

MASTER OF SCIENCE IN COMPUTER SCIENCE

A DEMONSTRATION OF THE SUBVERSION THREAT: FACING A CRITICAL RESPONSIBILITY IN THE DEFENSE OF CYBERSPACE

Emory A. Anderson, III-Lieutenant Commander, United States Navy

B.S., United States Naval Academy, 1989

M.S., University of Maryland, 1998

Master of Science in Computer Science-March 2002

Advisors: Cynthia Irvine, Department of Computer Science

Dr. Roger Schell, President, æSec Corporation

This thesis demonstrates that it is reasonably easy to subvert an information system by inserting software artifices that would enable a knowledgeable attacker to obtain total and virtually undetectable control of the system. Recent security incidents are used to show that means, motive, and opportunity exist for an attack of this nature. Subversion is the most attractive option to the professional attacker willing to invest significant time and money to avoid detection and obtain a significant payoff.

The objective here is to raise awareness of the risk posed by subversion so that the decision makers responsible for the security of information systems can make informed decisions. To this end, this work provides a complete demonstration of a subverted system. It is shown how a few lines of code can result in a very significant vulnerability. The responsibility to defend information systems cannot adequately be met without considering this threat.

Addressing this threat gets to the very nature of the security problem, which requires proving the absence of something – namely, a malicious artifice. Several techniques for demonstrating security are shown to be inadequate in the face of this threat. Finally, a solution is presented with a proposal for future work.

KEYWORDS: Subversion, Cyber Attack, Computer Security, Network Security

NETWORKED HUMANOID ANIMATION DRIVEN BY HUMAN VOICE USING EXTENSIBLE 3D (X3D), H-ANIM AND JAVA SPEECH OPEN STANDARDS

Ozan Apaydın-Lieutenant Junior Grade, Turkish Navy

B.S., Turkish Naval Academy, 1996

Master of Science in Computer Science-March 2002

Advisor: Don Brutzman, Department of Information Sciences

Second Reader: Xiaoping Yun, Department of Electrical and Computer Engineering

Speech-recognition technology is beginning to be used in automobiles, telephones, personal digital assistants (PDAs), medical records, e-commerce, text dictation and editing. Speech recognition can also be integrated into Virtual Environments (VEs) to create responsive virtual entities. Like the mouse, keyboard, and the trackball, speech-recognition technology can enhance the control of a computer and improve communication.

Dramatically expanding interest in the Internet and VEs has been gated by limited interactivity with human-avatar models. As more users begin interacting with avatars in VEs, designers are prompted to create more realistic, humanlike avatars. This quest for realism needs to go beyond visual aspects to include speech-recognition technology, which can greatly augment the realism of these avatars.

COMPUTER SCIENCE

This thesis presents design and development of a Voice User Interface (VUI), which maps to a set of behavioral motions for humanoid avatars using Extensible 3D (X3D) graphics, the Virtual Reality Modeling Language (VRML), Humanoid Animation (H-Anim) Standard and Java Speech API. The VUI includes a suitable speech-recognition component for application-command vocabularies. This thesis also demonstrates interchangeability of both avatars and animation behaviors, and creates networked humanoid animation driven by a human voice.

KEYWORDS: Humanoid Animation (H-Anim) Specification, Avatars, X3D, X3D-Edit, VRML, Java, Java Speech API, Java Speech Grammar Format, Web3D Consortium, Voice User Interface (VUI)

GROUP COLLABORATION IN ORGANIZATIONS: ARCHITECTURES, METHODOLOGIES, AND TOOLS

Werner K. Baasch-Lieutenant Commander, Chilean Navy

Naval Electronic Engineer, Naval Polytechnic Academy, Chile, 1990

Master of Science in Computer Science-March 2002

Master of Science in Information Technology Management-March 2002

Advisors: Magdi Kamel, Department of Information Sciences

Gilbert Lundy, Department of Computer Science

In a world that is increasingly more connected using networks of all types, collaboration becomes a way to leverage these connections to benefit both individuals and organizations. Currently there are numerous technologies, to support different types of collaboration. In order to make informed decisions, it is necessary to be familiar with these technologies and adopt a formal methodology to capture the organization's collaborative requirements. However, no methodology currently exists to help an organization determine which technologies and tools would enable and support its specific collaborative requirements.

This thesis analyzes collaboration as an organizational phenomenon and a network application, presents ideal collaborative environment characteristics, surveys existing collaborative environments and tools, and proposes a methodology for selecting and building a collaborative environment. This methodology is based on a synthesis of the traditional System Development Life Cycle methodologies used to analyze, design, and implement information systems.

