Trusted Computing Group's Trusted Network Connect Technology Standards Development for Network Security Interoperability

Standardization feedback for Sub-Committee on Standards

Submitted by: The Trusted Computing Group Trusted Network Connect Adoption Subgroup

Submitted to: Sub-Committee on Standards, National Institute of Standards and Technology (NIST), US Department of Commerce

Submitted: 7 February 2011

Response to Request for Information notice by National Institute of Standards and Technology on 12/08/2010 "Effectiveness of Federal Agency Participation in Standardization in Select Technology Sectors for National Science and Technology Council's Sub-Committee on Standardization"

Document Citation: 75 FR 76397
Docket No. 0909100442-0563-02

Introduction

The Trusted Computing Group (TCG) provides open standards that enable a safer computing environment across platforms and geographies. Benefits of systems based on Trusted Computing include protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity. Organizations using built-in, widely available trusted hardware and applications reduce their total cost of ownership. TCG technologies also provide regulatory compliance that is based upon trustworthy hardware.

TCG is headquartered in Beaverton, Ore., with more than 100 member companies located worldwide. The TCG is governed by a Board comprised of Promoter members Advanced Micro Devices; Fujitsu Ltd.; Hewlett-Packard; IBM; Infineon Technologies AG; Intel Corporation; Lenovo Holdings Ltd.; Microsoft; and Wave Systems. Elected Contributor Advisor Board members include representatives from Dell and Samsung.

Through its member-driven work groups, TCG has extended its efforts into a variety of related devices, including mobile devices, servers, peripheral devices, storage, infrastructure, and cloud security. TCG has created software interface specifications for development of applications to build on TCG technology. TCG also has published a specification for ensuring endpoint integrity to protect networks against attacks and unauthorized users and a specification for mobile phone security, with a storage security specification available as well.

A number of products support TCG specifications. The most widely deployed example today is the Trusted Platform Module (TPM). Virtually all enterprise PCs, many servers and embedded boards include the Trusted Platform Module (TPM). The TPM specification includes a secure cryptoprocessor that can store cryptographic keys that protect information that offers facilities for the secure generation of cryptographic keys, and limitation of their use, in addition to a hardware pseudo-random number generator. It also includes capabilities such as remote attestation and sealed storage.

This Request for Information (RFI) response will focus specifically on the work of the Trusted Network Connect Work Group (TNC-WG).

TNC standards enable secure computing and communications by integrating separate networking and security components into an intelligent, responsive coordinated defense based on sound architectural principles and open standards.

For organizations that use the TNC standards, the benefits are considerable. The network becomes more intelligent and better integrated, leading to a reduction in false alarms and undetected breaches with an ultimate benefit of increased productivity and lower management costs. Because all devices obtain identity information through the TNC standards, an organization-wide security policy can be written once and used everywhere. Compliance with these policies can then be automatically ensured, measured, and documented. Security is less intrusive, providing a more graceful and efficient experience for end-users. Security becomes an enabler and not a roadblock. The multi-vendor interoperability enabled by the TNC standards lets customers freely choose products based on their needs. The bottom line is that security, flexibility, and efficiency are increased while cost and risk are reduced.

The benefits to vendors of adopting TNC standards are substantial. Vendor products become more capable by obtaining information from other products and more valuable by sharing their own information. A product that adopts the TNC standards is no longer an island. The cost of integrating with other vendors' products is greatly reduced by the use of open standards. Instead of vendors developing separate integration solutions for each partner, supporting the TNC standards provides a single integration framework for all partners. By adopting the TNC standards, vendors see lower costs, newly available markets, and increased revenue as customers abandon proprietary platforms for open ones.

TCG's Trusted Network Connect (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC provides pervasive security, Network Access Control (NAC) and interoperability in multi-vendor environments.

TNC Offers Interoperable Standards For:

- Secure Guest Access- With TNC, guests obtain restricted network access, without threatening the host network.
- User Authentication- TNC integrates user authentication with network access to better manage who can use the network and what they are allowed to do.
- Endpoint Integrity- TNC performs a health check for devices connecting to the network. Devices out of compliance can be restricted or repaired.
- Clientless Endpoint Management- TNC offers a framework to assess, manage and secure clientless end points connected to the network, such as IP phones, cameras and printers.
- Coordinated Security- Security systems coordinate and share information via the IF-MAP (Interface for Metadata Access Points) standard, improving accuracy, and enabling intelligent response.

Detailed Response

Standards-Setting Processes, Reasons for Participation and the Benefits of Standardization

Participation in standards-setting activities
The Trusted Computing Group (TCG) seeks to have a broad membership base of companies and other organizations committed to the development of open standards for increasing the security of the computing environment across multiple platforms and operating environments. TCG also desires active participation in Work Groups in order to create the best technical solutions for the industry and foster rapid adoption. The TCG Board of Directors encourages all organizations supportive of the purposes of TCG to join the Corporation and contribute to its success.

