A FRAMEWORK FOR EVALUATION OF INFORMATION SYSTEMS SECURITY

Job Asheri Chaula[a], Louise Yngström[b], and Stewart Kowalski[c]

[a]Department of Computer and Systems Sciences, Stockholm University/KTH, Sweden

[b]Department of Computer and Systems Sciences, Stockholm University/KTH, Sweden

[c]Department of Computer and Systems Sciences, Stockholm University/KTH, Sweden

[a]si-jac@dsv.su.se , Forum 100, 164 40 Kista, Tel: +46 (0) 8 161992, Fax: +46 (0) 8 703 90 25

[b]louise@dsv.su.se , Forum 100, 164 40 Kista, Tel: +46 (0) 8 161610, Fax: +46 (0) 8 703 90 25

[c]stewart.kowalski@ericsson.com, Forum 100, 164 40 Kista, Fax: +46 (0) 8 703 90 25

ABSTRACT

Evaluating information systems security is a process which involves identifying, gathering, and analysing security functionality and assurance level against criteria. This can result in a measure of trust that indicates how well the system meets a particular security target. It is desirable that the trust one can have on system is measurable and quantifiable through out the systems life cycle. Generally this is referred to as Information Security Assurance.

However, security assurance is costly and time consuming. This can partly be attributed to non technical assurance factors, the choice of assurance technique and tools, composition, lack of reuse, life cycle assurance and lack of metrics which are essential for cost and effort estimation. Assurance for complex systems like electronic commerce is still abstract because when the systems complexity increased, it becomes harder to examine whether security requirements has been met and therefore the concept of perfect security proves to be unachievable goal for both computer systems vendors and consumers.

This work is based on the Common Criteria (CC) which is an established method for security functions identification, assurance levels classification and development of Protection Profiles. In this research an Information Security Assurance Framework is proposed. This can be used to address the Information Security Assurance problem taking into consideration non-technical assurance factors, re-use of Protection Profiles and use of security metrics in the process of information assurance. A Protection Profile defines an implementation-independent set of IT security requirements for a category of IT products. Such products are intended to meet common consumer needs for IT security. Consumers can therefore construct or cite a PP to express their IT security needs without reference to any specific product.

KEY WORDS

Information Security Assurance Framework, Security evaluation, security metrics, Protection Profile, Common Criteria and Protection Profiles re-use.

A FRAMEWORK FOR EVALUATION OF INFORMATION SYSTEMS SECURITY

1. INTRODUCTION

Today the understanding of key organisational goals or key performance indicators like cash flow, customer satisfaction, shareholder value, strategic plans, new designs, return on investment, etc. is essential to organisations success. In order to achieve these goals, organisations invest in Information and Communication Systems which are used to store, process and transfer information over private and open networks. While the benefits ICT brings to business success are indisputable, there exist serious security problems that can be attributed to technical factors and non technical factors that may cause information systems to fail any time in systems life cycle. This implies that information security assurance must be taken into consideration as part of the business and systems engineering processes [Viega2003, Bishop 2002, and Schneier 2000].

Information systems security assurance is an aspect of trust, on the system, which is based on the system's specification, design and implementation. This requires specific steps to ensure that the system and its components will not violate the specification under normal conditions. Although the Columbia shuttle accident, in 2003, was not caused by software but by a physical damage on the left wing tile that resulted heat due to re-entry to penetrate inside and eventually destroy all the 7 crew and the shuttle [CAIB 2003]. This accident reminds engineers in all field how assurance is necessary in the systems life cycle.

After in-depth investigation about 45 fixes were suggested by the investigation board and more than 100 by NASA. Now NASA has a trust that the shuttle is safe enough for launch to the International Space Station and the eventual re-entry. Moreover, while the shuttle is in space, NASA has provided for a mechanism for the exterior of the shuttle to be inspected and repaired if any crack is found. Indeed this is assurance through out the life cycle.