KEYWORDS: Collaboration, Groupware, CSCW, Knowledge Management, Collaborative Environment, Development Methodologies

SCHEDULING AND PROTOTYPING OF DISTRIBUTED REAL TIME SYSTEMS (AN APPROACH USING JINI/JAVASPACE)

Tolga Demirtas-Lieutenant Junior Grade, Turkish Navy

B.S., Turkish Naval Academy, 1996

Master of Science in Computer Science-March 2002

Advisor: Man-Tak Shing, Department of Computer Science

Second Reader: LCDR Joseph Puett, United States Navy

Scheduling is one of the basic issues in building real-time applications on a distributed computing system. A distributed computing system is typically modeled as a collection of processes interconnected by a communication network. For real-time applications, scheduling is needed to meet applications timing constraints.

The major difference between single processor and distributed processors scheduling is that, in addition to deciding which order to execute tasks, distributed processors' scheduling algorithms must also decide which processors the task should run on. Moreover, these algorithms must also take into consideration practical network issues like transmission delay, loss of messages, and synchronization in the absence of a global clock. This thesis proposes a formal model to capture these network constraints and develops a proxy-based network buffer technique to support the inter-process communication for the user-defined distributed real-time systems prototypes generated by the Distributed Computer Aided Prototyping

System (DCAPS). The proxy-based technique builds on the Jini/JavaSpaces infrastructure. Several experiments were conducted to measure the response time of inter-process communication via JavaSpaces. The effectiveness of the proxy-based technique was demonstrated by creating an executable prototype of a user-defined distributed real-time system specification.

KEYWORDS: Computer Aided Prototyping, Distributed Real-Time Systems, Jini, JavaSpaces, Scheduling, Prototyping

GRAPHICAL USER INTERFACE TOOL KIT FOR PATH-BASED NETWORK POLICY LANGUAGE

**Tufan Ekin-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1996**

Master of Science in Computer Science-March 2002

Advisor: Geoffrey Xie, Department of Computer Science

Second Reader: James Bret Michael, Department of Computer Science

The Path-based Policy Language (PPL) is a formal network policy language for constructing models of Internet service and access control. Seven changes have been made to the LEXER and YACC code of PPL. Five of the changes are related to the syntax of policy rules in PPL. Two of the changes are related to the semantics of the language.

A graphical user interface tool kit for creating, validating, archiving and compiling policies represented in PPL has been developed. The tool kit has a field-by-field interface that allows a policy maker to input and update PPL compliant policy rules, while hiding the subtle details of the PPL syntax from the user. Prior to the work reported here, policy files were created separately and the PPL compiler had to be invoked manually from a command line interface. The GUI combines the processes of forming a policy file and compiling. These processes are performed automatically from the menu items of the tool kit.

The GUI itself is password protected, permitting only authorized users access to the system. Protection of the policy rules is also provided via the tool kit.

KEYWORDS: Policy Language, Path-Based, Graphical User Interface, Network Management, Conflict Detection, Conflict Resolution, GUI, Network Policy Language, Policy Tool

A HIGHLY ADAPTABLE GENERIC EVENT-BASED MESSAGE CHANNEL DESIGN FOR LOOSELY COUPLING SOFTWARE MODULES

**Cihat Eryigit-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1995**

Master of Science in Computer Science-March 2002

Advisor: Geoffrey Xie, Department of Computer Science

Second Reader: LCDR Chris Eagle, USN, Department of Computer Science

Component-based software engineering is an emerging software development approach based on the fundamentals of object-oriented technology. This approach moves programmers' focus from component development to component assembly. Event-based programming is one of the techniques that can be used to assemble software components into applications.

In this thesis, a new, generic, highly adaptable and flexible event channel has been designed and implemented. The main product is a Java utility package called "channel package" which should help Java application developers create or enhance large systems using an event-based programming approach. The new channel design has several demonstrated performance advantages over existing event channel implementations. The flexibility and adaptability of the channel package has also been validated by a successful upgrade of the channel mechanism of the SAAM prototype system.

KEYWORDS: Event Programming, Event Channel, Server and Agent based Active Network Management (SAAM) Architecture, Inter-object Communication

COMPUTER SCIENCE

CLASS TRANSLATOR FOR THE FEDERATION INTEROPERABILITY OBJECT MODEL (FIOM)

Shong Cheng Lee-Defence Science and Technology Agency, Singapore

B.S. , National University of Singapore, 1994

Master of Science in Computer Science-March 2002

Advisors: Valdis Berzins, Department of Computer Science

Luqi, Department of Computer Science

Second Reader: CAPT Paul Young, USN, Department of Computer Science

There is a growing need for systems to inter-operate in order to facilitate information sharing and to achieve objectives through joint task executions. The differences in data representation between the systems greatly complicate the task of achieving interoperability between them. Young's Object Oriented Method for Interoperability (OOMI) defines an architecture and suite of tools to resolve representational differences between systems. The OOMI architecture and tool suite will reduce the labor-intensity and complexity of the integration of disparate systems into a cooperative system of systems (federation of systems) and their subsequent deployment. At the heart of this architecture is the definition of translations between any two different classes of objects and a run-time component (the *Translator*) that will execute such translations.

