WETICE 2006
Eleventh Securities Technologies (ST) Workshop Report

David P. Gilliam* & Matt Bishop**
Co-Chairs, WETICE Securities Technologies Workshop
** dpg@jpl.nasa.gov; ** bishop@cs.ucdavis.edu,*

1. Introduction

The Securities Technologies (ST) Workshop for WETICE 2006 accepted papers covering a wide-variety of topics that had applicability to the other WETICE workshops. The cross-over interest of papers in this, and other, workshops was discussed in the wrap-up presentation on the final day.

The ST workshop had ten papers submitted to it this year. Six papers were accepted for the workshop as full papers.

The topics had a wide range and included the following:

1. Some Problems in Sanitizing Network Data
2. Authorisation using Attributes from Multiple Authorities
3. Enterprise Collaborative Contexts and their Provisioning for Secure, Managed Extranets
4. Security Verification Techniques Applied to PatchLink COTS Software
5. Security Constraints in Access Control of Information System Using UML Language
6. Autonomous Information Unit: Why Making Data Smart Can Also Make Data Secured?

2. Presentations and Discussions

The papers were presented on Day 1 of the WETICE workshop. For day 2, the group had the opportunity to participate with other WETICE workshops and discuss with them security issues in their presentations on collaboration and technologies.

2.1 Invited Talk: Some Problems in Sanitizing Network Data

Matt Bishop, from the University of California at Davis, discussed the problem of sanitizing IP addresses in network traffic. This problem arises because institutions would like to share data collected from the network without exposing the particular IP addresses used. The paper presented a model in which a set of collectors gathered network traffic, sanitized it, and gave it to analysts for security analysis. The adversary received the same data as the analysts. The goal of the adversary was to determine the unsanitized IP addresses.

The work identified three key problems: consistency in data from multiple collectors, the fact that namespaces are finite, and the semantics of names. The talk presented a tool, *tcpsani*, that prototyped several methods of sanitization and was being used to explore the issues.

The talk concluded with a discussion of related work and open problems, comparing the sanitization problem to several other classic problems.

2.2 Best Paper Award: "Authorisation using Attributes from Multiple Authorities"

The Best Paper was awarded to Authorisation using Attributes from Multiple Authorities by David Chadwick of the University of Kent, UK. This paper was selected due to the topic, content and flow, style and grammar.

The paper covered how to provide authorization from multiple authorities while maintaining security and privacy. For example, users hold multiple attributes from multiple authorization authorities (AA) such as an IEEE membership, a university degree, roles in organizations, *et al.* Resources may require attributes from multiple AAs, *e.g.* a university employee who is IEEE member gets special discounts at an online book store. Users have different IDs on different AAs. Different AAs may have different naming schemes. Attribute linking may breach users' privacy.

If the user can link together his attributes in different AAs whilst ensuring the user's privacy, and these attributes can only be released to a resource when the user says so, then we have the basis for a solution. When a resource contacts one of the AAs to authenticate and return the locally assigned attributes of the user, the AA can also return referrals to the other linked AAs that also have attributes for the same user.

Proceedings of the 15th IEEE International Workshops on Enabling Technologies:Infrastructure for Collaborative Enterprises (WETICE'06)
0-7695-2623-3/06 $20.00 © 2006 IEEE

2.3 Enterprise Collaborative Contexts and their Provisioning for Secure, Managed Extranets

The work that David Moreland from CSIRO, Australia, presented could also have been presented in the DMC workshop as it had wide applicability. This paper focused on service layer for collaborating parties to work together with a guaranteed quality of service (QoS) in a secure, trusted environment that spans multiple ISPs. Service providers can provide a secure infrastructure on top of ISP services for a collaboration environment between entities that have agreed to work together. A Virtual Network Operator (VNO)\ provides the service to the collaborators with a service level agreement (SLA) that includes a quality of service (QoS) that they must negotiate with the underlying ISPs who are providing the connections and bandwidth. It presented results from a project that tested and verified the approach.

2.4 Security Verification Techniques Applied to PatchLink COTS Software

David Gilliam discussed an integrated life-cycle approach to software security that was tested with a commercial off-the-shelf application. Model checking validated the specifications and architectural design. Property-based testing checked the code for violations of specified security properties. These proved of value in discovering some weaknesses in the software artifact as well as verifying the viability of the instruments and approach to software security.

2.5 Security Constraints in Access Control of Information System Using UML Language

Aneta Poniszewska-Maranda from the Technical University of Lodz, Poland, focused on application of UML concepts to security policies and roles using the RBAC model. The research provides a definition and expression of access control constraints using an object-oriented modeling language, UML, and in particular the Object Constraint Languate (OCL). It addresses three types of conditions: pre-conditions, post-conditions, and invariants Security constraints are specified by class diagrams and sequence diagrams.

2.6 Autonomous Information Unit: Why Making Data Smart Can Also Make Data Secured?

This paper was written by Ed Chow and focused on a fine-grain distributed information protection mechanism that can self-protect, self-discover, self-organize, and self-manage. The approach decomposes data into smaller pieces to provide individualized protection along with a policy control mechanism to allow "smart" access control and context based re-assembly of the pieces. By combining smart policies with individually protected data, better protection of sensitive information is achieved. This approach provides solutions for problems such as distributed information protection and identity theft.

3. Focus for WETICE Security Technologies (ST) Workshop, 2007

The focus for WETICE 2007 ST Workshop was discussed and two foci were agreed on as goals for the next workshop:

1) Security and Privacy: Granular protections for personal data in highly distributed environments
    a) Databases & Web services
    b) Application services and protocols
2) Unified and coordinated security services in a global, heterogeneous environment
    a) Provisioning
    b) Underlying Support Technologies
    c) Cooperation/collaboration between services & providers

Where overlaps occur with the other workshops, the ST Workshop will submit areas for cross-collaboration and presentations. The ST Workshop will also work to come up with a list of recommended further areas of research.

4. Conclusion and Observations

This year's ST 2006 Workshop was smaller than the previous workshops due to the smaller number of papers received. This may be a result of the larger number of security-oriented workshops now being held. The smaller number of papers presented allowed for more time to present the research work, more time for feedback on the work presented, and time for discussion of tangential security issues not covered in the workshop, including time to mix with the other WETICE Workshops and participate in their discussions. We hope that this cross-workshop participation will provide more cooperative efforts where there is potential for collaboration and discussion.

Proceedings of the 15th IEEE International Workshops on Enabling
Technologies:Infrastructure for Collaborative Enterprises (WETICE'06)
0-7695-2623-3/06 $20.00 © 2006 IEEE