

MASTER OF SCIENCE IN COMPUTER SCIENCE

ANALYSIS OF SECURITY SOLUTIONS IN LARGE ENTERPRISES

Carmen F. Bailey-DoD Civilian
B.S., University of Richmond, 1996
M.S., Boston University, 2001
Master of Science in Computer Science-June 2003
Advisors: Paul C. Clark, Department of Computer Science
Cynthia E. Irvine, Department of Computer Science

The United States Government and private industry are facing challenges in attempting to secure their computer network infrastructure. The purpose of this research was to capture current lessons learned from government and industry with respect to solving particular problems with regards to securing large networks. Nine thesis questions were generated to look at common problems that enterprises face in securing large networks. Research was predominantly gathered through personal interviews with professionals in the computer security area from both the public and private sector. The data was then analyzed to determine lessons learned by both the public and private sector in regards to several leading computer security issues. The results of this thesis were twofold. Lessons learned involving employee education, government involvement in the computer security area, and other important areas were generated as a product of examining each of the nine topics addressed in the thesis questions. In addition, several lessons learned were formulated into case studies to be used as graduate level teaching materials.

KEYWORDS: Large Enterprise Systems

USABILITY ANALYSIS OF THE CHANNEL APPLICATION PROGRAMMING INTERFACE

Christopher A. Brown-Ensign, United States Navy
B.S., San Diego State University, May 2002
Master of Science in Computer Science-June 2003
Advisor: Geoffrey Xie, Department of Computer Science
Second Reader: Rudolph P. Darken, Department of Computer Science

This thesis presents a usability analysis of the Channel Application Programming Interface (API). This API provides an event-driven message-channel for assembly of complex message paths between stand-alone code modules in a single application. In the thesis that proposed and developed the API, the author provided a technical analysis of the API's performance with respect to communication metrics. However, only the author/designer has ever used the API; hence, no analysis was accomplished with respect to usability attributes. The project sponsor desires public release of the API, especially within the Department of Defense (DoD). However, a usability analysis is first required to ensure wide acceptance and use of the API.

In order to analyze the API, an analysis method and associated metrics were developed. Little work has been done in the field of Human Computer Interface (HCI) with respect to treating an API as an interface and programmers as the end users. This thesis follows an IEEE published case-study and well known HCI usability analysis methods to develop a procedure to test the API for general usability attributes, as well as to investigate specific features of the API.

The results from testing the API are used to determine required enhancements to the API and its documentation.

KEYWORDS: Usability Analysis, Application Programming Interface, API Analysis, Channel API, Message Channel

COMPUTER SCIENCE

CONTINUOUS BIOMETRIC AUTHENTICATION FOR AUTHORIZED AIRCRAFT PERSONNEL: A PROPOSED DESIGN

Cassandra M. Carrillo-DoD Civilian

B.S., New Mexico State University, 2001

Master of Science in Computer Science-June 2003

Advisors: Cynthia E. Irvine, Department of Computer Science

Timothy Levin, Department of Computer Science

Today, there is no way to ensure that the personnel working within the cockpit of an aircraft in flight are authorized to be there. The primary goal of this thesis is to propose a hypothetical design for the use of a non-intrusive mechanism on the flight deck of an aircraft to provide continuous or periodic authentication of authorized aircraft personnel. The mechanism should answer questions such as: "Is the person who is flying the plane actually the person who they say they are?" and "Is the correct person in control of the aircraft throughout the whole flight segment?" Biometrics will be investigated as a possible security mechanism.

In this thesis, various biometric methods are examined and their application in the flight deck is shown. Studies that have been conducted on real biometric devices are examined and their results are reported. Also examined are the current practices and procedures that take place in the flight deck, so that the proposed designs can be understood to not interfere with current activities therein.

Two biometric solutions (i.e. proposed designs) to provide continuous or periodic authentication of authorized personnel in the flight deck are introduced. The proposed designs are general and can be used with different types of biometric device(s), and can be extended to include multi-biometrics.

KEYWORDS: Biometrics, Multi-biometrics, Multimodal Biometrics, FAA, Biometric Authentication System, Continuous Authentication, Periodic Authentication, Flight Deck Biometrics, Avionics and Biometrics, Computer Security for Aircraft, Hypothetical Biometric Authentication System Design

FEASIBILITY OF AUTOMATING FIWC WEBSITE NONCOMPLIANCE MONITORING AND ENFORCEMENT ACTIVITIES

Victoria Josephine-Galante-DoD Civilian

B.S., University of Southern California, 1966

Master of Science in Computer Science-June 2003

Advisor: Thomas J. Otani, Department of Computer Science

Second Reader: J.D. Fulp, Department of Computer Science

This thesis provides research, design and implementation details for a fully automated Website Compliance Application for DoN FIWC (Department of Navy's Fleet Information Warfare Center). The thesis begins with an introduction, which provides the setting for the proposed solution. This is followed by a background summary, describing the Department of Defense initiative that dictated regulations governing the content and format of DoD-domain publicly accessible websites. The thesis goes on to describe the proposed procedural and database design. Following this, a prototype implementation, built from the design, is presented in functional detail. Finally, the solution is recapped in a conclusion.

