Themes and Highlights of the New Security Paradigms Workshop 1999

Panel Chair - Mary Ellen Zurko, Iris Associates

Panelists

Nathan A. Buchheit, United States Military Academy, Department of Electrical Engineering and Computer Science

Ronda R. Henning, Harris Corporation

Dean Povey, Security Unit, DSTC

Prof. Peter Reiher, Computer Science Department, University of California, Los Angeles

Session abstract

This panel presents a selection of the best, most interesting, and most provocative work from The New Security Paradigms Workshop 1999 (sponsored by ACM). For seven years, the New Security Paradigms Workshop has provided a productive and highly interactive forum in which innovative new approaches (and some radical older approaches) to computer security have been offered, explored, refined, and published.

This year, NSPW accepted papers on a wide variety of subjects including market forces and security, adaptive traffic masking, security and dependability, security policy enforcement, security modeling, architecture based design, protocol analysis, group management, seat management and cost of ownership, redundancy, survivability, access controls, and information warfare. We have selected the four papers that we believe have the most potential for generating engaging discussion at the NISSC panel session. Their abstracts follow.

Position statements from each panelist

Strike Back: Offensive Actions in Information Warfare

Nathan Buchheit, Anthony Ruocco, and Donald J. Welch, United States Military Academy, West Point

The danger is real and the threat is immediate. “Attacks on decision makers, the information and information-based processes they rely on, and their means of communicating their decisions,” [1] are occurring with increased frequency. In this case we are referring to Information Warfare and not criminal activity. Information Warfare is conducted by political organizations (nations, terrorist groups, and nationalist groups) whose primary aim is to weaken another political organization and does not have to take place within the context of a declared war or armed conflict. It may replace or compliment terrorist activity. It is happening on a battlefield unconstrained by political or geographic borders where combatants can attack from any place and at any time.

Attacks are being conducted and orchestrated by governmental and non-governmental organizations using sophisticated professionals motivated more by money or nationalistic zeal. In light of this, we believe that the current position of only providing a “defense in depth” [1] to deter attacks is inadequate to respond to the current threat to our national defense.

One of the time-tested principles of warfare is that to win you must go on the offensive. You cannot win any conflict solely through defense. Sun Tzu said the “ability to defeat

the enemy means taking the offensive." [5] When you are on the defensive your adversary chooses the time and place for the battle. He will attack when he has what he considers sufficient resources to maintain the attack until he is successful or he runs out of resources. The resources of conventional war (people, material, national will, etc.) are far more constrained than in information war. It is conceivable that a determined adversary could mount millions of attacks from computers across a wide region. In such a case it is inevitable that he will eventually succeed.

Regardless of foe, the United States needs to conduct the necessary offensive operations. In this era of information warfare, it needs to strike decisively and send a clear message; the electronic equivalent of "speak softly but carry a big stick." This paper supports the viewpoint that our position should be one of offensive counterattack against aggression via the "electronic superhighway". The best defense against cyberattack will be a strong offensive counter cyberattack against anyone foolish enough to risk it.

Security Architecture Development and its Role in the Seat Management and Total Cost of Ownership Environments

Ronda R. Henning, Harris Corporation, USA

Corporate information systems have been moving towards platform standardization and the outsourcing of an organization's data management infrastructure. Within this context, two ideas repeatedly surface:

1. Total cost of ownership, or TCO, in which an organization can track the cost per employee for infrastructure, help desk support, upgrades, and ongoing maintenance.

2. Seat Management, whereby an organization is benchmarked against best practices in similar organizations, and recommendations to improve cost effectiveness are suggested. These recommendations include standardization of hardware and software suites, centralization of network management functions, and consolidation of help desk support.

While standardization of the enterprise's computing infrastructure is a desirable economic goal, it is not a good strategy from an information survivability perspective. Current thought in information survivability favors a diversity of hardware and software within an organization. In this scenario, an organization's ability to survive an intrusion is increased when all of an organization's platforms are not subject to the same vulnerabilities or attack scenario.

In both TCO and Seat Management environments, an organization's network services are considered a utility, and user organizations are billed on a per seat or per user basis for information systems services. Current TCO and seat management analysis tools address the selection of hardware and software suites for clients and servers as well as speed and quality of network service.

If an organization's network infrastructure has been privatized or leased from a vendor, the tenant organization may have minimal assurance that security is being correctly managed. The contracting organization is dependent on the security services that the service provider has in effect. There may be shared storage media with other customers, a lack of protection for network connections, or no cohesive incident response capability. An important, and often missed aspect, is the concept of shared risks and vulnerabilities. For example, if a Department of Defense (DoD) site connects to the Defense Information

Systems Network (DISN) and uses an outsourced infrastructure for its own intranet, that shared infrastructure becomes a potential vulnerability to DISN.

This presentation discusses the definition of Service Level Agreements (SLA) for security with the Seat Management/TCO context. With SLAs in place, an organization has a measurable, quantifiable set of standards that can be applied to security management services. The issues under discussion are:

- Can security services be quantified into contractually binding, measurable capabilities?
- Can an effective information survivability policy be incorporated in this scenario, or does an organization sacrifice survivability for economies of standardization?