There are several challenges in the process of assurance. One is how to increase software systems engineers' assurance awareness [Bishop 2002], Composition when systems with different assurance level are integrated or have to interoperate [Cater 2004], non-technical assurance factors, lack of harmonised assurance metrics for high assurance products and high cost and effort.

In order to address some of these challenges, a Framework for Information Systems Assurance is proposed. The primary objective of the framework is to improve the assurance process through out the systems life cycle by taking into account no-technical assurance factors, Protection Profiles re-use and the examination of assurance metrics and systems composition. This work is based on The Common Criteria assurance standard [CCIMB-2004-01-003], The Systemic Holistic approach [Yngström 1996] and the social technical model [Kowalski 1994]. The combination of these models is useful for addressing the assurance of information systems security today where our world is no longer defined by physical boundaries and cultures. As a result non-technical factors are real factors in systems assurance process. Therefore a holistic approach and frameworks to examine the human element and organisational behaviour are required.

2. INFORMATION SYSTEM ASSURANCE FRAMEWORK

Figure 1 represents framework key components in a logical arrangement. The input is a non trusted system which we want it subjected to the assurance process. Practically this could be a system we want to develop or to procure and we want assurance to be part of the overall system engineering process. The assurance life cycle is necessary to address assurance needs in the entire life cycle of the system because errors and flaws can happen either due to faulty policy, design, implementation

or operation procedure. The non technical issues are difficulty to handle because they encompass social and cultural parameters which cannot be easily defined, predicted and controlled. These are the factors which mostly define the environment in which the system will be used.

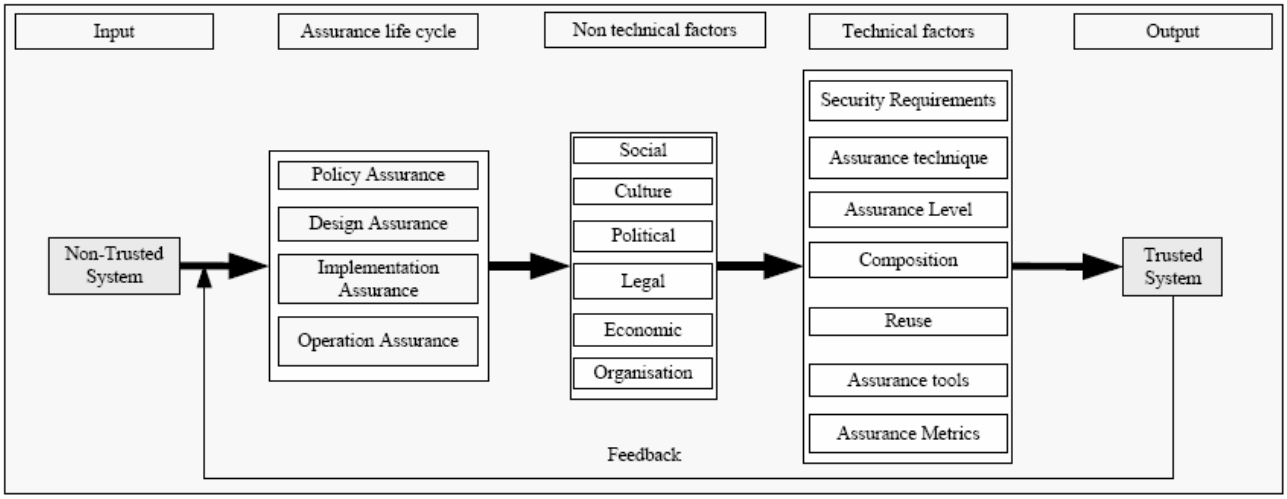

Figure 1 Information security assurance framework key components

The technical factors are real factors in the sense that the need for assurance technique may vary depending on the environment in which the system is used. The output is the evaluated system which might be updated or reconfigured. Consequently this may affect the security of the system. The feedback is necessary to make sure the evaluated systems assurance is maintained whenever the system undergoes some changes.

