# SECURITY METRICS AND EVALUATION OF INFORMATION SYSTEMS SECURITY

**Job Asheri Chaula[1], Louise Yngström[2], and Stewart Kowalski[3]**

Department of Computer and Systems Sciences, Stockholm University/KTH

Forum 100, 164 40 Kista, Sweden
Tel: +46 (0) 8 161992
Fax: +46 (0) 8 703 90 25
E-mail: {si-jac[1], louise[2], stewart[3]}@dsv.su.se

ABSTRACT

The evaluation of information systems security is a process in which the evidence for assurance is identified, gathered, and analysed against criteria for security functionality and assurance level. This can result in a measure of trust that indicates how well the system meets particular security target. However, as the information systems complexity increases, it becomes increasingly hard to address security targets and the concept of perfect security proves to be unachievable goal for computer systems developer, testers and users.

In this paper a framework for developing security requirements of information systems is examined. In this process qualitative metrics are used to yield quantifiable information that can be used to improve the evaluation process especially risk assessment, vulnerability assessment, protection profiles, and test coverage which are important aspects of systems specification. This work is based on the Common Criteria (CC) and the Systems Security Engineering Capability maturity Model (SSE-CMM). These are useful established methods for security functions identification, assurance levels classification and security processes and organisations maturity levels classification.

The security requirements are developed based on security functionality of the system and policy. In this research other aspects of systems security are taken into account. These include ethics and social aspects. In all aspects security metrics facilitate improved understanding of various security process, performance, and informed decision making of various security mechanisms and procedures implementation. Moreover, security metrics are useful for indication and determination of critical and non-critical security parameters, measuring test coverage and effort direction when evaluating a system and security processes. In this research it is expected that the out put will be a system specification framework that takes into account not only the technical aspect but which includes the social and technical issues. Systems specification in CC is referred to as Protection Profiles (PPs). This study is conducted in the developing world and x.509 certificates using application will be used as case study.

KEY WORDS

Security evaluation, security metrics, risk assessment, security process, protection profiles, and information systems.

# SECURITY METRICS AND EVALUATION OF INFORMATION SYSTEMS SECURITY

## 1 INTRODUCTION

The security evaluation, testing, risk assessment, and protection profiling (PPs) of information systems are processes in which the evidence for assurance is analysed against criteria for security functionality and assurance level [Bishop 2002]. The Common Criteria defines seven metrics for specifying and evaluating systems [CCIMB-2004-01-003]. This can result in a measure of trust that indicates how well the system meets a particular security target. Schneir asserts that systems insecurities are mainly due to lack of testing [Schneier 2000]. This is true and may be attributed to cost of systems testing, limitations in various testing methods and lack of harmonised security metrics. PPs development effort is directly related to specifying security targets and assurance levels [CCIMB-2004-01-003]. In this paper the development of PPs for X.509 certificate-using application in developing world environment is examined by making use of security metrics that are useful in the analysis of threats and risks [RFC 3280].

Security metrics are important indicators of how well security services are present in the information system and can be used to measure organisation's security maturity level [SSE-CMM]. Security metrics is tool that facilitates improved understanding, performance, Coverage, and decision making of various security processes, mechanisms and procedures [Swanson 2003] [Jelen 2000]. These are important aspects to be understood by users of information systems since normally they face insecurities problems that are not only related to technology but also which are related to their environments.

The Federal Bridge Certification Authority [FBCA 2002] has developed five certificate policies for use by FBCA to support PKI interoperability with other PKIs [FBCA 2002]. In this project certificate policy that represents assurance levels for public key certificates are developed and the following assurance levels are defined: Rudimentary, Basic, Medium and High. These levels are metrics that used classify critical and non-critical security functions of the system.

Ammann and Black, in their famous paper "A specification based coverage metrics to evaluate test sets"[Ammann 1999] they developed a methodology to test the coverage of test sets using metrics during testing high assurance applications using formal methods. Their objective was to compare test generation methods, evaluating the coverage of systems tests and minimizing the test sets [Ammann 1999].

The International Systems Security Engineering Association (ISSEA) has proposed 22 processes areas that need metrics formulation [SSE_CMM 2003]. The methodology used by ISSEA to develop metrics was adopted from [Swanson 2003]. Swanson is part of the team that developed metrics for NIST and these have been standardised as NIST 800-55 [Swanson2003]. Table 1.0 presents the ISSEA proposed PA01 to PA22 process areas that require metrics development. The PA01 through PA22 processes encompass organisational security processes that are necessary to measure organisational maturity level.

