
HIT Standards Committee: Hearing on Health Information Technology Security Issues, Challenges, Threats and Solutions

Building Trust panel

Author: Thomas Hardjono, PhD

Affiliation: MIT Kerberos Consortium
Massachusetts Institute of Technology
77 Massachusetts Avenue W92-152
Cambridge, MA 02139

Date: November 19th, 2009

Building Trust panel – to address issues and challenges related to building and maintaining trust in the HIT ecosystem, and the impacts that real and perceived security weaknesses and failures exert on health organizations, individual providers, and consumers.

1 Briefly describe your organization and your information security approach to building trust with business partners and with consumers.

- **Organizational Background:**

The current MIT Information Services and Technology (IS&T) organization performs all of the IT related functions within MIT. The IS&T organization is further divided into the following departments: Client Support Services, Infrastructure Software Development and Architecture, Operations and Infrastructure Services, Student and Administrative Information Systems (SAIS), IS&T Finance and Administration and IS&T Human Resources. The primary customers are the students and faculty members, student administration units, business and finance and the senior management of MIT. Additionally, alumni and other affiliated organizations also represent an important customer based to IS&T.

- **Trust: Social/Business Trust and Technical Trust**

The digital era and the Internet has necessitated the need for a re-evaluation and even re-definition the notions of trust previously accepted in the pre-digital society. Generally speaking one definition of trust that is used in the area of

trusted computing is as follows: *something can be trusted if it behaves in an expected manner for a particular purpose*. This simple definition maps readily into technology (hardware/software devices) and into the psychological expectations of the user. A human user will accept and develop positive expectations regarding a piece of technology (e.g. mobile phone) if it performs in an expected manner (i.e. on all the time) for a particular purpose (i.e. to make telephone calls). We refer to this as *technical trust*.

Similarly, an end-user will develop *social trust* in an IT Services organization only if the end-user understands the expected process/behavior (e.g. isolate networks in an emergency, etc) adopted by that IT Services organization in response to given IT-related problem (e.g. malware outbreak, etc). Business trust is created when an IT organization has a well-defined and published security practices statement.

There are many forms of *interfaces* between technical trust and social trust. For example, since the average user does not in reality have direct control over local networks, the Internet and its underlying infrastructures, the IT Services organization to a large degree represents an interface between technical trust and social trust.

- **Approaches to Building Trust**

There are a number of aspects and principles relating to building social trust – based on sound technical trust – with business partners and consumers in the IT security context. These include, but not limited to the following:

Selection of safe & current security algorithms and protocols:

Technical trust in security-related components (software/hardware) depends on the correct selection of well-studied security algorithms and protocols for deployment within systems in the IT environment. The knowledge that an IT organization is deploying safe and current algorithms and protocols (e.g. those recommended by NIST and the NSA) provides a foundation of social trust with business partners and customers. For example, NIST has recommended the deprecation of old cryptographic algorithms (eg. DES and 3DES) and the use of stronger algorithms (e.g. SHA-2 family).

Standards-based algorithms and protocols:

The “locked-in” effect of proprietary algorithms and solutions applies equally to IT security. Thus, choosing standards-based algorithms and protocols (e.g. from the IEEE, IETF, W3C, Oasis, etc) is crucial to the implementation of technical trust and the acceptance of the IT organization practices by the community of partners and consumers.

Heterogeneity of deployment environment:

Heterogeneity of platforms and systems deployed within an IT environment is important for the survival of an IT organization in the face of catastrophic events, such as malware outbreaks, large-scale Denial-of-Service (DoS) attacks and others. The ability of an IT organization to deploy and maintain these heterogeneous platforms in a secure and consistent manner is an important factor in building good reputation and trust.

Architecture transparency:

The security architecture of an IT system and the components making-up the system must be clear and well understood by all members of an IT organization. Although it is unrealistic to expect all members of the IT organization to understand details of the architecture to the same degree, each member should have a general understanding as to how and why security-relevant components are arranged in the given manner.

Clear incident reporting process:

Medium to large IT organizations should have a distinct security team that handles security incident reporting/response. The team should communicate to the broader IT community relevant reported incidents and explain the steps taken to address these. This process is important in building social trust.

Clear security policies & enforcements:

Every IT organization should develop and define security policies – across different layers of the IT architecture – as well as methods of enforcement. These security policies and enforcement methods needs to be clearly communicated to all IT personnel.

