ARCHITECT'S GUIDE:

BYOD Security Using TCG Technology

June 2012

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

Bring your own device (BYOD) is a rapidly evolving challenge to corporate and information technology (IT) cultures. Instead of having all computing devices supplied by the employer, employees are eager to bring their own smartphones, tablets, and laptops into the work environment.

Unlike many changes in the corporate environment, employees have embraced BYOD and are excited about using their own devices for work and enjoying increased empowerment, agility, mobility, and simple convenience. An effective BYOD program can be a source of increased employee satisfaction and productivity. However, dealing with security and establishing trust in such devices must be the foundation of the BYOD program. Otherwise, sensitive corporate data may be exposed to and even stored on thousands of user-owned devices with inadequate controls, leading to an increase in data breaches.

Standards created by the Trusted Computing Group (TCG) can be used today to implement BYOD security. Developed over the last decade, these standards provide increased security for servers, desktop computers, portable devices, data at rest and in motion, and the network, as well as weak links in network security such as printers and other unmanaged devices.

This Architect's Guide shows IT executives and architects how TCG technologies can be applied today to solve an important enterprise problem: BYOD security.

Critical strategies for architects include:

1. **Continuous assessment** of the user, device, network, physical location, etc.
2. **Reducing risk** by provisioning countermeasures
3. **Controlling access** to sensitive resources based on established corporate policies
4. **Monitoring and responding** using standards-based techniques, automatic or manual

Introduction / BYOD Use Case

Companies and employees are increasingly exploring and embracing the concept of BYOD in the workplace. BYOD allows employees, partners, contractors, or guests to have an appropriate level of access to the enterprise network through their own mobile devices. The advantages are obvious:

- The company obtains increased productivity and possibly reduces equipment cost
- The user has the convenience of carrying a single personalized device that they chose based on their own criteria

Updates and improvements occur almost daily to mobile products (smartphones, tablets, and other mobile devices). The flood of announcements include an increasing number and variety of available products with enhanced capabilities, and greater usage for existing products through new apps. What's not to like? According to Forrester[1], nearly 60 percent of organizations support a BYOD program today. In fact, eleven percent of information workers are using tablets to do their jobs[2], while 26 percent of workers use Android smartphones and 22 percent use iPhones. Most of these products were purchased by employees.

Both employers and employees are excited and, unlike other business changes, employees love this new opportunity. However, there is a downside — reduced security for the enterprise network and data.

To enable enterprises to take advantage of BYOD without compromising security, the Trusted Computing Group (TCG), a not-for-profit organization comprised of industry experts from a variety of product and service companies, is addressing the security issues that BYOD poses.

This Architect's Guide provides a basic framework for BYOD security based on standards and architectures from the Trusted Computing Group, and is an extension of the *Architect's Guide: Mobile Security Using TNC Technology*[3]. TCG has already developed security solutions for computers and servers based on a Trusted Platform Module (TPM), for mobile devices through the Mobile Trusted Module (MTM), for data integrity and privacy based on Self-encrypting Drives (SEDs), and for enterprise networks based on the Trusted Network Connect (TNC) specifications (*see sidebars, page 4*). These open standards are implemented in a variety of products and collectively provide a comprehensive solution to BYOD security issues. When used in conjunction and standards from other organizations, the approach described in this guide enhances overall security for BYOD.

Solution Overview

The solution approach in this Architect's Guide builds on the premise developed in the *Architect's Guide: Mobile Security Using TNC Technology*[3]. *escalating trust brings increased access.* The major difference is the use of a BYOD product that is not owned, supplied, or managed by the enterprise. This lack of enterprise control increases the difficulty of establishing trust.

