Maintaining Perspective on Who Is The Enemy in the Security Systems Administration of Computer Networks

William Yurcik James Barlow* Jeff Rosendale
National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign
605 E. Springfield Avenue
Champaign, IL 61820 USA
{byurcik,jbarlow,jeffr}@ncsa.uiuc.edu

ABSTRACT

Human operators in security systems administration of large and complex networks have the difficult task of maintaining the integrity of operations and network service availability while a multitude of organizational users accidentally misconfigure, misuse, and break software and hardware. This is also a position where adversaries actively try to avoid detection and circumvent protection in order to maliciously misconfigure, misuse, and break software and hardware throughout the network. Add the constant stress of new vulnerabilities, new attacks, new patches to be installed, and 24X7 user help desk/network operations coverage (where the most serious events fall outside of business hours) and this is the short life of a network security systems administrator before burn-out. This paper argues that, at the most basic level, tools to help a human operator distinguish between users and adversaries will make a significant impact toward improving this situation.

Keywords

security operations, incident response, intrusion detection

THE PROBLEM

Sometimes it is hard to tell the good guys from the bad guys. In computer network security systems administration this is a major problem. Alarms indicate security events but do not reveal intentions. After reacting in quick response to many false alarms, innocent accidental events, and actual attacks, human operators become dulled to distinctions between their customer user community and malicious attackers such that it becomes us (security system administrators) against the rest of the world. Of course this is not a healthy long-term attitude to maintain (for either the security system administrator or the organization being protected).

A large part of the problem is the asymmetry between offense and defense in computer network security. Computer network security is a continuously escalating battle with increasing stakes and no end in sight. While defenders harden operating systems, networks, and applications, attackers search for vulnerabilities in any of these areas. There are five fundamental asymmetries that favor attackers in this battle:

- Although Internet connectivity provides productivity to users via worldwide access to information, Internet connectivity also provides worldwide access for all attackers directly to any machine.
- While defenders must track and continuously patch every vulnerability, an attacker must only find one unpatched or previously unknown vulnerability to exploit and bring down an entire system.
- Defenders are dependent on the security of all systems within their community-of-interest perimeter. A peer system intrusion compromises all peers, attackers can act independently although they often work in crews.
- While attackers can focus on one system, defenders must protect against all attackers. All it takes is one attacker to develop exploits which are often shared worldwide.
- Attackers have the element of surprise since they can develop new exploits (ϕdays) and release them at any time, defenders cannot continuously protect against every possible attack (although they try).

All is not lost, however, since human ingenuity is the best defense. Successful managers quickly learn to rely on human experts rather than automated security devices (firewalls, intrusion detection systems, etc.) for protection. Security system administrators use dynamic defenses and intimate knowledge of their networks to their advantage in a way similar to how military leaders use indigenous knowledge of terrain and physical characteristics of terrain (elevation & flat, urban & jungle) for strategic advantage.

For the purposes of this paper we focus on security system administrator knowledge of the network via monitoring, a well-established strategy [2,4]. The sysadmin knows what assets comprise the network and profiles of normal operation benchmarks. The problem is that attackers often

* corresponding author and workshop participant, telephone: 217-244-6403.

look like users because they use deception and because attackers represent such a small percentage of malicious activity amongst large volumes of legitimate activity.

The remainder of this paper is organized as follows: Section two briefly describes the typical activities of a security systems administrator of a large network. Section three discusses visual tools we are developing to augment the security sysadmin in-the-loop. Section four presents analysis and an approach to solving the friend/foe identification problem. We end with a summary and conclusions in Section five.

A DAY IN THE LIFE OF A SECURITY SYSADMIN

Given the complexity of current large-scale computer networks and the fact that human administration costs generally outweigh equipment costs by as much as an order of magnitude, most monitoring approaches are moving toward removing the human-from-the-loop [8]. At NCSA we take the exact opposite approach by explicitly choosing to include the human-in-the-loop as the critical assessment point and decision-maker.