Table 1.0 presents the ISSEA proposed PA01 to PA22 process areas that require metrics development. The PA01 through PA22 processes encompass organisational security processes that are necessary to measure organisational maturity level.

*Table 1 Security process and security metrics areas as defined in [SSE-CMM 2003]*

| Process Areas | Process Areas Description |
|---|---|
| PA01 | Administer Security Control |
| PA02 | Assess Impact |
| PA03 | Assess Security Risk |
| PA04 | Assess Threat |
| PA05 | Assess Vulnerability |
| PA06 | Build Assurance Argument |
| PA07 | Coordinate Security |
| PA08 | Monitor Security Posture |
| PA09 | Provide Security Input |
| PA10 | Specify Security Needs |
| PA11 | Verify and Validate Security |
| PA12 | Ensure quality |
| PA13 | Manage configurations |
| PA14 | Manage Project Risks |
| PA15 | Monitor and Control Technical Efforts |
| PA16 | Plan Technical Efforts |
| PA17 | Define Organisation's Systems Eng. Process |
| PA18 | Improve Organisation's Systems Eng. Process |
| PA19 | Manage product line evaluation |
| PA20 | Manage Systems Eng. Support Environment |
| PA21 | Provide ongoing skills and knowledge |
| PA22 | Coordinate with suppliers |

Common Criteria (CC) also defines seven assurance levels namely EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, and EAL7, which are metrics, used to rank assurance on evaluated products [CCIMB-2004-01-003]. Further, related work has been done by [Stal 2000] who developed security targets for Entrust, the security metrics development in the X.509 Certificate Policy project for the Federal Bridge Certificate Authority [FBCA 2002], Department of Defence Public Key Infrastructure Token Protection Profile [PKIKMITKNPP-MR 2002], Public Key-Enabled Application Family of Protection Profiles [USMC 2002], and The PKI Secure Kernel Protection Profile [PKIPRO 2002].

Protection profiles are needed when setting a standard for a particular product type [CCIMB-2004-01-003]. Government agencies, organisations/consumers or developers can set these standards. PPs are also used to create specifications for systems or services as the basis for procurement. A Protection Profile is defined as "an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment" [CCIMB99-033]. These statements indicate that an in-depth understanding of the environment in which the PP will be applied is of great importance. This can be achieved through PP metrics standardisation. Efforts to standardise metrics is presented in [SSE-CMM] as an ongoing work, [CCIMB-2004-01-003] as guideline which indicate the depth of testing for a specific product to qualify for one of the seven assurance levels that are specified in [CCIMB-2004-01-003]. [Swanson2003] presents a metrics development methodology and examples of metrics useful for measuring organisational security processes maturity level.

The purpose of this research is to examine a framework that can be used to develop PPs by applying various established methods like CC, SSE-CMM, SBC and a social technical model. Security metrics that are critical for protection profile development work will also be examined. Although PPs may vary on varying environments, metrics that can be used to measure various

parameters in various environments can be standardised. Figure 1 presents the key processes areas when developing a PP. APE_ENV security environment involve the identification and analysis of threats and organisational policy [CCIMB-2004-01-003]. The security requirements are the function security requirements as outlined in [CCIMB-2004-01-002].