Optimistic Security: A New Access Control Pardigm
Dean Povey, Security Unit, DSTC

Despite the best efforts of security researchers, sometimes the static nature of authorizations can cause unexpected risks for users working in a dynamically changing environment. Disasters, medical emergencies or time-critical events can all lead to situations where the ability to relax normal access rules can become critically important.

The paper presents an optimistic access control scheme which looks to provide a system where enforcement of rules is retrospective. The system administrator is relied on to ensure that the system is not misused, and rollback is provided to ensure that the system integrity can be recovered in the case of a breach. It is argued that providing an optimistic scheme alongside a traditional access control scheme can provide a useful means for users to exceed their normal privileges on the rare occasion that the situation warrants it.

The idea of a partially-formed transaction is introduced to show how accesses in an optimistic system might be constrained. This model is formally described and related to the Clark-Wilson integrity model.

Securing Information Transmission by Redundancy
Jun Li, Peter Reiher and Gerald Popek
Computer Science Department, University of California, Los Angeles

Many approaches have been used or proposed for providing security for information dissemination over networks, including encryption, authentication, and digital signatures. These mechanisms do not, however, necessarily help ensure that a security-related message is delivered at all. Attacks that try to destroy or intercept security messages require other mechanisms. Authenticated acknowledgements are sometimes useful for this purpose, but do not scale well.

This paper discusses the use of redundancy to combat attempts to prevent information dissemination. Redundancy has been widely used in other areas, such as high availability data storage, file replication, and some fault-tolerant systems. The security problem has different characteristics that require different approaches to redundancy.

A network may already have some inherent redundancy and reliability mechanism to adapt to failure and dynamics. But they are far from enough to counteract interruption

threats. To achieve better security, transmission redundancy has to be added to enhance the resiliency and improve the availability.

This is difficult. While two distinct disks or processors can be used, in this arena it is not always true that two or more disjoint paths can be easily located for reaching a specific destination through a network. And in order to deploy redundancy in large-scale networks, the system has to be adaptive in dealing with application specificity and other factors such as location and transmission characteristics, and be secure itself.

We further present one example of using redundancy to increase assurance of security updates delivery. The system is called Revere, where redundancy is built into a self-organizing structure to push and pull security updates in a large-scale network.

Short bio of panel chair and speakers

Mary Ellen Zurko is a security architect at Iris Associates, home of Lotus Notes. She has written on public key infrastructures, distributed authorization, user-centered security, security and the web, privacy, and A1 operating systems. Her current interest is security for active content and agents. She has a MS and BS from MIT.

Peter Reiher received his Ph.D. from UCLA in 1987. He worked at JPL on the Time Warp Operating System until 1992. He is now an Adjunct Associate Professor in the computer science department of UCLA. His research interests include distributed operating systems, distributed systems security, active networks, mobile computing, and parallel discrete event simulation. Home page of authors: http://fmg-www.cs.ucla.edu/.

Dean Povey is a Research Scientist in the Security Unit of the CRC for Enterprise Distributed Systems. He has published several papers in the fields of Distributed Systems Security and Public Key Infrastructures, and is a current member of the Standards Australia working group on Public Key Authentication frameworks. Dean has also worked on the development of the cryptographic toolkits Oscar and JCSI and is currently contributing to the OMG standard for PKI services

Ronda Henning is the senior Secure Systems Engineer for Harris Corporation, Government Communications Systems Division; a Melbourne, Florida based international communications and electronics company. Ms. Henning currently leads the Information Assurance center of excellence, an interdisciplinary engineering group responsible for information assurance technology research and development as well as assurance technology insertion large scale systems integration opportunities. A member of the Harris Engineering Process Group, Ms. Henning developed the Harris Secure Systems Engineering Guidebook, and was a founding member of the National Security Agency (NSA)/Industry consortium responsible for the System Security Engineering Capability Maturity Model (SSE-CMM). Prior to her employment at Harris, Ms. Henning was a deputy branch chief of information security research and development at the National Security Agency. A Certified Information Systems Security Professional (CISSP), she holds an M.B.A. from the Florida Institute of Technology, an M.S. in Computer Science from Johns Hopkins University, and a B.A. from the University of Pittsburgh.

Mary Ellen Zurko
Iris Associates
5 Technology Park Drive
Westford, MA 01886
978-392-6018 (voice)
978-692-7365 (fax)
mzurko@iris.com

Nathan A. Buchheit
United States Military Academy
Department of Electrical Engineering and Computer Science
TH1114, Thayer Hall
United States Military Academy
West Point, New York 10996
(914) 938-2193 (914) 938-5956 fax.
DN5017@exmail.usma.edu

Prof. Peter Reiher
Computer Science Department
University of California, Los Angeles
Boelter Hall 3564
Computer Science Department
University of California, Los Angeles
405 Hilgard Ave
Los Angeles, CA 90095
Phone number - (310) 825-8332
Fax number - (310) 825-2273
Email: reiher@cs.ucla.edu

Dean Povey
Cooperative Research Centre for Enterprise Distributed Systems
Level 12, S-Block
Queensland University of Technology
Brisbane Qld 4001
Australia
ph: +61 7 3864 5120
fax: +61 7 3864 1282
Email: povey@dstc.edu.au

Ronda R. Henning
Harris Corporation, USA
Government Communications Systems Division
P.O. Box 98000,
Mail Stop W2/7756
Melbourne, FL 32902
ph: 407-984-6009
fax: 407-674-1108
Email: rhenning@harris.com