

A Guide to Categorising Computer Security Research into Definitive Research Themes

William M. Fitzgerald, *Telecommunications Software & Systems Group (TSSG), Waterford Institute Of Technology Ireland*

Abstract—Developing new security mechanisms to provide a stable computing environment can be a daunting task. Knowing what it is that needs to be solved is hard to define and it is even harder when you are not sure what research space it should or could fall under. The aim of this paper is to list and explain different security research categories to help researchers focus their potential research ideas into definitive research themes. This methodology greatly improves and strengthens a projects goal.

Index Terms—Security, Research Categorisation

I. INTRODUCTION

THE aim of this paper is to highlight the possible areas that computer security research can be categorized into. Often when trying to come up with new security measures it is hard to define what the scope of that idea maybe. By categorising security research into definitive areas as described in this paper, one can readily choose an area of research to focus on and then define what needs to be addressed in that space.

Take for example (described in the next section) the comparison of Smart Cards and Biometric research areas. The research goal is to develop biometric data that utilizes smartcard technology. There is a potential problem with defining the project scope and solidifying the research in that is one trying to solve a whole host of issues to get to the desired research goal?

By classifying your research objectives as discussed in this paper one can decide if the research is going to define new a biometric mechanism and will use existing smart card technologies as a transport medium or the research will aim at developing new smart card technology to transport biometric data or both.

This paper will discuss the security categorisation areas and show some real examples of European Security projects classified under the papers category structure.

Manuscript written 01 March, 2005. "A Guide to Categorising Computer Security Research into Definitive Research Themes"

William M. Fitzgerald is with the Telecommunications Software & Systems Group, at Waterford Institute of Technology, Ireland (phone: 00353 51 302937; fax: 00353 51 302901; e-mail: wfitzgerald@tssg.org).

II. SECURITY RESEARCH CATEGORISATION

THE following subsections from A-O define what the author believes are the research categories that computer security fall under.

A. Mobile Security (MS)

The research area focuses on novel security models, advanced cryptography for multimedia mobile and m-commerce, secure software for mobile platforms, novel trust and security models for mobile and ubiquitous computing, dependable home connectivity as the advent of ambient intelligence, privacy, authentication, accounting and reliability for mobile Internet.

B. Internet Security (IS)

Focuses on security models and technologies for the Internet as a whole. It will address advanced cryptography for multimedia Internet and Internet ecommerce applications, secure software for the future Internet, novel trust and security models for Internet and interoperable ubiquitous computing environment, Internet home connectivity with the advent of ambient intelligence internet devices, privacy, authentication, accounting and reliability for Internet, digital passports.

C. Application Security (AS)

Directed at improved and novel approaches to application level security measures. New architectures and end-to-end security design issues to protect at an application level in future networks. The following areas are starting points: security tools, policies, context management, allowing trusted users to view documents, single sign-on, digitally signing web pages for example, application vulnerability validation, anti-virus and so forth.

D. Dependability & Critical Infrastructure (DCI)

Here the main interests lie in a holistic view of dependability in society, security of communication for critical emergency infrastructure, dependability technology, information dependability, highly dependable embedded devices, fault tolerance, micro and nanotechnologies for homeland security, interdependencies of control systems and so forth.

E. Smart Cards (SC)

Mainly concerned with cryptography design,

authentication, digital signatures, smart card protocols, contact-less abilities, security standardization and international co-operation, chips and smart card electronics, tamper resistance measures.

F. Biometrics (Bio)

Interested in new algorithms, alternative solutions, novel pattern recognition approaches, multi-modal biometrics, data fusion issues, standardization of testing bio data and so forth.

G. Privacy & Identity Management (PIM)

Research focusing towards digital identity management, privacy mediation, personal data environments, privacy and authentication within the mobile/Internet environment and so forth.

H. Digital Asset Management (DAM)

Developing novel watermarking and stereophony algorithms, advanced cryptography, standardization of services for digital rights management and payments, securing CD/DVD copyrights, virtual electronic licensing and so forth.

I. Cryptography (Crypt)

Focusing on advanced and novel cryptography algorithms, PKI, Digital signatures and so forth.

