TRUSTED COMPUTING GROUP™

ARCHITECT’S GUIDE: CYBERSECURITY

October 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 and Action Items

Enterprises are under attack — and the frequency and severity of the resulting breaches continues to escalate. No one is immune, and the odds of success remain in attackers’ favor. A single employee, clicking on a link in a phishing email, can be all an attacker needs to establish a beachhead inside an enterprise network that can be used to steal secrets or sabotage systems.

This Architect’s Guide shows enterprise security architects how they can design and deploy successful, highly automated security solutions based on open architecture and standards to solve today’s most pressing cybersecurity challenges.

Critical strategies for architects include:

1. **Pursue consistent approaches** based on industry standards
2. **Restrict access** to sensitive information and systems
3. **Layer security** to improve defenses and contain breaches
4. **Employ authentication** to verify identity and security policy compliance
5. **Encrypt storage** to protect secrets
6. **Automate security** to rapidly identify threats, and block and remediate attacks

Introduction / Cybersecurity Drivers

TCG's cybersecurity standards address the four top cybersecurity challenges facing businesses today:

Prevent downtime: The single biggest cost stemming from cyber attacks is lost revenue owing to network and system downtime, which prevents employees from working or customers from buying. In the oil and gas sector, the cost of a major cyber attack that causes 24 hours of downtime can exceed $8 million. But the costliest cyber crimes involve DDoS attacks, such as the Operation Ababil disruption campaign against U.S. banking websites that began in 2012, or the use of malware to wipe 48,000 systems used by South Korean banks and broadcasters.[1]

Safeguard crown jewels: The goal of many APT attackers is to steal an organization's most valuable intellectual property. Successful APT attacks can be devastating: Attacks attributed to China against U.S. defense contractors, for example, resulted in information theft that calls into question the combat-readiness of some new military weapons systems, including the F-35 Joint Strike Fighter.

TOP CYBERSECURITY CHALLENGES

1. **Prevent Downtime**
2. **Safeguard Crown Jewels**
3. **Maintain Reputation**
4. **Protect Critical Infrastructure**

Maintain reputation: Security breaches can be a public relations nightmare. Hacktivists associated with Anonymous, for example, have publicized their causes by hacking into businesses — including Sony and Stratfor — and releasing customer records, credit card numbers and sensitive emails. Breaches of LinkedIn, Last.fm and eHarmony, meanwhile, only came to light when customer records surfaced on underground hacker forums, calling into question those businesses' cybersecurity preparedness.

Protect critical infrastructure: The vast majority of critical infrastructure systems — comprising the power, oil, water, telecom, finance and transportation industries — are privately owned. The networked industrial control systems that support these industries are aging, largely unsecured, and exploitable. Congress continues to weigh laws that would require businesses to prove that their critical infrastructure systems are secure. Attacks against these systems are not theoretical, as the highly destructive Stuxnet and Saudi Aramco attacks demonstrate.

WHY APT ATTACKS ARE SO DAMAGING

An Advanced Persistent Threat (APT) refers to an online attack that is part of a long-term strategy with specific goals and sophisticated methods. APT attackers may work for months or years to research targets, infect systems, reconnoiter the enterprise network, and then either steal secrets or attempt to cause maximum hack-attack damage.

Solution Overview

Businesses and government agencies are under attack. By creating an effective cybersecurity program, organizations can blunt these attacks and safeguard valuable intellectual property and computing resources.

The Trusted Computing Group (TCG), a not-for-profit organization comprised of information security experts from leading organizations, helps enterprises build better cybersecurity programs through open standards.