KEYWORDS: FIWC, Website Monitoring, Recordkeeping, Noncompliance, Content Violation

STREAM SPLITTING IN SUPPORT OF INTRUSION DETECTION

John David Judd-Ensign, United States Navy

B.S., Eastern Michigan University, 2001

Master of Science in Computer Science-June 2003

Advisors: James Bret Michael, Department of Computer Science

John McEachen, Department of Electrical and Computer Engineering

One of the most significant challenges with modern intrusion detection systems is the high rate of false alarms that they generate. In order to lower this rate, the authors propose to reduce the amount of traffic

sent to the intrusion detection system via a filtering process termed “stream splitting.” Each packet arriving at the system is treated as belonging to a connection. Each connection is then assigned to a network stream. A network stream can then be sent to an analysis engine tailored specifically for that type of data.

To demonstrate a stream-splitting capability, both an extendable multi-threaded architecture and prototype were developed. This system was then tested to ensure the ability to capture traffic and found to be able to do so with minimal loss at network speeds up to 20 Mb/s. It was also shown that the stream splitter was able to correctly implement a traffic separation scheme.

KEYWORDS: Intrusion Detection System, Stream Splitting, Fuzzy Logic

USING THE BOOTSTRAP CONCEPT TO BUILD AN ADAPTABLE AND COMPACT SUBVERSION ARTIFICE

Lindsey Lack-DoD Civilian

B.S., Stanford University, 1994

Master of Science in Computer Science-June 2003

Advisor: Cynthia E. Irvine, Department of Computer Science

Second Reader: Roger R. Schell, Asec Corporation

The attack of choice for a professional attacker is system subversion: the insertion of a trap door that allows the attacker to bypass an operating system’s protection controls. This attack provides significant capabilities and a low risk of detection.

One potential design is a trap door that itself accepts new programming instructions. This allows an attacker to decide the capabilities of the artifice at the time of attack rather than prior to its insertion. Early tiger teams recognized the possibility of this design and compared it to the two-card bootstrap loader used in mainframes, since both exhibit the characteristics of compactness and adaptability.

This thesis demonstrates that it is relatively easy to create a bootstrapped trap door. The demonstrated artifice consists of six lines of C code that, when inserted into the Windows XP operating system, accept additional arbitrary code from the attacker, allowing subversion in any manner the attacker chooses.

The threat from subversion is both extremely potent and eminently feasible. Popular risk mitigation strategies that rely on defense-in-depth are ineffective against subversion. This thesis focuses on how the use of the principles of layering, modularity, and information hiding can contribute to high-assurance development methodologies by increasing system comprehensibility.

KEYWORDS: System Subversion, Computer Security, Artifice, Trap Door, Bootstrap, Assurance, Layering, Information Hiding, Modularity

AN EXFILTRATION SUBVERSION DEMONSTRATION

Jessica Murray-DoD Civilian

B.S., University of Michigan, 2001

Master of Science in Computer Science-June 2003

Advisor: Cynthia E. Irvine, Department of Computer Science

Second Reader: Roger R. Schell, Asec Corporation

A dynamic subversion attack on the Windows XP Embedded operating system is demonstrated to raise awareness in developers and consumers of the risk of subversion in commercial operating systems that may be safety critical. SCADA (Supervisory Control and Data Acquisition) systems that monitor and control the critical infrastructure depend on embedded systems.

The attack can be loaded onto a fielded system that has been subverted with a small software artifice. The artifice could be inserted into the system at any time in the system’s lifecycle. The attack provides a flexible method for the attacker, who may not be the same individual who inserted the artifice, to gain total control of the subverted system. Due to the dynamic loading property of this subversion, the attacker does not have to decide the aspect of the system to be targeted until a time of her choice.

The attack does not exploit an existing flaw in the target module, but is possible because the initial artifice is inserted into the kernel of an operating system where adversaries have access to source code.

COMPUTER SCIENCE

This thesis discusses certain aspects of known methods for developing systems free from subversion. Several projects that utilized these methods are presented.

