Enterprise Security Planning (ESP)

L. Ertaul
California State University,
Hayward.
Dept. of Mathematics
and Computer Science,
25800 Carlos Bee Blvd.
Hayward, CA, 94542, USA.
E-mail: lertaul@csuhayward.edu,
www.mcs.csuhayward.edu/~lertaul

T. Braithwaite
Enterprise Architecture
Certification (FEAC) Institute
1255 C Street SE,
Washington DC**,** USA
tim_braithwaite8@msn.com
http://www.feacinstitute.org

Beryl L. Bellman,
California State University at LA,
Dept of Communication Studies
5151 State University Drive,
Los Angeles 90032 CA, USA
bbellma@exchange.calstatela.edu
Enterprise Architecture Certification (FEAC) Institute
1255 C Street SE, Washington DC**,** USA.
bellman@feacinstitute.org
http://www.feacinstitute.org

Abstract: *Enterprise security planning (ESP) is the aligning of information security policies and practices and applicable security technologies with the business rules and the evolving information models and technical architectures being used by a government agency or business. In this paper ESP is discussed and its security knowledge management tools (SKMT) are proposed along with implementation issues of SKMT with the secure intelligent mobile agents, within the context of prevailing Enterprise Architecture (EA) methodologies - the most notable being the pioneering framework developed and described by Zachman. Using the Zachman Framework as a foundation, we propose the development of an ESP methodology and its implementation using modern analytic methods and techniques. We show that this allows information security to be integrated into the overall Enterprise Architecture (EA) of a Government agency or business. We ensure that the resulting ESP techniques will be compatible with the Federal Enterprise Architecture (FEA) Reference Model, Capital Planning and Investment Control (CPIC) guidelines, and provide the baseline for continuous Security Program Management as required by the Federal Information Security Management Act. With the implementation of ESP's SKMT elements, we propose an ´´**expert in a box**´´ solution in which the knowledge to manage a security "**incident**" exists in the form of a community of intelligent secure mobile agents present within the system itself.*

Keywords: Enterprise Security Planning, Zachman Framework, Network Security, Mobile Agents Security.

1. Introduction

Since the passage of the Clinger-Cohen Act [Clinger, 1996] all federal agencies are mandated to develop enterprise architectures. The E-Government Act, Title III, includes the Federal Information Security Management Act (FISMA) [FISMA 2002]. FISMA continues the annual review and reporting requirements introduced by earlier legislation but also includes new provisions aimed at further strengthening the security (i.e. integrity, confidentiality, and availability) of Federal government's information and information systems. In implementing Clinger-Cohen, the Federal CIO Council and its working groups have developed a Federal Enterprise Architecture Framework (FEAF) [FEAF, 1999] and the program management office has published a set of Office of

Management and Budget (OMB) suggested references models associated with it [Architecture, 2000], [FCIO, 2000], [FEA,2001]. The reference models are to be used in describing the business, technology, data and application, and service/performance components of an agency. OMB also designed an IT portfolio management system for Capital Planning and Investment Control (CPIC) [FCIO, 2000] and requires yearly compliance in providing updates on enterprise architectures by filing yearly reports.

The highly critical process, in this age of increased security, involving the creation and integration of an information security architecture within the Enterprise Architecture (EA) is given only ancillary attention even though an information security architecture is essential to having a completed EA. Equally important, a security architecture is absolutely necessary to fully understand the nature of all information technology threats facing an enterprise. A security architecture is also necessary to satisfy the increased security requirements of FISMA and its' annual reporting demands. Generally this need for security integration is well understood and many agencies have commented that research in this area should be aggressively pursued so that their respective security staffs could better participate with on-going EA activities. If information security is to be both cost effective and operationally efficient in the 21st century, Enterprise Security Planning (ESP) is a "***must have***" requirement.