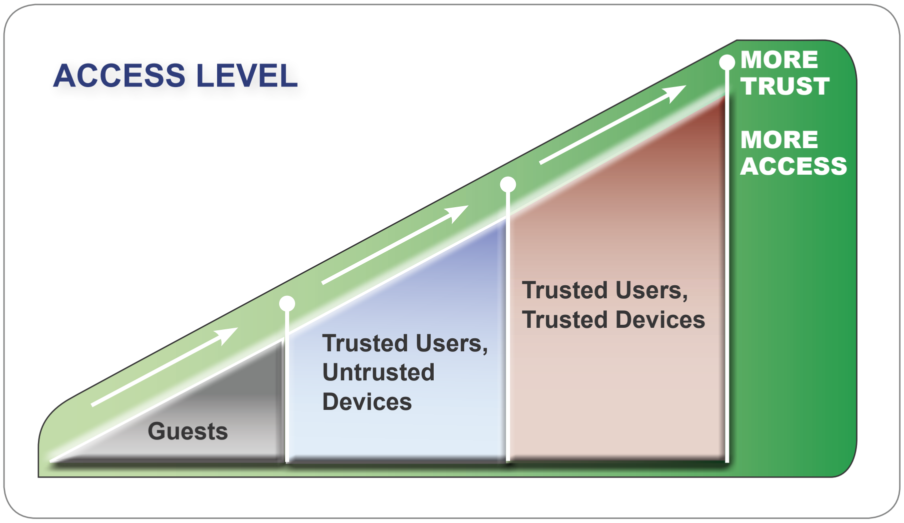
ACCESS LEVEL
MORE TRUST
MORE ACCESS
Guests
Trusted Users, Untrusted Devices
Trusted Users, Trusted Devices

Figure 1: Escalating trust brings increased access

The Mobile Security Architects Guide recommends that different users be given different levels of access to corporate resources based on how much the enterprise trusts them (*Figure 1*). Guests, with a low level of trust, get minimal access. Trusted users with trusted devices (such as managed corporate laptops) are given the most access. In between are users at different levels of trust, such as staff with unmanaged devices including smart phones, or contractors who should have only "need to know" access. Granting appropriate access and transitioning these unmanaged user devices to secure devices is the goal of this guide.

An important part of this solution is a unified approach to the BYOD aspect of mobile security. Using a combination of international and industry standards, network managers can design and deploy solutions that provide seamless mobile services to users on the enterprise campus and while traveling.

[1] http://www.zenprise.com/solutions/bring-your-own-device
[2] http://www.forrester.com/home?cmpid=mkt:ppc:goo:Forrester Researchhome&gclid=CJTt7ba7568CFWcHRQod0Gj93A#/Forrester+Half+Of+US+Information+Workers+Split+Time+Between+Office+And+Remote+Locations/-/E-PRE1380
[3] http://www.trustedcomputinggroup.org/resources/architects_guide_mobile_security_using_tnc_technology

Four Steps to BYOD Security

BYOD security should be implemented in four sequential steps: continuous assessment, risk reduction, access control, and monitoring and response. The following provides a brief overview of each of these areas.

1 **Continuous Assessment.** The enterprise assesses some or all of these factors to determine risk: user (identity, role, groups); device (identity, type, state, security); network (security, quality of service); resource requested (identity, label, classification); physical location (security, consistency with laws and regulations); threats; and countermeasures that are already in place. The set of factors assessed will depend on enterprise policy and on the technical capability of collecting attributes.

2 **Risk Reduction.** Enterprise policies may attempt to reduce risk by establishing additional countermeasures. For example, this can include requiring the user to run a security agent on their device; configuring the device to close more protocol ports and disable selected services; configuring agents to leverage roots of trust to establish integrity and identity; creating a secure "sandbox" or partition on the device; provisioning a secure virtual private network (VPN) to the device, and/or installing remote terminal software on the device to avoid the need for local storage of enterprise data. When properly employed, these countermeasures lower the risk factors assessed in the first step.

3 **Access Control.** Based on policy, identity, device configuration and integrity factors, the enterprise decides what access to grant. This can be the full access requested, or access limited to certain resources, perhaps with the requirement to use a self-encrypting drive, secure partition, web-based application, or a remote terminal window.

4 **Monitoring and Response.** If data is downloaded to the device, the enterprise may monitor the security of the device and dynamically respond to threats. For example, the device may be frozen if the unlock password is entered incorrectly five times in a row. Enterprise data may be remotely wiped or access to encrypted data revoked if the user reports the device lost or stolen or if the user loses authorization. Events (including data access) may be recorded for audit purposes.

