

MASTER OF SCIENCE IN COMPUTER SCIENCE

DYNAMIC PARAMETERIZATION OF IPSEC

Christopher D. Agar-Lieutenant, United States Navy

B.S., University of Florida, 1992

Master of Science in Computer Science-December 2001

Advisor: Cynthia E. Irvine, Department of Computer Science

Second Reader: Timothy E. Levin, Department of Computer Science

The Internet has become the medium of choice for communications between most Government and Military organizations. Unfortunately the key Internet protocols were not designed to provide security and their security vulnerabilities have become apparent. IPsec was developed to provide users with a range of security services, for both confidentiality and integrity, enabling them to securely pass information across networks. Automated security mechanisms are typically designed and/or calibrated to meet an organization's security policy. However, once the mechanism is in operation the implemented policy is in a static state, and cannot be adjusted according to dynamic environmental conditions. This means that security mechanisms fail to reflect the policy that is appropriate for the changing contexts. Dynamic parameterization enables security mechanisms to adjust the level of security service "on-the-fly" to respond to changing conditions (i.e. INFOCON, THREATCON). This work includes the extension of the attributes encoded by the KeyNote Trust Management System and modification of the IPsec mechanism to incorporate dynamic parameters into the security service selection mechanism, and the construction of a graphical user interface, for demonstrating "proof-of-concept" of Dynamic Parameterization of OpenBSD 2.8 IPsec.

KEYWORDS: KeyNote, ISAKMP, IKE, IPsec, Graphical User Interface, Security Association (SA), Security Policy Database (SPD), Security Association Database (SAD), Security Proposal

LEGACY SYSTEM UPGRADE FOR SOFTWARE RISK ASSESSMENT

Byron V. T. Alexander-Lieutenant, United States Army

B.S., United States Naval Academy, 1994

Master of Science in Computer Science-December 2001

Advisor: Valdis Berzins, Department of Computer Science

Second Reader: Michael Murrah, Department of Computer Science

This thesis is an exercise in upgrading a legacy system licensed to the DoD, VitéProject, for use with ongoing DoD research that seeks to discern truly quantifiable criteria that can be used to more accurately estimate the length of time needed to complete any software project. Accurately projecting software development times and accurate software development costs have eluded software developers for decades.

KEYWORDS: Legacy System, Risk Assessment, VitéProject, Software Timeline, Software Engineering

COMPUTER SCIENCE

AN ASSESSMENT OF EMERGING WIRELESS BROADBAND TECHNOLOGIES

Leonidas Fountanas-Lieutenant, Hellenic Navy

B.S., Hellenic Naval Academy, 1993

B.S., University of Aegean (Greece), 1999

Master of Science in Computer Science-December 2001

Advisor: Bert Lundy, Department of Computer Science

Second Reader: James Bert Michael, Department of Computer Science

This thesis provides an objective assessment in emerging wireless broadband technologies that are proposed as a solution to the “last mile” problem. Local Multipoint Systems (LMDS), Free Space Optics (FSO) and High Altitude Long Endurance (HALE) systems are examined by comparing alternative technological options and solutions.

Additionally, these systems are compared with the wired competitor technologies. The main benefits of wireless versus wired technologies are ease and fast deployment, lower deployment cost, demand-based buildout and better performance in terms of bandwidth. Although xDSL and cable networks are the dominant technologies in providing broadband services today, emerging wireless broadband technologies are expected to significantly increase their market share over the next years.

Deploying a wireless network is a difficult task requiring more than an understanding of the technological concepts. This thesis provides guidelines for the deployment of both LMDS and FSO systems by dividing the areas of interest into three categories: identifying the target market, developing the business case and deploying the network. The factors that affect each category are explained, and finally a deployment strategy is provided.