Enterprise security planning is the aligning of information security policies and practices and applicable security technologies with the business rules and the evolving information models and technical architectures being used by a government agency or business. Additionally, security management information needs to utilize the technology of "wireless" to allow timely dissemination in a "wireless" world. In this paper we discuss ESP and its security knowledge management tools (SKMT) implemented with secure intelligent mobile agents consistent with prevailing Enterprise Architecture (EA) methodologies - the most notable being the pioneering framework developed and described by Zachman [Zachman, 1987],[Sowa, 1992],[Zachman, 1995],[Zachman 1995],[Zachman, 2004].

There are a number of different frameworks used to build enterprise architectures. The earliest and which often serves as a benchmark reference framework for others is the Zachman Framework [O'Rouke, 2003], [Zachman, 2004]. In the Untied States government there are several derivative frameworks that the Federal Enterprise Architecture Framework (FEAF) used by federal agencies in the United States, the Treasury Enterprise Architecture Framework (TEAF) that predated the FEAF and now relates to it and the Department of Defence Architecture Framework (DODAF). The Open Group developed its own framework that focuses more on IT than business architecture and incorporates Zachman, the FEAF and the DODAF.

In the course of its certification training, the Federal Enterprise Architecture FEAC Institute has developed a Security framework that is based on the Zachman cells, the Security Knowledge Framework (SKF) (Braithwaite, 2003). In this paper we discuss how the SKF enables an advanced security analysis methodology that is integrated with existing enterprise architecture techniques. We then discuss the implementation of SKMTs, which create an enterprise–wide environment where appropriate security information is available on demand and is effectively integrated with other organizational governance systems, using secure intelligent mobile agents as the "***expert in a box***".

2. Enterprise Architecture Models

An Enterprise Architecture (EA) is the explicit documented description of the current and desired relationships among program/business and management processes and information technology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its information technology portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the

roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies.

Agencies must implement the EA consistent with the following principles [OMB, 2000]:

- Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms.
- Meet information technology needs through cost effective intra-agency and inter-agency sharing, before acquiring new information technology resources; and
- Establish a level of security for all information systems that is commensurate to the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

Security is commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls [OMB, 2000]. Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide – (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information [FIS, 2002].

Clearly, a reading of these operative definitions leads one to conclude that the most effective and efficient time to identify and specify the integrity, confidentiality, and availability requirements of information and information systems is when the architecture of the enterprise, as a whole, is being defined and documented.

3. The FEAC Security Knowledge Framework

The Security Knowledge Framework (SKF) (Fig. 1)and (Fig. 2 derived from the original works of John Zachman, equips the enterprise with an analytic guide to assure that appropriate information security "artifacts" and systems security knowledge is being gathered and/or created to develop an enterprise architecture complete with an integrated "security architecture" [Braithwaite, 2003]. The SKF can also be used to guide an audit of existing system security "artifacts" and supporting documentation needed for "due diligence" purposes and for certification and accreditation activities.

As shown in Fig. 1 and Fig. 2 for each of the thirty-six cells (i.e. the intersection of rows and columns of the Zachman Framework described above), specific information security interrogatives, "artifacts", and supporting items of documentation are identified. During an EA exercise, the contents of every cell are identified and gathered and/or created as the essential relationship of each to the overall security architecture of the enterprise becomes clear. Since the SKF is based on the Zachman Framework, it is consistent with the FEAF and can be used as input to the DODAF. It supplements both models by providing a security-focused analysis of on-going EA activities and provides agency officials with clearly defined security architecture and plans for its implementation.

ESP Project deliverables are indispensable for federal employees and contractors who are tasked with:

- Developing secure enterprise architectures for their agency.

- Participating in the EA initiative of their agency for the purpose of developing the security architecture for the EA currently under development.
- Acquiring valuable knowledge needed to effectively integrate security with the on-going EA initiatives of the agency.
- Enhancing existing expertise with a specialized area of knowledge required for developing successful enterprise architectures.