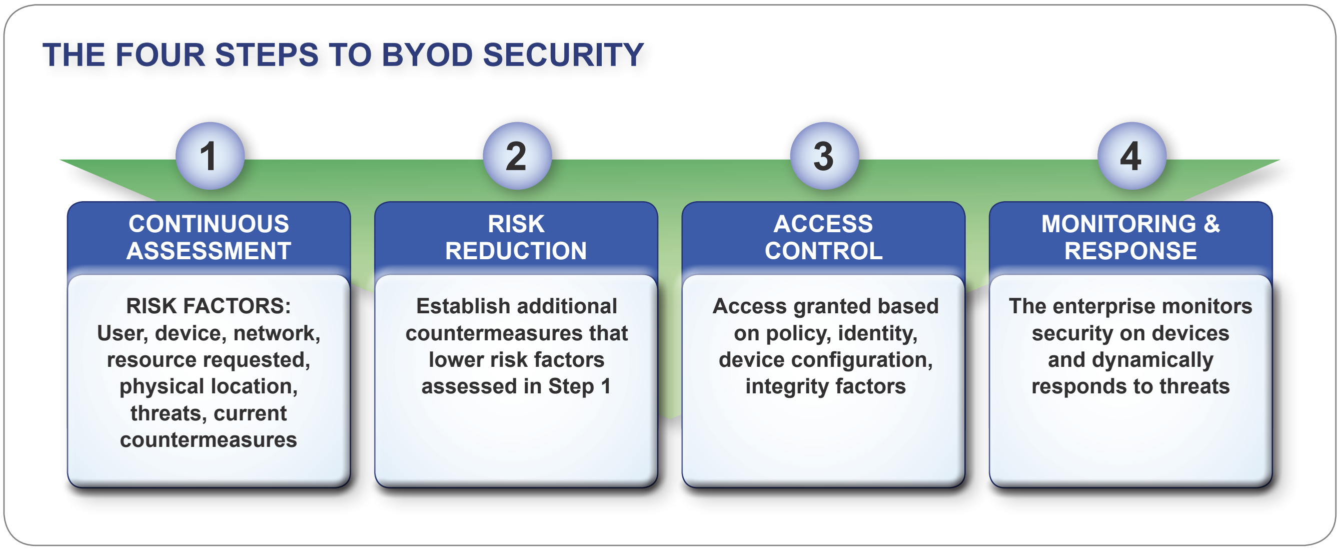
THE FOUR STEPS TO BYOD SECURITY
1
CONTINUOUS ASSESSMENT
RISK FACTORS: User, device, network, resource requested, physical location, threats, current countermeasures
2
RISK REDUCTION
Establish additional countermeasures that lower risk factors assessed in Step 1
3
ACCESS CONTROL
Access granted based on policy, identity, device configuration, integrity factors
4
MONITORING & RESPONSE
The enterprise monitors security on devices and dynamically responds to threats

Figure 2: The four steps to BYOD security

Implementing the Four Steps

While the four steps to BYOD security seem reasonable and perhaps obvious, implementing them is not an easy task. Fortunately, TCG has developed a framework and open standards to simplify the solution. This section discusses the recommended methodology used to implement the four steps (*Figure 3, page 5*).

1 **Continuous Assessment.** The TNC standards define an architecture for gathering information needed for continuous assessment.

- The user's identity can be established with many widely-used techniques including username/password, certificates, etc.
- Device identity can be established using a SIM card or other device credentials. User or device identity secured in a non-removable hardware root of trust such as TPM, Secure Element, or UICC provides a higher level of assurance than SIM cards.
- Device type and security-related configuration can be determined using information obtained through the web browser, a resident agent, or an external scan. By providing hardware measurements of device state, the TPM can increase the security of device assessment protocols.
- SEDs (often an after-market upgrade) can be a key means of addressing theft and loss concerns via protected storage, reducing the risk of data breaches and increasing trust in mobile devices.
- Other factors (network, resource, physical location, threats, and countermeasures) can be gathered from IF-MAP, a TNC protocol enabling coordination among networking and security components for security automation (*see TNC sidebar*).

These forms of continuous assessment are supported by commercial products as well as open source implementations.

What is it?

Trusted Platform Module or TPM

The Trusted Platform Module[4] (TPM) is a hardware security component built into a computing device. The TPM provides a hardware root of trust for user and device identity, network access, data protection, and more.

TPMs have been shipped in over half a billion end systems, including many laptops. Tablets with TPMs are already in the market. However, not all current mobile devices include a TPM.

Self-Encrypting Drive or SED

Performing exactly like other storage devices, Self-Encrypting Drives[5] (SEDs) automatically encrypt all user and system data. SEDs allow secure ranges on the drive to be isolated completely from non-authorized applications. Operating without the inherent performance degradation caused by software-based encryption, an SED can hold a rich local policy data store. In addition to providing secure storage of installed applications, an SED can help perform a secure remote wipe of enterprise data with separate secure ranges on the SED treated as logically-separated hard drives.

Trusted Network Connect or TNC

TCG's Trusted Network Connect[6] (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also include network-based access control enforcement—granting or blocking access based on authentication, device compliance, and user behavior. TNC provides pervasive security, Network Access Control (NAC) and interoperability in multi-vendor environments. Support for TNC standards is included in products from over two dozen commercial and open source vendors.

[4] http://www.trustedcomputinggroup.org/solutions/authentication
[5] http://www.trustedcomputinggroup.org/solutions/data_protection
[6] http://www.trustedcomputinggroup.org/solutions/network_security

2 **Risk Reduction.** In response to problems uncovered by continuous assessment, countermeasures may be called for.

Common countermeasures include installing a security agent, configuring the device more securely, creating a secure sandbox or partition on the device, provisioning a secure VPN to the device, or installing remote terminal software on the device. These countermeasures may be provisioned through a web page or through proprietary mechanisms, such as protocols supported by a resident security agent.

TNC protocols provide the ability to send instructions for risk reduction. TPMs and MTMs provide a standard way to establish hardware-based security on mobile phones, tablets, and laptops. .

3 **Access Control.** A TNC-enabled policy server is commonly used to decide what access should be granted to a mobile endpoint, with a TNC-enabled enforcement point enforcing these decisions. Depending on the network topology, the enforcement point may be a switch, wireless access point, VPN gateway, firewall, or server. This design is widely implemented and supported by products from a variety of vendors.

What is a Mobile Trusted Module or MTM?

The Mobile Trusted Module[7] (MTM) is a subset of the TPM that is appropriately scaled for the mobile environment. Similar to the TPM, the MTM can be used to store passwords and digital keys to uniquely identify the mobile device. Functions in the MTM rely on the same mandatory cryptographic algorithms, key lengths, and equivalences defined for the TPM. In addition, shielded locations and protected capabilities are designed to resist the same spectrum of attacks as the TPM. General availability of MTMs in mobile devices is expected in the near future.

4 **Monitoring and Response.** TCG's IF-MAP protocol standard is commonly used to monitor device behavior and trigger a response (either automatically or manually). Syslog, SNMP, and RADIUS are commonly used for auditing and monitoring.

