabilities and bad press. In addition to authorizing and authenticating user access to all resources, encryption is a viable approach to safeguard sensitive and confidential public sector information from prying eyes.

Although encryption can prevent stolen content from being misused, it cannot stop data theft. Data encryption is often used to secure data in transit and data at rest by converting data from readable or plain text format into an unreadable ciphertext format so that encrypted content is unreadable until decrypted. Advanced Encryption Standard (AES) has been used by the U.S. government and consumer technologies around the globe.

The million-dollar question is whether the encrypted data can ever be hacked. As encrypted data in transit travels across networks, malware may sniff the data. Encrypted data at rest may also be vulnerable to malware attacks as well as unauthorized use. Hackers could access encrypted data if they compromise the encryption keys via phishing and social engineering techniques.[4] Therefore, the “key keepers” must always be on alert.

An irrefutable approach to strengthening information security is the Hardware Security Module (HSM) – the foundation of trust in securing digital transformation and the trust anchor for cryptographic systems. As the use of encryption to protect sensitive and confidential information proliferates, there is a considerable increase in demand for HSMs. These cloud-ready, blockchain-ready, and post-quantum HSMs are secure, tamper-resistant hardware that store cryptographic keys and support cryptographic processing such as encryption. Securing the integrity and confidentiality of cryptographic keys with an HSM can help prevent encryption keys from being stolen or misused.

A Key Management Interoperability Protocol (KMIP) v2.1 certified HSM with market leading support for third-party applications and pre-qualified solutions can help address data security and data privacy priorities, regardless of whether the data is stored on premises or across hybrid cloud environments.

[3] https://www.forbes.com/sites/moorinsights/2021/07/13/mapping-hpes-zero-trust-efforts-to-the-current-cyber-threat-landscape/?sh=5c6bd84657d9

[4] https://www.wired.com/insights/2013/05/9-biggest-data-encryption-myths-busted-2/

Strong hardware-based security is a preferred solution to help prevent data loss or data breach while offering the best performance, optimal total cost of ownership (TCO), and peace of mind through strong hardware-based security. For example, one of the largest healthcare and insurance providers takes advantage of the centralized view of all nodes and keys through a single pane of glass to help protect data across tens of thousands of servers globally. This client can respond faster when security issues do occur. Thanks to the separation of duties and implementation of dual-access control, the client has also achieved compliance with the most stringent U.S. Health Insurance Portability and Accountability Act (HIPAA).

Encryption paired with effective key management as a dynamic duo can help protect sensitive and confidential information. If the keys are compromised or lost, there is a good chance that users might be locked out of their own data. Effective key lifecycle management is therefore top of mind for IT and key management.

Key management may arguably be the most critical component of the information security stack. A key lifecycle management plan anchored on a well-designed key management system can help U.S. Federal agencies and other organizations manage perceived risks and realize the full benefits of encryption. Many organizations rely on effective key management to generate, import, and export keys in support of hundreds of thousands of devices.

Tokenization is another proven technology for enabling the secure substitution of a surrogate value for sensitive data. Replacing a sensitive data element with one that has no financial value can help reduce the complexity of the data protection solution simply because the cryptography and key management required to implement a tokenization solution is handled by the token vault, which is the secure token repository.

Tokenization is often sought after to satisfy compliance and security initiatives that address mandates including PCI and EMV. Effective tokenization requires a well-designed and cryptographically secure token connection profiles with TLS 1.2.

Perhaps nothing is as important as protecting customer privacy and preserving brand trust. Implementing the right combination of information security capabilities is an important step in designing an organization's zero-trust plan – growing as a trusted enterprise, avoiding data breaches, and achieving FIPS 140-2 compliance.

To learn more, please see these resources:

Watch the Key Encryption to Strengthen Information Security webcast:
https://www.securetechalliance.org/secure-technology-alliance-webinar-to-highlight-key-encryptions-role-in-securing-federal-agencies/

Download ESKM and HPE ProLiant Deliver Enhanced Protection for Data at Rest brief:
https://hsm.utimaco.com/executive-order-on-protecting-us-federal-data/

Publication Acknowledgments

This white paper was developed by the Secure Technology Alliance to highlight key encryption's vital role in securing critical data, implementation challenges, and integration solutions.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

Trademark Notice