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)	• Identify external data needs • R&D data needs • Customer data and competitor data needs • Partner data needs • **Value of strategic information to the Enterprise?**	• Business processes • Critical success factors • Interfaces • Supply chain nodes • **Value of unique business processes?**	• # of locations • Carriers • Number of support vendors • CONUS • OCONUS • Internet Providers - **Value of connectivity to the Enterprise?**	• Employees, roles responsibilities and authorities • Organizational charts • Office Locations • Supply chain members/vendors • Personnel policies • HR Security policies • Employee Unions	• Market fluctuations • Time to market estimates • Contract renewals • Patent/Renewals • Business cycle dependencies	• Business goals & objectives • Enterprise Business Plan • IT Capital Investment Plan • Security & Privacy Regulations • Audit Standards • HR rulings	**Role supporting National Critical Infrastructure** **Participation in industry ISACs**
Business Model (B)	-data accuracy metrics • Data sensitivity • Classification schemes • Accounting rules • Auditing rules • **Value of business data?**	• Data/information workflows • Decision points • Inputs/outputs • Process criticality • Control objectives • **Value of knowing "How" a process works?**	**Type and Volumes** • Data • Voice • Mail • Courier • Encryption • Authentication • **Value of knowing "How" communi-cating works?**	**Functions** - Who • Where • Authorizations • Work place location • Need- to- know rules • Interfaces • Audit Findings	**Business Cycles:** • Sales/Marketing • Product Development • Budget • **Demand Cycles:** • Triggers • Prompts • Queries	**Standards:** • De-facto • ISO **Business Rules** • Personnel Policies • Security Policies **Audit Reports** **Industry Threat Analysis**	**Emerging legal requirements** **Pending legislation and regulations** **Evolving "due diligence" precedents**
Information Systems Model (C)	**Quality factors:** • Accuracy, etc. • Data relationships • Data exchanges • Data flows/views • Back-up demands • Test data • **Value of having the Systems Model?**	**Quality factors:** • Integrity, availability, confidentiality, etc. • Logical processes • Internal controls • Logical tests • Test data • **Value of process quality/integrity?**	**Quality factors:** • Accuracy, etc. • Volumes • Dedicated Lines • Internet • VPN • Wireless • **Value of connectivity specifications?**	**Quality factors:** • Confidentiality policy • Access policy • Separation of duties • User permissions – read/write, delete, append, etc.	**Quality factors:** • Real-time defined • "as of" requirements • Timeliness • Turn-around • Through-put & volumes	**Technology** - Stability of basic technology • Availability of skilled personnel **Application Risk Analysis**	**Evolving "best practices" for IT systems management**

Fig. 2 Security Knowledge Framework (ii)

4. ESP Development and Its Implementation

In order to satisfy the need for an expanded security focus the ESP Project has been designed to incorporate the real-world, day-to-day experiences of agencies as they attempt to include information security into their agency's enterprise architecture. The ESP concentrates on:

- Advancing the developing of a formal ESP Methodology, consistent with prevailing EA techniques and tools, to be used in successfully defining, implementing, and managing comprehensive security architectures as an integral element of an agency's enterprise architecture
- Reducing, through an application of EA principles, the risk and cost to the agency of implementing and managing the securing of e-Business changes required by law or brought about through innovation.
- Producing a much more complete and viable agency security architecture by providing a Secure EA Knowledgebase that can be used in on-going critical system security "certifications" to manage the day-to-day security posture of the agency.
- Defining business-rule based security metrics for use in evaluating the performance of security controls and maintaining on-going security effectiveness.
- Defining and recommending a automated security governance tool-set to be used as a critical element of change control – thus making the agency's secure EA an on-going success.

The major elements proposed in the ESP are.

- A Security Knowledge Framework (SKF)

The Security Knowledge Framework (SKF) is an analytic tool for public use that ensures that during any EA undertaking the appropriate and adequate business and security requirements knowledge and artifacts are being gathered and/or created, as necessary, for inclusion in the EA of the agency.

- Security Knowledge Management (SKM) Techniques and Tools

This element manages an ongoing comprehensive security program – one that maintains consistency with the enterprise architecture of the agency. This project element results in the development of a Security Knowledge Management (SKM) model implemented using intelligent secure mobile agents. This element builds on the SKF and functions within the existing systems management framework of the IT organization using the developed SKM toolset. The SKM automates traditional security methodologies with knowledge management functionality to centralize the coordination, collection, and analysis of security-related information (content) and the distribution of the results of such analysis to appropriate employees within the enterprise in a clear, concise, and timely manner. We advocate an ´´***expert in a box***´´ solution in which the knowledge to manage a security "incident" exists virtually within the system itself in the form of a community of intelligent secure mobile agents. This concept is very important and seems to be needed because one does not always have easy access to expert knowledge about a developing security incident and the proper course of action to take while in a "wireless" operational setting.

