SECURITY

Considering Convergence?

The Tao of Network Security Monitoring: Beyond Intrusion Detection

My book The Tao of Network Security Monitoring: Beyond Intrusion Detection *explains how to implement products, people, and processes to identify and respond to intrusions on computer networks. I focus on collecting alert, session, full content, and statistical network evidence, but maintain a distinction between preventing and detecting intrusions. This article explains why the detection-oriented tools and techniques in* The Tao *(Chinese for "the way," pronounced "dow") should complement but not converge with protective devices and methods.*

Richard Bejtlich

During the 1990s telecommunications vendors promised a single converged pipe carrying voice, video, and data. Economically, transporting bits on a single line makes sense. From a reliability perspective, redundant communications links are preferred. If the power dies and my cable modem goes dead, at least my phone line works. If the phone line is cut, I can turn to my amateur radio rig.

Convergence has also appeared in the digital security realm. Vendors promise to solve all of our security needs with multi-function appliances, brushing aside intrusion detection systems (IDSs) which perform strict detection functions in favor of intrusion prevention systems (IPSs) which supposedly detect and prevent intrusions.

The convergence we have seen thus far has occurred in the wrong product set. Users should avoid products which consolidate protection and detection in a single system, and favor vendors who keep those functions separate. Only by preserving the distinction between these two security processes can we ensure each performs its duties adequately.

Protection is often implemented by access control devices like firewalls, which try to filter out malicious traffic. Preventative tools and techniques decrease the likelihood of compromise by shielding vulnerable targets from an intruder's reach. Modern IPSs are simply firewalls that work above the address and port layer, making decisions on application data as well.

Detection has two meanings; first, detection can mean the identification of malicious traffic. Any protective device must do this in order to stop attacks. Second, detection can mean discovering protective failures. Not only is malicious traffic seen, but the fact it is seen represents a failure of a firewall or other protective measure. This second meaning for the term "detection" points to the primary reason why converged devices should not perform protection and detection on a single platform using the same technology and processes, and could be the fault of a person, process, and/or product.

A "converged" device offering protection via access control and detection via traffic inspection is unlikely to do both jobs equally well, and will not be able to compensate for weaknesses in either capability. An access control device must be able to detect attacks in order to stop them. If the device doesn't stop an attack, it either (1) saw the attack but wasn't configured to stop it, or (2) didn't see the attack at all. Either case represents a failure of the security process.

When access control and detection are separated, the processes are more likely to complement each other. Indeed, access control and detection should be performed not only by separate products, but also by separate people following separate (albeit coordinated) processes. Only by keeping these functions separate can one hope to identify failures. This concept seems fairly new to the security world but it is well-known to any third party financial audit firm.

Consider the following scenario, which is based on incident response experiences at several companies. While working on its border router, a company inadvertently disables all inbound access control lists (ACLs). While the ACLs are down, an intruder discovers and exploits multiple vulnerable services on the organization's exposed network. After the router maintenance finishes, the ACLs are restored.

Unfortunately, the organization was unaware of two facts: (1) it did not know its ACLs were temporarily disabled; and (2) it did not know an intruder took advantage of the configuration error to install covert back doors.

This organization relied on converged access control and detection in the form of router ACLs and router logs, and suffered further damage due to human error. (The possibility of human error is only increasing in an ever more complicated, heterogeneous technical environment, and is not an indictment of the skill of this organization's staff.) The company discovered the compromise days later when customers complained of unauthorized charges, and turned to expensive incident response consultants to investigate and mitigate the event.

Compare that experience with the following scenario, also based on real incident response situations. A different company needs to troubleshoot an email transport problem. At some point the company disables all inbound firewall rules, without giving full consideration to the potentially adverse consequences of so drastic a decision.

Meanwhile, an independent network security monitoring (NSM) operation performs its detection duties, watching the email troubleshooter's perimeter. Suddenly the NSM analyst console identifies dozens of exploitation attempts, as shown by alert data from its IDSs. Examination of content-neutral, non-signature-based session data reveals multiple other intrusion attempts not detected by the IDS alert data. Investigation of full content data collected by the sensor shows the vast majority of these security events failed to compromise the target, but a few appear disturbing. The independent NSM operation notifies the company of its detective work, and the company reinstates its firewall rules.

If convergence should occur at all, it should take place within the access control market itself, not between the access control and detection arenas. Products filtering spam, XML, SQL, HTTP, and other application data should converge around a single access control device for all layers of the OSI model. The detection market should remain separate, with a focus on flagging intrusions and protective failures via network awareness and passive vulnerability identification. Discovery of malicious sessions or "flows," and integration with host-based audit data, is also promising.

Convergence is a good idea when the process does not violate security engineering principles. Should consumers continue to purchase products from vendors who promise to "do it all," they will suffer the consequences. Customers should remember that while detecting attacks is important, detecting failures in prevention is more important. Access control devices tend not to admit errors; if they had identified the attack they missed, why didn't they stop it? Indepenent third party products and services, oriented towards network audit, are more likely to identify preventative failures, thereby decreasing the window of exposure for vulnerable networks.

This article is written by Richard Bejtlich, author of *The Tao of Network Security Monitoring: Beyond Intrusion Detection*, Addison-Wesley, © 2005, ISBN 0-321-24677-2, $49.99US.

Former Air Force intelligence officer Richard Bejtlich is a security engineer at ManTech International Corporation's Computer Forensics and Intrusion Analysis division. A recognized authority on computer security, he has extensive experience with network security monitoring, incident response, and digital forensics. He maintains the TaoSecurity Blog at *taosecurity.blogspot.com*.

Recommended Reading

Exploiting Software: How to Break Code by Greg Hoglund and Gary McGraw, Addison-Wesley, ©2004, ISBN 0-201-78695-8, $49.99US.

Malware: Fighting Malicious Code by Ed Skoudis with Lenny Zeltser, Prentice Hall PTR, ©2004, ISBN 0-13-101405-6, $44.99US.

WI-FOO: The Secrets of Wireless Hacking by Andrew A. Vladimirov, Konstantin V. Gavrilenko, and Andrei A. Mikhailovsky, Addison-Wesley, ©2004, ISBN 0-321-20217-1, $34.99US.

Secure Architectures with OpenBSD by Jose Nazario and Brandon Palmer, Addison-Wesley, ©2004, ISBN 0-321-19366-0, $34.99US.

READ SAMPLES CHAPTERS

from these titles today at:
www.awprofessional.com/ddjnov
www.phptr.com/ddjnov