Databases of threats and countermeasures

Jim Williams (Chair), The MITRE Corporation
Natalie Brader, L-3 Network Security
Douglas McGovern, Ray-McGovern Technical Consultants
Kenneth Olthoff, NSA
Adam Shostack, BindView Development
Pascal Meunier, Purdue University (Alternate Panelist)

Abstract:

Public databases of vulnerabilities, threats, and safeguards are increasingly common and sizable. They are being developed by many different kinds of groups: security vendors, large software vendors, academics, hackers, and even government organizations. Our goal is to discuss how we can best use them and how they should be designed for best use. Uses fall into two main categories, security testing (including vulnerability assessment) and security design. Interestingly, both groups tend to begin with what's real: known vulnerabilities in the case of security testing, and known threats in the case of security design. Consequently, there is some difference in emphasis.

Database quality and utility will be discussed from multiple perspectives. Issues that we plan to cover include the following:

Need for an accepted vocabulary
Database quality and utility
Optimal abstraction level for databases
Costs and Benefits of Secrecy
Classification schemes, taxonomies, and thesauri
Possibilities for standardization
Application to security testing
Security Requirements authoring
Pre-deployment security testing
In-field security testing

Panelist Perspectives

Natalie Brader will discuss the effort in creating and maintaining the database for the L-3 Network Security product line, as well as, the problems in product comparison due to vocabulary differences.

Doug McGovern will discuss the threats that derive from evaluation of physical objects such as smart cards and how these differ from purely logical threats against software. In this context, databases are useful but not all of the answer, due to the fact that the real world is not well behaved.

Kenneth Olthoff will address the structure, language and abstraction level used in vulnerability tools and databases. He believes that these factors will shape our consideration of the problem, perhaps in unanticipated ways.

Adam Shostack will discuss the effort in creating and maintaining the database for the HackerShield product line, as well as issues involved in security testing, and how issues of terminology and taxonomies will make sharing of data painful for some time to come.

Jim Williams will discuss the use of threats-and-countermeasures databases as an aid to the construction of security specifications, with emphasis on Protection Profiles in the sense of the Common Criteria. This will include a short overview of the CC Toolbox, a free automated tool being developed under NSA/NIAP sponsorship.

Pascal Meunier plans to discuss vulnerability databases from educational, consumer and research perspectives. He is currently unhappy with all the databases he knows, including his own efforts, inasmuch as they should represent knowledge, organize it, help with its analysis and manipulation, as well as being practical references, without requiring an inordinate amount of time to construct.

Panelist Biographies

Natalie Brader is the Director of Engineering Support for L-3 Network Security. In addition to supervising the Quality Assurance and Research departments, she is providing database design for L-3 Network Security™ Expert™ and Retriever™. The databases provide vulnerability, threat and safeguard (countermeasure) information in support vulnerability and risk assessments performed using the L-3 Network Security product line.

Doug McGovern is Vice President of Ray-McGovern Technical Consultants, Inc. After retiring from a career at Sandia National Labs he is consulting on security. His most recent assignment has involved developing protection profiles for smart card systems.

Kenneth Olthoff has been working in Information Security at the National Security Agency since his graduation from Purdue University Calumet. He tends to habitually ask questions. The views expressed may not be those of the management.

Adam Shostack, Director Of Security Technologies for Bindview Development, has lead the creation, evolution and maintenance of a product oriented vulnerabilities and testing database to support the HackerShield product line.

Jim Williams, Lead INFOSEC Scientist at the MITRE Corporation, has played a lead technical role in adapting threat-and-countermeasure information for use in creating Protection Profiles under the Common Criteria (CC). Previously, Dr. Williams was actively involved in the review of the CC and in the development of its predecessor, the U.S. Federal Criteria.

Pascal Meunier is a Master's student in computer sciences at CERIAS, Purdue University, and recently worked in the Security Systems group at Hewlett-Packard. He is considering an open vulnerability database, and the representation of vulnerabilities, threats and attacks in relation to resources and policies in an object-oriented structured database. Dr. Meunier's previous achievements are described in Marquis' Who's who in Science and Engineering.

Background of audience you are trying to attract

We want to talk with the developers and users of databases of threats and safeguards:

Those who maintain them for use in security products.

Those who need to know what's in them in order to specify secure products.

Those who do research on how to organize and improve these databases.

Panelist Contact Information

Panelist contact information:

Natalie Brader
L-3 Network Security
613 NW Loop 410, Suite 100
San Antonio, Texas 78213
(210) 344-3200 x 117 (w)
natalie.brader@l-3security.com

Douglas E. McGovern
Ray-McGovern Technical Consultants, Inc.
22304 East 67th Street
Broken Arrow, OK 74014
ph 918/355-3522, fax 918/355-1026
demcgovern@aol.com

Kenneth G. Olthoff, NSA / V22
9800 Savage Road
Ft. Meade, MD 20755
Ph. 410 854 6318 or 410 789 5534
kolthoff@radium.ncsc.mil

Adam Shostack, BindView Development
Adam Shostack
55 New York Ave
Framingham MA 01701
508 620 0644 x225
adam@bindview.com

Jim Williams (Chair)
The MITRE Corporation
202 Burlington Rd.
Bedford, MA 01730
Ph. 781-271-2647 (w), 781-271-3957(fax)
jgw@mitre.org

Pascal Meunier (Alternate Panelist)
COAST Lab (CERIAS), Purdue University
Ph. 765-494-2636
pmeunier@purdue.edu