# National E-business Trust Infrastructure Evaluation Scheme

Süleyman Kondakci, IT Consortium of Turkey,
Division of Information Security, The Netsekuritas
kondakci@itconsortium.org

*Abstract*- **Building E-business trust infrastructure is a challenging task. The Web poses some trust issues that most users are rarely aware of, and business should at the most consider liabilities and necessary efforts to minimize risks. However, issues related to control, IT auditing and IT security test and evaluation procedures and mechanisms have never been addressed in a clear text in Turkey. This paper presents a fundamental approach to a National Common Methodology for Information Security Evaluation (CEM) Scheme. A multinational supported common methodology has already been developed in several works. Similar to this, the methodology presented here is mainly based on ISO/IEC 15408 and Common Criteria for Information Technology Security Evaluation (CC). Unfortunately, due to lack of governmental policy and unforeseen technological standards regarding IT and IT security test and evaluation, we will customarily concentrate on practical approaches rather than presenting solutions to accomplish full compliance with the CC. We hope that this work will initate a nationwide formal awareness program, serve as the basis to establish IT security test and evaluation facilities and formal regulations, and to assure confidence in IT consumer relations.**

**Keywords:** *National Information Security Evaluation Scheme, ISO/IEC 15408 and Common Criteria with Turkey in perspective, forgotten entropy.*

## I INTRODUCTION

Turkey holds a great share in Internet usage and in general IT deployments, which indeed as a nation is a loyal importer of IT, and has never managed to develop systems for even small market shares. This fact has shadowed concerns about IT security in general, and inherently security of distributed network services. Many enterprises have not yet fully mastered security measures in their existing and rapidly growing e-business environment. Despite this growth, concerns about security of Web-enabled services present a considerable obstacle to motivate a forward motion in growth of e-consumers.

Since, Turkey is making strenuous efforts to obtain EU membership, the need for a full Common Criteria [1] conformance will be unavoidable. Majority of EU countries, US and Canada, have already established CC-based IT security evaluation scheme. This paper, in that sense, should serve as a basis to further development of full CC compliance in preparation to entering a future EU membership. Indeed, the major impact of this paper will most probably increase information security awareness for industry, government, users, procurers, and vendors. In this paper, we will also pinpoint the need for a national scheme to evaluate the strength of the security measures of systems and products before they can be deployed.

## II CURRENT SITUATION

Traditionally, our IT consumers and providers have primarily functional requirements as the prevailing technical requirements in their mind. The users have been slow in perception of security issues, and the IT providers have a common objective of short-term investments, thus increasing monthly recurring revenue, and keeping down the total cost of services and systems they provide. Fortunately, a vast amount of work is being done by several foreign technological bodies and key industries to address major security requirements. In fact, there have been deployed proven security services based on

widely accepted technologies such as, Secure Electronic Transaction (SET), Secure Socket Layer (SSL)/Transport Layer Security (TLS), and the Public Key Infrastructure (PKI).
Lack of national policy in IT security auditing, and user's weak perception in security awareness have made Turkey a paradises for IT providers. One can hardly find products that have been deployed after a thorough test and evaluation process. There is mainly a one-to-one trust relationship between the vendor and the IT procurer. The user has merely to accept using that product regardless of any approved trustworthiness.

On the other hand, the major impact of this desperate tendency brought Turkey into a huge technology-garbage. Though, the ultimate result may sound lucrative for individual IT merchants, we actually have a tremendous amount of cash flow out of Turkey. Diverse research results done for the national budget show an income-loss ratio of *5/23*. A great percentage of the loss is due to total cost of ownership (TCO), which can be calculated semi-quantitatively as,

$$TCO = \sum_{i=1}^{N} System_i + \sum_{s=1}^{M} Unavailability_s$$

where, *Unavailability* is a cumulative measure of degradation in efficiency and service capability, service down time, and other malfunction expenses per system, and *System* is a measure of regular maintenance cost per system. Merchants, banking and financial institutions deploying such expensive systems, have been rigorously distributing the TCO on the consumer's budget.