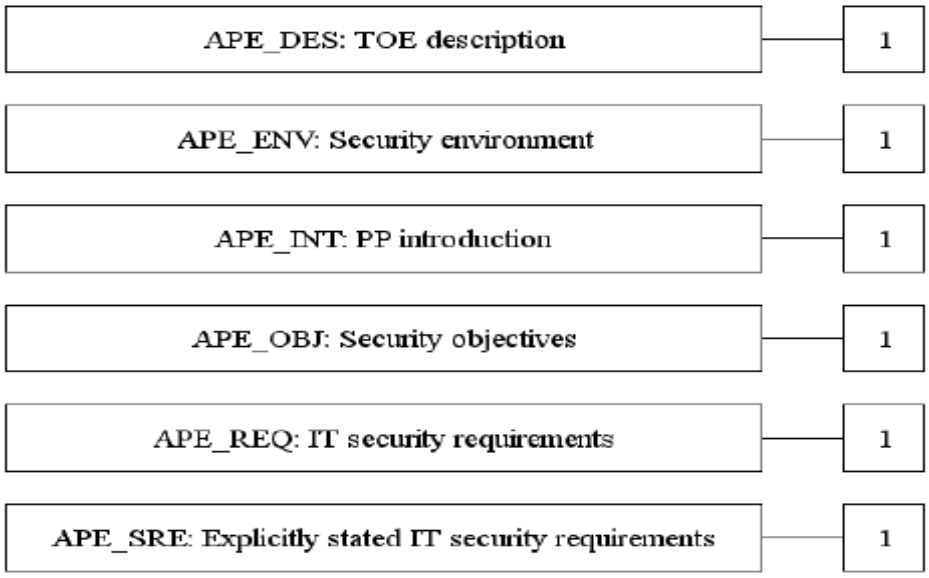


*Figure 1 Protection profile evaluation Class decomposition.*
*Source: [CCIMB-2004-01-003]*

In this research key process areas are critical assets identification, policy review, assessing how people perceive IT risks, measuring what people considers to be unethical and ethical when using IT systems, Identification of threat agents and perform threat analysis, performing risk assessment, performing analysis of security functions and finally developing the Protection Profile. These are summarised in Figure 2 below and further explained in section 3.

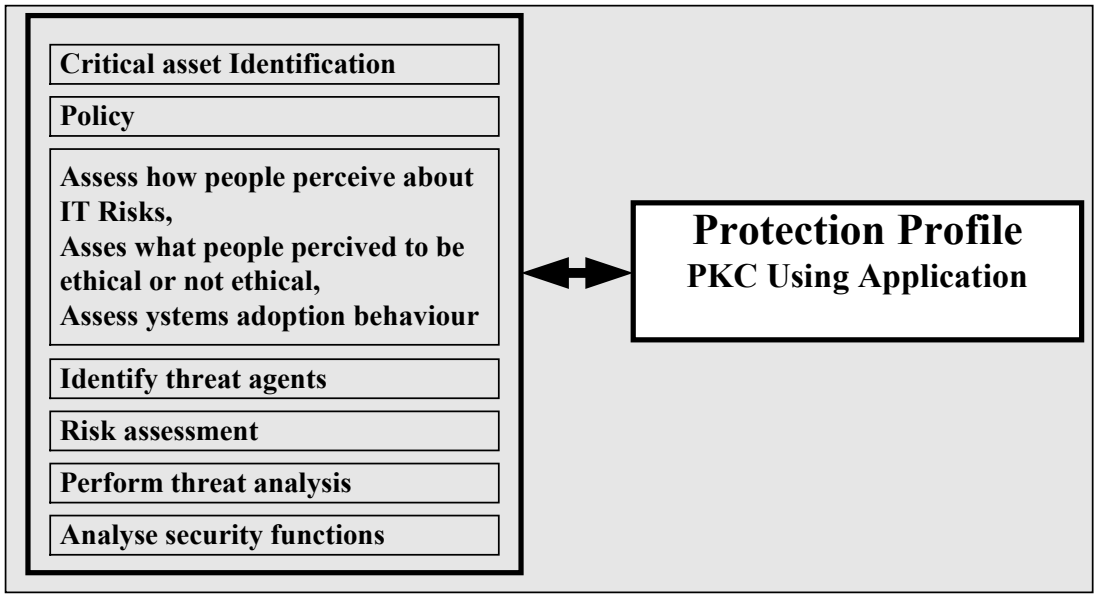


*Figure 2 Components of the PP development process*

## 2 RESEARCH APPROACH

The method in this research encompasses the use of the Common Criteria [CCIMB-2004-01-002] to identify security functions of a X.509 certificate using application in PKC environments. Threats associated with these security functions were identified and appropriate metrics were used to determine their impact. In this process metrics for ensuring coverage of security functions were developed. These are applicable in the process of developing protection profile where the issue of coverage is of great importance. Metrics proposed in [SSE-CMM] and [Swanson, 2003] are used to develop other metrics that are directly related to the security functions and the environment for instance assessing personnel security awareness, documentation, and other environmental related security processes. The contribution to the subject knowledge will be a framework for security specification. In the CC standard the specifications are termed PPs. These are normally based on security functions identified, policy, and environment. In this framework we want the environment to take into account other issues like ethics, social issues and legal environment. We believe it is difficult to address security issues using technology only. There must be a balance between technology and issues related to people behaviour. The study is conducted in the developing world. However, the findings may be useful for small and medium enterprises (SMEs).