3. ASSURANCE LIFE CYCLE

The life cycle starts when the system is considered for development/procurement and use. The life cycle ends when the system is no longer used. The concept of lifecycle addresses security decisions that are often made outside the engineering field in business environment. Assurance requires a life cycle model in every step. For a small project where teams are small and the interaction with other stakeholders is not much, an informal assurance model could suffice. However, for a complex project formal assurance model may work best. A typical life cycle process is defined in stages: policy, design, implementation and operations. Assurance in these stages involves establishing the evidence that the security requirements are met. This is important because most of us know that ad hoc add on techniques tend not work [Viega 2002].

Table 1 Assurance life cycle

Policy Assurance	Design Assurance	Implementation Assurance	Operational assurance
Is a process of establishing that security requirements in the policy is complete and address the technical and non technical factors	Is the process of establishing that the design meets the requirements of the security policy	Is the process of establishing evidence that implementation is according to security requirements of the security policy and the design	Is the process of establishing evidence that the systems policy security requirements are not compromised during installation, configuration, patching, and daily operations

Patches must meet the same security requirements as the original product. Third part extensions as well must meet the same security requirements. Since systems we use are extensible security flaws can easily be introduced into the system when third party software is installed. It is crucial to maintain the assurance level of the original development whenever need to install third party extension arise.

4. NON-TECHNICAL FACTORS

Ross J. Anderson [Anderson 1974] in his famous paper, why cryptosystems fail, pointed out non technical assurance factors which are still true today. Systems fail partly because of implementation and management errors which can be attributed to human factor, organisational factors and other environmental factors. Figure 2 represent how non technical factor generate/influence the human and organisation factor. These may eventually affect the technical assurance factors. Kolwaski [Kowalski 1994] in his social technical model, have examined ethical attitudes, political and legal issues. [Schlienger 2003] has presented related work where he points out that human are real factors in the process of security assurance.

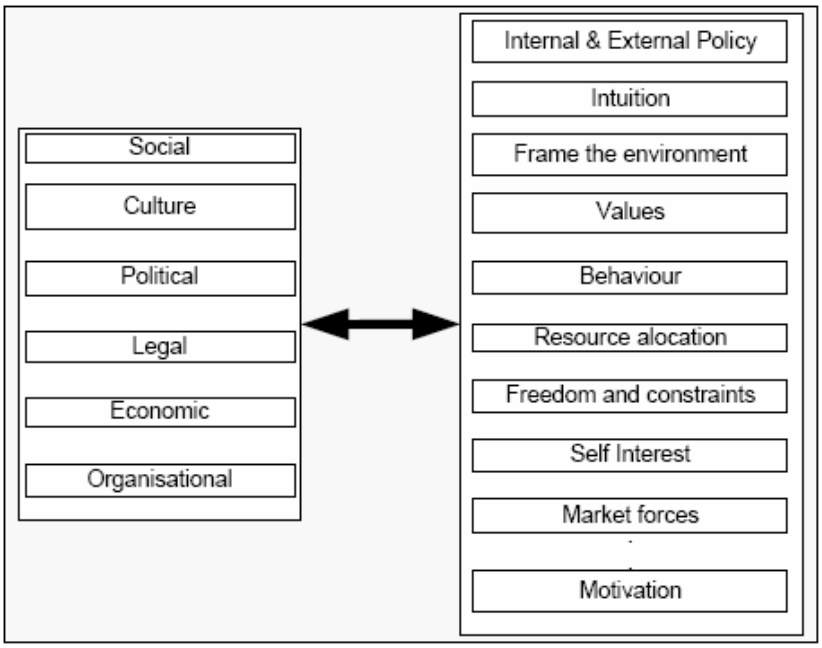

Figure 2 Non technical assurance factors

Social system of values, norms and beliefs influence the cultural and political system. Culture has to do with power distance, individualism, collectivism, quantity and quality of life, uncertainty avoidance and orientation for short term and long term [Robbins 2003]. These attributes of culture influence behavior, tolerance, expressions and art. The political system is influenced by cultural forces and plays big role in adjudication of resource allocation, defines formal mechanisms for redress of problems and determines the shift between reactive and proactive. The legal system codifies the social, cultural and political beliefs. It is expected to regulate behavior and set standards for dispute resolution. The economic system is based on the political system and is guided by competition and market forces.