The developed SKM, and its' mobile agent implementation, will be comprised of the following five security management components and will easily integrate with the existing IT and EA management practices required of Clinger-Cohen and the FISMA of 2002.

- *Security Policy Management*: The policy management module of the SKM will enable organizations to import or create security policies based on ISO, NIST or industry-unique standards, distribute them on-line, educate and train employees, and track compliance, exceptions and violations. We propose the design of an implementation of this function using secure mobile agents. This capability greatly eases annual reporting required of FISMA.
- *Threat Management*: The threat management module provides organizations with a proactive approach to the management of threats affecting information and technology assets by notifying the owners and users of system of assets when new vulnerabilities are identified. The threat management module receives threat input from all major threat and vulnerability sources, both academic and commercial, and feeds this information to appropriate security officials within the enterprise. We propose the design of an implementation of this function using secure mobile agents. This capability implements the threat management requirements of FISMA.
- *Asset Management*: This module of the SKM allows organizations to manage system and security assets and the process for determining the proper controls (patches, fixes, updates, and procedures) to be implemented on specific infrastructure assets based on use and potential risk to the agency. It provides an integrated task management system that alerts users when "new" security tasks have been assigned to them and provides a summary of the impact of that task on the assets for which they have responsibility. This function is accomplished with secure agent technology. This capability implements the security profile management requirements of FISMA.
- *Incident Management*: The next module of the SKM allows organizations to dynamically create incident-modules for the collection and distribution of security-related content and/or documents. With proper access rights, users will have complete security-related content creation and editing functionality, library services, and workflow staging abilities. Once created, these custom modules would be available to all appropriate personnel, specified user groups, or merely function as a personal incident description for its' creator. This management module function will be implemented with secure mobile agent technology.

- *Collaboration Management*: Finally the SKM will provide the benefit of creating a secure collaborative discussion and work area for structured interactions between users relative to a particular security subject. This function will be implemented using secure mobile agents.

5. Implementation of Security Knowledge Management (SKM) Techniques and Tools

Our society is becoming increasingly aware of the need for preventative and recovery measures against infrastructure failures and attacks such as *cyber-attacks* (recently termed *cyber-terroris*m). In a cyber-attack, a malicious party seeks to cause damage to a given resource not through traditional means, but through its computer systems. As our society has grown ever more dependant upon computer systems as a means for management and monitoring of critical infrastructure resources, so too has the need for efficient protection and response mechanisms for such systems. Even greater concern lays within the inherent vulnerability faced by smaller, more entities which could easily be uprooted by a strategically placed cyber-attack. Such a remote entities within an enterprise, which are prevalent across America, often do not have the resources or power to respond to such an attack and are faced with a difficult situation which could greatly undermine their critical infrastructure (such as banks, water/power, etc.).

One of the greatest threats to cyber-security within our nation lies in the sector of rural, home and small business networks. Very often they are poorly administered and few, if any, security mechanisms protect the network from potentially dangerous attacks. This leads to a particularly easy target for attack from malicious parties. Intrusion into such systems would allow for a jumping point into different, perhaps more sensitive enterprise networks. Such sectors in our network infrastructure provide a kind of backdoor which could be used to gain access to any given number of resources and systems. This plays a particular interest in systems that monitor critical infrastructure such as water and power systems, where intrusion and the subsequent takedown of such systems could lead to widespread emergency across a community. To circumvent this problem, we propose a Knowledge Management (SKM) Techniques and Tools as explained above. These techniques and Tools comprised of 5 elements. These elements will be implemented by using secure mobile agent technology [Bradshaw, 1997], [Ng, 2000], [Sergio, 2001], [Jansen], [Liotta, 2002], [Jane, 2002], [Pham, 1998], [Greenberg, 1998].

Our interest in mobile agents is not motivated by the technology per se but rather by the benefits agents provide for creating distributed systems. There are at least eight main benefits, or good reasons, to start using mobile agents [Danny, 1999]: They reduce the network load, they overcome network latency, they encapsulate protocols, they execute asynchronously and autonomously, they adapt dynamically, they are naturally heterogeneous and they are robust and fault-tolerant, personal assistance. Agent technology is a new approach of designing software. It focuses on agents as the main level of abstraction. Agents are active software components which can either reside at specific locations in a network (stationary agents) or travel between network nodes (mobile agents). Agents have the ability to find and filter information, negotiate for services, automate complex tasks, and collaborate with other software agents to solve even more complex problems [Bradshaw, 1997], [Ng, 2000], [Sergio, 2001], [Jansen], [Liotta, 2002], [Jane, 2002], [Pham, 1998], [Greenberg, 1998]. Agents can combine basic services to provide more complex services. They can be reconfigured during runtime by paramaterizing or by dynamically loading or unloading code modules, resulting in a component-based approach. Agents require distributed application platforms on which they can reside and travel between. These platforms need to provide a certain infrastructure to be used by the agents. Agent technology is considered in a wide range of telecommunication applications, such as mobile computing, military, electronic marketplaces for service provisioning, network management, and more.

We believe that, because of above reasons, mobile agents provides a practical methodology to detect and avoid intrusions and large scale attacks as well as provide critical information during such an emergency in order for a broader, effective response and prevention in rural, home, small networks

and large distributed networks. We propose that elements of SKM be done by a secure distributed agent system. In this system, autonomous and relatively intelligent pieces of software work together to maintain security and detect attacks against various network nodes; in case of an intrusion, the software will respond by fixing security holes and sharing information with other nationwide networks in order to circumvent further attack and minimize damage. This is of paramount importance in smaller communities and Enterprises where one does not always have access to expert knowledge on security; that's why we seek to provide an ´´***expert in a box***´´ solution in which the security knowledge, unique to each system, exists within the system itself in the form of a community of agents as shown in (Fig. 3).
The primary factor limiting the widespread availability and acceptance of mobile agents is their currently unresolved problems with security. Being a truly distributed environment, the common solutions to most enterprise security problems find little application to mobile agents. As a result, new approaches must be researched and applied to agent platforms in order to ensure they execute in a non-malicious and non-vulnerable manner. Studies have outlined various areas of security concern as well as possible solutions within the mobile agent paradigm [Ng, 2000], [Sergio, 2001], [Jane, 2002], [Greenberg, 1998], [Jansen], [Ertaul, 2000].

In our research work must be done to address the security problems that hinder widespread acceptance of the agent computing paradigm. Specifically, we must develop solutions to attacks from a host against a visiting agent so as to address the problem of an adversary (such as a terrorist) gaining physical access to a network to undermine its security agent infrastructure. Promising areas such as Blackbox Security, Mobile Cryptography and Code Obfuscation seem to offer steps in the right direction [Sander], [Sander, 1998], [Hohl, 1998], [Collberg, 1997], [Low, 1998], [McGraw, 2000], [Tyma, 2003], [Collberg, 2003], [Ertaul, 2004]. In the implementation of SKM modules these directions will be investigated to find proper solution to agent security problem to be able to use agents in the implementation of SKM modules.