Figure 2 represents the framework that will be applied in developing the protection profiles. CC and SSE-CMM are used to develop necessary metrics, identify security functions, and analyse threats that are not directly related to the society and organisational behaviour. The Systemic-Holistic model [Yngström 1996] and SBC [Kowalski 1994] are useful in this work for developing metrics that are related to security education, people, and society. However, they can also be applicable in other aspects of research in IT security.

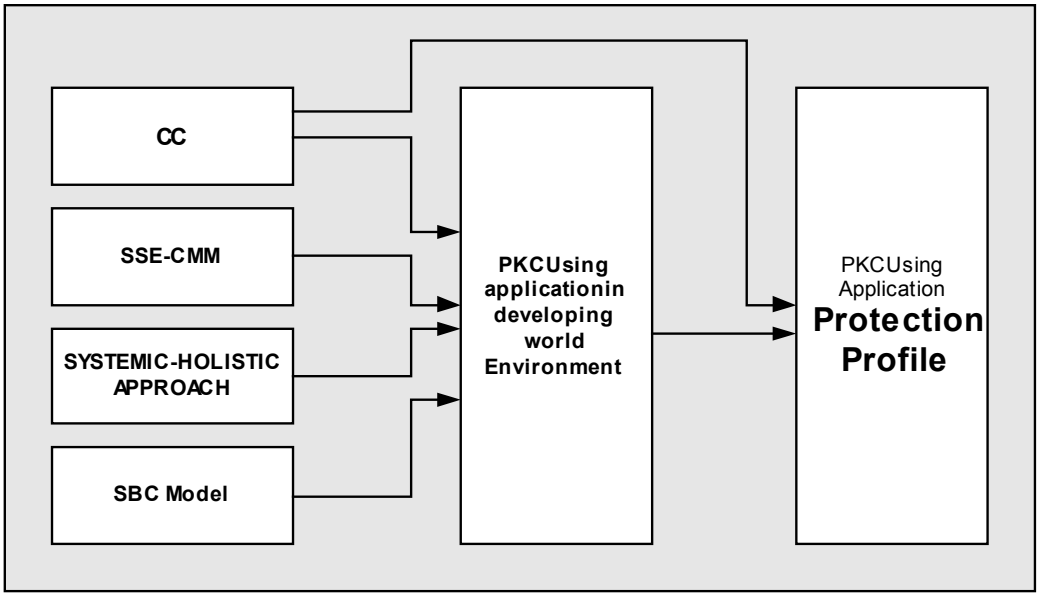


*Figure 3 Protection profile development framework*

## 3 METRICS, THREATS AND RISKS ASSESSMENT

These metrics can be used to indicate how severe an attack can be when a particular security function fails. This is useful in the view that in the protection profile such security functions that have high impact if it is compromised must be addressed by the TOE and tested with high coverage metrics. The metrics are classified into rudimentary, basic, medium, and high consequences. These are summarised in Table2 and are important in the process of PP development for indicating security functions that must be given more attention by the TOE and when verifying the PP itself.

*Table 2 Metrics for classifying Security functions impact to the organisation when compromised [FBCA 2002]*

| No. | Assurance Level | Applicability in security function prioritisation |
|---|---|---|
| 2 | **Rudimentary** | Security functions that are classified in this level provide data integrity security service |
| 3 | **Basic** | Security functions classified in this level are those involving objects that mitigate threats associated with data compromise |
| 4 | **Medium** | Security functions classified in this level are those involving objects that mitigate threats that may cause data compromise, fraudulent data access and malicious user. |
| 5 | **High** | This level applies to Security functions whose failure cause high consequences. |

### 3.1 Critical assets identification

In the process of developing PP prior to threat analysis the critical assets that we would like protected must be performed. Generally critical assets can be categorised in information, systems, software, hardware, and people. Information includes documentation, business plans, designs, customer base, human resource details, and financial information used to meet the mission of an organization. Information systems that process and store information comprise information, software, and hardware assets and any host, client, or server, access points, etc. Software comprise applications and services-such as operating systems, database applications, networking software, office applications, and custom applications. Hardware comprises information technology physical devices-such as workstations, servers, printers, photocopiers, network gadgets and physical transmission media etc. People the people in an organization who posses special skills, well trained, and experienced.

