MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY MANAGEMENT

AUTOMATING SUBMARINE TRAINING AND READINESS USING WEB-ENABLED APPLICATIONS

Kevin S. Anderson-Lieutenant, United States Navy
B.S., Jacksonville University, 1994
Master of Science in Information Technology Management-June 2001
and
David J. Murphy-Major, United States Marine Corps
B.S., Syracuse University, 1985
Master of Science in Information Technology Management-June 2001
Advisors: William J. Haga, Graduate School of Business and Public Policy
Douglas E. Brinkley, Graduate School of Business and Public Policy

This thesis examines the limits to on-board training and readiness imposed upon the submarine community by manual data collection and personnel record systems.

It proposes an integration of web-based applications under the Balanced Scorecard management approach as a solution. Specifications are included for fiber optic LAN Infrastructure design, network client workstations, network servers and IT-21 compliant network operating systems, producing applications and web augmentation tools. A description of relational database design is provided that encompasses database objects, data types and table relationships. Web design issues and network security issues are examined. Complete code for a prototype of the system in Microsoft Access is appended.

Recommendations are made for using an n-tier network architecture to automate the submarine training and readiness processes in small project modules using an incremental Prototype development approach. An n-tier architecture supports custom applications and commercial-off-the-shelf (COTS) components, supports component reuse and encapsulation, provides a consistent, secure and auditable access to data and will allow faster production at less risk. Recommendations are made for using Microsoft products that support n-tier architecture and are consistent with the Navy's IT-21 standards.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Manpower, Personnel, and Training

KEYWORDS: Automation, Local Area Network, N-Tier, Readiness, Submarine, Training, Web-Based, Web-Enabled

DESIGNING A RELATIONAL DATABASE TO FACILITATE MILITARY FAMILY HOUSING UTILIZATION DECISIONS

Jonalan Brickey-Captain, United States Army
B.S., United States Military Academy, 1991
Master of Science in Information Technology Management-June 2001
Advisor: Daniel R. Dolk, Information Systems Academic Group
Second Reader: LTC James E. Illingworth, USA, TRADOC Analysis Center Monterey

The Housing Welcome Center (HWC) in Monterey, CA manages more than 2,200 military family houses and provides services to approximately 4,500 service members. The current housing information system

consists of a proprietary legacy database system, a homemade non-relational database, a collection of word processing documents, and a static online application Web site. This semi-manual system can introduce errors, inconsistencies, and redundancies that may lead to frustration and possibly a decrease in quality of life.

This research presents a prototype Housing Assignments and Terminations System (HATS) that uses a top-down systems analysis design approach. The research defines requirements and models that are transformed into a relational database with connectivity to a Web site. A graphical user interface (GUI) provides intuitive menus to manipulate and view data. Decision support tools help decision-makers visualize the data in a spatial manner and make better decisions to improve the quality of life for service members.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: GIS, Legacy System, Decision Support Tools, Military Family Housing, Relational Databases

CORRELATION ANALYSIS OF FLEET INFORMATION WARFARE CENTER NETWORK INCIDENTS

Patrick W. Ginn-Captain, United States Army
B.B.A., North Georgia College, 1991
Master of Science in Information Technology Management-June 2001
Advisors: LT Ray Buettner, USN, Information Warfare Academic Group
Dan Boger, Command, Control, Communications, Computers, and Intelligence Academic Group

The Navy's Intrusion Detection process is currently reactive in nature. It is designed and programmed to detect and provide alerts to the Fleet Information Warfare Center (FIWC) of suspicious network activity while it is in progress, as well as, to record/store data for future reference. However, the majority of activity taking place within and across Naval networks is legitimate and not an unauthorized activity. To allow for efficient access and utilization of the information systems sharing the network the Intrusion Detection Systems must be set at a level that filters out activity deemed as normal or non-hostile, while still providing an appropriate level of security. With this filtering in place an IDS system will not register all suspicious activity, and may not detect mild and seemingly harmless activity. When increasing security, limits must be imposed upon access. This thesis examines FIWC network incident data from 1999 to see if a correlation can be drawn between United States visibility in the foreign media during 1999 and the occurrence of suspicious network incidents. A positive correlation may provide advance-warning indicators that could lead to the development of a procedure for increasing security posture based on the current environment. These indicators would provide a more proactive method of defense, significantly reduce potential damage caused by hostile network incidents and provide for more efficient network activity.