Humans bring special cognitive processing capabilities that are not approximated in artificial intelligence or expert systems that we endeavor to leverage: (1) high bandwidth visual processing (estimated to be 150 MB/s for a computer screen); (2) a very sensitive visual discrimination ability, known in perception psychology as the just-noticeable-difference; and (3) sophisticated pattern recognition for input visual stimuli especially if there are affordances for physical-world intuition (ecological design) [6]. Our intent is not for a human to be used as a machine to sit in front of a visual monitoring infrastructure 24X7 but to rather enhance human ability using visualization and automation to provide “situational awareness” [3].

For our specific environment we define “situational awareness” as the ability to effectively determine an overall computer network status based on relationships between security events in multiple dimensions. For instance in the space and time dimensions security events can be network-wide macro events (scans, denial-of-service attacks) versus individual machine micro events (compromised accounts, virus) or time accelerated versus deliberatively delayed in time (slow distributed scans). A human security operations system administrator is the one who makes the overall assessment addressing the following fundamental questions: (1) “Is anything bad occurring in the network?” (use of automated tools to distinguish suspicious behavior requiring further investigation), (2) “Where is something bad occurring in the network?” (spatial assessment of macro/micro assets), (3) “When did bad events first occur in the network?” (temporal assessment of activity), and (4) “How is something bad occurring in the network?” (mechanism of attack).

Given this continuous posturing against malicious attackers, there is really no typical day in the life of a security system administrator. However in order to convey a sense of structure, the following is a list of general activities:

- Monitoring systems via automated tools such as network intrusion detection systems (both network and host), honeypots (machines designed to detect and capture attacks), and firewalls/routers (machines designed to block network traffic).
- Keeping abreast of new information via global Email lists between security professionals and websites (FIRST, bugtraq at securityfocus.com, CERT advisories)
- Installing, configuring, patching, debugging software such as IDSs, routers, honeypots, log analysis tools
- Responding to attacks - incident response team following specific procedures
- Examining and restoring compromised computers
- Responding to user questions – network information center (NIC) function
- Interacting with other organizational units – at least some security functions should be distributed
- Security awareness public relations programs to keep the user community informed of status, potential attacks, and continuous reminders about mundane security (password integrity) and social engineering attacks.
- Developing new security software tools incorporating the latest technology since technology evolves both offensive and defensive strategies and tactics
- Internal meetings with security team and manager(s) to communicate situational awareness and marshal resources when necessary

In terms of organizational impact, a survey of help desk services reports that users are more likely to contact informal sources (colleagues) than to use a formal system (which is often automated) [7]. This validates similar situations at NCSA where certain sysadmin tasks and related user requests follow employees with corresponding expertise through different organizations despite mismatch with current tasking – users seek out known experts for help. The primary mission of the security sysadmin is to establish credibility as an organization’s security expert to do otherwise risks undermining.

SYSTEM MONITORING AND NOTIFICATION TOOLS

The state-of-the art in system monitoring and notification tools for security is mixed. The availability and scope of different types of tools is growing but the integration of human factors is poor and there is no one tool that provides insight into overall situational awareness. Security sysadmins must use multiple tools to monitor different parts of the network with each tool requiring specialized skills and yet providing only a limited view per tool. In addition these tools have short life spans such that security sysadmins must continually learn and incorporate new tools and few tools are coordinated for synergy.

Based on requirements elicited from security experts, we are developing two tools that facilitate the ability of a security sysadmin to provide an overall situational awareness of a large and complex computer network. At present we have (1) a static visualization of traffic on an entire Class B address space on one screen (with drill down capabilitiess) and (2) a dynamic animation playback of network traffic. These tools primarily augment the human-in-the-loop to provide insight into spatial and temporal dimensions. For instance, the dynamic tool is used to monitor events over time. When suspicious activity is identified using the dynamic tool, the static tool can then be used to assess macro/micro relationships for an overall situational awareness and action plan. Continuous monitoring is necessary since situational awareness can change instantly. At present we are approaching real-time visual monitoring with a delay of 10-15 minutes. We do receive real-time IDS alerts but find these alerts are usually not processed by humans in quicker than 15 minutes.