Openness to Open Source:

Not all IT environments require access to source of all executable code. However, in general heterogeneity of the IT building blocks – including infrastructure, applications and services – may necessitate the use of open source software. Many IT organizations derive numerous benefits from using open source components in their internal development of security-related solutions. Having access to source code allows the development team to gain confidence and technical trust in the resulting solutions.

Security & Privacy Practices Statement:

Every IT organization should publish internally (and perhaps externally) a Security & Privacy Practices Statement document that clearly defines the security tasks, roles and responsibilities of the IT organization as well the privacy policies adopted regarding data belonging to business partners and consumers. Such a

practices statement is crucial in developing and evolving social trust among the stakeholders of the services provided by the IT organization.

Risk management strategy and security cost-benefit analysis:

Communicating or publishing its risk management strategy and approaches is an important part of an IT organization. Such a document may also include cost-benefit analysis regarding the adoption of certain security technologies and services used within the IT organization.

2 Provide one or two examples of issues you have faced recently related to building and maintaining trust, and describe how you addressed these issues.

- *Example: Retirement of applications that use the DES cryptographic algorithm:* IT services within higher-education institutions often face interesting challenges in addressing and rectifying known security weaknesses of systems. One such example was the decision by the IS&T organization at MIT to remove the usage of the DES and 3DES cryptographic algorithms which are now deemed by NIST and the NSA as being weak algorithms. However, some older popular software applications did not have an upgrade-path that incorporated better crypto algorithms. As such, budget and training was allocated for the users of these old systems to move to newer softwares that used better algorithms. The clear communicating of information about the security weaknesses/issues (regarding the old software) to the user community was an important phase in the “weaning-off” process. Coupled with this was the importance of providing & supporting newer alternative softwares to the user community. The success of this process established good relations and trust in the community of users, as users now understood that removing usage of weak crypto algorithms was in their best interest and the interest of MIT as a whole.

3 What kinds of trade-off’s have you had to make between security and usability, and other operational considerations?

- *Security and Usability Trade-Offs:* The trade-off between security and usability must be guided by a number of parameters, including the value of data (should there be data stolen/lost due to weak security), the degree of convenience/inconvenience for the user and the operational complexity of certain solutions. An example is the use within MIT of a PKI hierarchy that is rooted at MIT (self-signed Root CA certificate), and the use of client-side certificates for browsers. Since many of the services offered to Students, Faculty and Staff are conducted over the web through Web Single Sign-On (Web-SSO), it is crucial

that mutual authentication be performed between the client (browser) and the service (web-server). Thus, prior to using web services at MIT a new user is briefly inconvenienced by the need to install a copy of the MIT Root CA certificate and to install a unique client-side certificate (based on the user's MIT ID). However, the gain is obtained by an increased security through Web-SSO instead of a continual prompting of the user's password. Operationally, running an internal CA server was considered more cost-effective than outsourcing to a commercial Certificate Authority (CA).

4 What information security standards are you currently using, or would you recommend, to help assure that a business is trustworthy as both a business partner and consumer services provider?

Security Standards: Deployment of security solutions based on technologies that have been standardized provides a number of positive advantages. This includes, among others, a high degree of interoperability of components, higher security quality through well studied protocol/algorithms, flexibility in substitution of components and freedom to upgrade or replace components. We believe that participation in standards creation is an important aspect of technology development and operational planning.

The IS&T organization at MIT deploys solutions using a number of standardized security components. These include:

- *IETF Standards:* The Kerberos authentication protocol standard, the PKI standards, the TLS standard, the IPsec standard, the GSSAPI standard and others. [Note: several people from the MIT Kerberos Consortium contribute to the IETF regularly. Additionally, a member of the MIT-KC chairs two Working Groups in the IETF.]
- *Oasis standards:* The Security Assertions Markup Language (SAML2.0) used for Identity Management (Shibboleth standard), WS-Security for web services security, and others. [Note: A member of the MIT-KC co-chair the SAML Security Servicemen technical Committee in Oasis.]
- *NIST standards/recommendations:* We follow closely recommendations and announcement from NIST. Specific standards of interest include the NIST 800-57 (on Key Management), NIST 800-67, and many others.
- *IEEE Standards:* The IEEE has published numerous standards that contain security components or technologies. Some examples include the IEEE802.1X

access control standard, 1619 standards, cipher/crypto and hash algorithms and modes, and others.