J. Cyber Crime & Forensics (CCT)

To develop the state of the art technologies to collectively prevent cyber crime and the provision of forensic technologies used to fight cyber crime. Cyber forensics should include research of origin of attacks, traceability, data recovery tools, identity theft and collecting evidence in un-cooperating networks.

K. Security Processes & Technologies (SPT)

New and enhanced security protocols such as IPv6 and IPsec, enhanced architectures, authentication protocols and non-repudiation methods and so forth.

L. Secure Policy Mechanisms (SPM)

Focusing on policies or rules management to define how to secure administration of applications, and data, autonomic policy management, Implementing and extending policies defined in ISO 7498-2 and so forth.

M. Future Threat Analysis & Countermeasures (FTAC)

Research novel approaches to defining security threats and countermeasure methodologies and technologies. Threats can be both physical in terms public areas and of a technical (ICT) nature. There is also the physical attacks on ICT systems to consider too.

N. Crisis Management Information Systems (CMIS)

Research areas involve crisis management, environmental protection, airport & sea dock infrastructures, health care, biological and chemical attacks and so forth.

O. Trust Establishment (TE)

To incorporate trust management elements into existing

standards. The investigation of the application of trust as a means of establishing confidence in the global computing infrastructure, recognizing trust as a crucial enabler for meaningful and mutually beneficial interactions. Incorporating law, philosophy and social sciences, mathematical equations to represent trust metrics within ad hoc environments.

III. CATEGORISATION OF EUROPEAN FP6 SECURITY PROJECTS INTO RESEARCH THEMES

THE table shows the classification of current European security FP6 projects into definitive research themes.

Project	Theme	MS	IS	AS	DCT	SC	Bio	PIM	DAM	CRYPT	CCT	SPT	SPM	FTAC	TE	CMIS
BIOSEC							**									
e-JUSTICE						**	*	*								
INSPIRED						**						*				
PRIME								**								
SECOQC										**						
SEINIT		*	*	*	*							**	**	*		
ECRYPT									*	**						
FIDIS								**								
BioSecure							**									
Digital Passport						**	*									
MEDSI																**
POSITIF												*	**			
SCARD														**		
SECURE JUSTICE							*	*	**			*				
SECURE PHONE		*					**	*		*						

Table Key: double red asterisk denotes the major field of security research and the black asterisk denotes sub security research fields as a consequence of the major research field.

IV. CONCLUSION

THIS paper has described the methods that can be applied to classify computer security research projects of the past and of the future into structured areas of research excellence. Thinking in this manner will help to focus and strengthen future research on what problem is to be solved and to what area does it apply to.



William M. Fitzgerald (MSc, BSc) obtained a Master of Science Degree in Computer Science from National University of Ireland Maynooth (N.U.I.M) in Maynooth in 2002 and an Honors Bachelor of Science degree (majoring in Computer Science & Mathematics) also from N.U.I.M in 2000.

He is currently employed as an applied researcher for the Telecommunications Software & Systems Group (TSSG) at the Waterford Institute of Technology in Waterford, Ireland. William is focused on the security arena within European projects such as SecurIST, Daidalos and the PASR initiative. His current research interests are security (wired & wireless) Malware (Virology, RAT's, Worms, Phyogenetic's). Prior to his current employment he was employed as an applied security researcher with Ericsson's Systems Expertise Group, Dublin, Ireland. There he researched security of Ad-Hoc networks, reputation based metrics and novel game theoretic approaches to network node cooperation.

Some of William's publications: (1) *An Approach for Network Forwarding Systems Quality*, Information Technology and Telecommunications (IT& T), Athlone, Ireland, pp 103 -111, ISSN 1649 - 1246, 2001, (2) *Performance Analysis of Host Based Routing*, Masters of Science, N.U.I. Maynooth Library, 2002, (3) *Ericsson OSS Security Architecture: Current State and*

Challenges Ahead, Ericsson R&D Ireland, 2003, (4) *Reputation and Cooperation in Ad Hoc Networks*, Ericsson R&D Ireland, Ericsson R&D Ireland, 2003, (5) Constructing a Wireless Intrusion Detection System with Snort, MySQL, Apache, PHP, ACID & BASE on a Linux Platform.
Visit www.williamfitzgerald.org