DoD KEY TECHNOLOGY AREAS: Other (Information Technology)

KEYWORDS: Fleet Information Warfare Center, Intrusion Detection, Network Incidents

NAVY/MARINE CORPS INTRANET INFORMATION ASSURANCE OPERATIONAL SERVICES PERFORMANCE MEASURES

Randall A. Gumke-Lieutenant, United States Navy Civil Engineering Corps
B.S., University of Florida, 1993
Master of Science in Information Technology Management-June 2001
Advisors: Daniel F. Warren, Department of Computer Science
Carl R. Jones, Information Systems Academic Group

Communicating in the Department of the Navy (DON) over the Internet is an everyday event. The DON is developing the Navy Marine Corps Intranet (N/MCI) to enhance this communication capability. The

security of communicating over the N/MCI has become a concern to the DON. The DON is relying on the N/MCI contractor to provide security for their communications. Key aspects of this secure communication will be provided through the use of a DON Public Key Infrastructure (PKI), which the N/MCI contractor is managing. To ensure the security of the PKI based communications the contract requires the monitoring of four PKI performance measures. This thesis analyzes performance measures, criterion, and standards then uses this analysis to review the contractual PKI performance measures and data collected from commercial PKI vendors. It recommends changes to these performance measures and provides additional performance criteria that should be included in the N/MCI contract. Finally, this thesis analyses how the N/MCI contract, specifically the PKI, impact DON members.

DoD KEY TECHNOLOGY AREA: Computing and Software, Other (Public Key Infrastructure)

KEYWORDS: Public Key Infrastructure, Public Key Cryptography, Navy Marine Corps Intranet, Service Level Agreements, Performance Measures, PKI, N/MCI

USING KNOWLEDGE MANAGEMENT TO INNOVATE USCG COMMAND CENTER PROCESSES

Randall J. Navarro-Lieutenant, United States Coast Guard
B.S., California State Polytechnic University, 1991
Master of Science in Information Technology Management-June 2001
Advisors: Mark E. Nissen, Graduate School of Business and Public Policy
Daniel R. Dolk, Information Systems Academic Group

The U.S. Coast Guard (USCG) responds to thousands of alerts received each year from the Search and Rescue Satellite-Aided Tracking (SARSAT) system. Each alert requires an efficient and effective response to assist a potential mariner in distress. This thesis provides an in-depth analysis of the process employed by USCG Command Centers in responding to SARSAT alerts. The purpose of this analysis is to identify alternatives that can improve the knowledge work performed in the process. This thesis builds on recent work that focuses on knowledge management and system design from three integrated perspectives: 1) reengineering, 2) expert systems knowledge acquisition and representation, and 3) information systems analysis and design. The integrated framework covers the gamut of design considerations from the enterprise process at large, through alternative classes of knowledge in the middle, and on to specific systems in detail. The SARSAT response process is examined using this integrated framework and identifies five technological and organizational alternatives that offer significant potential to improve the overall performance of the process.

DoD KEY TECHNOLOGY AREAS: Command, Control and Communications, Other (Knowledge Management)

KEYWORDS: Knowledge Management, Process Analysis, Process Re-engineering, Information Systems

USING MULTIPLE COLLABORATIVE AGENTS FOR ADAPTIVE QUALITY OF SERVICE MANAGEMENT OF C4ISR NETWORKS

Raymond A. Rivera-Lieutenant, United States Navy
B.S., United States Naval Academy, 1994
Master of Science in Systems Technology-June 2001
Master of Science in Information Technology Management-June 2001
Advisors: Alex B. Bordetsky, Information Systems Academic Group
John S. Osmundson, Command, Control, Communications, Computers, and Intelligence Academic Group

This research explores the potential of agent technology for adaptive quality of service (QOS) management of c4isr networks. With the growing emphasis on information superiority, any time savings or additional utilization of resources enabled by effective network management becomes increasingly important.

Intelligent agents are ideal for assessing information, adapting to dynamic conditions, and predicting future network conditions. In the kernel of the proposed multiple agent system (MAS) testbed are agent shared memory and majority rule architectures for agent conflict resolution. The case based reasoning (CBR) technique provides the foundation for building the agents' shared memory of qos management solutions and allows the individual agents to share their associations of feedback controls in response to application and user qos profiles. Based on the telecommunications management network (TMN) functionality, we use this agent architecture to effectively translate the warfighter's service layer application requirements across the network. The fundamental frameworks of service level management (SLM) and policy based management (PBM) serve as cornerstones in effectively gathering and applying specific application requirements. Finally, we utilize these techniques to investigate an actual C4I application at the pacific region network operating center (PRNOC) in Wahiawa, Hawaii as the real-world focal point of the thesis.