In many respects, the primary objective should provide the means to create a convenient and trusted e-business environment, where organizations and individuals can conduct communications, transactions and other business processes.

### *A. Web Security Considerations*

A Web-enabled application is typically a client/server program running over the Internet with the aid of TCP/IP protocol suite. Security threats on the web applications are *integrity, confidentiality, impersonation of legitimate users,* and *denial of service.* In addressing these familiar challenges of Internet computing, there are major new vulnerabilities, related to the ever-increasing scale of complexity of e-business. By the nature of frequent confrontations with various attacks via the Internet, Web-enabled applications are considered as the most vulnerable victims. Therefore, for web environments, we define four types of web applications,

- *security unaware*
- *security aware,*
- *security aware with security policy,*
- *security aware with both security policy and mechanisms.*

A typical example of the last mentioned type can be the environment of an e-payment system, where the client

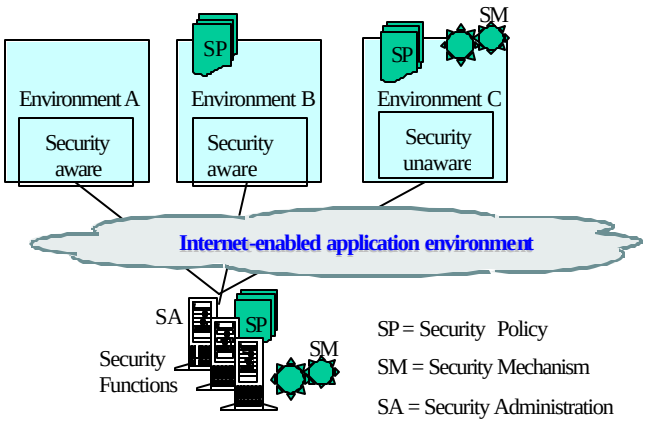


**Fig. 1:** Specification of web application environments

and server using SSL and public key cryptographic system to ensure a secure virtual channel for the transactions. Fig. 1 depicts the general environment of applications used in three different environments.

It is obvious that each of these environments will require different evaluation setups, but not necessarily different assurance levels.

## III THE SCOPE OF SECURITY

To assess effectively the security needs of an environment, and to evaluate and choose certified/validated security products and policies, we need to reveal these:

*Threats and attacks:* A threat is described as a potential for violation of security, and an attack is best described as an assault on system security that derives from an intelligent threat.

*Security architecture:* A security architecture, as detailed in [3], is a systematic approach to develop security features for products and services. X.800 suggests a division of services into five categories and fourteen specific services. The categories specified are *Authentication, Access Control, Data Confidentiality, Data Integrity,* and *Nonrepudiation.* An additional service is the *availability*, which is defined as prevention of unauthorized withholdings of information or resources.

*Security evaluation criteria:* A common standard for IT security specifications and evaluations. The Common Criteria version 2.1 is now formally recognized as ISO 15408, and is strongly supported by national security and standards organizations within Canada, France, Germany, the Netherlands, the United Kingdom and the United States. With this paper, we submissively present the very first effort of Turkey to become a part of the internationally accepted information security test and evaluation scheme.

## IV THE SCOPE OF EVALUATION

Suggested with our model, the evaluation process will, at a minimum, require test and evaluation of a security environment consisting of Protection Profile (PP), Security Target (ST), and Target of Evaluation (TOE). PPs are needed when setting the standard for a particular product type. The profile

will, in general, contain a detailed description of a given security environment for a particular class of security products and will include only the necessary functional and assurance requirements.

