Sharing Security Information for International Peace

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

It's a commonplace that information assurance suffers from two fundamental problems in information acquisition: failure of ascertainment (failing to realize that a breach of security has occurred) and failure of reporting (keeping apprehend breaches secret). In an overview of statistical methods in computer-crime reporting< http://www.mekabay.com/methodology/crime_stats_methods.pdf >, I pointed out that one of the most striking research studies of ascertainment and reporting was carried out by the United States (US) Department of Defense:

> In a landmark series of tests at the Department of Defense, the Defense Information Systems Agency found that very few of the penetrations it engineered against unclassified systems within the DoD seem to have been detected by system managers. These studies were carried out from 1994 through 1996 and attacked 68,000 systems. About two-thirds of the attacks succeeded; however, only 4% of these attacks were detected…. [O]f the few penetrations detected, only a fraction of 1% were reported to appropriate authorities.

One interpretation at the time was that if the US military was incapable of convincing its professionals to notice and report more than a tiny fraction of the minority of penetrations that were even noticed, the chances were low that non-military branches of the government, private industry, and other non-governmental organizations were doing even that badly.

One of the reports on this project is in the "Security in Cyberspace" document presented to the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs of the United States Senate for the 104th Congress, on May 22, June 5, 25 July & July 16, 1996. Several formats of the report are available online < http://archive.org/details/securityincybers00unit > including the 29MB PDF version.< http://archive.org/download/securityincybers00unit/securityincybers00unit.pdf >. There is a reference to the 65% successful penetration rate on page 37 of that document.

US Government Projects

There has been progress in information sharing about computer crime. For example, the Common Vulnerabilities and Exposures (CVE< http://cve.mitre.org/ >) Database run for the US government's Computer Emergency Readiness Team< http://www.us-cert.gov/ > of the National Cyber Security Division< http://www.dhs.gov/xabout/structure/editorial_0839.shtm > in the Department of Homeland Security(DHS< http://www.dhs.gov/index.shtm **>)** by MITRE Corporation< http://www.mitre.org/about/ > has been widely adopted< http://cve.mitre.org/compatible/index.html > by organizations around the world as a repository of shared definitions and descriptions of what it defines as follows: "An information security 'vulnerability' is a mistake in software that can be directly used by a hacker to gain access to a system or network." These definitions provide a basis for information sharing by standardizing terminology so that different software systems and databases can share data using the same

nomenclature. Even if internal names used within the different products don't match, tables of equivalence of the local names with CVE entries can still allow communications.

To search the CVE, use the National Vulnerability Database< http://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=all&cves=on > maintained by the National Institute of Standards and Technology (NIST). At the time of writing (mid-March 2012) there were 49,627 records in the database.

Another constructive US government contribution to security-information sharing is the "Information Sharing Strategy for the Department of Homeland Security" (ISS< http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf >) of 2008. The DHS summarized the strategy as follows:

> The President and Congress have directed the DHS to perform an essential and multi-faceted mission: prevent and protect against terrorist attacks; respond to both man-made and natural disasters; perform the law enforcement and other crucial functions of the Department's component agencies; and play a central role in augmenting the Nation's ability to gather, analyze and disseminate information and intelligence.
>
> To ensure that information and intelligence flow where and when they should, DHS must foster information sharing, consistent with law, regulation and policy, in each of the following ways: i) internally within DHS, ii) horizontally within the U.S. government between both law enforcement agencies and the intelligence community, iii) vertically with State, local, territorial, tribal and private sector partners, and iv) horizontally with the law enforcement and intelligence agencies of foreign allies and appropriate international institutions.< http://ise.gov/mission-partners/department-homeland-security >

The ISS established Information Sharing Standards described as follows (summarizing p.7):

- Functionality in the critical infrastructure is primary, not technological details;
- Information sharing will maximize interoperability regardless of technical infrastructure;
- Readily-available commercial standards and protocols will be the standard for information interchange;
- Information sharing will respect privacy and security of the shared data.

The overview page< http://www.dhs.gov/files/programs/sharing-information.shtm > for information-sharing projects run by DHS includes details and links for three computer-related services among the nine listed:

- Automated Critical Asset Management System (ACAMS< http://www.dhs.gov/files/programs/gc_1190729724456.shtm >)
- CIKR Asset Protection Technical Assistance Program (CAPTAP< http://www.dhs.gov/files/programs/gc_1195679577314.shtm >)
- Protected Critical Infrastructure Information (PCII< http://www.dhs.gov/files/programs/editorial_0404.shtm >) Program

UK & EC Programs

In the United Kingdom (UK), plans released in November 2011 for a UK cyber-security and cyber-crime strategy include a special unit with the National Crime Agency<

http://www.homeoffice.gov.uk/crime/nca/ >. Writing for eWeek< http://www.eweek.com/c/a/Security/UK-CyberSecurity-Strategy-Beefs-Up-Defenses-Information-Sharing-409924/ >, Fahmida Y. Rashid added that

> The plan outlined a new public-private sector collaboration in which the government and businesses will exchange information on cyber-threats and responses…. [T]he partnership will allow organizations to receive classified details about cyber-attacks and information on how to counter them."