### 3.2 Security family and component structures

Table 3 Summarises some examples of the CC functional class family mapping to some of the security functional components of PKC application. This is one of important steps in PP development process. CC security functions are useful because they are designed to help evaluators to be able to understand, define and eventually prioritise security functions based on the impact of an attack to the system when a particular security function is compromised.

Table 3 Functional Family mapping to security functional component test cases

| PKC Application Security function Component structure [RFC 3280] | CC Security Function Family |
|---|---|
| Signature | User-subject binding (FIA_USB) |
| Issuer name | User identification (FIA_UID) |
| Subject name | User identification (FIA_UID) |
| Validity period | Security attribute expiration (FMT_SAE) |
| Issuer uniqueID | User identification (FIA_UID) |
| Subject uniqueID | User identification (FIA_UID) |
| Key usage | Access control policy (FDP_ACC) |
| Certificate policy | Access control policy (FDP_ACC) |
| Subject alternative name | User identification (FIA_UID) |
| Issuer alternative name | User identification (FIA_UID) |
| Policy constraint | Access control policy (FDP_ACC) |
| Extended key usage | Access control policy (FDP_ACC) |
| Inhabit any policy | Access control policy (FDP_ACC) |
| CRL Distribution point | Revocation (FMT_REV) |
| Certificate list to be signed | User authentication (FIA_UAU) |
| CRL Signature | User authentication (FIA_UAU) |
| CRL This update | Security attribute expiration (FMT_SAE) |
| CRL Next update | Security attribute expiration (FMT_SAE) |
| Revoked Certificate | Revocation (FMT_REV) |
| CRL Invalid date | Security attribute expiration (FMT_SAE) |

## 3.3 Threats analysis

Organisations either provide services, products or both. Apart from services and production businesses, organisation has the third category of key businesses that is management. One of the success factors in any organisation is how to manage people, information and other resources, when performing threat analysis it is important to take into account the three categories. Table 4 presents some of the IT assets, critical assets and threats associated to the identified assets. This process is important for understanding what is being protected or what the organisation wants protected.

*Table 4 PA04 Threats analysis*

| Core Businesses | Description | IS/IT Assets | Important information assets | Threats |
|---|---|---|---|---|
| **Services** | May include Business and Technical consulting Competency Development and Public service etc. | People, Hardware, software, information, systems | Patents, copyrights, Trade secrets, Trademark, Design, business plan, management information, customer information | Loss, Modification, Disclosure, damage, interruption |
| | | | | |
| **Products** | May include Systems, Transmission and Transport networks | People, Hardware, Software, Systems, Information | Patents, copyrights, Trade secrets, Trademark, Design, customer information | Loss, Modification, Disclosure, damage interruption |
| | | | | |
| **Management Functions** | Management information | People, Hardware, software, information, systems | Business strategies/plan, Financial information system, payroll, supplier information, corporate communications, Partners, Human resources, customer information/customer base | Loss, Modification, Disclosure, damage, interruption |

## 3.4 Threat agents

Table 5. Presents threats agents. These are causes of threats. Understanding threat agents is vital when developing strategy to hedge the threat. In this research the human threat agent will be studied

using the Systemic-Holistic and SBC models [Yngström 1996], [Kowalski 1994]. This is useful for developing PP that addresses environmental security problems.

*Table 5 Threat agents*

| Threat Agent | Definition |
|---|---|
| **Human** | Humans can be a threat using networks and physical access breaches. This can either be accidental or deliberate |
| **System malfunction** | The threats in this class are problems with an organisation's information technology systems. Examples include hardware defects, software defects, denial of service, Malicious code, viruses, Trojan horses, and other systems-related problems like buffer overflow, race conditions, determinisms problem in random number generation etc. |
| **Act of God or natural calamity** | The threats in this class are those beyond the control of an organisation. This includes natural disasters such as volcano, floods, earthquakes, tornadoes, and lightning. Other man made catastrophes are terrorism, Power outages, broken water pipes, rain leakage and poor infrastructure. |

## 3.5 Risks mapping and prioritisation

Table 6 presents some examples of risk mapping. If the likelihood of risky event is high and risk impact is high such risk should be considered critical and high level of assurance of security function that deals with it should be considered. Risk prioritisation can be made by grouping risks into key risks, these are those with high likelihood and high impact; secondary risks are those that either have high likelihood to occur or have high impact; and law priority risks, these are those with law and likelihood and impact [Alberts 2002]. Validity period risk impact is disastrous and the likelihood is high because time keeps changing and it is hard to predict when the verification will fail. The impact is disastrous because if the certificate is used outside the validity period it means a misuse and confidentiality might be compromised. Issuer and subject name risky incident likelihood is low because if the name encoding and the application configuration are done properly the occurrence of risky incident is minimal.