The relation between non technical issues defined the frame of the environment in which information system are developed and operated, the human behavior, values, the way people think, syntax and semantics, etc. Therefore, security failure can be due to any of these factors. These should be understood by systems engineers because are useful to understand how security failures can happen as opposed to the traditional way of looking at what failures can happen. The two should be treated as a set. If non technical issues are taken into consideration, the way assurance techniques, tools and metrics are chosen will improve and eventually the way policies are developed and the whole assurance life cycle may improve as well.

5. TECHNICAL FACTORS

Security assurance technical factors encompass policy, assurance technique, tools, re-use, and composition and assurance metrics. The choice of these tools assurance level requirements and the environment on which system is being used. Some assurance techniques are useful by evaluators

who are really concerned with quality of system engineering process. Others are useful to engineers who are concerned with evaluating the system itself and its component. Also metrics that can be used to evaluate a process vary from those used to evaluate products.

5.1 Security Policy

A security policy is a high-level specification of the security properties that a given system should possess through out the life cycle. It is a means for designers, evaluators, implementers and auditors to communicate with each other. It is a blueprint to drive a project from design through implementation validation and operations [Anderson 2001].

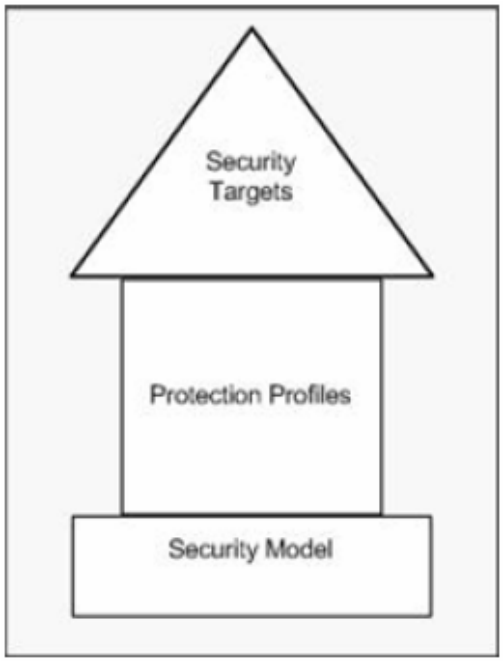

Figure 3 Security policy

A good policy must explicitly state the protection mechanisms and the way how breaches are to be detected. To address this need, in the Common Criteria standard terms like protection profile and security target are introduces. A Protection profile is an implementation independent security requirement. It is implementation independent to allow comparison of evaluated products and their versions. A security target is a detailed description that a specific implementation must provide [CCIMB-2004-01-003]. Detailed and implementation independent security policies must base on a security policy model. A security policy model usually is less than a page description of the security properties that a system must have.

5.2 Assurance techniques

Assurance techniques development has been underway for the past several decades. Today the Common Criteria [CCIMB-2004-01-003] has been widely accepted for evaluation of information systems. Common Criteria (CC) defines seven assurance levels namely EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, and EAL7, which are metrics levels used to rank assurance on products. The strictness of security requirement increases from EAL1 to EAL7. EAL7 demands formal specification methods. Today the international community has embraced the CC through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of CC evaluations performed by other CCRA members. This minimizes duplicate evaluations of similar product by consuming and producing nations. However CC evolves and later version must address issues related to composition and reuse of protection profiles and the evaluation of cryptographic algorithms. If the system included cryptographic algorithms, then FIPS140-1 can be used to validate the cryptographic algorithm.

