ZRÍNYI MIKLÓS NATIONAL DEFENSE UNIVERSITY
DEPARTMENT OF MILITARY SCIENCE
PHD INSTITUTE IN MILITARY TECHNOLOGY

KRASZNAY CSABA

INFORMATION SECURITY SOLUTIONS OF HUNGARIAN ELECTRONIC GOVERNMENT APPLICATIONS

PHD THESIS BROCHURE

SUPERVISOR:
PROF. DR. LÁSZLÓ KOVÁCS LT COL

BUDAPEST, 2011.

INTRODUCTION

In the operation of Hungarian Republic's public administration, e-government services become more important, and they are inevitable in G2G (Government-to-Government), G2B (Government-to-Business) G2C (Government-to-Citizen) relations. Both central administration institutes and local administration organizations have to extend their IT based electronic operation in accordance with the principles of European Union. Secure operation of these services is a critical question from national security viewpoint because the country's economical and social operation can be seriously blocked without them. Security of services are tried to assure with legislation, but on some areas there aren't uniform technical recommendations, which specify the service confidentiality, integrity and availability requirements.

International trends and domestic experiences show that the e-government services are constant target of organized crime, hackers and other country's agencies. Providing perfect protection means excessive cost, but publicly available services shall be developed using the due diligence principle. This means that security considerations shall appear from the design phase of new applications. Developing security functionality for e-government systems is possible in multiple levels. In administrative way, with the preparation of policies, with the development of secure physical environment, and with logical controls, such as firewalls. However, it is very important to **determine security requirements** in the whole application lifecycle. But appropriate security controls in the application development lifecycle are usually missed in practice, because neither clients nor developers know these criteria. Therefore applications operate with security errors, which can result side effects for services and indirectly for the whole electronic public administration.

RESEARCH OBJECTIVES

My research is intended to constitute an **application development framework and the requirements** for the e-government area with the use of such services the level of security can be significantly increased. On this basis, **the national security risks incurred can be greatly reduced**. The scientific importance of this area is that the security aspects of application development is poorly developed in many areas, neither the customers nor the developers have procedures that can be used in practice, which can be used to improve the security of applications in a measurable way. I want to reach my goal with the usage and further development of industry standards and best practices and with the adoption to the security needs of e-government. Level of security in e-government services can be increased in several ways but in my study **I focus only one specific topic**, namely the **security of applications behind these services**. **In the selection of research areas I focus on those topics which are unfinished and unresolved problem worldwide in the public sector.**

I picked up the following priorities:

1. Development of a Protection Profile toolkit for e-government applications

My goal is to develop a **Protection Profile toolkit** based on Common Criteria (a.k.a. ISO/IEC 15408, Hungarian IT Evaluation and Certification Scheme), which describes the security assurance and functional requirements of applications used in the electronic public services of the Republic of Hungary and to determine the description of the expected operating environment. Choice of Common Criteria is motivated by the fact that Hungarian technical recommendations are based on this standard; that was a requirement in several e-government developments, and in my opinion, it is the most comprehensive framework for secure application development. The document contains the threats, assumptions and policies, which apply to such applications. Currently, publicly cannot be achieved a Common Criteria Protection Profile which applies to this field. Because of the significant differences between e-government systems one Protection Profile is not sufficient, but the functional requirements derived from my study must appear as a minimum in affected Protection Profiles and Security Targets.

2. Development of assurance requirements for developer environment as demanded by Common Criteria

In the practice of application development the biggest problems caused by the achievement of security assurance requirements. This includes from the creation of appropriate functional specification, through the security of development environment to the appropriate security testing a number of areas. The most underdeveloped area is the security questions of developer environment. The research aim is the preparation of a **practical framework** that clarifies for developers working in the electronic administration what are the expectations of security-related activities and assist in their preparation. The scientific value of the task is that the standard only determines the requirements in high level, the interpretation and practical use of this is an undocumented area.

