Symposium on Computer & Network Security

The Cyber Security Revolution: Protecting Critical Infrastructure with the Emperor's New Armor

Joe Pato, Hewlett-Packard

For e-business to become business as usual, we must protect our critical infrastructure. But who are the "we" who must act? What are the measures that must be taken by individuals, corporations, organizations and governments? How do we overcome the lack of effective trust among and between the actors in the information society? This talk will examine some of the technical challenges we are facing and national and international approaches to addressing critical infrastructure protection.

A System-Level Analysis of Biometric User Authentication

Stephen Kent, BBN

Biometric authentication technology, the use of personal physical characteristics or behavior to verify a user's identity claim, has been used successfully in high-security contexts as part of physical access control systems for many years. Its use in the information-security context, with sensors attached to or part of individual workstations and laptops, is a more recent phenomenon, made possible in large part by declining prices for biometric authentication hardware. Biometrics may even be used in a very local context, e.g., to activate crypto tokens such as smart cards.

Many vendors of biometric technology for information systems promote their products based on improved security. However, in order to evaluate this claim, one has to evaluate the perceived threat environment, something that rarely seems to be part of vendor or technical literature. One also should consider the security of these technologies in a broad system context, e.g., what are the larger implications for a user if there is a security compromise of a biometric authentication server? For example, biometrics may be employed in different ways to provide user authentication in the Internet or an intranet, with dramatically different security and privacy implications.

This presentation discusses system-level characteristics of biometric authentication technologies in several contexts, examining their security properties relative to various threat models. This analysis suggests that perhaps the best rationale for using biometrics is ease of use and cost effectiveness, but that attempts to make biometrics more secure often negate this latter feature. The presentation concludes with a discussion of ways to make use of biometrics that avoid these problems.

Shibboleth—A New Model for Controlling Access to Web-Based Resources

Steven Carmody

Shibboleth is an Internet2-sponsored project that is developing an architecture, policy structures, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. It is a functioning SAML (security attributes markup language) instantiation supporting federated administration with privacy built into the design. While the norm on the Internet has been to control access via identity, Shibboleth has developed a framework that more closely mirrors the physical world, where a wide variety of attributes (separate from identity) can be used to gain access to services. A key issue for Shibboleth has been to explore how people manage their privacy and when they are willing to trade off privacy for services.

How to Build an Insecure System out of Perfectly Good Cryptography

Radia Perlman, Sun Labs

This talk starts with a tutorial on network security protocols, key distribution mechanisms, and PKI models. Then it discusses example mistakes people have made when designing or implementing network protocols. Examples include an e-mail standard that allowed forging of signatures, a public key scheme less secure than a secret key scheme, a system that thought encryption implied integrity protection, public key certification chain rules that are unworkable in practice, and some of the fundamental flaws with the IKE protocol (the key exchange protocol for IPsec). The talk ends with a list of reasons that security hasn't been deployed yet.

System Security Methodology: Protecting Your ASSets

Christopher Spirito, EMC

Once you figure out how your systems were compromised and determine how much of your ASSets are and were exposed, you are going to start wondering where you went wrong. In many cases, you have a networking team very savvy in securing their routers and firewalls, an OS team who can lock down their servers, and application developers who usually have no clue how to implement security in their applications but rely upon the other two teams to protect their ASSets, the data.

Using a sound System Security Methodology will bring these teams together to approach their tasks within a common framework. Starting with a somewhat clear mission statement, each team will understand what information or data will be passing across areas of their responsibility. Drafting the Threat & Adversary model will allow the teams to match up their technical and personnel countermeasures with known attacks and exploits, quantifying the quality of countermeasures necessary. Lastly, many industries have regulations that dictate how specific types of information are to be protected.

This approach will allow for a comprehensive defense-in-depth Information Assurance program to be implemented, protecting and defending you and your information.

Distributed Data Authentication

Roberto Tamassia, Brown University

Security is an essential requirement of distributed platforms for business applications. We address the problem of authenticating high volumes of data and transactions in non-trusted distributed environments. We present a distributed authentication framework where a data set maintained by a trusted source is replicated at several non-trusted responders, which provide authenticated answers to queries on the data set posed by user. We also discuss applications of this framework to Web services, wireless roaming, and end-to-end integrity of electronic documents.