KEYWORDS: Operating System Subversion, Computer Security, Verifiable Protection, Software Wiretap

SECURE WIRELESS HANDOFF

Romelo B. Nafarrete-DoD Civilian

B.S., University of California-San Diego, 2001

Master of Science in Computer Science-June 2003

Lionel J. Valverde-DoD Civilian

B.S., California State University, 2001

Master of Science in Computer Science-June 2003

Advisor: George Dinolt, Department of Computer Science

Second Reader: Gurminder Singh, Department of Computer Science

With the rapidly growing demand for portable devices such as laptops, handheld computers, and Personal Digital Assistants (PDAs) with wireless networking capabilities, the need for reliable wireless data network communication has also increased. Just like in mobile voice communication, users demand uninterrupted, secure wireless data communication as they move from place to place. Mobile IP satisfies some of these demands - it enables mobile devices with fixed IP addresses to be permanently reachable even as their point of attachment to the network changes. This allows for routing of data packets to and from the mobile device irrespective of its location on the network. While uninterrupted data flow can be achieved with Mobile IP, it introduces additional security vulnerabilities, including data privacy, data integrity and authentication. The goal of this thesis is to investigate such vulnerabilities and explore implementations to overcome them.

KEYWORDS: Mobile IP, Mobile Node, Foreign Agent, Home Agent, Internet Protocol, IPSec, WEP

A DESIGN COMPARISON BETWEEN IPV4 AND IPV6 IN THE CONTEXT OF MYSEA, AND IMPLEMENTATION OF AN IPV6 MYSEA PROTOTYPE

Matthew R. O'Neal-Ensign, United States Navy

B.S., United States Naval Academy, 2002

Master of Science in Computer Science-June 2003

Advisor: Cynthia E. Irvine, Department of Computer Science

Second Reader: Thuy D. Nguyen, Department of Computer Science

Internet Protocol version six (IPv6), the next generation Internet Protocol, exists sparsely in today's world. However, as it gains popularity, it will grow into a vital part of the Internet and communications technology in general. Many large organizations, including the Department of Defense, are working toward deploying IPv6 in many varied applications.

This thesis focuses on the design and implementation issues that accompany a migration from Internet Protocol version four (IPv4) to IPv6 in the Monterey Security Enhanced Architecture (MYSEA). The research for this thesis consists of two major parts: a functional comparison between the IPv6 and IPv4 designs, and a prototype implementation of MYSEA with IPv6.

The current MYSEA prototype relies on a subset of Network Address Translation (NAT) functionality to support the network's operation; and, due to the fact that IPv6 has no native support for NAT, this work also requires the creation of a similar mechanism for IPv6.

This thesis provides a preliminary examination of IPv6 in MYSEA, which is a necessary step in determining whether the new protocol will assist with or detract from the enforcement of MYSEA policies.

KEYWORDS: MYSEA, IPv4, IPv6, MLS, IP Next Generation, Network Address Translation, NAT, Multilevel Security

COMPUTER SCIENCE

ADAPTIVE RULES IN EMERGENT LOGISTICS (ARIEL)-AN AGENT-BASED ANALYSIS ENVIRONMENT TO STUDY ADAPTIVE ROUTE-FINDING IN CHANGING ROAD-NETWORKS

Thomas Orichel-Captain, German Army

Dipl.-Ing., University of Federal Armed Forces Munich, 1994

Master of Science in Modeling, Virtual Environments and Simulation-June 2003

Master of Science in Computer Science-June 2003

Advisors: LTC Eugene P. Paulo, USA, Department of Operations Research

John Hiles, Modeling, Virtual Environments, and Simulation Institute

The delivery of supply in combat operations is very important and often results in the success or failure of a mission. This activity, as well as other transportation problems, has traditionally been modeled using global optimization techniques, such as linear programming. However, the goal of this thesis is to examine the feasibility of an agent-based solution to study the movement of material through a road network. The requirement is to build an agent-based system that finds the optimal route through a given road network and is capable of adapting to disruptions introduced to the network and then find alternative routes through the network. The agents act from a local perspective, and can represent more realistically the decisions being made throughout the delivery process. This thesis implements an analysis environment for road networks and develops an agent-based model to build truck-driver agents that are capable of delivering supplies through a changing road network.

KEYWORDS: Complex Adaptive Systems, Agent-Based Modeling, Multi-Agent Systems, Optimization, Network-Routing, Complexity Theory, Modeling and Simulation.

A FRAMEWORK FOR DYNAMIC SUBVERSION

David T. Rogers-Ensign, United States Navy

B.S., United States Naval Academy, 2002

Master of Science in Computer Science-June 2003

Advisor: Cynthia E. Irvine, Department of Computer Science

Second Reader: Roger R. Schell, AESEC Corporation

The subversion technique of attacking an operating system is often overlooked in information security. Operating Systems are vulnerable throughout their lifecycle in that small artifices can be inserted into an operating system's code that, on command, can completely disable its security mechanisms.

