PANEL SESSION: SECURITY REQUIREMENTS FOR PKIs

Panel Chair: Alfred W. Arsenault, Jr., NSA
Panelists: Marc LaRoche, Entrust
Kathy L. Lyons-Burke, NIST
Eric S. Rosenfeld, Spyrus

BIOGRAPHY: Alfred W. Arsenault, Jr.

Alfred W. Arsenault, Jr. is a Senior Computer Scientist with the US Department of Defense. He has worked for DoD in the Computer Security and INFOSEC areas since 1983. During his career, he has also taught a variety of Computer Science classes as a member of the faculties of the University of Maryland-Baltimore County, and of the United States Air Force Academy. Mr. Arsenault has degrees in Physics and in Computer Science from Southeastern Louisiana University, and a Master of Science Degree in Statistics and Computer Science from Purdue University.

POSITION STATEMENT:

This panel session will explore the development of security requirements for the Certificate Issuing and Management components of Public Key Infrastructures (PKIs). The CIM components are those responsible for the issuance, management, and if necessary revocation of certificates in a system. Typical CIM components include Certification Authorities (CAs) and Registration Authorities (RAs). Overall security of a system protected by a PKI relies heavily on the security and correct operation of the CIM components.

Security of a CIM System (CIMS) includes a variety of things, such as:

- the platform - hardware, operating system, and middleware on which the CIMS runs
- the cryptography - algorithms and their implementation - used by the CIMS
- the procedures followed by the CIMS operators
- the qualifications and training of the CIMS operators; and
- the implementation of the CIMS itself

Attention has been focused on some of these factors before. For example, cryptographic standards such as FIPS 140-1 address the cryptography and its implementation. The procedures, qualifications, and training of personnel are typically covered by a Certification Practices Statements, and efforts such as Internet RFC 2527 provide guidance in that area. And the TCSEC, ITSEC, or Common Criteria could be used to look at the underlying platform.

However, until recently, little attention has been paid to the actual implmentation of the CIMS. In the last year, however, a number of efforts have started in this area. This panel will have speakers from a number of those efforts, explaining their views of the importance of this area, describing how they proceeded; and provided recommendations on the best way to proceed.

BIOGRAPHY: Marc Laroche, Entrust Technologies

Marc Laroche, Manager Product Evaluation at Entrust Technologies Limited is responsible for the security evaluation of Entrust products, including Common Criteria evaluations, FIPS 140-1 validations, and more.

Marc joined Entrust Technologies from the Communications Security Establishment (CSE), a Canadian federal agency. As the System Security Engineering unit head, Marc provided security engineering support services to the Canadian Federal Government Departments, wrote IT security technical reports and guidance documents, developed and delivered network security courses and training sessions. Prior to joining CSE, he served as a Communications and Electronic Engineer Officer in the Canadian Forces.

At Entrust Technologies, Marc manages the activities associated with the security evaluation of Entrust products, and conducts internal security reviews in support to the Entrust security assurance program. To date, these activities have resulted in the following accomplishment:

- Entrust Security Kernel (cryptographic module) version 3.1 and 4.0: FIPS 140-1 level 1 validated
- Entrust Security Kernel (cryptographic module) version 5.0: FIPS 140-1 level 2 validated
- EntrustFile and EntrustSession Toolkits version 4.0: endorsed by the Communications Security establishment under the Cryptographic Endorsement Program (CEP)
- Entrust/Authority and Entrust/Admin (from Entrust/PKI) version 4.0a: Common Criteria EAL3+ certified
- EntrustTrueDelete version 4.0: Common Criteria EAL1 certified
- Entrust/Authority and Entrust/RA (from Entrust/PKI) version 5.0: Common Criteria EAL3+ evaluation (in progress)

Marc has a bachelor's degree in electrical engineering from Laval University, Québec City, Canada.

POSITION STATEMENT:

The notion of trust is fundamental in public-key infrastructures (PKIs). For PKIs to be valuable, users must be assured that the parties they communicate with are safe, i.e. their identities and keys are valid and trustworthy. To provide this assurance, it is essential that the technology involved in binding the names of users to their public keys is trusted. The technology used to create these bindings includes security mechanisms and services that provide the secure generation, destruction, and distribution of cryptographic keys, cryptographic operations, complete access control, management of security functions and services, roles and separation of duties, audit of security critical events, secure communications, data protection, and more. These mechanisms and services contribute jointly in allowing the Certification Authority (CA) to securely bind together the user identities and public keys in a digital format known as a public-key certificate. In creating these certificates, CAs act as trusted third parties in a PKI. As long as users trust the CA and its business policies for issuing and managing certificates, they can trust the public-key certificates issued by the CA.

Trust can be defined as the degree to which one believes another will behave in a predictable or favorable manner. Trusting a CA implies that the people, processes and tools involved in the creation and management of public-key certificates can be trusted to make it so that the binding between users identities and public keys can always be relied upon. Thus there must be confidence that the technology involved in creating the public-key certificates can be trusted to operate with an appropriate level of security.

Security evaluations performed by certified third party evaluation facilities against recognized security criteria are instrumental in establishing trust in PKI technology. They allow unbiased security experts to analyze the security functions, interface specifications, guidance documentation and design of the product. The Common Criteria, which was newly adopted as ISO standard 15408, presents a suitable set of security functional and assurance requirements which can be used for defining PKI and CA security evaluation criteria in the form of a Security Target or Protection Profile. Such criteria allow the security community to share a common understanding and interpretation of what PKI and CA security requirements are, and what “trusted PKI and trusted CA” means.