3. Development of vulnerability testing procedures for the area of electronic government applications

One of the cornerstone of Common Criteria standard is the security vulnerability assessment carried out by the evaluator. Therefore, **my objective** is to develop a **vulnerability testing procedure**, which can be used specifically for e-government applications. The vulnerability analysis gives a comprehensive picture of the effectiveness of security controls used by the developer. A vulnerability analysis methodology does not currently exist in the e-government area, so the development such a methodology that use the experience of a number of other procedures can be a niche work. To underline the importance of vulnerability testing I present a possible cyber attack scenario and specify some requirements that support the development of our country's cyber defense. I also present a survey that deals with the opinion of our hacker community about cyber defense.

RESEARCH HYPOTHESES

At the beginning of my research my starting point was that on my chosen areas haven't been or only in certain sub-fields have been some research in Hungary, which I would rely on. I suppose that besides the high level of recommendations any specific requirements have not been determined in the Hungarian regulatory environment. Related to the first objective, I assume that there is no Protection Profile, which defines the Hungarian public administration system security functions according to the principles of the Common Criteria. It was assumed also that further development is needed in the security classification of each system described in the recommendations. I hypothesized that a Protection Profile toolbox and classification system could be developed, which is substantially used for the development of Hungarian public administration system.

My objective in relation to the second hypothesis was that there is no any security standard which limits the work of application developers working in the Hungarian public administration environment. I suppose also that typically all conclusions are limited only to the physical security, so it becomes necessary to develop a complete regulation framework. According to my hypothesis a security framework can be created, which substantially controls the developers related security questions on the basis of existing recommendations.

My third objective resulted from the presumption that there is no any specific procedure for application security testing, despite of the fact that the National Network Security Center and the National Security Authority are authorized to be perform such an investigation. A uniform framework is an important guide for both the developers and the customers, furthermore it assists the achievement of same security level in all systems. The hypothesis is that it is possible to define the rules, which enables security testing of applications.

RESEARCH METHODS

During my work I relied on extensive international and national literature research and hands-on experiences. I wrote down my experiences for information purposes, scientific conclusions cannot be used to take from these. I scrutinized the technical books, standards and recommendations that are in some way help my work. I thoroughly reviewed the domestic legal and technical regulatory framework. Second analysis was performed on some part of them described in this thesis, and I was trying to ascertain the adequacy of multiple sources with the method of critical adaptation. In addition, I participated in a number of e-government system development, where I tried to ascertain of my hypothesis, and also adapted the results of my scientific work.

During the research, I used also the method of induction and deduction. My experience, which only applies to certain systems, is generalized with induction method, and assured that it is correct. Meanwhile, the general principles of information security were used in a deductive way for these specific cases, so the generally accepted principles could be used in the practice.

I participated in many national and international conferences of these topics, often as a speaker, as well as I was trying to collect information from the experts from the government and the supplier sides in these events. Furthermore, I developed a questionnaire, which gives an overview from the opinion of the hacker community about cyber security in a representative way.

STRUCTURE OF THE THESIS

In the **first chapter** I established based on the examinations that in the last 40 years the **central administration base is essentially unchanged**, large databases and records are the most significant elements. I also noted that **governmental IT is strongly centralized and there isn't any significant IT system at local level**. Technical environment constantly changes so security philosophy and regulation of governmental systems' development and operation needs a major rethink. I compared many sources and **determined the scope of institutions to be protected**, focused on e-government.

In the chapter I reviewed the legislation, which affects the regulation of IT security in the time of writing this study, and **I proposed some security principles for legislative or regulation filing**.

I highlighted some technical characteristic of the complex Hungarian e-government infrastructure based on the e-government strategy and systems in operation. I listed relevant threats in my own system according to the known proposed technology. Starting from **these I proposed a Common Criteria Protection Profile toolkit** following the construction and formalism of the standard.

In the thesis **I defined three protection levels** to support the toolkit. These levels can be coordinated with the multiple levels described in Hungarian recommendations. Emphasizes can be different in protection levels, so **I determined the typical attack motivations**, and I confirmed with examples why the separation of the three types is reasonable. **I listed the security objectives for all levels**, to assure the relevance of Recommendation KIB 25's functional requirement set for different protection level.

In the first chapter **I sorted the objectives of environment infrastructure and the application**. With this work I identified the requirements of Recommendation KIB 25 as an environmental requirement. My recommendation is to use those functional requirements as the Target of Evaluation in the Hungarian e-government systems, which are costume-developed or created by the customization of a framework's security functionality.

Current central administration system developments require excessive security functionality. Besides, my experience is that developers use different procedures from project to project, and even they don't document well these procedures, so the base of Common Criteria development is missing. Two areas are highlighted, which in my experience there is no experience and tradition in our country, and these are the security of development environment and vulnerability assessment, so I took them into closer examination.

In the **second chapter I determined physical, administrative and logical requirements for developers**. As a fundamental I proposed that the administrative institute shall ensure the appropriate policy system of the general contractor responsible primary for successful implementation of development an operation. Evaluation of subcontractors is the task of the general contractor's Security Officer, who can fulfill this in internal audits. Because the costumer has no influence for the development procedure, the evaluation requirement of secure application development process and policies can be defined in the contract. I presented three possible solutions for that.

I reviewed relevant parts of Recommendation KIB 28., and I stated that it describes high level requirements. In my opinion the thesis is consistent with the Recommendation and although there are some differences in the wording of protection levels, **my thesis is useful in the practical usage of the Recommendation**. In addition I found that Hungarian law doesn't tell a word about information security requirements, even in classified systems, but they give a starting point for personnel and physical security controls.

In the chapter **I proposed security roles and responsibilities and clearance for developers of governmental applications**. In addition I translated the logical and physical requirements of Recommendation KIB 25. and 28. to **the requirements of application development environment**, using the levels described in the study.

In the **third chapter** I presented a cyber attack scenario based on the study of international examples, which shows the real IT based threats of critical information infrastructures. To avoid these threats I proposed to create an organization with appropriate human stock, and **I laid down the basis** of this organization within the volunteer reservist armed forces using the legislative framework. I made a propose for the members of volunteer reservist cyber defense forces, for the information protection strategy and **I measured the cooperation willingness** of target groups using a questionnaire sent to the mailing list of Hacktivity 2009 hacker conference.

I reviewed the methodologies starting from high level, which help to ensure the security level of e-government applications using testing procedures. I systemized the most common concepts mentioned in the literature, and **I created a terminology used in the thesis for vulnerability assessments**.

I established three protection levels, like in the previous chapters for the protection of e-government applications. I aligned these for security testing, and **I worked out the methodology of reasonable security testing for Hungarian governmental systems**. In addition I wrote down the quantified attack potentials, tailored for protection levels.

SUMMARY OF CONCLUSIONS

I set up several hypotheses at the beginning of my thesis, and I drove off the proof long. I proved that the Hungarian legal and technical regulatory environment is not sufficient to specify the aspects of application development security. I tried to overcome this lack. It was further proven that although in the developments Common Criteria as a requirement appears, there is no common base, which could be relied upon. Although the recommendations use this approach, they allow too much freedom for the developers, which I believe is not acceptable. This is also true for the classification system, which is controversial within the recommendations also, so a single, simple approach is required for these.

At the beginning of the study I identified those institutions with multi-source analysis, that are particularly important according to IT aspects in the central administration, and I propose to extend the Hungarian legal system according to information security aspect. Then I prepared a Protection Profile toolbox according to Common Criteria, which could be the base of the development of the security functionality in e-government systems.

Three protection levels have been identified, which allow easier comparison than the current recommendations. For these protection levels I determined functional and assurance (including vulnerability assessment) requirements, so an easy to use, practical system was created. In this context, I analyzed the practical feasibility of basic recommendations and the completeness of the legislative background, and I determined detailed administrative, physical and logical security requirements against the developers of public administration systems.

With my Tutor a cyber-attack script was built up, which is directed against Hungary, and its feasibility has been raised by happened cases. I have proposed the realization of the basic of domestic cyber security based on the volunteer reservist armed forces, and I proved the feasibility of this with research, involving potential volunteers. I determined the attack potential of the public administration's attackers. Finally, security levels related security testing methodologies were described.