The TCG offers several levels of membership for corporations, industry organizations and academic institutions, including Promoter, Contributor, and Adopter.

Both Promoter and Contributor members have the right to attend and participate in compliance workshops, submit proposed revisions and addendum proposals for the Specifications and design guide and review and comment on specifications and relevant materials related to the specifications.

Reasons for participation
Member companies, particularly at the Promoter and Contributor levels have a substantial economic interest in the advancement of Trusted Computing Standards, or the advancement of the standards will have some other tangible impact in the Corporation's success in fulfilling its stated purpose.

Benefits of developing standards for this sector
Security is built into an increasing number of general purpose ICT products, and security standards are fundamental to the integrity and sustainability of the global ICT infrastructure. The Trusted Computing Group (TCG) believes that open, interoperable, and internationally vetted standards are critical for the success of trusted computing, and that the multilateral approach to creating such standards is most effective.

TCG works within the international standards community, and has liaison and working group relationships with the Internet Engineering Task Force (IETF) and the JTC1 joint committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The Trusted Platform Module is defined by an ISO/IEC international standard*. The TCG Certification Program leverages established and recognized security

evaluation standards. This program relies on certification by laboratories operating under the supervision of National Schemes of Common Criteria members and also on TCG-specific interoperability and compliance tests.

In support of open security standards, TCG encourages all nations to adopt global best practices around standards development and adoption. An open process fully supports worldwide participation from industry, academia, and government with fair and transparent development and decision processes. Specifications must be fully transparent and available to all participants, both during development and for implementation. TCG supports the use of published, peer reviewed standards and cryptographic algorithms.

TCG only supports open standards that are developed through a transparent development process, have undergone rigorous open review, and are compatible with existing global standards. Closed standards hamper both existing and emerging markets, and are detrimental to the security of global ICT infrastructure, representing an obstacle to technology innovation and industry growth.

TCG recognizes international standards in the field of IT security as the most appropriate method to ensure efficacy, interoperability, adoption and user acceptance. TCG takes into consideration international market requirements through international membership and welcomes participation from industry, academia, and governments in a unified, worldwide Trusted Computing standards development process.

Impact to organizations, their competitiveness and innovation

The TNC architecture has advanced cyber security capabilities of the participating company's technologies through the integration and interoperability it affords. The TNC standards support continued innovation by promoting interoperability without stifling vendor creativity. TCG supports this approach of using open standards to enable interoperability between products while supporting innovation within each product.

Current phase of the standards development for TNC technology

Over the last few years, Trusted Computing Group (TCG) has developed and released the widely accepted TNC (Trusted Network Connect) architecture and standards for network security.

The TCG now offers the TNC certification program, a rigorous testing program to assure customers that certified products properly implement the TNC specifications and interoperate with one another. TNC certification is available for IF-IMC (InterFace for Integrity Measurement Collectors), IF-IMV (InterFace for Integrity Measurement Verifiers) and IF-PEP (InterFace for Policy

Enforcement Points). Testing for other specifications in the TNC architecture will be added in the future, including IF-MAP (Interface for Metadata Access Points).

TNC tests interoperability between vendors products at TNC testing events, called TNC PlugFests. Vendors with products that support the various TNC specifications can connect with other products in a simulated enterprise environment on a production network. To complete the interoperability testing aspect of TNC certification, products must successfully interoperate with all other relevant products while completing a rigorous series of enterprise test cases.

Several vendors offer COTS products that support TNC standards, and there are several which have been TNC certified including a TNC open source implementation.

How the standards-setting processes is managed and coordinated

The TCG is organized with a Board, Committee, and Work Group structure with supermajority voting. The Board appoints the chairperson of each Committee and Work Group from Promoter and Contributor member companies.

The output of all Committees and Work Groups, including the all standards and specifications, are reviewed and approved by the individual groups, and subject to the review and approval or rejections of the Board of Directors prior to publication.

Any Promoter or Contributor member may propose to the Board the establishment of a Work Group. The chairperson of each Work Group sets the procedures that govern that group, as long as they adhere to the minimum standards set by the Board of Directors. Any Promoter or Contributor is entitled to have a voting representative on each Work Group. Work Groups conduct regular meetings to advance the standards to which they contribute.

Perspectives on Government's Approach to Standards Activities

How Federal agencies participate in TNC standards development

The Trusted Computing Group (TCG) is an international industry standards group. TCG members are generally commercial entities which have an economic stake in the success and adoption of the standards developed in that group.

However, the TCG welcomes experts from non-commercial organizations to participate in TCG work groups as liaison members (for interested organizations like governments) or as invited experts (for individual experts). This open work group model creates an environment whereby experts from each technology category can work together to develop the specifications. This fosters a uniquely

neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable.