This thesis describes a prototype framework that implements the OOMI, a prototype class translation code generator that assists an Interoperability Engineer in the definition of the translations and a prototype *Translator* that executes these translations.

KEYWORDS: Interoperability, System of Systems, Class Translation, Type Conversion, XML, Command Control and Communications, Computing and Software

A NOVEL APPROACH FOR THE SIMULATION AND MODELING OF STATE-OF-THE-ART MULTIJUNCTION SOLAR CELLS

Panayiotis Michalopoulos-Lieutenant, Hellenic Navy

B.S., Hellenic Naval Academy, 1993

Master of Science in Computer Science-March 2002

Master of Science in Electrical Engineering-March 2002

Advisor: Sherif Michael, Department of Electrical and Computer Engineering

Second Reader: Bret Michael, Department of Computer Science

Second Reader: Todd Weatherford, Department of Electrical and Computer Engineering

In this thesis, a new method for developing realistic simulation models of advanced solar cells is presented. Several electrical and optical properties of exotic materials, used in such designs, are researched and calculated. Additional software has been developed to facilitate and enhance the modeling process. Furthermore, specific models of an InGaP/GaAs and of an InGaP/GaAs/Ge multi-junction solar cell are prepared and are fully simulated. The major stages of the process are explained and the simulation results are compared to published experimental data. Finally, additional optimization is performed on the last state-of-the-art cell, to further improve its efficiency. The flexibility of the proposed methodology is demonstrated and example results are shown throughout the whole process.

KEYWORDS: Solar Cell, Multijunction, Material Parameters, Tunnel Junction, Model, Simulation, Development, Silvaco

COMPUTER SCIENCE

ROLE-BASED ACCESS CONTROL FOR LOOSELY COUPLED DISTRIBUTED DATABASE MANAGEMENT SYSTEMS

**Greg L. Nygard-Lieutenant, United States Navy
B.S., University of Arizona, 1993**

and

**Faouzi Hammoudi-Captain, Tunisian Air Force
Laureate in Electronic Engineering, University of Naples, 1992
Master of Science in Computer Science-March 2002
Master of Science in Information Technology Management-March 2002
Advisors: James Bret Michael, Department of Computer Science
John Osmundson, Department of Information Sciences**

Much of the work to date to apply Role-Based Access Control (RBAC) to database management systems has focused on single database systems or an integrated distributed database system. For situations where the need exists to consolidate multiple independent databases, and where the direct integration of the databases is neither practical nor desirable, the application of RBAC requires that policy be enforced via a method that is distinct from the databases. The method must provide for the verification of the RBAC policy, while allowing for the independence of the various databases on which the policy is enforced. This paper proposes a model for an application that provides for a web-based interface for users to be granted access to data held in various independent databases. The application enforces a strict RBAC policy on a well-defined set of accesses, while alleviating the need for users to have a separate account on each of the databases.

KEYWORDS: Database Management, Distributed Computing, Role-based Access Control, Security Policy

LINUX, OPENBSD, AND TALISKER: A COMPARATIVE COMPLEXITY ANALYSIS

**Kevin R. Smith-Lieutenant, United States Navy
B.S., Boston University, 1994**

**Master of Science in Computer Science-March 2002
Advisor: Cynthia E. Irvine, Department of Computer Science
Second Reader: Timothy E. Levin, Department of Computer Science**

The design of a trusted system is a delicate process, involving the selection of appropriate and consistent feature sets together with an appropriate degree of assurance that the features have been assembled and implemented correctly. In this thesis, the methodology for building secure operating systems using trusted system design elements and software design principles is discussed after a brief overview of secure system characteristics. A case study of the Multics Project is then presented to review the lessons learned from retrofitting security in an existing system. The management of complexity in operating system development will then be discussed with an introduction to the McCabe Cyclomatic Complexity metric. The capabilities of the Imagix 4D reverse-engineering tool and the experimental data gathered for the study will be presented. And finally, the results from comparative analysis of the Linux, OpenBSD, and Talisker operating systems will be shown.

