TRUSTED COMPUTING: AN EFFECTIVE APPROACH TO CYBERSECURITY DEFENSE

April 2013

Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 | Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Executive Summary

The Trusted Computing Group (TCG) is a non-profit organization that creates open standards related to information security. The standards created by TCG are widely implemented across all sectors to address the formidable threats posed by sophisticated attackers. This document describes the technology and standards developed by TCG, documents related best practices, points out gaps, and recommends next steps. The complete list of recommendations is summarized at the end of the document.

Introduction

On February 26, 2013, the National Institute of Standards and Technology (NIST) issued a Request for Information (RFI) on Developing a Framework to Improve Critical Infrastructure Cybersecurity[1]. After gathering information on available techniques for defending against cyber attacks and gaps that should be filled, NIST plans to issue a Cybersecurity Framework that can guide organizations in reducing cybersecurity risks for critical infrastructure. The Trusted Computing Group is pleased to respond with this document.

The Trusted Computing Group[2] (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. TCG has more than 130 members, including for-profit, non-profit, and government organizations from around the world. TCG and its members over the last ten years have developed dozens of standards that have been implemented in thousands of products and adopted by international standards organizations including ISO and IETF. To date, almost two billion endpoints have been secured using TCG standards.

Because the TCG standards support a hardware-based root of trust (HRoT), they are an important design element that helps address important cybersecurity threats to critical infrastructure. HRoT strengthens the defense in a variety of endpoints, servers, networks and other areas, providing protection from sophisticated attacks, but the cost of a HRoT is quite small (generally less than a dollar and effectively free if provided by an existing component).

TCG standards are in use today by customers across a wide range of critical infrastructure sectors: government, finance, health care, manufacturing, utilities, etc. While these organizations tend to be quite reticent about publicly disclosing information about their security measures, this document provides a summary of uses of TCG technologies. More details including customer case studies and copies of the TCG specifications may be found on the TCG web site: http://www.trustedcomputinggroup.org.

Risk Management

TCG recognizes the value and importance of a framework of common risk management practices across organizations and sectors. There are challenges associated with the developing of such a framework that warrant close examination.

- By its nature, critical infrastructure is fundamental to all sectors of the U.S. economy. No organization can afford to ignore the cyber risks to critical infrastructure in assessing its own risks. Cybersecurity has become an integral component of national security, corporate security, and personal security.

[1] http://www.nist.gov/itl/csd/upload/fr_noticerfi_framework_cybersecurity_2-26-13.pdf

[2] http://www.trustedcomputinggroup.org

Recommendation:

The NIST Cybersecurity Framework should help all organizations understand the cyber risks they face today.

- Because of the scale of the cyber threat and because critical infrastructure is highly interdependent, no organization can fully address its cyber risks alone. Cooperative efforts are necessary and open standards are the best way to achieve such cooperation.

Recommendation:

The NIST Cybersecurity Framework should support sharing information about cybersecurity threats across organizational boundaries, using open standards. These standards should include a consistent schema for categorizing, labeling, and handling risk and threat information.

TCG can assist with this task. For example, part of the foundational work that is needed to further enhance cybersecurity frameworks and guidelines is to define a common taxonomy to represent the various levels of endpoint security and identity assurance (similar to NIST SP 800-63). TCG can help develop a device identity and state framework taxonomy in an open and transparent way that can help foster a common expression of the device attributes for making cybersecurity risk management decisions. In doing so, TCG could make use of ontologies and taxonomies that already exist in the area of cybersecurity and fill gaps that have not yet been addressed.

Use of Frameworks, Standards, Guidelines, and Best Practices

TCG, through the efforts of its members in its Work Groups, has developed several important technologies that have broad applicability in reducing cybersecurity risks. These technologies are defined in TCG specifications in such a manner that any party may implement the technologies in a commercial product or open source implementation. So long as the implementation properly implements the TCG specification, it should be interoperable with other compliant implementations. For customers who want to ensure that the products they're using are actually compliant with the TCG specifications, TCG offers a certification program whereby products are tested and certificates issued by TCG for products that pass the necessary tests.

The following bullets describe the TCG technologies that are most applicable to cybersecurity for critical infrastructure.

- **Trusted Platform Module**

  The most widely known and implemented TCG technology is the Trusted Platform Module (TPM)[3]. Most commercial-grade laptops shipped in the last six years include a TPM. Some desktop and server computers also include one and it enables integrity and assurance in distributed computing, such as cloud and other virtual environments. The TPM is a hardware module that supports secure key storage, cryptographic functions, and integrity measurement. These capabilities enable strong user and device authentication, secure storage, and hardware-based verification of firmware and software integrity.