*Table 6 PA02 Risk assessment: mapping and prioritisation*

| **Risks** | **Risk Impact** | | | | **Risky Incident Likelihood** | | |
|---|---|---|---|---|---|---|---|
| **(Examples of fields of [RFC 3280])** | **Metrics** | | | | **Metrics** | | |
| | **Disastrous** | **Significant** | **Small** | **Rudimentary** | **High** | **Medium** | **Low** |
| Signature verification failure | X | | | | | X | |
| Issuer name verification failure | X | | | | | | X |
| Subject name verification failure | X | | | | | | X |
| Validity period verification failure | X | | | | X | | |
| Issuer uniqueID verification failure | | X | | | | | X |
| Subject uniqueID verification failure | | X | | | | | X |
| Authority key Identifier verification failure | | X | | | | | X |
| Subject key Identifiers verification failure | | X | | | | | X |

## 3.6 Security functions, Security services, and Assurance level

Table 7 summarises some of the security function of the certificate using application that are critical for ensuring certificate processing is accordance to the target. These security functions are based on [RFC 3280], [PKIX 2002] and are identified using the Common Criteria [CCIMB-2004-01-002].

The assignment of assurance levels to security functions of X.509 certificate is subjective to the environment or the usage of the application that verify the certificate. Assurance level could differ depending whether the application is used in a financial, school, or other business environments. However, assurance level for signature verification, issuer, subject name, and the validity period of the certificate are critical to the validity of certificate. These are also used to verify the bound between the subject and the certificate. It is recommended to keep the assurance for these functions high in all the environments and usage.

*Table 7 Security services addressed by security functions and the assurance levels*

| No | Applications Security Function [RFC 3280] | Threat Vs Security Service | | | | | | Assurance Level | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Integrity | Confidentiality | Authentication | Availabilit | Access-control | Nonrepudiation | Rudimentary | Basic | Medium | High |
| 1 | Certificate serial number verification | | | | | | | | X | | |
| 2 | Signature verification | X | X | X | | X | X | | | | X |
| 3 | Issuer name verification | X | X | X | | X | X | | | | X |
| 4 | Subject name verification | X | X | X | | X | X | | | | X |
| 5 | Validity period verification | | X | X | | X | X | | | | X |
| 6 | Issuer uniqueID verification | | X | X | | X | X | | | | X |
| 7 | Subject uniqueID verification | | X | X | | X | X | | | | X |
| 8 | Authority key Identifier verification | | | | | X | | | | X | |
| 9 | Subject key Identifiers verification | | | | | X | | | X | | |
| 10 | Key usage verification | | X | | | X | X | | | X | |
| 11 | Certificate policy verification | | X | | | X | X | | | | X |
| 12 | Policy mapping verification | | X | | | X | X | | | X | |
| 13 | Subject alternative name verification | | | X | | X | X | | | X | |
| 14 | Issuer alternative name verification | | | X | | X | X | | | X | |
| 15 | Name constraints | | X | | | | X | | | X | |

## 3.7 Social and ethics aspects of systems security

One of the critical IT assets identified in this paper is people. This may be one hardest of all to deal with in the process of securing information systems [Schneier 2000]. In this study this component will be given more attention where ethical issues, systems adoption, and how people perceive IT risk in developing world will be investigated. This objective will be approaching by the use of questionnaires that will be used to gather information from sample government agencies, hospitals financial institutions, and academic institutions. The inclusion of social/cultural aspect in the process of developing PP is a decisive factor between PP developed in developed world and the one developed in developing world. This study is expected to yield results that can be applied to develop PPs for other information systems that are required for use in the developing world.

Metrics that will be used in this case are quantity of people and time. These two are useful to determine early information systems adopters, early and late majority and those who late last to adopt information systems technology. Also same metrics will be used to measure what people consider to be ethical on unethical in regard to computer misuse and crime.

### 3.8 Policy metrics

Table 7 presents metrics that are related to policy. In the process of developing PP policy affects the PP requirements. Therefore, metrics of the existing policy has to be studied to determine the suitability of the policy on which PPs will base [PKIPRO 2002].