Trusted systems can be developed by applying assurance techniques to the process of developing the system. This kind of assurance techniques takes into account issues like the quality of system engineers training and the team management [SSE-CMM]. The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning. The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The model is intended to be used as a tool for engineering organizations to evaluate security engineering practices and define improvements to them and as a Standard mechanism for customers to evaluate a provider's security engineering capability.

5.3 Re-use

Re-use is a central issue in OO programming. Re use of classes and functions is generally believed to reduce the effort required to complete the entire product. This will eventually reduce total development cost. Similar motive can be applied for Protection Profiles re-use. PPs are structured into the following sections: Introduction, TOE description, Security Environment, security Objectives, Functional and Assurance requirements and Rationale. The CC structure also provides great flexibility in the specification of secure systems. Consumers and vendors can specify the security functionality of a product in terms of standard protection profiles, and independently select the evaluation assurance level from a defined set of seven increasing Evaluation Assurance Levels (EAL), from EAL1 up to EAL7. Re-use could be achieved by upgrading or down grading the PP to meet the security requirements of the new system.

5.4 Composition

Re-use and composition are somewhat related problems. Since systems are layered for example operating systems and the applications or the software and hardware. Composition is tricky in the sense that a security component in one layer which is designed to handle critical data may pass data to components in another layer which are only assumed to be secure. To address such problems a through analysis of composition type has to be performed, the interface and the dependence of functions should be identified and analysed, and functional properties preservation analysis must be conducted. Most important is the analysis of policy composition is very important. The composite policy will eventually be used as abase for the rest of composition process.

6. CASE STUDY

The framework has been applied at the Tanzania electric supply company (Tanesco) specifically at the energy prepayment section. The company believes this systems is better than the conventional billing systems due to the following factors: Improve Revenue collection- (payment is up front), Improve Customer care, No meter readers required, no account posting or additional billing system required, no disconnection and reconnection fees, cost effective, time of use tariffs, no need to access the customer’s property, etc. In addition to these the vendor asserted that the system especially the hardware is secure. However our analysis revels that it is possible to defraud the system in many ways. Point of failures is spread across technical factors and non technical factors.

Figure 4 depicts the prepayment system. The system has off line and online disk transfer mechanisms to transfer data from vending stations to the regional office and finally from the regional office to the head office. Electricity meters at the customer site are not smart meters in the sense that they are only meant to accept data from the CDU and SMS they do not send back data to the system either offline or online. Currently there are two types of meters token and keypad. The CDU comprise a database, the LUKU application, Print Reader Writer (PRW) and a touch screen. The PRW is used to read the token, code power into the token and also can cancel power from the token. PRW interface to the system is called ISBX.

The security module contains keys and algorithm that are necessary to complete a transaction.

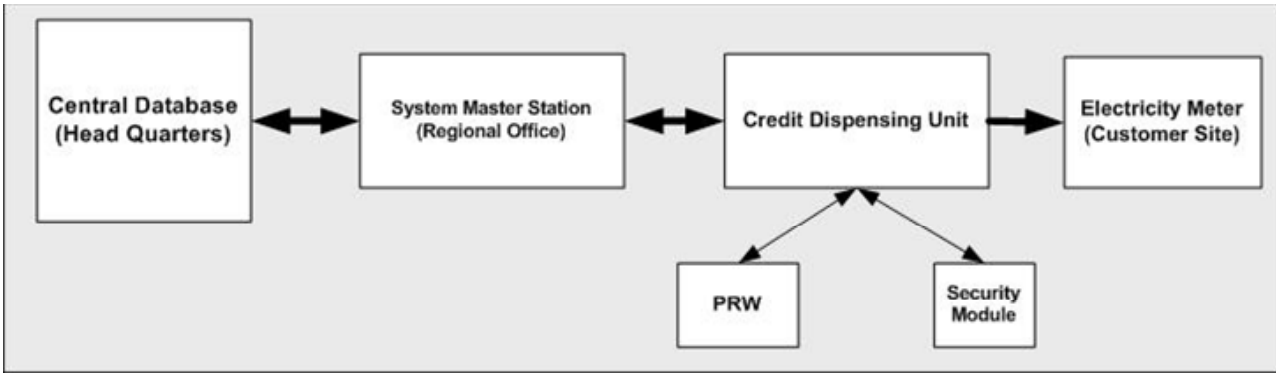

Figure 4 Tanesco Electricity Pre paid system (LUKU)