A PP will play an important role, when developing a particular system or product, while evaluating the product a Security Target (ST) will play the major role. Security Targets are rather specific implementations of PPs, and used as the basis against which an evaluation is performed. As an example, a set of security requirements and a specification of security enforcing functions of a particular firewall product are composed in the ST document for that particular firewall. There is a high degree of commonality between a PP and an ST, so that an ST can claim compliance with a PP with no additional functional or assurance requirements. The ST contains summary specification of security functions and assurance measures, TOE security threats, objectives, and requirements. The consumer of a product should use the ST to check whether the security functionality of the TOE and its assurance package are consistent with his requirements and whether the evaluated configuration is consistent with the proposed environment.

A Target of Evaluation (TOE) is an IT system or product, which is subjected to security evaluation. A TOE should also present detailed information about the IT product or system and its associated administrator and user guidance. The TOE will further contain its resource, TOE Security Functions (TSF), TOE Security Policy (TSP), and TOE Security Functions Interface (TSFI).

### *A. Development of Protection Profiles*

Any evaluation scheme should consider the use of evaluated and certified PPs. To do so, we propose establishment of a single national PP repository.

The evaluation process will accept only the products that comply with evaluated and certified PPs. This requirement may sound unbusinesslike for developers of products with no predefined PPs, but will serve the users by ensuring through analysis of security threats, objectives, and risks for the target of evaluation.

A national repository of PPs, produced either internationally and certified by the National Certification Body (NCB), or produced locally, will serve as the basis for production of high quality security services and products. The System Security Engineering Capability Maturity Model (SSE-CMM) [10] provides a standard metric to establish security engineering as a mature and measurable discipline. A SSE-CMM based engineering process increases the likelihood that a quality PP will be developed. Engineers can improve the predictability of their process so that the difference between the target and actual results will be kept at the minimum. The model recognizes that security engineering is a complex undertaking that requires interaction of several different processes and parameters. Fig. 2 shows the general environment addressed by a risk assessment process, where threats and assurance elements are modeled with respect to vulnerabilities caused by the threat environment and the TOE.

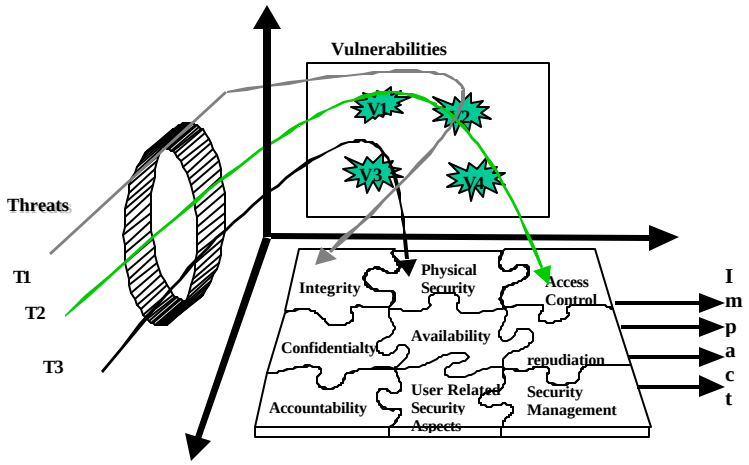


**Fig. 2:** Threat-Impact model

*C. National Scheme for IT Security Evaluation*

We will herby suggest establishment of a National Information Security Body (NISB). The NISB will, furthermore, have the responsibility for conducting a scheme to evaluate and certify the trustworthiness of security features in IT products and systems. The National Information Security Evaluation Scheme (NISES) will have the objective to meet the needs of Industry and Government for cost effective and efficient security evaluation and certification of IT products and systems with conformance to CC Evaluation Validation scheme. The scheme should also provide a framework for the international mutual recognition of certificates in compliance with the CC. The scheme will have the main role of offering evaluation and certification services to vendors, procurers, and accreditors.