KEYWORDS: Protection, Secure Operating Systems, Security Kernel, Cyclomatic Complexity, Software Development, Reference Monitor Concept, Trusted Computing Base, Multics, Verification, Assurance

COMPUTER SCIENCE

FREE SPACE OPTICS AND WIRELESS BROADBAND RADIO FREQUENCY TECHNOLOGY: BRINGING HIGH SPEED NETWORK ACCESS TO THE LAST MILE

John Sprague-Lieutenant Commander, United States Navy

B.S., Pennsylvania State University, 1990

Master of Science in Information Technology Management, 1996

Master of Science in Computer Science-March 2002

Advisor: Bert Lundy, Department of Computer Science

Second Reader: J. Bret Michael, Department of Computer Science

Existing copper phone and cable line infrastructure can no longer provide the required broadband necessary for many of today's emerging applications. Homes and businesses in the "last mile" require the same access to broadband speeds available from fiber optic cable. It is not economically feasible, however, to bring fiber optic cable to each and every home and business in the "last mile."

Free Space Optics and Wireless Broadband Radio Frequency are two technologies gaining popularity as an alternative broadband infrastructure. Free Space Optics uses lasers and Wireless Broadband uses radio frequency waves to send large amounts of data from one place to another. Both are wireless technologies that use free space. As a result, they are quickly deployed, easily scaled, and cheaper to install and upgrade. These characteristics support missions of the Armed Forces where wire-bound infrastructure is not dependable, is impractical to build and maintain, or requires a high degree of mobility.

In this thesis, the "last mile" problem is addressed including why current infrastructure will not provide a broadband solution. Free Space Optics and Wireless Broadband Radio Frequency technologies are explored and discussed. Finally, an economic analysis of alternative network designs utilizing the two emerging technologies is applied to a fictitious city of one million people.

KEYWORDS: Free Space Optics, Wireless Networking, Wireless Broadband, Radio Frequency, Network Infrastructure

WEB-BASED DATABASE APPLICATIONS: AN EDUCATIONAL, ADMINISTRATIVE MANAGEMENT SYSTEM FOR MILITARY ACADEMIES

Rasim Topuz-Lieutenant Junior Grade, Turkish Navy

B.S., Turkish Naval Academy, 1996

Master of Science in Computer Science-March 2002

Master of Science in Information Technology Management-March 2002

Advisors: Thomas Otani, Department of Computer Science

William Haga, Graduate School of Business and Public Policy

Not only does a military academy have all the information overload of a normal university but it also has the extra burden of the military environment. Without a reliable information system, administrative and educational functions cannot be performed.

This thesis deals with the problem of administrative overload in managing student, faculty, regiment personnel and course data in a military academy. It proposes an Educational Administrative Management System (EAMS), a Web-based data management system, as a solution. With this goal in mind, existing client-server architectures, server side application development tools and database technologies are explored, and the best configuration of these tools is selected. Some of them are recommended.

As a result of the study, Java Servlets and Java Server Pages are found as the optimal server-side programming tool for the application. A working prototype of the system is provided based on Oracle 8i DBMS, Apache Tomcat Web server, Java Servlets and Java Server Pages.

Suggestions are provided for coping with change management issues during the implementation of the system.

KEYWORDS: Internet, Web Based Architecture, Java, Java Servlets, Java Server Pages (JSPs), Structured Query Language (SQL), Java Database Connectivity (JDBC), Database and Military Academy

BEST EFFORT TRAFFIC MANAGEMENT FOR SERVER AND AGENT-BASED ACTIVE NETWORK MANAGEMENT (SAAM)

**Corey D. Wofford-Lieutenant, United States Navy
B.S., Michigan State University, 1994**

Master of Science in Computer Science-March 2002

**Advisors: Geoffrey Xie, Department of Computer Science
Bret Michael, Department of Computer Science**

Server and Agent-based Active Network Management (SAAM) is a promising network management solution for the Internet of tomorrow, “Next Generation Internet (NGI).” SAAM is a new network architecture that incorporates many of the latest features of Internet technologies. The primary purpose of SAAM is managing network quality of service (QoS) to support the resource-intensive next-generation Internet applications.

Best effort (BE) traffic will continue to exist in the era of NGI. Thus SAAM must be able to manage such traffic. In this thesis, a solution is proposed for management of BE traffic within SAAM. With SAAM, it is possible to make a “better best effort” in routing BE packets. Currently, routers handle BE traffic based solely on local information or from information obtained by link-state flooding which may not be reliable. In contrast, SAAM centralizes management at a server where better (more optimal) decisions can be made. SAAM’s servers have access to accurate topology and timely traffic-condition information. Additionally, due to their placement on high-end routers or dedicated machines, the servers can better afford computationally intensive routing solutions. It is these characteristics that are exploited by the solution design and implementation of this thesis.

KEYWORDS: Next Generation Internet, Quality of Service, Best Effort Traffic, Networks, Routing, Resource Management