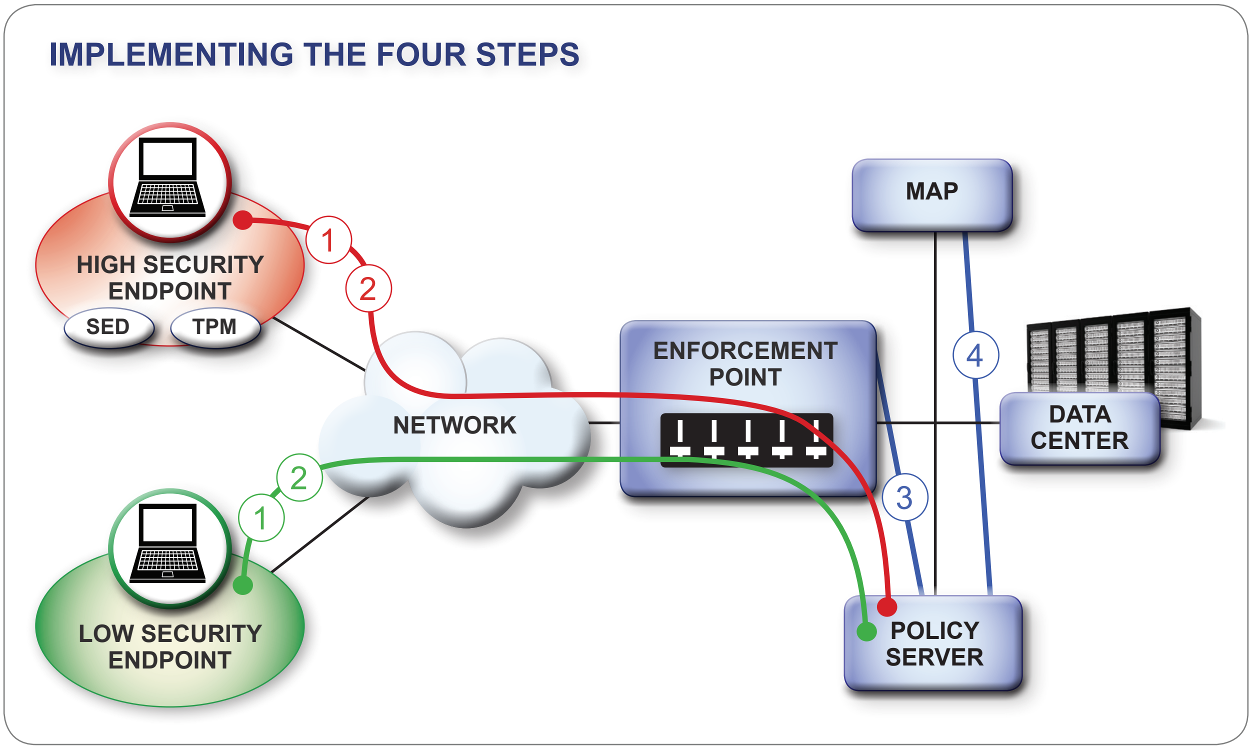

Figure 3: TCG standards support easy and interoperable implementation of BYOD security.

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

Future

TCG is currently working on challenges such as contractors who work for multiple and even competing enterprises and establishing trust in cloud computing providers when accessed from outside the enterprise network. Security for virtualized platforms represents another area of active innovation for TCG. The capabilities of Trusted Computing technologies continue to expand to address these new challenges.

Case Study: Educators Embrace BYOD

Educational institutions are among the organizations that are rapidly embracing BYOD. The Naperville, Illinois school district (located 28 miles from Chicago) provides an example of a successful BYOD security implementation[8]. A private gigabit fiber network connects its schools, administrative buildings, primary data center, and a secondary data center. This school district anticipates that 17,000 laptops, tablets, PCs, projectors, interactive whiteboards, e-readers, iPod touch devices, and other computing devices will eventually be connected to the network.

Using existing network and security solutions[8] that take advantage of TCG standards, the school district now offers wireless guest access as part of the initial implementation of its BYOD initiative. The software creates a network access policy for each user based on the user's identity, device configuration, and network location. With this capability, the school district's security policies are enforced, and students, teachers, and staff can use their personal and district-owned laptops and other mobile devices on the school's wireless local area network (WLAN).

Conclusion

BYOD security can be implemented today 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. The following bullets summarize TCG's recommendations for BYOD security:

- Control and monitor access to sensitive corporate data using the TNC protocols
- Encrypt corporate data on all mobile devices, preferably using SEDs
- Authenticate users and devices, using hardware such as TPM and MTM

Call to Action

- Design BYOD security solutions customized for your unique environments
- Contact TCG-certified vendors and insist on acquiring standards-based technology solutions
- Deploy solutions in pilot first, observe and correct issues and then deploy into production
- For more information on TCG technologies and architects guides, please visit the Trusted Computing Group web site http:www.trustedcomputinggroup.org
- Additional information on BYOD security will be available over the next several months.
- Contact us at admin@trustedcomputinggroup.org with any questions.

[8] http://www.trustedcomputinggroup.org/resources/naperville_school_district_enhances_the_learning_experience_with_onetoone_computing_enabled_by_juniper_networks