This Architect's Guide provides a basic framework for cybersecurity that's based on standards and architectures from the Trusted Computing Group. TCG has already developed security solutions for computers and servers based on the Trusted Platform Module (TPM), for mobile devices through the TPM Mobile, for data integrity and privacy based on self-encrypting drives (SEDs), and for enterprise networks based on the Trusted Network Connect (TNC) specifications (see sidebar, page 5).[2]

These open standards are implemented in a variety of products and collectively provide a comprehensive cybersecurity approach. When used in conjunction with standards from other organizations, the approach described in this guide enhances an organization's overall information security posture. An important part of this solution is a unified approach to cybersecurity, backed by detailed security policies that are applied consistently, thus helping minimize the likelihood — or ramifications — of human error.

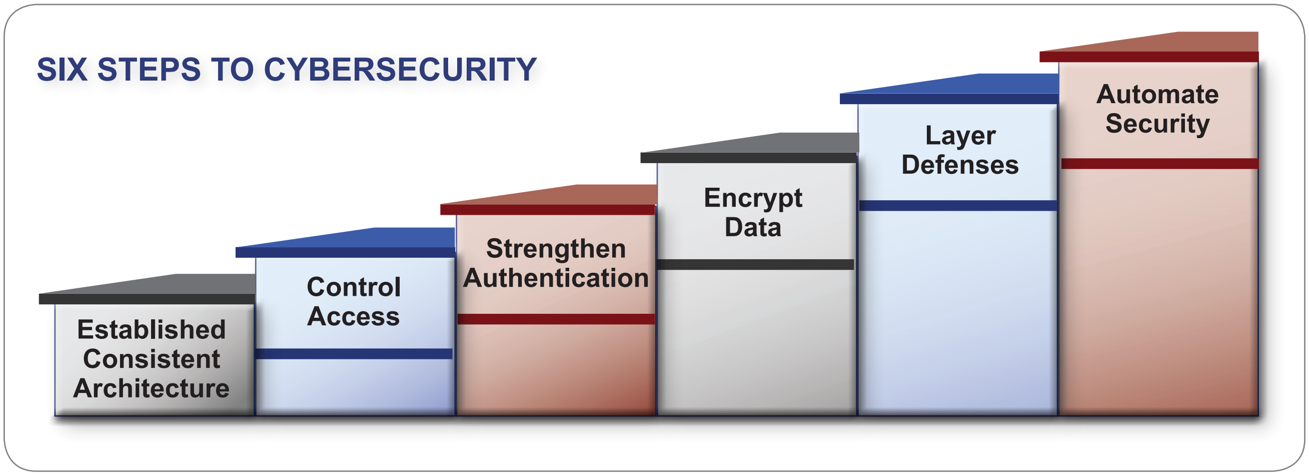
[1] http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6 .pdf

[2] For detailed guidance: http://www.trustedcomputinggroup.org/resources/tcg_architects_guides

Six Steps to Cybersecurity

For maximum effectiveness, cybersecurity programs should take the following six steps:

1. **Establish consistent architecture.** Use a consistent security architecture across all devices and networks. This enables security policies to be written once, then enforced consistently with controls for every conceivable access scenario: corporate user, contractor, managed or unmanaged "bring your own device" (BYOD), guest WiFi, and more.
2. **Control access.** Know who and what's on your network, check the health of the devices on your network, and then use access controls to ensure that only authorized personnel with secure devices are granted access to sensitive data.
3. **Strengthen authentication.** Require strong user and machine authentication for any accesses to your most valuable assets. For many businesses, crown jewels involve intellectual property — such as the secret formula for your product — and customer databases.
4. **Encrypt data.** Encrypt all sensitive data in transit and at rest. The average cost of a data breach, according to Ponemon Institute, is $5.5 million.[3] Encrypting stored data — which prevents data from being exposed, and exempts organizations from issuing expensive data breach notifications — costs far less. But as demonstrated by ongoing breaches, from lost laptops at NASA to unsecured Washington state court system servers, too many organizations haven't gotten the message.
5. **Layer defenses.** Layer security defenses, not only to repel attacks but to better contain intrusions. According to the 2013 Verizon Data Breach Investigations Report, a phishing attack campaign that uses just six emails has an 80% chance of seeing an included link or attachment get clicked on or opened by a recipient.[4]
6. **Automate security.** Automate security controls to provide rapid attack detection and response. Automation frees scarce information security resources from dealing with spam, malware, and other nuisances, allowing them to focus on more high-value security activities, such as refining policies and remediating attacks. With the BYOD[5] trend, as more employee-owned devices touch the corporate network, automation ensures that these devices keep sensitive information secure at all times.[6]


