Summary Report on Enterprise Security Workshop

David Gilliam
California Institute of Technology,
Jet Propulsion Laboratory
dpg@jpl.nasa.gov

Abstract

This report summarizes the presentations of the 7th IEEE Workshops on enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002), Enterprise Security (ES) Workshop.

The ES Workshop had 13 papers, 2 poster papers and 1 specialty paper presented. The topics covered the following: Anonymity and Cryptography, Authentication and Access Control, Communication Security, Intrusion Detection, and Software and Network Security.

Professor Jeannette Wing of Carnegie Mellon University, gave the Plenary Address on the topic of "Vulnerability Analysis of Networked Systems."
At the joint WETICE session, the ES Workshop Summary Report was presented describing the activities and discussions.

1. Introduction

The ES workshop has four domains covering the following topics and their associated sub-topics: Internet security, Distribution, Secure infrastructures, and Security management, with each topic have multiple sub-domains.

The presentations at the 7th ES Workshop covered several of these domains including:

- Anonymity and Cryptography
- Authentication and Access Control
- Communication Security
- Intrusion Detection
- Software and Network Security

An invited talk by Professor Jeanette Wing of Carnegie Mellon University on the topic of "Vulnerability Analysis of Networked Systems," reported on efforts on using modeling techniques for attacking vulnerabilities on networked systems and the potential for exploiting the system. This work is being sponsored by NASA's Ames Research Center (ARC).

A brief excerpt of each presentation and the associated discussion in the workshop is presented below. The excerpts provide the reader information primarily on the workshop proceedings. Detailed information on each paper and the authors is not repeated here. The workshop papers and the associated slide presentation can be found on the WETICE'02 ES workshop web site: http://wetice02.jpl.nasa.gov/presentations.

2. Anonymity and Cryptography:

Several presentations on anonymity and cryptography were given in this workshop:

- Analysis of an Anonymity Network for Web Browsing
- A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection (Poster Paper)
- Infinite Length Hash Chains and Their Applications
- Hydra: A Decentralised Group Key Management
- Mobile Agent Clone Detection System with Itinerary Privacy

The presentation on "Analysis of an Anonymity Network for Web Browsing," gave an analysis of the tradeoffs between performance and security in an anonymity network for web browsing. Dummy traffic is used to hide any correlations in the traffic; the analysis examines how network utilization, user-perceived performance, and security are affected as different amounts of dummy traffic (and with different characteristics, such as queuing delay) are used. The authors show one way of using dummy traffic without unduly impacting performance. Discussions focused on latency and "baselining" traffic using this scheme, and susceptibility to Distributed Denial of Service attacks.

The Poster Paper, "A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection," gave a description of maintaining pseudonymity in the delegation of signature authority. Here, the proxy's identity is hidden using an alias. If needed, the alias issuing authority would be able to identify the proxy using the alias. The scheme work by others noted in the presentation. Its unique contribution is in proxy privacy and privacy revocation through the use of an alias.

Another presentation on "Infinite Length Hash Chains and Their Applications," covered a method for making hash chains of infinite length to increase their security, providing greater security for internet transactions as in electronic micro-payments. Questions were raised on the performance cost of using infinite hash chains, metrics, and their use with symmetric and asymmetric keys.

"Hydra, A Decentralised Group Key Management," examined a method for group key management. Instead of having one key server distributing keys to a group whenever the group changes, a number of servers play the role of a key server. This proposed method provides flexibility and scalability of key distribution in large distributed environments. The potential of greater risk to keys being compromised by using multiple systems to distribute the keys generated discussion and was contrasted to the security of being able to continue to exchange new keys in the event of an attack to one.

The "Mobile Agent Clone Detection System with Itinerary Privacy," described how to detect clones of mobile agents using a protocol based on detecting double-spending of e-cash. It was brought out that this research addresses unauthorized cloning. The research should also address how it can be coupled with other research or technology to provide a full solution to cloning including host replay attacks and authorized cloning.

While there are still a number of weaknesses in providing anonymity and managing cryptographic keys, the research presented addresses several key areas. There are methods that seem to enhance the security of the protocols and passing of keys / re-keying. However, these efforts need to work more closely with those working in secure authentication, access control, and communication

3. Authentication and Access Control:

Presentations on authentication and access control included:

- What are Multi-Protocol Guessing Attacks and How to Prevent Them
- Towards Scalable Authentication in Health Services
- Selecting a Security Architecture for a New Model of Distributed Tutorial Support
- Towards an Access Control System for Mobile Peer-to-Peer Collaborative Environments

The presentation on "What are Multi-Protocol Guessing Attacks and How to Prevent Them," depicted schemas for breaking passwords used over the network. Techniques to analyze multi-protocol exchanges for vulnerability to password guessing attacks were discussed. Use of the same password for multiple systems and re-using passwords provide the greatest vulnerabilities that allow them to be compromised through these guessing attacks. Using different passwords over the networks and changing them more frequently can help thwart guessing attacks through these techniques.

"Towards Scalable Authentication in Health Services," describes a system to overcome authentication problems in health services. It focuses on solving the problem of interoperability in authentication and authorization mechanisms. It examines the interaction of different smart tokens by user's authenticating to different servers with varying authentication methods. It also examines authorization issues. HIPPA compliance is a key goal in this research effort. The research is attempting to provide a comprehensive mechanism for doctors and patients to communicate securely using different types of authentication methods and mechanisms. This problem will continue to require more research as biometrics, token-based devices, including use of wearable computers, PDA'S, etc., are impacting secure communication.