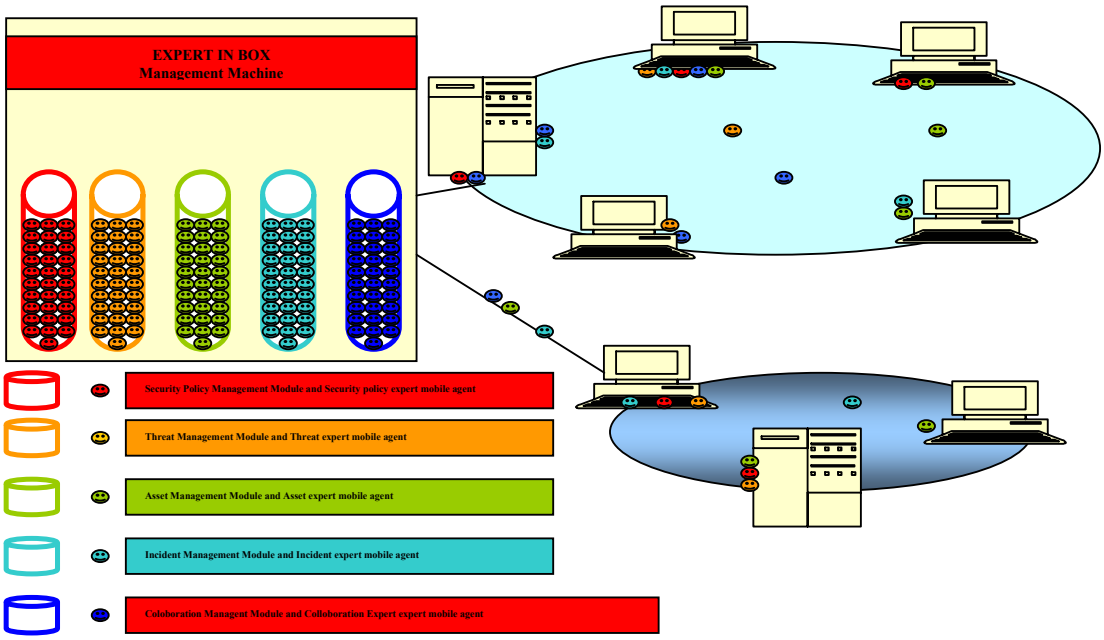

Fig. 3 "Expert in a box" model for SKM

6. Conclusions

In this paper, issues related to the need to develop an ESP framework in the context of federal agency's development of their respective Enterprise Architectures were discussed. Using the Zachman Framework as a foundation, we identify and implement modern analytic methods and techniques that will allow information security to be integrated seamlessly into the overall Enterprise Architecture (EA) of an agency or business. Resulting ESP products are compatible with the Federal Enterprise Architecture (FEA) Reference Model, Capital Planning and Investment Control (CPIC) guidelines, and provide the baseline for continuous Security Program Management as required by the Federal Information Security Management Act and prevailing corporate governance guidelines. In this paper, to implement developed techniques namely security knowledge management tools, we propose secure intelligent agents as "***expert in a box***". In expert in box solution the knowledge exists virtually within the system itself in the form of a community of agents. In addition, to address security of mobile agents, which has paramount importance in the usage of mobile agents in today's technology, new advanced techniques such as Blackbox Security, Mobile Cryptography and Code Obfuscation are proposed as direction to solve the security problems in mobile agent's field.

References.

Architecture Alignment and Assessment Guide, 2000.

Bradshaw, J. M., 1997, An Introduction to Software Agents. Software Agents, chapter 1, AAAI Press/The MIT Press.

Braithwaite, T, 2003, Lecture Notes: FEAF and DoDAF Course Outlines and Materials – FEAC Institute.

Clinger-Cohen Act of 1996, 1996, Public Law 104-106.

Collberg, C., Christian, C., Clark, T., Low, D., 1997, A Taxonomy of Obfuscation Transformations. Technical Report, University Of Auckland.

Collberg, C., Thomborson, C., 2003, WaterMarking ,Tamper-Proofing and Obfuscation – Tools for Software Protection. University of Arizona Technical Report.

Danny, B.L. & Mitsuru, O., 1999, Seven Good Reasons for Mobile Agents. Comm of ACM, V. 42, No. 3.

Department of Defense, C4ISR Architecture Working Group, 1997, DOD C4ISR Architecture Framework, Version 2.0.

Ertaul, L. & Tekin, A., 2000, Security of Mobile Agents. ISCIS XV, Proc. of the 15th International Sciences.

Ertaul, L. & Venkatesh, S., 2004, JHide-A Tool Kit for Code Obfuscation, IASTED, SEA2004 Proceedings.