Lottery Enterprise Open Systems Initiative at GTECH

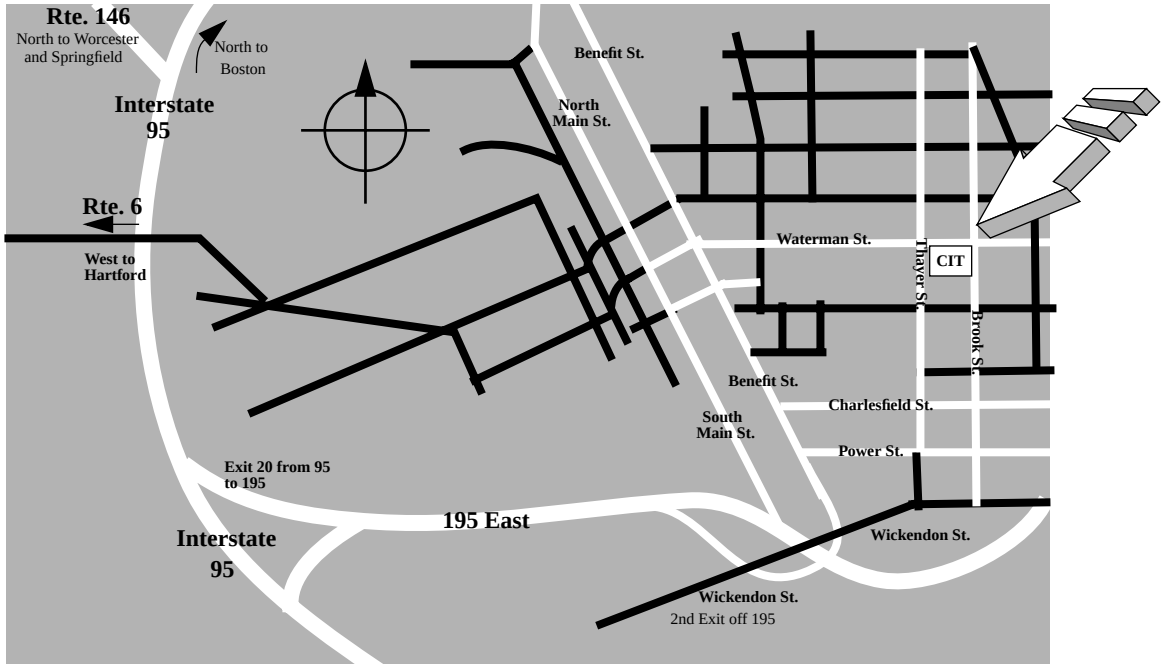
Miroslaw Kula, Didier Vereque, GTECH Corporation

GTECH's new strategic direction is anchored in a number of macrotrends developing in information technology at large as well as in the technology and fundamental business conditions of GTECH's core business.

Continued →

SCHEDULE

8:30	B R E A K F A S T and Registration 4th floor, CIT Building
9:00	**Introduction and Overview** Tom Dean, CS Chairman Michael Black, IPP Director Tom Doeppner, Host
9:30	**The Cyber Security Revolution** Joe Pato, Hewlett-Packard
10:30	B R E A K
10:45	**A System-Level Analysis of Biometric User Authentication** Stephen Kent, BBN
11:45	**Shibboleth—A New Model for Controlling Access to Web-Based Resources** Steven Carmody, Brown CIS
12:15	B U F F E T L U N C H
1:30	**How to Build an Insecure System out of Perfectly Good Cryptography** Radia Perlman, Sun Microsystems
2:30	**System Security Methodology: Protecting Your ASSets** Christopher Spirito, EMC
3:00	B R E A K
3:15	**Distributed Data Authentication** Roberto Tamassia, Brown CS
4:15	**Lottery Enterprise Open Systems Initiative at GTECH** Miroslaw Kula, Didier Vereque, GTECH
4:45	PANEL DISCUSSION
5:30	R E C E P T I O N (5th floor)



GTECH's next-generation transaction delivery and management system will rest on the existing secure online transaction processing system technology and will leverage the power of standard applications and communications to create new distribution opportunities while lowering total costs of ownership. It will integrate with retailer POS devices, e-tailing technologies, and enterprise business systems. And it will leverage the opportunities of IP-driven standards and provide access to services over multiple consumer-driven devices at a sustainable cost.

The presentation outlines the new company strategic vision, its technical manifestation, the known and new security challenges and what the company intends to do about them. The emphasis is on the peculiarities of the security domain as seen from the standpoint of the lottery business.

◆I◆I◆

This symposium is a benefit of membership in our **Industrial Partners Program**.
Member companies are: Compaq, EMC, Invensys (Foxboro), GTECH, IBM, MERL, Microsoft and Sun. There is no charge.

EMAIL REGISTRATION

To: sjh@cs.brown.edu
By: Monday, April 22, 2002
Please include the following:
Name, title
Company, Department
Postal address
Phone/Fax

DIRECTIONS TO THE CIT BUILDING

- From I-95 N or S, take Exit 20 to I-195E.
- From I-195E take Exit 2, Wickenden St.
- Go LEFT on Wickenden, LEFT again at the 2nd light onto Brook St.
- The red-brick CIT Building (Center for Information Technology) is on the left at the intersection of Brook and Waterman (1st light).
- *Registration is on the 4th floor.*

PARKING

Because most of the visitor parking has been assigned to University employees, I'm afraid we're unable to provide parking. Street parking is usually available for early birds, but watch out for newly designated 2- and 3-hour zones, which used to be all-day spots. You might try the residential area NW of the CIT.

The 29th IPP Symposium

Department of Computer Science

BROWN UNIVERSITY

SYMPOSIUM ON COMPUTER AND NETWORK SECURITY

Thursday April 25, 2002

Host: Professor Tom Doeppner

INDUSTRIAL PARTNERS PROGRAM