Because of that neutral environment, it becomes more appropriate that Federal agencies become involved in providing insight and guidance to the development of the specifications this group will develop. That insight will lead toward more useful technology deployments for Federal agencies.

Further, contribution to and adoption of open standards which are commercially driven enables Federal agencies to benefit from standards that commercial entities are already vested in.

One example of contribution to the TNC standards is The National Security Agency's (NSA) engagement in work with industry to lead and influence trusted computing technology and solutions through participation in the Trusted Computing Group.

In 2010, the NSA hosted the Trusted Computing Conference and Expo. Speakers from U.S. Government agencies, leading vendors and enterprises address challenges in cyber security. Applications of Trusted Computing, including the Trusted Platform Module, self-encrypting drives and network security, were discussed for the first time by large enterprise users. Hundreds of attendees also see Trusted Computing demonstrations.

How Federal agencies can benefit from TNC

Open-standards based technologies like TNC are completely vendor-neutral. Open, vendor neutral standards offer the ability to derive more value from best-in-class security tools, rather than being committed to a single, proprietary platform. This is particularly relevant in the current era of evolving threats. The interoperability that TNC provides, allows organizations to leverage the investments they've made in tools that are already deployed on the network.

How Federal agencies can further support the development and adoption of TNC standards

Because of the commercial interest of the groups involved, should Federal agencies choose to adopt TNC as a supported or required standard, the vendors who have adopted the TNC standard will benefit from increased market opportunity with in the Federal sector.

Federal standards activities and TNC together

One example of how TNC's activities work with Federal standards can be seen in the interoperability of TCG's Trusted Network Connect (TNC) specification and Security Content Automation Protocol developed by the U.S. Commerce Department's National Institute of Standards and Technology (NIST).

The TNC standards handle network security. The SCAP standards focus more on endpoint compliance. By using these standards together, customers can ensure that only properly configured endpoints are allowed to connect to the enterprise network. Other endpoints can be quarantined and remediated.

By TNC-SCAP integration, we mean that scanners based on SCAP can be used with network security gear based on the TNC specifications to identify and quarantine unhealthy devices. This will automate checking and compliance for millions of PCs and other devices.

TNC and SCAP will continue to each be managed independently by their respective standards bodies but work will continue on integration. The growing capabilities of the TNC and SCAP standards should allow additional forms of integration with additional features and benefits.

Issues Considered During the Standards Setting Process

Handling intellectual property rights & impact on development of standards

The Members of the TCG understand that in certain lines of business they may be direct competitors, and agree to uphold certain standards of conduct within the TCG context. Members agree only to share information which is necessary for the purposes of the TCG's work.

Member companies agree to nondisclosure and confidentiality stipulations requiring them not to disclose confidential information disclosed within the TCG context.

Each member organization retains all rights to their individual intellectual property. However when becoming members, the companies agree to reasonable and non-discriminatory (RAND) patent licensing policy between Members.

Process Review and Improvement Metrics

Standards development in complex technologies

The TNC architecture and its underlying protocols support complex and evolving technologies. An example of how TNC has continued to evolve its standards to support further development of these technologies can be seen in the advancements of the IF-MAP protocol specifically.

The IF-MAP protocol was first published by the TCG on April 28, 2008. Originally, the IF-MAP specification was developed to support data sharing across various vendor's devices and applications for network security. The standard has also been adopted for additional use cases of data-sharing including physical security.

TNC found that customers and vendors were using IF-MAP for many surprising purposes that were not originally anticipated, such as industrial control system (ICS) and cloud security. To support these new uses, IF-MAP has been separated into two parts: a base spec and a network security metadata spec. This split enables more responsiveness and flexibility to the spec as new uses develop and new metadata is developed for the publish/search/subscribe primitives provided in the IF-MAP 2.0 base protocol.

Version 2.0 of the IF-MAP spec was published on September 13, 2010. The 2.0 version separated the base protocol from the metadata definitions that standardize how different types of information are represented. The goal in separating the base protocol from the metadata definitions within the standard was to allow the standard to be adopted across other technologies, such cloud computing, Industrial Control Systems, smart grid, to leverage their existing data models within the MAP framework.

End users benefit from the ability to leverage their IF-MAP infrastructure across more applications as vendors from different industries adopt IF-MAP in their products. Both vendors and end users gain a richer set of protocol functionality and a more mature standard.

Measuring the effectiveness of TNC standards

The ultimate measure of the effectiveness of TNC standards, as with any technology standard, is in their level of adoption.

The TNC has developed a list of milestones toward furthering adoption of the standard, which the group believes will be the measure of the standard's success. These milestones include: a market environment where most or all endpoints, networking and security products support the TNC standards; many RFIs and RFPs require TNC support; widely-known customer deployment; other standards organizations adopting or recognizing the TNC standard.

Finally, one of the milestones to measure the effectiveness of TNC standards, is for TNC to enable trusted computing in critical areas such as physical security, virtualization security, cloud security, control system security, and others.