*Table 8 Policy documentation metric [Swanson 2003]*

| | |
|---|---|
| **Testing Goal** | To determine if there sufficient documentation explaining how IT systems has been installed. |
| **Associated question** | Is there any policy document? |
| **Metric** | Percentage of applications with documentation is file |
| **Purpose** | To make sure that IT systems police exist and well documented |
| **Implementation Evidence** | • How many organisations have IT policy<br>• Is the national ICT policy in place? |
| **Frequency** | Annually |
| **Formula** | Number of organisations with policy to Total number of surveyed organisations |
| **Data source** | Documentation repository/ National public documents |
| **Indicator** | The target is to 100 percent. As the percentage approach 100 it is an indication good best practice |

Remarks: The documentation metric can be applied further to determine the user awareness, existing security processes in the country/organisations.

## 4 DISCUSSION

The purpose of this work is to develop protection profiles of PKC using applications in the developing world. This requires an in-depth study of the environment, applications security functions, environmental assumptions, threats, and existing policy, ethics, criminology, legal environment and various mechanisms [FBCA 2002], [PKITKNPP-MR 2002], [USMC 2002], [PKIPRO 2002]. The most interesting part of this study is the study of people and society that we plan to carry out in Tanzania as a case study to represent the developing world. Understanding human behaviour and the way they behave when using IT systems is of vital importance in the field of IT security.

CC and SSE-CMM proves to be handy when identifying and developing security functions and metrics. CC presents the technical metrics and SSE-CMM presents metrics that are more environmental and these are really useful when examining environmental threats. However, in order to study the social part of the IT systems, Systemic-Holistic approach and SBC models are suitable. These will be applied to capture the nitty-gritty of how and why people misuse, mistreat, misunderstand etc. information systems. The assumption here is that, when the methodology is applied in the developing world environment the resulting PPs should be more suitable for the developing world than using PPs developed in a different environment, the developed world.

The metrics presented in this paper are sample metrics. These metrics will be applied in research, contacted in sample organisations and government agencies to determine the need and method that can be reusable in the future to develop PPs, specifications for procurement and specifications for systems development in the developing world. Risks impact and likelihood metrics which are presented in table 5, are some to extent subjective because the judgement whether they are catastrophic or the incident will happen in two years or ten years depends on the environment, time and other organisational factors.

To my knowledge, there is no PKC PP developed so far for the developing word. It is anticipated that this study is important and useful for the IT security research community to

understand the security needs of the developing world that is increasingly becoming connected to the developed world but the legal environment, ethics, criminology, altitude, and technology adoption behaviour remains different.

## 5 ACKNOWLEDGEMENT

We acknowledge the full sponsorship of SIDA for this research work

## 6 REFERENCES

**[Bishop 2002]** Matt Bishop, 2002, Computer Security Art and Science

**[Gollmann 2000]** Dieter Gollmann, 2000, Computer Security

**[Yngström 1996]** Louise Yngström, (1996), A systemic-holistic approach to academic programmes in IT security.

**[Ammann1999]** P. Ammann and P. Black, 1999, A specification-Based Coverage Metrics to Evaluate Test Sets, "Proceeding of the 4th IEEE International Symposium on High-Assurance Systems Engineering".

**[Ann 2001]** Ann Frisinger 2001 "A generic Security Evaluation Method for Open Distributed system", PhD thesis, Dept. Of Computer and Systems Science, Royal Institute of Technology, Forum 100, 164 40 Kista.

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

**[Stallings 2000]** William Stallings (2000), Network security essential applications and standards

**[Anderson 2001]** Ross Anderson, 2001, Security Engineering: A guide to building dependable distributed systems

**[Viega 2003]** John Viega, 2003, Building secure software

**[Alberts, 2003]** Christopher Alberts and Audrey Dorofee, "Managing Information Security Risks", The OCTAVE Approach. Addison Wesley, ISBN: 0-321-11886-3.