SIX STEPS TO CYBERSECURITY
Established Consistent Architecture
Control Access
Strengthen Authentication
Encrypt Data
Layer Defenses
Automate Security

[3] http://www.ponemon.org/data-security

[4] http://www.verizonenterprise.com/DBIR/

[5] http://www.trustedcomputinggroup.org/resources/architects_guide_mobile_security_using_tnc_technology/

Implementing The Six Steps to Cybersecurity

Building a cybersecurity program from scratch would be a daunting challenge for any organization. Accordingly, TCG's standards and frameworks have been designed to ease the implementation of the six steps described above. Here's how to craft a related implementation plan:

1. **Establish consistent architecture.** Create security policies that clearly state requirements and rules for everything from security audits and data breach response to network and mobile security, then use automated controls to enforce these policies. Every organization should implement the four controls detailed under the Australian Strategies To Mitigate Targeted Cyber Intrusions, which will block 85% of targeted cyber intrusions.[6] The SANS Institute's 20 Critical Security Controls list, meanwhile, provides an even bigger information security boost.[7] Indeed, the U.S. State Department reported that implementing those 20 controls reduced its cybersecurity risks by 94%. To create a consistent cybersecurity architecture, consider off-the-shelf solutions built using open standards such as the TCG frameworks. This approach facilitates greater interoperability, cost reduction, scalability, reusability and overall security effectiveness.[8]
2. **Control access.** Security policies spell out which employees should have access to which information. To maintain access controls, many businesses use a TNC-enabled policy server — which assesses what access levels should be granted to any given endpoint — backed by a TNC-enabled enforcement point, which enforces these access decisions. While specific approaches will vary based on network topology, enforcement points can be a switch, wireless access point, VPN gateway, firewall, or server. Numerous products and vendors support TNC-based access controls, which are widely implemented.
3. **Strengthen authentication.** For authentication, more is required than usernames and passwords, or "fingerprinting" devices. Both banks and Facebook, for example, use step-up authentication to require additional access credentials to authorize high-risk or unusual behavior.[10] Many enterprises are also employing a hardware root of trust, using non-removable hardware such as the TPM built into many laptops, desktops and mobile devices, which can also assess device compliance with security policies.[11]

The U.S. State Department reported that implementing The SANS Institute's 20 Critical Security Controls reduced its cybersecurity risks by 94%.

4. **Encrypt data.** Modern operating system tools — BitLocker (Windows) and FileVault (Mac OS X) — provide software-based full-disk encryption to protect data at rest. But for best results, use self-encrypting drives. These offer higher-performance, hardware-based encryption, ensuring that attackers can't bypass the encryption, and users won't even know it's there.[12]
5. **Layer defenses.** Effective security requires layered defenses. For starters, build multiple rings of access control — especially via VPN access gateways and firewalls — to lock down networks, even from inside. Whenever possible, install behavioral profiling and intrusion prevention tools that will monitor for unauthorized access attempts or odd behavior, then restrict access and alert security personnel if a suspected intrusion attempt is detected.[9] For unmanaged devices, limit their access to corporate data.
6. **Automate security.** Automation is essential for ensuring that devices and network behavior comply with established security policies. Sensors installed on endpoints, firewalls and other networked resources feed into an intrusion detection and analysis system. When violations are detected — as a result of APT-delivered zero-day exploits, insider attack, malware-infected smartphones, or any other threat — signals sent via a TNC information-sharing protocol can initiate network access restrictions for an endpoint or even full quarantine and remediation. As that demonstrates, linking infrastructure and security tools together facilitates response systems that make dynamic, intelligent, automated decisions, thus reducing risk and increasing remediation speed.[13]