6.1 Identified fraud

Firstly, The CDU operators can simply defraud the system by inserting the second token while the printer is coding power in the token which is inserted previously. This results into disturbing the PRW speed setup and error message, ISBX error please insert card, is generated. If another card is inserted the PRW does a speed setup and coded the second token with the same amount of energy of the previous token. Then the operator goes ahead cancelling the transaction and sells the token. Further investigation revelled that the database does not record cancellation. The second flaw happens when there is a power cut the system loose data and a recapturing has to be done. If this happens when a transaction is being processed it is possible that the transaction will not be recorded although the token is coded. At the end of the day there will be more cash than the amount in the database. Currently the system has been updated to record cancellation and also the database is upgraded from Msaccess to Oracle and tokens are audited to prevent any misuse and fraud.

Secondly, one operator attempted the similar fraud and millions went missing. This time before firing the operator, the company filled a legal case. During court examination the defence attorney posed questions ranging from weather the operator new the system, trained, given exam, passed the exam and whether given a certificate as evidence. Unfortunately the answer to the last question was no. No certificate was issued because the training was in house training. The verdict to this case was the defendant is free because the evidence was not beyond reasonable doubt. Unlike the previous cases of point of failure, in this case the point of failure was a procedure which is non technical. In this case the organisation can do little to influence the legal system, it can do more to improve procedures like issuing exams and certificated after in house training courses.

Thirdly, since the meters are not smart in the sense we described above, outsiders manage to manufacture both types of tokens and sell them in the streets at around half price. While this is more damaging than the previous two cases, the framework can only be used by the company to minimise the probability of such attacks to occur but it requires other state law enforcement like the legal system to attempt to address the problem.

After the analysis of the system flaws and threats, one component of the framework had been implemented that is developing, protection profile, and a mid level policy which details implementation independent security requirement of energy prepaid system using an assurance technique Common Criteria [CCIMB-2004-01-003] which is well established.

Figure 5 summarises the key component of the protection profile for the energy industry prepaid system in Tanzania. The introduction section of the PP comprises the identification of the PP and its overview. This section includes the title of the PP, authors, version number and the assurance level.