5 What challenges have you had to address in implementing these standards (e.g., training)?

Some issues in implementing standards include, but are not limited to the following:

- *Lack of (affordable) products:* Although standards specifications may be published, often there are too few products on the market in compliance or conforming to the specifications. As such, there is always the risk of product/vendor lock-in without verification of interoperability of products. Additionally, some products that are first to market following a new standard may be too costly to deploy.
- *Lack of open source code:* Often a sign that a standard is successful can be seen from the adoption and implementation of that standard by the open source community. MIT is also very supportive of open standards. As such, many projects at MIT use open source software.
- *Lack of reported interoperability test/benchmark results:* One issue in deciding on products that claim to implement certain standards is that of the lack of public reports regarding interoperability test result. Often, organization such as the IETF, Oasis and IEEE conduct interoperability “fests” or events, and also perform compliance verification. In the absence of such reports (particularly for new standards), often the purchase for new products is deferred.
- *Lack of knowledge regarding new standard:* With new standards it is natural to expect that many staff members are not knowledgeable regarding the contents, usage and issues surrounding a new standard. Thus, training and seminars must be conducted in order to bring staff members up to date regarding the new standard.

6 What is the role/value of interoperable information security standards in helping building and maintain trust?

Standardization of IT technologies opens the market to competing products, and consequently provides a wider choice to IT buyers to acquire interoperable products from differing vendors.

Interoperable information security standards – in which specifications development were conducted in an open manner within open standardization bodies – provides technical trust to a large degree. That is, since the security specifications have been

reviewed and vetted by experts in an open manner, there is a higher degree of acceptance by the technical community and more willingness in deploying implementations of the specifications. A case in point is the AES cryptographic standard, whose development originated from a world-wide public competition and whose internal mechanics (specification) was open to public review.

Standardization of information security technologies also allows a faster discovery of flaws subsequent to the publishing of the standards. Such flaws would then be rectified by the open community, leading to a general increase in the security quality of solutions deploying the standards.

7 What are the current limitations or gaps in interoperable information security standards with respect to building and maintaining trust?

In the current digital era where the nation's economic, health and national security infrastructures increasingly depends on IT technologies, there are a number of issues pertaining to trust establishment and maintenance. Some gaps in security standards include the following:

- *Provenance of components*: Currently there are no standards to capture and express information about the provenance (origin) of components (software/hardware) making-up a given computing platform. Thus, when IT buyers (e.g. consumers, Government) acquire a computing platform (eg. laptop) from the major OEMs, there is no way for the buyer to find out which manufacturer created a given component on the platform.
- *Root of Trust establishment*: Currently there are no standards to allow a manufacturer of a component (software/hardware) to vouch for the correctness and safety of its product. That is, there is no way for the IT buyer to establish the *root of trust* in a given component on his/her computing platform. Since the IT buyer cannot physically verify the accuracy of the hardware implementation of standards by the manufacturer, the buyer places "blind faith" in the OEM. Although blind faith in the OEM may be sufficient for home-computing users, in the future a better solution will be needed for corporate and Government IT buyers.
- *Ratings and trust scoring*: There are currently no global standards for assigning a *trust score* to components (software/hardware) on a given computing platform. Similar to financial credit ratings computed for human persons, a trust score is computed value based on a number of input parameters. Some examples of input parameters include the correctness of all software components (e.g. correct

digital signatures over all executables), current state of the platform, provenance information for components, and others.

8 What new and emerging trust issues do you foresee over the next 2-3 years?

- *Trust in the internet infrastructure:* The Internet is increasingly becoming the backbone for the US digital economy. As the transactions across the Internet increase in value and in volume, the infrastructure underlying the Internet itself becomes prey to attacks from individuals and state-sponsored “digital terrorism”. The resilience of the Internet infrastructure (e.g. interdomain routing, DNS and naming service, etc) is key to its trustworthiness in the eyes of the average user, and by extension the trustworthiness of all the services offered over the Internet.
 - *Trust in digital identities:* As users increasingly conduct transactions over the Internet and use various cloud services, the problem of the mapping between identities in the real (legal) world against identities on the Internet becomes an important trust issue. Thus, at the heart of the problem is the need for digital identities that are fraud-resilient, carrying legal standing and with a controllable degree of privacy (as dictated by the owner of the identity).
 - *Trust in privacy-maintaining systems:* Related to digital identities on the Internet is the need to maintain privacy regarding the transaction conducted by any given identity. As such, in the future some solutions will be needed which would allow transaction to be conducted with services with either a “blinded” identity or with no identities revealed (e.g. zero-knowledge protocols). The ability for users to transact with the digital identities whilst maintaining privacy will be crucial to the users trusting those services. Additionally, on the services side database security and control of information leakage will be increasingly relevant.
-