THESIS

I found the following scientific results:

1. **I created a Protection Profile toolkit,** which supports the development of Hungarian e-government systems using uniform security principles.
2. **I determined logical, administrative and physical controls** for developers of Hungarian governmental systems.
3. **I proposed the foundation of national cyber security within the volunteer reservist armed forces.**
4. **I proposed a security testing methodology,** which supports vulnerability detection in Hungarian governmental systems.

RECOMMENDATIONS AND PRACTICAL USAGE

I wrote my study to help resolving weaknesses experienced in development of governmental systems. In all three chapters I proposed a solution for a serious problem which appears at applications developers and clients. So I recommend my thesis:

- To attention of experts who are responsible for legal and technical regulation, and responsible for specification and development of governmental systems.
- I recommend the third chapter to experts responsible for cyber security of public and private critical information infrastructures.
- I suggest my results to use widespread in the government, even as a technical recommendation.
- I recommend for further research the possible solutions of cyber defense within volunteer reservist armed forces, because there are many interesting and unanswered questions, from international law, through organization problems to specific technical protection.

LIST OF PUBLICATIONS

Hungarian book chapters

1. **Krasznay, Cs.**, *Introduction and operation of Information Security Management System*. In Muha, L. (Ed.), *Recommendation KIB 25.: Vol. 25/1-1.: Information Security Management System (ISMS) Version 1.0*
2. **Krasznay, Cs.,** *Digital signature*. In Szigeti, Sz. (Ed.), *Recommendation KIB 25.: Vol. 25/3.: Information Security Recommendations for SME (IBIX) Version 1.0*

Peer-reviewed journal articles

1. **Krasznay, Cs.**, *Security analysis and development opportunities of Hungarian e-government*, Hadmérnök, 2009. 1., http://hadmernok.hu/2009_1_krasznay.php, ISSN 1788-1919
2. **Krasznay, Cs.**, *Software development requirements in certified environment: Administrative requirements*, Hadmérnök 2009. 4., http://hadmernok.hu/2009_4_krasznay.php, ISSN 1788-1919
3. **Kovács, L., Krasznay, Cs.**, *Digital Mohács – Cyber attack scenario against Hungary*, Nemzet és Biztonság, 2010. február, http://neb.kezek.hu/letoltes.php?letolt=285, ISSN 1789-5286 (50% participation)
4. **Krasznay, Cs.**, *Vulnerability assessment of e-government systems and applications*, Hadmérnök 2010. 3., http://hadmernok.hu/2010_3_krasznay.php, ISSN 1788-1919

Articles in foreign language publication

1. **Krasznay, Cs., Szabó, Á.**, *Developing interoperable e-government solutions in Hungary*, eGOV INTEROP'06 Conference

International peer-reviewed foreign language presentations published in conference proceedings

1. **Krasznay, Cs.**, *Hackers in the national cyber security*, Cyter 2009 Conference Prague, 2009. június, ISBN 978-80-01-04372-1
2. **Krasznay, Cs.**, *Software Development Security in Complex IT Environments*, EuroCACS 2010 Conference, 2010. március

Hungarian language presentations published in national conference proceedings

1. **Krasznay, Cs.**, *Security of mobile devices*, Hacktivity 2004 Conference
2. **Krasznay, Cs.**, *Evaluation laboratories under the Hungarian IT Evaluation and Certification Scheme*, HiSec 2004 Conference
3. **Krasznay, Cs.**, *Bluetooth security*, Hacktivity 2005 Conference
4. **Krasznay, Cs., Szigeti, Sz.**, *Security analysis of Hungarian e-government system*, Networkshop 2006 Conference
5. **Krasznay, Cs.**, *Common Criteria evaluation in Hungary*, IT Security Day 2006
6. **Krasznay, Cs.**, *Phishing and spam in Hungary and worldwide*, Hacktivity 2007 Conference
7. **Krasznay, Cs.**, *Security of mobile devices*, IT Security Day 2007
8. **Krasznay, Cs.**, *Information security from the other side: Hackers in Hungary*, Robotwarfare 7. Scientific Conference
9. **Krasznay, Cs.**, *Web service threats in e-government environment*, Networkshop 2009 Conference
10. **Krasznay, Cs.,** *Logging in e-government systems*, Networkshop 2010 Conference

CURRICULUM VITAE

Name:	**Krasznay Csaba**
Date of birth:	**11th October 1979**
Place of birth:	**Budapest**
Phone:	**+36-30-2020290**
E-mail:	**csaba@krasznay.hu**

Education

2008-2010: Zrinyi Miklós National Defense University, studies in the PhD Institute in Military Technology. Research focus: Security of electronic government systems.