  TPM has been used widely for strong authentication across all sectors. TPMs can meet the requirements for strong user authentication[4] by using a private key stored on the TPM in their device.

[3] https://www.trustedcomputinggroup.org/solutions/authentication

[4] NIST SP 800-63 Level 3 or 4

Even when TPMs are not needed for user authentication, they can be used for strong device authentication. For example, NSA IAD recommends using TPM for strong device authentication when using Windows BitLocker.[5] Because TPM works with existing authentication technologies using PKI or shared secrets, it's fairly easy to deploy for authentication.

Recommendation:

> The NIST Cybersecurity Framework should include Trusted Computing and the use of TPM for device and user authentication

TPM can also be used to verify firmware and software integrity. NIST SP 800-155[6] describes the use of a TPM to protect against firmware compromise. Microsoft Windows 8 implements some of these recommendations[7], measuring early stages in the boot sequence so that they can be verified by anti-malware software. Google's Chrome OS uses TPM to prevent firmware and software rollback[8]. And IBM's Power Systems[9] use virtual TPMs to ensure that virtual machine images are booted securely.

Recommendation:

> The NIST Cybersecurity Framework should encourage widespread use of TPM-based integrity checks.

- **Self Encrypting Drives**

All drive manufacturers now offer Self Encrypting Drive (SED)[10] technology based on TCG's OPAL series of specifications[11]. For only a modest cost increment (generally <$5 per drive), SEDs provide a huge increase in security and performance. All data on the drive is always encrypted, using hardware encryption built into the drive. Performance gains over software encryption are enormous while security improves as well because the encryption key never leaves the drive with an SED. Perhaps the biggest benefit is that the drive can be completely and securely erased by simply sending a properly authorized command telling the drive to generate a new encryption key. Previous erasure techniques such as degaussing and physical destruction are highly inefficient in comparison.

Adoption of SEDs has been projected to grow rapidly[12] over the last few years. A significant percentage[13] of mobile devices are lost or stolen each year, often with unencrypted confidential data –

[5] http://www.nsa.gov/ia/_files/factsheets/I731-FS-20R-2007.pdf

[6] http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

[7] http://technet.microsoft.com/en-us/library/jj131725.aspx

[8] http://www.chromium.org/developers/design-documents/tpm-usage

[9] http://www.ibmsystemsmag.com/power/Systems-Management/Security/PowerSC_intro

[10] https://www.trustedcomputinggroup.org/solutions/data_protection

[11] https://www.trustedcomputinggroup.org/developers/storage

[12] http://www.forbes.com/sites/tomcoughlin/2011/09/27/encrypted-drive-adoption-to-address-the-costs-and-dangers-of-insecure-storage-devices/

posing a sizable risk to businesses and individuals. For less than the cost of assessing what data was lost, the addition of SED can eliminate the risk of data breach. Because the incremental cost of SEDs is small, SEDs should be considered for universal adoption.

Recommendation:

> The NIST Cybersecurity Framework should include the use of SEDs that implement the OPAL standards for all long-term data storage.

- **Trusted Network Connect**

TCG provides a wide-ranging set of network security standards called Trusted Network Connect (TNC). The TNC standards include support for endpoint assessment with continuous monitoring, Network Access Control (NAC), and security automation. Before we continue, we will define each of these terms in a single paragraph.

Endpoint assessment is the process of assessing the security of an endpoint. Endpoint assessment is a fundamental part[14] of cybersecurity defense today. High quality communications protocols and cryptographic algorithms make encrypted communications hard to intercept and decrypt. Thus, attacks have shifted towards compromising the endpoints of the communications, such as laptops, smartphones, tablets, servers, printers, and other network-connected devices. Assuring the security of these endpoints is paramount. While there are many ways to improve the security of endpoints (secure software development, hardening, etc.), there is only one reliable way to measure their security: endpoint assessment. Many techniques are used for endpoint assessment: local scans, unauthenticated scans, authenticated scans, and (most secure and reliable) hardware health checks[15]. Through these techniques, the security of an endpoint can be checked when it connects to a network and monitored continuously while it is connected. If a problem is discovered, the endpoint can be quarantined and remediated.

Network Access Control (NAC) is the process of controlling access to a network based on various factors such as user identity and role, endpoint identity and security, and/or user and endpoint behavior. NAC is widely used for secure networks and considered a best practice[16] in those environments. At a minimum, network access should be restricted to only authorized users and devices. Unauthorized users and devices can be blocked or directed into a “honeynet” where they can be monitored or restricted. Adding endpoint assessment permits endpoints with security problems (infected or vulnerable) to be rapidly detected and quarantined to make sure that they do not infect others. While in quarantine, their security problems can be automatically or manually remediated. Finally, user and/or endpoint behavior monitoring can be integrated with NAC so that bad or suspicious behavior (e.g. port scanning) leads to reduced network access.