For Entrust PKIs, the Common Criteria Evaluation of Entrust/Authority™ and Entrust/Admin™ serves as a fundamental extension to the FIPS 140-1 process in that it extends the security assurance to the services involved in issuing and managing the life cycle of public-key certificates. The certification of these products confirms that these products have met the specified Common Criteria Part 3 Evaluation Assurance Level (EAL) 3 augmented requirements, and can be trusted to reliably and securely deliver CA services.

BIOGRAPHY: Kathy L. Lyons-Burke

Ms. Lyons-Burke is a Computer Scientist for the Computer Security Division, Information Technology Laboratory of the National Institute of Standards and Technology (NIST).

Ms. Lyons-Burke's 20 year career in computer system technology has ranged from small system development efforts to management of large projects and has included numerous management responsibilities prior to joining NIST in 1998.

Ms. Lyons-Burke holds a Bachelor of Science and a Master of Science degree in Environmental and Forest Biology from the State University of New York, College of Environmental Science and Forestry and a Master of Science degree in Computer Science from the Johns Hopkins University.

Ms. Lyons-Burke is currently leading the Public Key Infrastructure (PKI) technologies and applications projects currently underway at NIST.

POSITION STATEMENT:

A Public Key Infrastructure (PKI) is an architecture that is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings and provide other services critical to managing public keys. A PKI consists of many components. A Certificate Issuing and Management System (CIMS) includes the components of the PKI that are responsible for the issuance, revocation, and overall management of certificates and certificate status information. A CIMS always includes a Certification Authority (CA) and may include Registration Authorities (RAs) and other subcomponents. A CA is sufficient if all the mandatory functionality is included that enable a CIMS to perform its tasks.

A Certificate Issuing and Management Component (CIMC) consists of the hardware, software, and firmware that are responsible for performing the functions of a CIMS. A CIMC does not include environmental controls (e.g., controlled access facility, temperature), policies and procedures, personnel controls (e.g., background checks and security clearances), and other administrative controls.

NIST is developing a document that specifies the functional and assurance security requirements for a CIMC. The intent of this requirements document is to ensure specification of the complete set of CIMC requirements and not the specification of a subset of requirements implemented in a specific CIMC subcomponent. It includes all the technical features of a CIMC, regardless of which CIMC subcomponent performs the function. The document does not differentiate between functions that are typically performed by a CA and functions that are typically performed by a RA.

Identifying all the subcomponents of a CIMC as a single entity assists in ensuring that the subcomponents compliant with the security requirements will operate in a secure manner. This approach also promotes interoperability because a single vendor (or integrator) will typically develop (or bundle) all the subcomponents together as a single solution. Typically, this is consistent with the way products are currently designed and built. A single product solution may make purchasing decisions easier because the user (or procurer) will not need to select subcomponents that meet a subset of the requirements. Finally, a single solution approach promotes security because the CIMC must:

- Implement all the mandatory security requirements, regardless of how they are allocated to subcomponents, and
- Ensure that functions implemented in one subcomponent do not compromise the security functions implemented in other subcomponents.

CIMCs will be operated in a wide variety of environments, from a closed secure facility to a hostile open access facility. Also, the sensitivity of the information protected by the certificates issued by CIMCs will vary significantly. Users will be required to evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity of the information. To address the varying levels of risk, this document specifies security requirements at four increasing, qualitative levels of security: Security Level 1, Security Level 2, Security Level 3, and Security Level 4.

In order to maintain the security of a CIMC, the ability to perform many of the functions specified are allocated to distinct roles. A CIMC is not required to implement all of the roles listed, but is only required

to implement roles to meet the role separation requirements. A CIMC must ensure that no user is authorized to assume multiple roles if role separation is required for a specified Security Level. That is, a user shall be prevented from assuming multiple roles if the authorizations are assigned to different, mutually exclusive roles.

BIOGRAPHY: Eric S. Rosenfeld

Eric Rosenfeld is a Scientist at SPYRUS. Eric was a software engineer on the BBN Certification Authority Workstation, the cornerstone of the DMS PKI. At GTE CyberTrust, Eric served as a System Engineer for GTE Internetworking's VPN Advantage, providing expertise in the area of IPsec and PKI. Now at SPYRUS, Eric is working on Common Criteria evaluations for PKI products and other PKI-related system engineering activities.

POSITION STATEMENT:

Digital certificates are being deployed in increasing numbers of applications to address many security vulnerabilities. But digital certificates require a Public Key Infrastructure, or PKI, which has its own security vulnerabilities. The part of the PKI directly responsible for generation, issuance, and revocation of digital certificates is referred to as the Certificate Issuing and Management System, or CIMS. In order to secure applications using digital certificates, the supporting PKI, and in particular the CIMS, must also be secure.

Thus it is important to be able to evaluate a CIMS against a common set of security requirements. These security requirements should be written in internationally accepted terms, such as the Common Criteria. Furthermore, they should be generic enough so that a wide variety of architectures can be evaluated, but sound enough so that they can be used to provide a meaningful evaluation. The resulting evaluations would allow CIMS customers to accurately compare products or services that were built by different companies.

SPYRUS has developed a set of four Common Criteria Protection Profiles that can be used to evaluate CIMS products or services. These four profiles specify the minimum security requirements for different assurance levels.

The profiles define the assumptions about the security aspects of the environment in which the CIMS is used; define the threats that the CIMS must address; define implementation-independent security objectives of the CIMS and its environment; define functional and assurance requirements to meet those objectives; and provide a rationale demonstrating how the requirements meet the security objectives.