DoD KEY TECHNOLOGY AREA: Command, Control, and Communications

KEYWORDS: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), Agent Technology, Quality of Service (QoS), Case Based Reasoning (CBR), Service Level Management (SLM), Policy Based Management (PBM), Telecommunications Management Network (TMN)

DEFINING AND VALIDATING A COVERT ANALYSIS DETECTION (CAD) SYSTEM AND ITS STEALTHY DATA CAPTURE, CONTROL AND ANALYSIS CAPABILITIES

Glen F. Sharlun-Captain, United States Marine Corps
B.S., United States Naval Academy, 1992
Master of Science in Information Technology Management-June 2001
Advisors: John C. McEachen, Department of Electrical and Computer Engineering
Dan Boger, Information Systems Academic Group

A Covert Analysis Detection (CAD) system is an operationalized honeypot or honeynet that is designed to covertly capture, control and provide analysis capabilities of all traffic that flows through it. It was found that the covert data capture capability not only revealed the attackers tools (captured as source code) and tactics (collection of compromised systems), but also over time it revealed that that attacker's actual motive was the creation of a distributed denial of service (DDoS) network. The discovery of this lethal network tool and all the signatures of its creation and maintenance, proved the validity of the CAD's capabilities to aid in the enhancement of our information protection resources.

DoD KEY TECHNOLOGY AREA: Command, Control and Communications, Computing and Software

KEYWORDS: Network Security, Information Protection, Intrusion Detection, Deception, Deterrence, Honeypot, Honeynet, Distributed denial of service (DDoS)

THE COAST GUARD KNOWLEDGE BASE: BUILDING ONLINE COMMUNITIES, TEAMS AND EXPERTS TO FACILITATE RAPID CREATION, CAPTURE AND SHARING OF SERVICE RELATED KNOWLEDGE

Andrew J. Sorenson-Lieutenant Commander, United States Coast Guard
B.S., United States Coast Guard Academy, 1988
Master of Science in Information Technology Management-June 2001
Advisor: Mark E. Nissen, Graduate School of Business and Public Policy
Associate Advisor: Roger D. Evered, Graduate School of Business and Public Policy

The U.S. Coast Guard is reaching the limits of incrementalism. Extending aircraft and cutter service-lives, increasing work hours to compensate for reduced manpower, responding to data calls faster and squeezing another penny out of costs are the challenges of leaders today. But pursuing incremental improvements is similar to paving over cow paths. Today's technology provides the Coast Guard with the opportunity to

make exponential improvements in processes for managing knowledge, and to revolutionize business practices.

This thesis presents a knowledge management architecture that addresses articulable limits to fast, efficient, knowledge management within the cutter community. Building upon a foundation of messaging and collaboration, the architecture provides modules maximizing the ability to manage informal and formal knowledge. The results are a transparent interface for the creation, sharing and capture of organizational knowledge. Successful implementation is dependent upon the improvement of the Coast Guard's IT infrastructure and the creation of a culture friendly to knowledge sharing.

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Command Control and Communications, Computing and Software, Human Systems Interface, Manpower Personnel and Training

KEYWORDS: Coast Guard, Knowledge Management, Information Technology, Knowledge Architecture, High Endurance Cutters, Medium Endurance Cutters

REQUIREMENTS FOR THE DEPLOYMENT OF PUBLIC KEY INFRASTRUCTURE (PKI) IN THE USMC TACTICAL ENVIRONMENT

Alan R. Stocks-Major, United States Marine Corps
M.S., Troy State University, 1996
Master of Science in Information Technology Management-June 2001
Advisors: Daniel F. Warren, Department of Computer Science
Cynthia E. Irvine, Department of Computer Science

Marine forces are expeditionary in nature yet require the full range of Public Key Infrastructure (PKI) services at deployed sites with limited bandwidth and access to their respective Registration Authority (RA). The development of a PKI solution for the tactical arena is a fluid and complex challenge that needs to be answered in order to ensure the best support of tactically deployed forces. Deployed Marine forces will need the capability to issue and re-issue certificates, perform certificate revocation, and perform key recovery within the command element of the deployed unit. Since the current United States Marine Corps (USMC) PKI was not designed with the tactical environment in mind, the full extent of PKI deficiencies for field operation is unknown. This thesis begins by describing public key cryptography, the implementation and objectives of a USMC PKI, and the components necessary to operate a PKI. Next, tactical issues that have been identified as areas of concern along with their proposed solutions are presented. Supporting material describes design issues, such as scalability and interoperability, and technical challenges, such as certificate revocation lists (CRL), key escrow and management of tokens

DoD KEY TECHNOLOGY AREA: Other (Public Key Management)

KEYWORDS: Public Key Infrastructure (PKI), Computer Security, Navy Marine Corps Intranet (NMCI)

DYNAMIC ASSEMBLY FOR SYSTEM ADAPTABILITY, DEPENDABILITY AND ASSURANCE (DASADA) PROJECT ANALYSIS

Charles A. Stowell, II-Lieutenant Commander, United States Naval Reserve
B.S., The Citadel, 1985
M.S., Central Michigan University, 1997
Master of Science in Information Technology Management-June 2001
and
Wayne S. Mandak-Major, United States Marine Corps
B.S., Allegheny College, 1983
Master of Science in Computer Science-June 2001
Advisors: Luqi, Department of Computer Science
Man-Tak Shing, Department of Computer Science
John S. Osmundson, Command, Control, Communications, Computers, and Intelligence Academic Group
Richard Riehle, Department of Computer Science

This thesis focuses on an analysis of the dynamic behavior of software designed for future Department of Defense systems. The DoD is aware that as software becomes more complex, it will become extremely critical to have the ability for components to change themselves by swapping or modifying components, changing interaction protocols, or changing its topology. The Defense Advanced Research Programs Agency formed the Dynamic Assembly for Systems Adaptability, Dependability, and Assurance (DASADA) program in order to task academia and industry to develop dynamic gauges that can determine run-time composition, allow for the continual monitoring of software for adaptation, and ensure that all user defined properties remain stable before and after composition and deployment. Through the study, a review of all the DASADA technologies were identified as well as a thorough analysis of all 19 project demonstrations.

This thesis includes a template built using the object-oriented methodologies of the Unified Modeling Language (UML) that will allow for functional and non-functional decomposition of any DASADA software technology project. In addition, this thesis includes insightful conclusions and recommendations on those DASADA projects that warrant further study and review.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Computing, Software, Software Engineering, Software Demonstration

HUMAN FACTORS IN COAST GUARD COMPUTER SECURITY - AN ANALYSIS OF CURRENT AWARENESS AND POTENTIAL TECHNIQUES TO IMPROVE SECURITY PROGRAM VIABILITY

Timothy J. Whalen-Lieutenant, U.S. Coast Guard
B.S., United States Merchant Marine Academy, 1990
Master of Science in Information Technology Management-June 2001
Advisors: Cynthia Irvine, Department of Computer Science
Douglas E. Brinkley, Graduate School of Business and Public Policy

The Coast Guard is becoming increasingly reliant upon our nation's information infrastructure. As such, our ability to ensure the security of those systems is also increasing in import. Traditional information security measures tend to be system-oriented and often fail to address the human element that is critical to system success. In order to ensure information system security, both system and human factors requirements must be addressed.

This thesis attempts to identify both the susceptibility of Coast Guard information systems to human factors-based security risks and possible means for increasing user awareness of those risks. This research is meant to aid the Coast Guard in continuing to capitalize on emerging technologies while simultaneously providing a secure information systems environment.

DoD KEY TECHNOLOGY AREA: Command, Control and Communication, Computing and Software, Human Systems Interface

KEYWORDS: Computer Security, Human Factors, Human Computer Interaction, Coast Guard, Trust, INFOSEC

THE USE OF INTELLIGENT REAL TIME TECHNOLOGIES TO IMPLEMENT, MONITOR AND FORECAST MEDICAL READINESS

Michael Whitecar-Lieutenant, United States Navy
B.S., Park University, 1991
Master of Science in Information Technology Management-June 2001
Advisors: John Osmundson, Command, Control, Communications, Computers, and Intelligence Academic Group
Gary Porter, Command, Control, Communications, Computers, and Intelligence Academic Group

One of the various essentials of military readiness is the administering and continual execution of medical immunizing agents. Service members and civilian personnel working under contract are required to maintain a satisfactory level of medical readiness pursuant to the environment or platform they are assigned to. However, the guidance that oversees and classifies this "satisfactory" level is numerous in volume, broad in terms of definition, and difficult to interpret in terms of the methodology used to assign a specific rating.

Because of the many interpretations of medical readiness, receiving a designated rating of C2 is considered to be acceptable in wartime interactions. Therefore, annual immunization requirements may be neglected throughout one's tenure while still engaging in a wartime environment with the risk of becoming exposed to influenza infection.

The collection, tracking, and analyzing of medical readiness data is interpreted differently thereby prohibiting the facilitation and compilation of adequate information. Medical systems are developed using many different technologies that omit the ability to interface with one another, are in adaptive to change, and do not provide an interactive gateway to permit service members to become proactive and responsible for their own medical readiness state.

DoD KEY TECHNOLOGY AREA: Computing and Software, Manpower, Personnel, and Training

KEYWORDS: Medical, Readiness, Intelligent, Technologies, Web Application