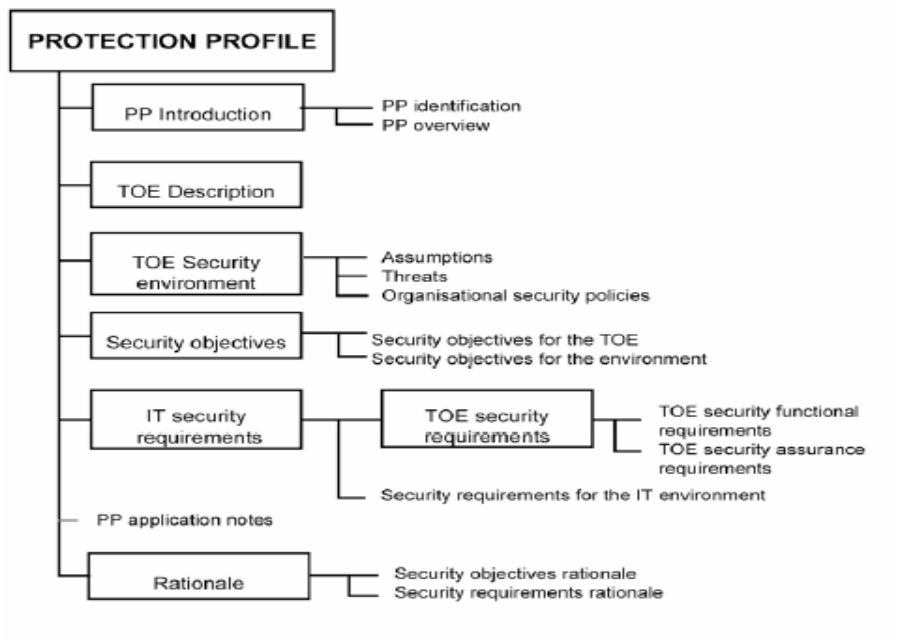

Figure 5 Energy Prepaid System Protection Profile Content [CCIMB-2004-01-003]

The assurance level for this PP is AEL3+ this level is detailed in [CCIMB-2004-01-003]. This Protection Profile specifies the Information Technology (IT) security requirements for TANESCO Electricity Prepayment System application. The system comprises the credit-dispensing unit (CDU), System master Station, Electric Dispensers (meters). The same application software runs on the SMS and CDU. The security requirement in this PP applies only to the application software.

6.2 Attacker capability

Attackers are assumed to have various levels of expertise, resources, and motivation. Attackers can either be insiders or outsiders. Relevant expertise may be in general semiconductor technology, software engineering, hacker techniques, or the specific system. Resources may range from personal computers and inexpensive card reading/coding devices to very expensive and sophisticated engineering test, measurement devices, and replica of Tanesco vending devices. They may also include software routines, some of which are readily available on the Internet. Motivation may include economic reward, resentment, or notoriety of defeating high-grade security. Given sufficient time and expertise, any electricity vending application software can be compromised.

6.3 Threat to Security

The PP is required to counter threats that may be broadly categorized as:

- Threats addressed by the system:
    - Threats associated with physical attack on the system
    - Threats associated with logical attack on the system
    - Threats associated with control of access
    - Threats associated with unanticipated interactions
    - Threats regarding the security module
    - Threats that monitor information
- Threats addressed by the Operating Environment

Table 2 Summary of the components of the PP

No	PP COMPONENT	DETAILED COMPONENT
1	**System security Environment**	Assumptions regarding threats
		Assumptions regarding policies
		Threat addressed by the system
		Detailed attacks countered by the system
		Threats addressed by the system with support by the
		Attacks countered by the environment
		Organisations general security policies of the system
		Organisations detailed policies assigned to the
		Organisations general security policies for system
		Organisational detailed security policies assigned to
2	**Security Objectives**	Security objectives for the system
		Security objectives for the environment
3	**IT security Requirements**	Systems security functional requirements
		Security assurance requirements
4	**PP application notes**	Notes on evaluating this PP
		Document construction method
		Assurance requirements for FIPS 140-1
5	**Rationale**	General threat and attack rationale
		Attack and security objectives correspondence
		Detailed policy and general policy mapping
		Detailed policy statement and security objective
		Security objective security requirements rationale
		Security requirement dependence analysis

Policy is central in the process of developing PPs. The management need to make sure policies are available especially to the technical people who are working on systems on a daily bases. Security environment includes analysis of threats that the system will address together with the environment. The security objectives have to do with administrative capability in regard with user data and high level and low design, misuse, etc. The application notes include document construction method and profiling knowledge base. The security requirements details security audit, user data protection, trusted path, identification and authentification, etc. The rationales will details functional dependency rational as well.

This protection profile can apply to any similar application regardless of the implementation requirements. It could be used immediately when Tanesco would like to upgrade the system or path the system to include more secure functions. Also they can use the PP for procuring a new system or auditing the existing system.