1998-2003: Budapest University of Technology and Economics Faculty of Electrical Engineering and Informatics, specialty of electrical engineering, main specialization of Computer systems and technology of applications, sub specialization of Telecommunication management. Thesis: secure e-business on PKI bases.

1994-1998: Táncsics Mihály Secondary School

Special education / professional exam

2011: BCS
ITIL Version 3 Intermediate Certificate Service Offerings & Agreements certification

2010: Examination Institute for Information Science
ITIL V3 Foundation Certificate in IT Service Management certification

2010: PCI Security Standards Council
PCI DSS Awarness Training

2008: Government Centre for Public Administration and Human Resource Services
Trainer

2008: National Communications Authority
Electronic signature service expert certification

2008: EC-Council
Certified Ethical Hacker certification

2007: Hunguard Kft.
Hungarian Common Criteria expert certification

2006: International Information Systems Security Certification Consortium (ISC)²
Certified Information Systems Security Professional (CISSP) certification

2006: Information Systems Audit and Control Association
Certified Information Security Manager (CISM) certification

2005: Information Systems Audit and Control Association
Certified Information Systems Auditor (CISA) certification

2005: Informin Kft.
ISO 9001 and BS 7799 internal auditor

2001: BUTE Center of Information Technology
E-business solution developer: the course focuses to the practical technologies and assets covered by the framework of IBM. It introduces the basic technologies of the Internet and related IBM tools and their common usage for developing complex e-business solutions.

2001: BUTE Center of Information Technology
E-business bases: introductory course for discussing the structure and significance of Internet in the view of business and familiarize the operation of Internet and e-business.

Other scholarship / prize / membership

2011: IT Security Day: Guiding Security Expert of the Year

2010: Magyary Zoltán Association for e-Government Sciences: member of the board

2006: Information Systems Audit and Control Association (ISACA): member of the Ethics Committee

2004: Hungarian Association for Electronic Signature (MELASZ): member (former member of the board)

2001: Scientific Students' Associations 1st price in the section for Sociology and communication with "The possibilities and limitations of the spreading of digital signature"

Professional experience

2009-: HP Hungary
IT security consultant
participating in various projects in connection with IT security

2007-2009: Kancellár.hu Kft.
IT security consultant
participating in various projects in connection with IT security (consulting, education, vulnerability assessment)

2003-2006: Budapest University of Technology and Economics Centre of Information Technology
research associate
participating in various projects in connection with IT security (electronic signature, virus, Common Criteria, CERT, PKI, e-government, IT security)

2003: E-group Hungary Rt.
evaluator
preparing and evaluating an electronic signature creation application for the certification of the Communications Authority of Hungary by Common Criteria

2002-2003: Prohardver Kft.
expert
shaping out the firm's network and security infrastructure

2002-2003: Budapest University of Technology and Economics Centre of Information Technology
expert
participating in the research work in connection with electronic signatures

2001: Prime Minister's Office's Commission of Informatics
observer
participating in the development of Government's Certification Authority.

2001: Budapest University of Technology and Economics Centre of Information Technology - Communications Authority of Hungary
tester
participating in the development of Methodology for the auditation of the software for qualified certification

2001: Budapest University of Technology and Economics Department of Telecommunications Electronic Data Security Lab
student
participating in the research work of former E-biz Lab (now Crysys Lab)

1998-2001: Medincorp Kft.
web developer
participating in the development of Hungary's most significant medical portalwww.informed.hu

1997-2000: Carnett Bt.
vendor
assembling and selling new computers, repairing defective machines

Language skills

English: high-level
Spanish: mid-level

14 November 2011, Budapest

Krasznay Csaba