The scheme will establish the National Certification Body (NCB) to certify the results of evaluations of IT systems and products. The NCB will also conduct and monitor the entire evaluation certification process. The NCB procedures should comply with ISO Guide 65 [4]. The scheme should also establish an organizational and procedural framework for the conduct of evaluation facilities, who carry out the evaluations, and establishment of approved techniques and procedures. In conjunction with this, the NCB will mandate Certification Laboratories (CL) to perform evaluations. There are already established certification laboratories around the world, e.g., Science Applications International Corporation Common Criteria Testing Laboratory [12]. The NCB plays an active role in the evaluation process by:

- Determining whether a TOE will be certifiable in principle before accepting a proposed evaluation into the scheme,
- Monitoring all evaluations conducted under NISES in a manner appropriate to the assurance level.
- Assessing all evaluation results and issuing certificates as appropriate.

The NCB recognizes the sets of evaluation criteria and methodologies associated with them, whose currently recognized scheme will be based on Common Criteria/Common Methodology for Information Security Evaluation.

## V CONCLUSIONS

We have shown that a great part of Turkish e-business relies on non-evaluated IT products. In order to decrease the negative cash flow from the national treasury, the level of confidence in consumers should be increased for involving them more into the e-business. Furthermore, we have summarized the security requirements of Web-enabled applications, and proposed an indispensable scheme to evaluate security systems and products. We have also emphasized the importance of a national certification scheme and a certified PP repository, and conformance of the national scheme NISES with the widely accepted international standard CC/CEM. The NISES and its conformance to Common Criteria/ISO IS 15408 are worth nothing if not government approved national standards and policies are in place and enforced by the majority of IT community. The industry and government supported standards and policies should, at a minimum, specify the followings:

- Support of the use of certified products,
- Building and managing national PP repository, specially including certified PPs,
- Designating certified evaluators and accreditation authorities,
- Supporting non-governmental commercial evaluation facilities,
- Creating policies for use by developers and vendors, and legalize enforcement of the policies,
- Encouraging consumers to use certified products,
- Endorsing establishment of information systems security certifications consortium and task the consortium to certify industry professionals and practitioners in an international standard,
- Endorsing establishment of National Institute of Information Technology and task the institute to develop necessary standards and policies for IT and IT security,
- Augmenting and legalizing the national certification system with cross-certifications so that mutual recognition arrangements can be signed with EU or other nations supporting the CC.

Stated that, all necessary measures are taken by the government for establishing NISES, there would be a small step further to achieve the unforeseen confidence in the Internet consumer of Turkey. Last but not least, with respect to ISO/IEC 15408 and European Union (EU), Turkey will also have to join the internationally recognized mutual recognition scheme.

## REFERENCES

[1] Common Criteria/ISO IS 15408, Version 2.1, October 1999, http://csrc.nist.gov/cc/ccv20/ccv2list.htm
[2] ITU-T X.509 www.itu.int/itudoc/itu-t/rec/x/x500up/x509.html
[3] ITU-T X.800 Security Architecture for Open System Interconnection, http://www.itu.int/itudoc/itu-t/rec
[4] NIST: http://www.nist.gov/
[5] RFC 2246 The TLS Protocol, http://www.ietf.org/rfc/rfc2246.txt
[6] RFC 2828 Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt
[7] RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[8] ISO/IEC 15292 Information technology -Security techniques- Protection Profile registration procedures, http://www.csrc.nist.gov/cc/t4/wg3/27n2601.pdf
[9] ISO Guide 65 Assessments of Organic Certifying Agencies: http://www.ams.usda.gov/lsg/arc/audit.htm
[10] System Security Engineering Capability Maturity Model, Version 2.0, April 1999, http://www.sse-cmm.org/metric/metric.htm
[11] ISO/IEC JTC 1/SC 27/WG3 N452, Guide for Production of PPs and STs, Version 0.6, July 8 1998, http://csrc.nist.gov/cc/t4/wg3/3n452.pdf
[12] Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL), September 2002, http://www.saic.com/infosec/pdf/CCTL-ITE.pdf.