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

**[CEM-99/045]** 1999, Common Methodology for Information Technology Security Evaluation Methodology Version 2

**[Clark 1988]** Clark, David D., Wilson, David R.A., 1998, Evaluation of model for computer integrity.

**[CMM 1995]** Systems Engineering Capability Maturity Model, (SE-CMM Version 1.1). 1995, [Online] Available at: http://www.sei.cmu.edu/cmm/cmms/cmms.html (Accessed in August 2003)

**[CTCPEC 1993]** CTCPEC, 1993, Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) version 3.0

**[FIPS PUB 180-1]** Federal Information Processing Standards Publication 180-1, 1993, Available at: http://www.itl.nist.gov/fipspubs/fip180-1.htm, (Accessed October 2002)

**[Housley 2001]** Russ Housley, 2001, Planning for PKI: Best Practices guide for deploying public key Infrastructure

**[ITSEC 1991]** ITSEC, 1991, Information Technology Security Evaluation Criteria

**[Jelen 2000]** George Jelen, 2000, SSE-CMM security metrics. [Online] Available at: http://csrc.nist.gov/csspab/june13-15/jelen.pdf (Accessed in May 2003)

**[CCIMB-2004-01-002]** CCIMB-2004-01-002, 2004, Common Criteria for Information Technology Security Evaluation, Security functional requirements.

Security Evaluation, Security functional requirements.

**[McClure 2001]** Stuart McClure, Joel Scambray, George Kurtz, 2001, Hacking Exposed: Network Security Secrets & Solutions, Third Edition

**[NICT 2003]** NICT, 2003, National Information and Communication Technologies Policy. Ministry of Communication and Transport, Tanzania. Available at: http://www.ethinktanktz.org/esecretariat/ArchiveDoc.htm (Accessed in June 2003)

**[PKIX 2002]** IETF, 2002, "Public Key Infrastructure" [Online] Available at: http://www.ietf.org/html.charters/pkix-charter.html (Accessed July 2003).

**[RFC 3280]** RFC 3280, 2002, X.509 Version 3 Certificates and CRL version 2, IETF.

**[Schneier 2000]** Bruce Schneir, 2000, Secrets and lies: Digital security in a networked world

**[Skott 1999]** Skott Oaks (1999), Java security

**[Skoudes. 2002]** Ed. Skoudes, 2002, Counter Hack: A step by Step Guide to computer Attacks and effective defenses

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

**[Stal 2000]** Darryl Stal, 2000, Security Targets. Entrust Technologies. Available at: http://www.commoncriteria.org/stRpt/EntrustRA51.pdf (Accessed November in 2003)

**[Swanson 2003]** Marianne Swanson, Nady Bartol, John Sabato, Joan Hash, and Laurie Graffo, 2003. Security Metrics guide for Information Technology Systems. Available at: http://csrc.nist.gov/csspab/june13-15/sec-metrics.html (accessed September 2003)

**[SW-CMM 2003]** SW-CMM, 2003, CBA IPI and SPA Appraisal Results 2002 Year End Update (CMM based Appraisals for Internal Process Improvement (CBA Ibis) and Software Process Assessments (SPAs) [Online] Available at: http://www.sei.cmu.edu/sema/pdf/SW-CMM/2003apr.pdf (Accessed in July 2003)

**[TCSEC 1985]** TCSEC (1985), Trusted Computer System Evaluation Criteria

**[Williamson 2003]** Robert L.Williamson, Jr.,Tammy S. Compton, James L. Arnold, Jr., and J. Mark Braga Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) Technical Directorate, SAIC CCTL. Available at: http://www.saic.com/infosec/pdf/CCTL-ITEA.pdf. (Accessed in June 2002)

**[PKIPRO 2002]** PKI protection profile, 2002, The PKI Secure Kernel Protection Profile Version 1.1 Evaluated. Available at www.safelayer.com

**[USMC 2002]** USMCPKEPP_V2.5, 2002, USMC Public Key-Enabled Application Family of Protection Profiles, Version 2.5, 31 October 2002. Available at: **http://niap.nist.gov/cc-scheme/PP_VID3004.htm** (Accessed in Feb, 2004)

**[PKITKNPP-MR 2002]** PKIKMITKNPP-MR_V3.0, 2002, Department of Defense Public Key Infrastructure Token Protection Profile. Available at: http://niap.nist.gov/cc-scheme/PP_PKIKMITKNPP-MR_V3.0.html (accessed in Nov 2003)

**[FBCA 2002]** X.509 Certificate Policy, 2002, Federal Bridge Certification Authority. Available at: http://www.cio.gov/fpkipa/documents/fbca_cp_09-10-02.pdf (Accessed in November 2003)

**[Robbins 2003]** Stephen P. Robbins, 2003, Essentials of Organisational Behaviour