[13] According to insurance company Asurion, 10% of cell phones are lost or stolen each year. Various studies and testimony cited at http://www.bcs.org/upload/pdf/laptop-loss.pdf show the comparable rate for laptops ranges from .1% for high-security organizations to 1% for commercial enterprises.

[14] Endpoint assessment is critical to controls 1, 2, and 3 of the SANS Top 20 Critical Security Controls. (http://www.sans.org/critical-security-controls). NIST SP 800-155 also calls for endpoint assessment.

[15] NIST SP 800-155 describes how to assess endpoint firmware using a HRoT such as a TPM.

[16] SANS Top 20 Critical Controls, “Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.”

Security Automation refers to tools, processes and flows of real-time information that can be used to automate rapid responses to cyber security events. By reducing human intervention a security automation system also enables more effective use of scarce information security talent in an organization. TNC standards focus on the flows of real-time information by enabling sharing of actionable information among security systems within the organization. This allows, for example, a behavior sensor to notify a NAC system of improper user or endpoint behavior so that the endpoint can be quarantined, typically without human intervention.

The TNC standards have now been accepted as IETF standards[17] also, making them the only internationally recognized standards for endpoint assessment and NAC. They provide complete support for endpoint assessment and NAC and have been implemented in dozens of products and millions of devices since that time. When an endpoint has a TPM, the TNC standards support TPM-based hardware health checks. However, they also include explicit support for legacy devices without a TPM or SED.

Recommendation:

> The NIST Cybersecurity Framework should include the TNC standards for endpoint assessment and NAC.

Recommendation:

> The NIST Cybersecurity Framework should recommend further development of security automation technology using open standards such as the TNC standards.

The creation of secure overlay networks for ICS/SCADA[18] environments is another innovation in network security based on the TNC standards. TCG recently published (for Public Review) an IF-MAP Metadata for ICS Security[19] specification that fits into an ISA[20] architecture for protecting ICS devices by ensuring that they only communicate with the proper authorized ICS and SCADA devices and ignore unauthorized devices. While this work is not yet mature, the direction is promising.

Recommendation:

> The NIST Cybersecurity Framework should encourage continued development of ICS/SCADA security technology, using open standards. Other sectors where network-connected systems need to securely exchange critical/sensitive information with properly authorized devices (e.g. health care and financial) should investigate using similar technologies and related standards.

[17] The Internet Engineering Task Force (IETF) has adopted three of the TNC standards as Internet Proposed Standards. These are IF-M (equivalent to IETF RFC 5792), IF-TNCCS (IETF RFC 5793), and IF-T for TLS (IETF RFC 6876). One more TNC standard is in IETF's approval stages now: IF-T for EAP (known in IETF as PT-EAP). Once this final standard is approved as an IETF RFC, all of the TNC endpoint assessment standards will be approved by IETF.

[18] Industrial Control Systems / Supervisory Control And Data Acquisition

[19] https://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_ics_security

[20] International Society of Automation

Conclusion

TCG applauds the RFI's focus on standards, guidelines and best practices. Efficient cybersecurity defense requires cooperation among defenders, which requires the use of open standards while remaining flexible to accept and encourage new innovations. TCG will continue to focus on building open and flexible technologies and standards for cybersecurity.

Summary of Recommendations

This section repeats the recommendations given above.

Recommendation:

The NIST Cybersecurity Framework should help all organizations understand the cyber risks they face today.

Recommendation:

The NIST Cybersecurity Framework should support sharing information about cybersecurity threats across organizational boundaries, using open standards. These standards should include a consistent schema for categorizing, labeling, and handling risk and threat information.

Recommendation:

The NIST Cybersecurity Framework should include Trusted Computing and the use of TPM for device and user authentication.

Recommendation:

The NIST Cybersecurity Framework should encourage widespread use of TPM-based integrity checks.

Recommendation:

The NIST Cybersecurity Framework should include the use of SEDs that implement the OPAL standards for all long-term data storage.

Recommendation:

The NIST Cybersecurity Framework should include the TNC standards for endpoint assessment and NAC.

Recommendation:

The NIST Cybersecurity Framework should recommend further development of security automation technology using open standards such as IF-MAP.

Recommendation:

The NIST Cybersecurity Framework should encourage continued development of ICS/SCADA security technology, using open standards. Other sectors where network-connected systems need to securely exchange critical/sensitive information with properly authorized devices (e.g. health care and financial) should investigate using similar technologies and related standards.