WHO IS THE ENEMY? - NOT AS EASY AS US & THEM

While most attention has focused on external attackers trying to infiltrate and disrupt while the security sysadmin stands guard, practically speaking this is not reality. The reality is the majority of security events have an organizational insider with privileged access and information as the root cause [5]. Thus the ability to distinguish friend from foe is not as easy as internal and external to an organization. We characterize the enemy as:

1) External attackers
2) Internal users who attack with insider access
3) Internal users who enable successful attacks

Categories (1) & (2) are obvious if it they can be identified and distinguished from each other. Category (1) is often detected and chased away but seldom prosecuted. Category (2) is usually detected and typically fired/prosecuted. While determining intent is difficult, the positive actions necessary for categories (1) and (2) are premeditated and thus arguably malicious without regard for damage levels.

Category (3) is ambiguous. What level of negligence constitutes responsibility for a successful attack? While this appears to be blaming the victim, organizations establish minimal security levels (strong passwords, antivirus software, change default configurations, eliminate unnecessary services, keep up with patches, backup early/often, protect against losses) with consequences for noncompliance. Practically internal users must be trusted for compliance but this trust is tempered with verification using vulnerability scanning and traffic monitoring.

CONCLUSIONS

The pivotal role of the security sysadmin is to serve as the thin line of defense protecting an organizational computer network. There is no substitute for a good sysadmin as much of the knowledge is obtained through (often painful) experience. We identify the need for automation to support sysadmins but argue that (at present) humans are irreplaceable in determining "situational assessment". Finally, we reopen a previously posed question - Who is the enemy?[1] The security sysadmin is strained focusing in three different directions – external attackers, internal attackers, and negligent internal users – thus all traffic and internal systems must be monitored. We hope this stimulates more discussion about the appropriate role of the security sysadmin and ways to enhance computer-human interaction in support of this role.

REFERENCES

1. Adams, A. and Sasse, M. A. Users are Not the Enemy. *Comm. of the ACM*, 42(12), (Dec 1999), pp. 41-46.
2. Anderson, J. *Computer Security Threat Monitoring and Surveillance.* (1980). <http://csrc.nist.gov/publications/>
3. D'Ambrosio, B. et al. Security Situation Assessment and Response Evaluation (SSARE), *DARPA Info. Survivability Conf. & Expo., (2002).* <http://www.computer.org /proceedings/discex/1212/volume1/12120387abs.htm>
4. Bishop, M. A Model of Security Monitoring, *Computer Security Applications Conference* (1989), pp. 46-52. <http://seclab.cs.ucdavis.edu/papers/pdfs/mb-89.pdf>
5. *CSI/FBI Computer Crime and Security Survey*. (2002). <http://www.gocsi.com/press/20020407.html>
6. Fawcett, T. and Provost, F. Activity Monitoring: Noticing Interesting Changes in Behavior. *ACM KDD* (1999). <http://www.hpl.hp.com/personal/Tom_Fawcett/papers/>
7. Govindarajulu, C. The Status of Helpdesk Support. *Comm. Of the ACM 45*, 1 (January 2002), pp. 97-100. <http://portal.acm.org/citation.cfm?doid=502269.502272>
8. Korzyk, A. and Yurcik, W. On Integrating Human-In-The-Loop Supervision Into Critical Infrastructure Process Control Systems. *SCS Infrastructure Protection/Emergency Mgmt. Symposium*, (2002). <http://www.sosresearch.org/publications/astc2002_humaninloop.PDF >

SHORT BIOGRAPHY (workshop participant)

James Barlow has been a system administrator of AFS and Kerberos systems for six years at NCSA. For the last two years he is the senior systems engineer on the NCSA Security Team where his responsibilities also include intrusion detection, data mining, and log analysis. Prior to this he was a flight simulator software engineer at Frasca Inc. for five years. His interest in the workshop topic stems from an ongoing research project that has resulted in tools to visualize security events in order to make security systems administration more intuitive and thus more effective. Related work he finds interesting and relevant to this workshop can be found in Bruce Schneier's monthly Crypto-gram newsletter: <http://www.counterpane.com/crypto-gram.html/>.