Rashid writes that the definition of national infrastructure will be expanded to include more of the private sector, and the public will have a centralized system for reporting cybercrimes and receiving technical advice on appropriate responses.

At the European Community (EC) level, a report by Tom Espiner in ZDNet< http://www.zdnet.co.uk/news/security-threats/2011/12/07/certs-hindered-by-lack-of-sharing-says-eu-agency-40094599/ > discussed a report< http://www.enisa.europa.eu/act/cert/support/proactive-detection/ > by the European Network and Information Security Agency (ENISA) that failure to share information about cyber-incidents among national computer emergency response teams (CERTs) is reducing the effectiveness of the organizations. ENISA published its report in English< http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report/at_download/fullReport > and also a summary of the survey< http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report > that was used in preparing the full report. The report describes and evaluates 30 different "Services for the proactive detection of network security incidents" (p 27 ff using the page numbers in the document, not the PDF page numbers) and 12 "Tools/mechanisms for the proactive detection of network security incidents" (p75 ff). The report continues with detailed analysis of "shortcomings in the proactive detection of incidents" (p 108 ff) and ends with several pages of recommendations (p 128 ff) for both data providers and for data consumers. The conclusions (p 133) end with the assertion about the importance of data sharing: "The end goal is improving data sharing and cooperation in proactive detection and incident handling between CERTs – an essential element for the successful mitigation of cyber-attacks."

Private Sector

Internationally, organizations such as SANS< http://www.sans.org/ > do their best to share security information using "Consensus Research Projects" which currently include the following three relevant titles:

- 20 Critical Security Controls< http://www.sans.org/critical-security-controls/ >
- Top Cyber Security Risks < http://www.sans.org/top-cyber-security-risks/ >
- Top 25 Software Errors < http://www.sans.org/top25-software-errors/ >

Among the countless research scientists constantly publishing valuable insights into systemic and specific errors in security and recommending practical improvements, Peter G. Neumann< http://www.csl.sri.com/users/neumann/ >, Principal Scientist for the SRI International Computer Science Laboratory < http://www.csl.sri.com/ > is one of the stars of the academic firmament. He has been moderating the "Forum on Risks to the Public in Computers and Related Systems" (usually just called the *Risks Digest*< http://catless.ncl.ac.uk/Risks/ >) continuously, brilliantly and amusingly (he is an inveterate punster) since 1985. As a contribution to ease of access, I

have compiled PDF files< http://www.mekabay.com/overviews/risks/index.htm > for each volume from 1 to 25 (1985-2010) and will be adding the next volumes within a few months of this writing. Readers may also download a single ZIP archive< http://www.mekabay.com/overviews/risks/risks_01-25_pdf.zip > file with all the PDF files for volumes 1 to 25 and another ZIP archive< http://www.mekabay.com/overviews/risks/risks_01-25_pdx.zip > with PDF index (PDX) files for rapid local lookup.

Concluding Remarks

I want to finish with a few personal comments about how I see the international implications of data sharing to fight cyberattacks and rectify vulnerabilities.

Criminals and terrorists worldwide now have the power to engage in asymmetric warfare against the critical infrastructure of nation-states. A few people can create and control botnets< http://www.honeynet.org/papers/bots/ > involving thousands of compromised systems that can spread malware and launch distributed denial-of-service attacks that can impede access to or even crash targeted production systems. Tailored malware such as Stuxnet< http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 > can target specific models and brands of supervisory control and data acquisition (SCADA) systems. Volunteer hacktivists can reveal vast volumes of classified materials< http://wikileaks.org/ >, with unpredictable effects on public reaction, government policy, and international diplomacy. Such electronic gangs may even be out-stealing< http://www.wired.com/threatlevel/2012/03/hacktivists-beat-cybercriminals/ > cybercriminals. And state-sponsored actors could easily carry out attacks on a particular target using IP-spoofing< http://www.sans.org/reading_room/whitepapers/threats/introduction-ip-spoofing_959 > to divert attention from their country to some other target in the hope of provoking international conflict.

As the reliance on information systems in critical infrastructure has increased over the last several decades, the need for information sharing has grown not only to increase technical resistance to failures and to attacks: information sharing has become essential to prevent international conflicts based on the behaviour of non-state actors, on misunderstandings, and on deliberate sabotage and misrepresentation. Effective information sharing, especially between and among potential adversaries, may be a tool for increasing cooperation and reducing hostility on the international stage.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *