Global Information Assurance Certification Paper

Network Attack – An InfoSec Topology Required

Michael A. Bumpus

December 30, 2000

High profile figures in the Information Security community have raised an interesting concept to describe network attack trends. They reveal that there have been three "waves" of network attack: physical, syntactic, and semantic. Identifying these attack trends helps set the conceptual framework for follow-on analysis, resulting in an increased level of professional understanding within InfoSec circles. Developing a profound knowledge of network attacks and other related aspects of InfoSec should help practitioners to better address today's threats and vulnerabilities (risk) and improve decision support.

The alarming situation, however, is that InfoSec experts are poorly postured to defend corporate and government resources against the current (syntactic) attack climate. As we progress further into the third wave era, the security situation worsens. Semantic attacks will force us to look beyond chic, cool, and expensive technology solutions to achieve only mediocre success. Security's scorecard in the war against network attacks means that we must also carefully address another aspect of security, the complex world of "human" factors – also known as the "soft" side of information and network security. Optimistically, our actions to make appreciable strides in security requires researchers, vendors, management and practitioners to gain a deeper understanding of numerous security elements and to understand the interconnected nature of networks, technology, the use of technology, and the human interface – an InfoSec topology.

Attack trends

Libicki's essay "The Mesh and the Net" discusses the future of military warfare from an information warfare perspective.[1] He codifies an approach to deal with network attack trends, and develops profiles according to the "targets" of such attacks. Cryptologist Bruce Schneier takes Libicki's three-wave scenario and explains them from an information security perspective.[2] The initial, or *physical,* wave dealt with attacks against targets such as electronics, computers, switches, databases, and power sources. This target set can be characterized as generally easy problems with which to contend, and normally of limited impact. This attack profile was mitigated by the use of distributed protocols and architectures, which created redundancies to prevent single critical nodes or points of failure.

The next phase, *syntactic*, employs attacks against a different target, that of the operating logic of computers and networks. This type of attack has been occurring for several years and continues today: against software vulnerabilities, cryptographic algorithms, protocols, and denial of service vulnerabilities. This category is a tougher problem set than the previous one. Significant expenditures are spent on efforts to combat this wave – which includes a distinct reliance upon technology such as firewalls, intrusion detection, and anti-virus scanning software.

The third and emerging type is called the *semantic* wave. Schneier shows that targets in this category are no longer electronic devices, but instead the human interface. The effective response to this wave is less obvious than the first and second waves. In addition to continuing to devise technical expertise to defend against syntactic attacks, InfoSec professionals must also address the human dimension and know how people assign meaning to content.

Responses reflect serious disconnect

The overwhelming response to Schneier's "The Third Wave Of Network Attacks" article appear to miss the mark by dealing with only parts of the problem. Based on comments at Slashdot.com, most respondents failed to understand the basic premise[3] as they focused on techniques or methods of attacks, vice the *targets* of attacks. Despite several assertions to the contrary, "semantic" does not equal "social engineering" nor does it solely mean "insider" abuse. A credible case can be made that social engineering and insider abuse certainly are elements of semantic attacks, but there are numerous other considerations as shown in the initial network attack topology below.

Type	Target	Vulnerability	Method	Results	Examples	Mitigation
Physical	trunk wires, computers, electronics, switches, databases, power	Design Procedures Security void	Physical Electronic - malicious code: virus, Trojans, worms	Limited: - single/few facility, computer, networks	Laptop theft	Physical, technology focus Redundancy, Distributed protocols
Syntactic	s/w products, protocols, crypto algorithms, operating logic -computers -networks	Poor design Poor testing Accountability	Electronic - malicious code: virus, Trojans, worms	Widespread: - many different sites, computers, networks	Morris worm DOS/DDOS Lovebug Melissa Mitnick	Techno focus - Intrusion detection - Incident response - Auditing - Passwords - biometrics - policy - - anti virus scanning - Firewalls
Semantic	Human Information - databases - raw - analyzed - reported - in-transit	Human - trust level - naïveté - analysis threshold Information - access - data classification	Social engineering Dumpster diving Competitive Intelligence Disinformation Hoax, scams Data diddling	Widespread or significant: - High $$$ - Life threatening Gain access Innaccurate intel Fraud Insider abuse Research, knowledge	Emulex Hoax Web defacements MidEast Cyber conflict	 Human/computer interface Human focused - situational awareness - education - policy data handling -Intent

			Subversion Espionage InfoWar	False information Perception mgmt, Mass manipulation		

In addition to the Slashdot responses, a McClure and Scambray weekly security commentary discuss the idea of "mass manipulation" and America's presidential race. They correctly comprehend the human aspect, quote Schneier's Third Wave article, and further assert, "…problems with misinformation aren't going to be fixed by technological 'magic wands' because they target people, not code."[4] This commentary however, then jumps to the conclusion that *policy* is the answer. Convenient to use the network attack scenario to discuss policy, but there likely needs to be a more holistic approach, as situational awareness and security training are two other "answers" which quickly come to mind.

To state the obvious, different InfoSec job functions yield different professional points of view. Individuals working intrusion detection issues focus on technical aspects to determine the answers to "what, how, and when" types of questions concerning unauthorized corporate intrusions, while intelligence analysts strive to determine the "who, where, and why" questions when looking at foreign penetration attempts. Meanwhile, law enforcement officials gather data on all categories to better apprehend perpetrators. There is a lack of, and therefore the opportunity for, social scientists to apply human factor research to the current network security problem set. The important point here is that it takes a convergence of technology and human factor perspectives to achieve InfoSec success.

InfoSec soul searching

As Schneier indicates, the InfoSec community is ill-prepared for such convergence. The SANS website also reflects a technology approach to InfoSec. The "Northcutt Interview Whether Certification Matters" and the "About the SANS Institute" page clearly focus on technical issues: "…the greatest threat to information security is the lack of people with technical security skills."[5] If one believes that SANS is an outstanding effort to reach consensus within the InfoSec community, then there is a strong reflection of the current InfoSec climate as being technology-oriented.

In early November 2000, the topics covered by Level One security papers revealed that there were 26 topic areas with a total of 169 security research papers.[6] A quick view of the 26 topic areas to determine the number of "technical" versus "non-technical" topics led to an interesting imbalance as shown below:

A snapshot of the Information Reading Room articles reveals that 89% of the 169 papers were "Technical" in nature, while a mere 11% appeared by title to be "Non-technical."

Where we're heading…

e a profitable future for security vendors and consultants seeking solely technical solutions to information security problems. The SANS Security Alert for December 2000's main article "Expert predictions for Security Trends in 2001" includes several experts' statements of continuing high levels of security expenditures.[7]

However, Forrester Research takes a contrary view of increasing security budgets, stating that this doesn't necessarily equate to good judgment or effective use of company resources. Despite estimates that security spending in the U.S. will grow by 300 percent through 2004, Forrester is concerned that much of this will be wasted effort. "Security managers aren't told what to secure so they oversecure… business managers don't want to spend the time or make the investment in order to come up with good textured security they just want to tell the other guy to make it safe," according to Frank Prince, a senior analyst at Forrester.[8]

The information security industry is unlikely to create silver bullets to completely safeguard e-commerce requirements. Imperfect technology is likely to reflect the capabilities of the fallible humans who design and maintain these technologies.[9] The key obstacle to overcome is that believing technology is the solution to the unreliability of human beings. Our high-level approach must blend human and technological considerations to improve security. One of the initial steps in this direction is for InfoSec professionals to develop an understanding of a comprehensive InfoSec topology.

Endnotes:

[1] Libicki, Martin. "The Mesh and the Net – Speculations on Armed Conflict In an Age of Free Silicon." Chapter 6, paragraph 6. March 1994. URL: http://www.ndu.edu/ndu/inss/macnair/mcnair28/m028ch06.html (26 Dec 2000).

[2] Schneier, Bruce. "Semantic Attacks: The Third Wave of Network Attacks." October 15, 2000. URL: http://www.counterpane.com/crypto-gram-0010.html (22 Dec 2000).

[3] "Swedish Lemon Angels." October 6, 2000. URL: http://slashdot.org/articles/00/10/06/055232.shtml (23 Dec 2000).

[4] Schneier, Bruce. Secrets and Lies. Wiley Computer Publishing, 2000. p. 7.

[5] McClure, Stuart and Scambray, Joel. "Mass Manipulation Isn't Reserved Just For Presidential Elections: IT World Be Warned." November 23, 2000. URL: http://www.infoworld.com/articles/op/xml/00/11/20/001120opswatch.xml (19 Dec 2000)

[6] Northcutt, Stephen. ""Northcutt Interview Whether Certification Matters." URL: http://www.sans.org/giactc/cert_dif.htm (15 Nov 2000).

[7] SANS Institute. "Information Security Reading Room. Version 2.66. URL: http://www.sans.org/onfosecFAQ/index.htm (4 Nov 2000).

[8] SANS Institute. "Expert Predictions for Security Trends in 2001. December 2000. URL: http://www.sans.org/SANSSecAlert2_102000.pdf (15 Nov 2000).

[9] Price, Frank. "Increased Security Spending Wasted" November 2000 URL: http://www.forrester.com/ER/Research/Report/Excerpt/0,1338,10707,FF.html (2 Nov 2000).

[10] Dumas, Lloyd. Lethal Arrogance. St. Martin's Press, 1999. p.12.