[6] http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

[7] http://www.sans.org/critical-security-controls/

[8] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility-roots-of-trust_regenscheid.pdf

[9] http://www.trustedcomputinggroup.org/resources/tcg_byod_architects_guide

[10] http://www.trustedcomputinggroup.org/resources/tcg_comply_to_connect_architects_guide

[11] For more information: http://www.trustedcomputinggroup.org/resources/architects_guide_mobile_security_using_tnc_technology

[12] For more information: http://www.trustedcomputinggroup.org/resources/tcg_data_security_architects_guide

[13] For more information: http://www.trustedcomputinggroup.org/resources/tcg_security_automation_architects_guide

WHAT IS IT?

Trusted Network Connect (TNC)

TCG's Trusted Network Connect[14] network security architecture and open standards help businesses create and enforce security policies as well as facilitating communication between security systems. Using TNC standards, network managers gain better visibility into who and what is on their network, and whether devices remain compliant with policies. More than two dozen vendors of commercial and open source products support TNC standards in their products.

Self-Encrypting Drive (SED)

Self-Encrypting Drives[15] silently and automatically encrypt all user and system data, making sure this information doesn't fall into the wrong hands if the device or drive gets lost. Such drives may also be remotely wiped if they're lost or stolen.

Trusted Platform Module (TPM)

The Trusted Platform Module[16] is a hardware security component built into a computing device that provides a hardware root of trust for user and device identity, network access, data protection, and more. TPMs are built into more than half a billion end systems, including many laptops and mobile devices.

What Is TPM Mobile?

TPM Mobile[17] is a scaled-down TPM designed for mobile environments, which retains the ability to cryptographically store passwords and digital keys, for example, to verify the device's identity. TPM Mobile is expected to be publicly available in the near future.

Future Proof: Build A Cybersecurity Foundation

Building a cybersecurity program that's based on vendor-neutral open standards maximizes interoperability, scalability, and reusability. This makes good business sense. Furthermore, it enables enterprises to create a foundation that they can easily extend in the future to get even more from their cybersecurity investments.

TCG standards work, notably, is currently underway to help deliver even more capabilities:

- **Actionable threat intelligence:** Crowdsourcing information on how attackers — APT or otherwise — operate, transforming this into machine-readable threat intelligence, and facilitating easier information collection will enable businesses to further refine their automated defenses.
- **Near real-time threat response:** Work continues on refining how technology can be used to safely detect, block and remediate attacks without human intervention. Blocking attacks — and launching cleanup operations — more quickly and completely minimizes a business' risk of data breach exposure.
- **Improved analytics and visualization:** Refined attack analysis tools and security dashboards will deliver better at-a-glance, actionable cybersecurity intelligence to security managers, helping them focus on what's most critical.
- **Industrial Control System Security:** TCG's IF-MAP Metadata for ICS Security[18] will help businesses improve the security of essential — but too often unsecured — industrial control systems used in many critical infrastructure environments.

Conclusion

Highly effective cybersecurity programs can be built and maintained in an open and vendor-neutral manner, thanks to Trusted Computing Group standards that are supported by many computing, storage, wireless, and network products and services. By taking this approach, enterprises can create cybersecurity programs that are agile, strong, and fast.

Call to Action

- Define your own cybersecurity architecture, based on the six steps described above
- Demand TCG-certified components from vendors
- Detect changing threats and continuously adapt
- Visit www.trustedcomputinggroup.org for more information
- Email admin@trustedcomputinggroup.org with any questions

[14] http://www.trustedcomputinggroup.org/developers/trusted_network_connect

[15] http://www.trustedcomputinggroup.org/solutions/data_protection

[16] http://www.trustedcomputinggroup.org/solutions/authentication

[17] http://www.trustedcomputinggroup.org/developers/mobile

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