Access control was the subject of "Selecting a Security Architecture for a New Model of Distributed Tutorial Support." The research focuses on Role-Based Access Control (RBAC) as a more flexible and efficient access control approach than other approaches (DAC, MAC). The approach uses RBAC with a focus on OASIS (Open Architecture for Secure, Interworking Services). It examines the OASIS RBAC for suitability in meeting the access control requirements of a distributed collaborative tutoring environment. OASIS supports a role definition language to classify clients in terms of names given them by services. RBAC is a flexible model and can meet most requirements of present distributed collaborative environments since it promises a more fine grained access control for today's de-centralized distributed systems. Although, RBAC address the most requirements of information security such as least privileges, separation of duties, whether it can be implemented to meet these features will depend on a robust implementation approach.

The last paper in this area, "Towards an Access Control System for Mobile Peer-to-Peer Collaborative Environments," presents an access control system that is able to work without dedicated servers and can be used even by weak end systems (in terms of memory, processing power, and connectivity) through the provisioning of access certificates by stronger peers. The system relies on XML and related technologies. The architecture supports both DAC and RBAC, as well as highly decentralized architectures. The Access Control Lists (ACL) can be hosted in virtually any environment, including a peer-to-peer network. A nomadic peer can be offline and still be in the network, but must synchronize when reconnected.

Discussion on this last presentation was on how access queries are composed: by applications, systems, users, or a combination. Also, discussed was what cryptographic schemes could be used, and how cookies and temp files were handled. The research proves promising and additional efforts will be of benefit. A key area to be addressed is scalability.

In these last three presentations on authentication and access control, scalability is a key issue, along with providing metrics on a simulated large-scale deployment.

4. Secure Communication:

Presentations on secure communication included:

- Maintaining Remote Services and Resources Over the Internet and Other Networks (Poster Paper)
- On Communication Security in Wireless Ad-Hoc Sensor Networks
- ActiveSync, TCP/IP and 802.11b Wireless Vulnerabilities of WinCE-based PDAs

"Maintaining Remote Services and Resources Over the Internet and Other Networks" was a poster paper presentation describing the collective use of several technologies to provide secure communication over insecure networks. The goal was to design and demonstrate a simple, flexible architecture for operating and maintaining servers (and services) at remote locations securely using existing technologies in combination.

The presentation "On Communication Security in Wireless Ad-Hoc Sensor Networks," described some of the security threats in wireless ad hoc networks. The solution to these threats is to encrypt the data sent between nodes at different levels. It uses a three tiered strategy for security in sensor networks. Each tier offers greater security for more sensitive data. The proposed model is one where all nodes are completely trusted and have been previously been setup with a set of master keys. The protocol does not use any key exchange or public key based algorithms in an attempt to minimize the overhead of the security mechanisms, and therefore is subject to latency. Metrics need to be provided on latency for mobile systems such as PDA's.

"ActiveSync, TCP/IP and 802.11b Wireless Vulnerabilities of WinCE-based PDAs" describes some of the vulnerabilities of these systems. The paper intends to make a study of the security limitations and loopholes on Win CE based PDA's. The research revealed weaknesses in the WEP protocol. However, the research did not address IR weaknesses and vulnerabilities in these systems, nor did it address web browser vulnerabilities or susceptibility to malicious code.

Since this area is still in its infancy and is growing, it is hoped that additional research delineating the weaknesses in wireless communication and small mobile systems, including wearable computers will be provided along with research in mitigating these weaknesses.

5. Intrusion Detection:

The research presented on intrusion detection and Intrusion Detection Systems (IDS) were as follows:

- Preemptive Distributed Intrusion Detection using Mobile Agents
- Honeypots for Distributed Denial of Service Attacks
- Intrusion Detection: Systems and Models

The first paper, "Preemptive Distributed Intrusion Detection using Mobile Agents," in this section covers several areas, including cryptography and access control. The research describes an agent-based, distributed Intrusion Detection System that blocks (or implements an alternate policy) when an intrusion is discovered. It addresses the clone detection problem in mobile agents with respect to the double spending problem in transferable e-cash. It then provides a method for adopting and adapting existing solutions in cryptography and access control to prevent unauthorized cloning in *e*business transactions. This research only addresses unauthorized cloning. It also needs to address how this research can be coupled with other research or technology to provide a full solution to cloning including host replay attacks and authorized cloning. Also, false positives and false negatives need to be addressed in this scheme, especially in networks requiring high availability.

"Honeypots for Distributed Denial of Service Attacks" (DDoS) describes a new approach on the use of and purpose for honeypots. Honeypots can be used to provide an additional layer of security in detecting and preventing DDoS attacks. A multi-operating system is used as a honeypot with multiple OS's communicating to each other as a self-contained network, mimicking an enterprises network. One system acts as a trap for DDoS attacks against another. The idea is to lure the attackers into a simulated environment and giving them a feeling of successful compromise. The potential exists then, to learn their techniques by trapping their attack in the multi OS also preventing or limiting actual attacks against the enterprise network. However, this approach only adds an additional layer of defense and only partially mitigates the problem of DDoS attacks.

A specialty paper on "Intrusion Detection: Systems and Models" was presented that provides the current state of the art in IDS systems. This research is useful by providing a description of the current state of IDS' and in providing a foundation for extending research in this area.

A fair amount of research still needs to be done in the area of IDS'. The issue of false negatives as well as false positives still provide a significant area of research as shown in this last research presentation. Network learning and reaction to intrusions or cloning in *e*business transactions still faces several unresolved problems as shown above.

6. Software and Network Security:

Application of formal approaches to software and system security was the subject of this last section:

- A Flexible Modeling Framework (FMF) for Software Security