To illustrate that this threat is viable, it is shown that it is not difficult for an attacker to implement the framework for the "two-card loader" type of subversion, a trap door which enables the insertion of arbitrary code into the operating system while the system is deployed and running. This framework provides several services, such as memory allocation in the attacked system, and mechanisms for relocating, linking and loading the inserted attack code.

Additionally, this thesis shows how Windows XP embedded designers can use Intel's x86 hardware more effectively to build a higher assurance operating system. Principles of hardware support are discussed and recommendations are presented.

Subversion is overlooked because critics believe an attack is too difficult to carry out. It is illustrated in this thesis that this is simply not the case. Anyone with access to the operating system code at some point in its lifecycle can design a fairly elaborate subversion artifice with modest effort.

KEYWORDS: Subversion, Linker, Subversion Framework, Hardware Security Requirements, Common Criteria, Verifiable Protection

COMPUTER SCIENCE

AN INTRODUCTION TO CERTIFICATION AND ACCREDITATION FOR NEW ACCREDITORS

Natalie Stauffer-DoD Civilian

B.S., California State University, 2000

Master of Science in Computer Science-June 2003

Advisors: Karen Burke, Department of Computer Science

Craig W. Rasmussen, Department of Applied Mathematics

The certification process can be defined as a comprehensive evaluation of all security features, both technical and non-technical, of an information system. This process ensures that the system design and implementation meets a distinct set of prescribed security requirements. The accreditation of a system ensures that networks, applications, and operating systems that make up the system are running at an acceptable level of risk. The Designated Approving Authority (DAA) is responsible for deciding what systems to approve for accreditation, and assumes the responsibility for running the accredited system at an accepted level of risk. This analysis of the certification and accreditation process stresses the vital aspects of the process that are of special concern to the DAA. The mission drives the process, and influences the ultimate accreditation decision. The DAA must understand the fundamental aspects of the certification effort, and be able to weigh factors such as the funding, time, and other resources available for the effort, as well as understand the scope of the system as a whole. This thesis covers the vital aspects of certification and accreditation, and provides the new DAA with a guide to the process.

KEYWORDS: Certification, Accreditation, DITSCAP, DAA

EVALUATION OF PROGRAM SPECIFICATION AND VERIFICATION SYSTEMS

Sonali S. Ubhayakar-DoD Civilian

B.S., University of California at Los Angeles, 2001

Master of Science in Computer Science-June 2003

Advisors: George Dinolt, Department of Computer Science

Timothy Levin, Department of Computer Science

Computer systems that earn a high degree of trust must be backed by rigorous verification methods. A verification system is an interactive environment for writing formal specifications and checking formal proofs. Verification systems allow large complicated proofs to be managed and checked interactively. Evaluation criteria are desired that provide a means of finding which verification system is suitable for a specific research environment and what needs of a particular project the tool satisfies. Therefore, the purpose of this thesis is to develop a methodology and set of evaluation criteria to evaluate verification systems for their suitability to improve the assurance that systems meet security objectives. A specific verification system is evaluated with respect to the defined methodology. The main goals are to evaluate whether the verification system has the capability to express the properties of software systems and to evaluate whether the verification system can provide inter-level mapping, a feature required for understanding how a system meets security objectives.

KEYWORDS: Verification System, PVS, ACL2, Formal Methods, Inter-level Mapping, Assurance, Verifiable Protection

COMPUTER SCIENCE

EVALUATING CONFIGURATION MANAGEMENT TOOLS FOR HIGH ASSURANCE SOFTWARE DEVELOPMENT PROJECTS

Lynzi Ziegenhagen-DoD Civilian

B.S., Stanford University, 1994

Master of Science in Computer Science-June 2003

Advisor: George Dinolt, Department of Computer Science

Second Reader: Michael Thompson, Department of Computer Science

This thesis establishes a framework for evaluating automated configuration management tools for use in high assurance software development projects and uses the framework to evaluate eight tools. The evaluation framework identifies a dozen feature areas that affect a high assurance project team's ability to achieve its configuration management goals and evaluates the different methods that existing tools use to implement each feature area. Each implementation method is assigned a risk rating that approximates the relative risk that the method adds to the overall configuration management process. The tools with the lowest total ratings minimize risk to high assurance projects.

The results of the evaluation show that although certain tools are less risky to use than other tools for high assurance projects, no tool minimizes risk in all feature areas. Furthermore, none of the existing tools are designed to leverage high assurance environments-i.e., none run on operating systems that have themselves been evaluated as meeting high assurance requirements. Thus, high assurance development projects that want to leverage the benefits of configuration management tools and achieve a sufficiently strong configuration management solution must employ existing tools in a protected environment that specifically addresses the risks created by the tools' implementation methods.

KEYWORDS: High Assurance, Configuration Management, Computer Software, Common Criteria, EAL7