KEYWORDS: Local Multipoint Distribution Services, Free Space Optics, High Altitude Long Endurance Systems, Wireless Broadband Technologies, “Last Mile”

MAGMA[®]: A LIQUID SOFTWARE APPROACH TO FAULT TOLERANCE, COMPUTER NETWORK SECURITY, AND SURVIVABLE NETWORKING

Scott A. Margulis-Lieutenant Commander, United States Navy

B.S., University of Florida, 1988

M.B.A., Webster University, 1996

Masters of Science in Computer Science-December 2001

Advisor: Geoffrey Xie, Department of Computer Science

Second Reader: Daniel Warren, Department of Computer Science

Next Generation Internet (NGI) will address increased multi-media service demands, requiring consistent Quality of Service (QoS), similar to the legacy phone system. Server Agent-based Active network Management (SAAM) acts like rush-hour traffic reporting helicopters. Upon routing request arrivals, SAAM server determines the best route and assembles the routing path, freeing up routers to provide faster, more reliable, forwarding services. SAAM server is a critical network node; therefore, it must be extremely robust. With Margulis Agent-Based Mobile Application (MAGMA[®]) liquid software, a SAAM server agent will remain inactive in resident memory of each router until it is stimulated by a message from the departing server. Then that agent will begin running a new server at a starting point determined from the prior server’s recent state information or a pre-determined point if that state information is not available. MAGMA[®] will provide SAAM increased fault tolerance and security against malicious attacks. In this thesis, the foundation for a mobile SAAM server was developed along with a protocol that extracts critical state information from the current server and periodically transports a compressed form of the information to potential next SAAM servers. MAGMA[®] will provide a revolution in today’s computer fault tolerance and security paradigms, benefiting industry through more survivable networks with guaranteed QoS.

KEYWORDS: MAGMA[®], Liquid Software, Mobile Code, Fault Tolerance, Computer Network Security, Survivable Networking, Agent-based Software

COMPUTER SCIENCE

NETWORK APPLICATION SERVER USING EXTENSIBLE MARK-UP LANGUAGE (XML) TO SUPPORT DISTRIBUTED DATABASES AND 3D ENVIRONMENTS

Clifton J. Williams-Lieutenant, United States Navy

B.E.E., Auburn University, 1993

Master of Science in Computer Science-December 2001

Master of Science in Information Technology Management-December 2001

Advisor: Don Brutzman, Department of Information Sciences

Advisor: Daniel R. Dolk, Department of Information Sciences

This thesis contributes to the U.S. Navy forces maintaining information superiority in a Network Centric Warfare environment. This research develops an Extensible Markup Language (XML)-based Web Publishing Framework, which supports the Web Enabled Navy (WEN) architecture infrastructure. The Web application framework easily supports connections to multiple distributed databases and XML-based presentations, specifically three-dimensional (3D) simulations utilizing Extensible 3D (X3D) and Virtual Reality Modeling Language (VRML). This research evaluates and demonstrates the functionality of an XML-based Web Publishing Framework. The research demonstrates ability to connect to both XML and non-XML heterogeneous database systems and provides a framework for the distribution data across heterogeneous systems. The system supports usage in multi-tier network architecture. 3D modeling and simulations provide insights into operations that cannot be realized using standard two-dimensional (2D) renditions.

The development of an application server to support 3D modeling and simulations for operational planning will provide the U.S. Navy a better way of realizing operational limits. This research addresses the Web publishing framework, which supports the development XML based data exchange, and the development of an “on the fly” X3D simulation presentation. This research evaluated the functionality of an XML based Web framework, which allows for the separation between application programming and Web presentation. This incorporation of a Model, View, and Controller (MVC) design approach provides a clean separation between different components (logic, presentation, and data) of information and the programming functionality. The Web framework addressed ability to provide a framework for the distribution data across heterogeneous systems.

KEYWORDS: Command, Control, and Communications, Computing and Software Extensible Mark-up Language (XML), Java Servlets, Web Application Framework, Distributed Databases, Heterogeneous Systems, Virtual Reality Modeling Language (VRML), Extensible 3D (X3D), and Extensible Stylesheet Language (XSL)