FCIO, Federal Chief Information Officer (CIO) Council, 2000, Capital Planning & IT Management Committee; Smart Practices in Capital Planning

FEA, A Practical Guide to Federal Enterprise Architecture, Version 1.0, 2001.

FEAF, Federal Enterprise Architecture Framework (FEAF), Version 1.1., 1999.

FISMA, Federal Information Security Act, 2002, Title III to Public Law 107-347 E-Government Act.

Greenberg, S. M., Byington, C. J., Holding, T. & Harper, G.D.,1998, Mobile Agents and Security. IEEE Commun. Mag.

Hohl, F., 1998, Time Limited Backbox Security: Protecting Mobile Agents from Malicious Hosts. Mobile Agents and Security, Lecture Notes Computer Science 1419.

Jane, W. & Karygiannis, T., 2002, Mobile Agent Security, NIST Special Publication 800-19.

Jansen, A. W., Determining Privileges of Mobile Agents, http://citeseer.nj.nec.com/.
Jansen, W. Countermeasures for Mobile Agent Security. NIST, http://citeseer.nj.nec.com/.

Liotta, A., Pavlou, G., Knight, G., 2002, Exploiting Agent Mobility for Large-Scale Network Monitoring, IEEE Network, Vol. 16 No. 3 pp 7-15.

Low, D., 1998, Protecting Java Code via Code Obfuscation, ACM Crossroads Student Magazine.

Mc Graw, G., Viega J., 2000, Make Your Software Behave: Security by obscurity. IBM Developer Work.
Ng, S.,2000, Protecting Mobile Agents Against Malicious Hosts. MPhill Thesis, The Chinese University of Hong Kong.

OMB Circular A-130, Management of Information Resources, 2000.

O'Rourke, C., Fishman, N., & Selkow, W, 2003, Enterprise Architecture Using the Zachman Framework. Course Technology, a division of Thomson Learning, Inc.

Pham, V.A. & Karmouch A., 1998, Mobile Software Agents: An Overview. IEEE Commun. Mag.

Sander T. & Tschudin, F.C., Towards Mobile Cryptography, International Computer Science Institute, http://citeseer.nj.nec.com/.

Sander, T, Tschudin, F.C.,1998, Protecting Mobile Agents Against Malicious Hosts. Mobile Agents and Security, Lecture Notes Computer Science 1419, Springer-Verlag.

Sergio, L.,2001, Mobile Code Protection. PhD Thesis, Institut Euecom, France.

Sowa, J.F. & Zachman, J.A., 1992, Extending and Formalizing the Framework for Information Systems Architecture. IBM Systems Journal, Vol 31, No 3.

Tyma, P., 2003, Encryption, hashing, and obfuscatio, ZD Net.

Zachman ,J. A, 1987, A Framework for Information Systems Architecture. IBM Sys. Journal, V. 26, No 3.

Zachman J. A., 1996, Concepts of the Framework for Enterprise Architecture. Zachman International.
Zachman, J. A., 1995, Enterprise Architecture and Legacy Systems. Zachman International.
Zachman, J. A., 1995, The Challenge is Change: A Management Paper. Zachman International.
Zachman, J. A., 2004, The Zachman Framework for Enterprise Architecture: Primer for Enterprise Engineering and Manufacturing. e-book.

Levent Ertaul: He is currently a full time Asst. professor at California State University, Hayward, in the department of Math & Computer Science. He is actively involved in security projects nationally and internationally. His current research interests are Mobile Agents Security, Wireless Security, Ad Hoc Security. He has numerous publications in Security issues.

Timothy Braithwaite: He is currently director of Federal Enterprise Architecture Certification (FEAC) Institute (Security Programs). He used to teach, as adjunct faculty, in the Department of Information Systems Management – University of Maryland. He is author of more then six security related books.

Beryl L. Bellman: He is currently a full time professor at California State University at Los Angeles in the Department of Communication studies. He is also Academic director in FEAC institute. His current research interests are ESP, Role and Function of EA in E-Gov, Knowledge Management and Information Systems.