7. HOW NON-TECHNICAL FACTORS COULD IMPROVE ASSURANCE PROCESS

Providing guidelines how to include non technical parameters in the process of security assurance is a big challenge because non-technical factors differ depending on the society and its culture. However, today teams which develop information systems are mult-culture and similarly vendors and consumers may have different cultural background. Therefore, understanding non technical issues is necessary prier to commencing assurance process. Non technical factors add value to the assurance process in the following aspects:

- To improve communications by asking the right questions before accepting the meaning
- To increase awareness
- They drive both internal and external policy
- They frame our environment and define many of our operating parameters
- They, more than technology, define who we are and what we feel is important
- They represent what we think and feel

8. CONCLUSION

Consumers of information systems have to drive information systems assurance. It is common for vendors to assert that the system is secure while they mean the system has a security component like login a module. Information security assurance requires planned selection of techniques and non technical factors study prier to technical assurance factors. Presently there numerous tools addressing security assurance in a somewhat different way, depending, on the environment more than one techniques can be combined to address a single product or process.

The proposed framework is useful to guide systems security engineers to understand non technical issues when developing requirements. This may minimise problems related to scenarios where completely the wrong thing is being protected or protecting the right thing in the wrong way. Traditional protection profiles surface to address technical systems requirements. However, the link between non technical issues to protection profiles is that protection profiles are developed based on the assumptions that are dependant on the environment. If the environment is not correctly understood there will be a risk of doing mistakes when developing requirements.

Issues related to assurance awareness amongst engineers and managers, and re-use are still research topics. Problem to awareness can be attributed to the non technical issues that are presented in this paper. Questions like do all managers mean the same this by information systems security? Do engineers mean the something when discussing about security assurance? These questions are not trivial today just like in the past because differences in cultures.

9. REFERENCES

[Viega 2003] John Viega, 2003, Building secure software, How to avoid security problems the right way. ISBN 0-201-72152-X, McGraw

[Scheneier 2000] Bruce Scheneier 2000, Secret and Lies, Digital Security in a Networked World

[Bishop 2002] Matt Bishop, 2002, Computer Security Art and Science, ISBN 0-201-44099-7.

[CAIB 2003] CAIB 2003, Columbia investigation Board, CAIB Report volume 1. http://www.caib.us/news/report/pdf/vol1/full/caib_report_volume1.pdf

[Cater 2004] Denise Cater, 2004, BT, Composition - can we "add" certified products, ICCC proceedings, Berlin, 2004

[Kowalski, 2004] Stewart Kowalski, Ericsson Research, Sweden, Protection Profile Reuse Can Save Time and Money, ICCC Proceedings, 2004, Berlin.

[CCIMB-2004-01-003] CCIMB-2004-01-003, 2004, Common Criteria for Information Technology Security Evaluation: Security assurance requirements and Protection Profiles Version2.2

[Yngström 1996] Louise Yngström, (1996), A systemic-holistic approach to academic programmes in IT security. ISBN 1101-8521, ISRN SU-KTH/DSV/R—96/21 SE

[Kowalski 1994] Stewart Kowalski, March 1994, “IT Insecurity: A Mult-disciplinary Inquiry” ISSN 1101-8526, ISRN SU-KTH/DSV/R—94/4—SE

[Anderson 1974] Ross J. Anderson, 1974, Why Cryptosystems fail, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/wcf.pdf

[Schlienger 2003] Thomas Schlienger, 2003, Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture, Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA’03) 1529-4188/03

[Anderson 2001] Ross J. Anderson, 2001, Security Policies, University of Cambridge, Computer Laboratory.

[Robbins 2003] Stephen P. Robbins, 2003, Essentials of Organisational Behaviour, ISBN 0-13-121448-7,

[Chaula 2003] Job Asheri Chaula, Security metrics and public key infrastructure interoperability testing, Philosophy of Licentiate Thesis, Department of Computer and Systems Sciences, Stockholm University (DSV), Stockholm University and Royal Institute of Technology, 2003.

[SSE-CMM] SSE-CMM, 2003, Systems Security Engineering Capability maturity Model, (SSE-CMM Version 3) [Online] Available at: http://www.sse-cmm.org/model/ssecmmv2final.pdf (Accessed in July 2003)