INFORMATION SECURITY IN ECONOMICAL INFORMATION SYSTEMS

Alin MUNTEANU
„TIBISCUS" UNIVERSITY OF TIMIŞOARA, FACULTY OF ECONOMICS

Abstract:
A well-run information security program provides a structured approach to the management of risk to an organization's information technology (IT) infrastructure and the information that it handles. In a typical business that continually faces new threats, the information security managers must ensure that they focus their efforts and budget money on the right initiatives and tools to gain the greatest risk reduction for the business at the least cost. This is not an easy task, as these decisions must be made in the face of a number of significant challenges.

Key words: *information security, information technology, risk management*

JEL classifications: *L86, H55, M15*

For many information security professionals, one of the greatest attractions to the field is that there is always something new going on: new threats, new technologies, new business initiatives, new regulations. This is often one of its greatest frustrations also, as it is impossible to ever achieve a state of perfect security in which all risks are mitigated to a level that is acceptable to the business.

After all, "security is a process, not a product." The security manager must constantly reevaluate the risk environment, gain agreement from the business side on risk prioritization, and adjust the focus of his or her program as needed to address new threats and requirements as they arise. But the end objective should not simply be to reduce information risk in the organization - this is the objective of a merely good security program. Rather, it should go beyond that, enabling the business to take on new ventures to increase revenue and shareholder value that would be too risky without an effective security program in place.

For the security manager new to an organization, or an existing one working to achieve maximum leverage with his or her limited budget, focusing on the right issues is critical to success. For example, in a less mature program it may be folly to spend time and money on advanced projects like identity management when much more fundamental things are broken. Some activities, however, are *de rigueur* for the security professional entering an organization at any maturity level: understand the business, understand the culture, understand the IT infrastructure, and win allies in key areas of the organization.

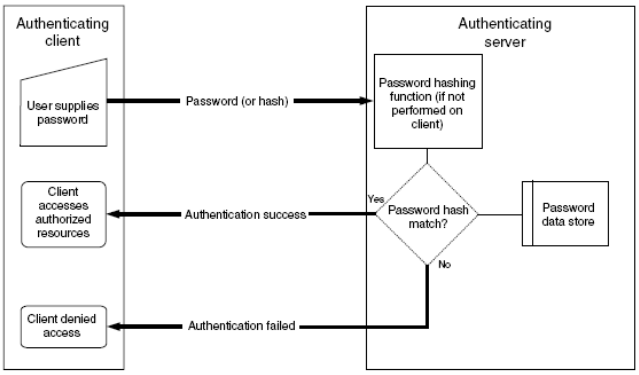

Figure 1. Client–server password authentication

In the mid-1990s, it became apparent that manual analysis of logs belonging to critical systems (UNIX in particular) was not practical. Systems administrators began to write “scripts” that would search through megabytes of data for certain events. For example, if the number of unsuccessful log - in attempts exceeded a certain threshold, the script would make a note. Other searches looked for direct “root” access and guest accounts. The practice became standard mainly in the UNIX community. The problems with this method were multifold:

1. The Windows operating system did not have the fl exibility of UNIX; scripts could not be easily written and did not extend to many events.
2. The strength of this method was only as good as the script including many of the common events (and even then, there were always some that were missed or overlooked).
3. The results would be dumped into a fi le, which would then be reviewed by an administrator or security personnel. In almost all cases, the results were not available until the next day or days later.

All of the above issues would then render the script method ineffective. It was not until a few years later that vendors used this methodology and designed software to address some of its shortcomings. However, it took a few more years before these products matured.

In a typical network, there are routers, switches, firewalls, Web servers, Web applications, etc. Each component generates messages either because of its own internal design or as it processes data. The components communicate with one another and in doing so generate more messages. There are interactions between E-Commerce systems, Web application servers, databases (more likely placed inside the network segmented by firewalls), and other pieces of the infrastructure spread out through the entire enterprise. It would be nearly impossible for typical human resources to sift through and decipher all these messages and even more challenging to make sense of events that happen separately but almost simultaneously in different areas of the network. This is certainly a daunting task. Event correlation provides the following:

1. It reduces the amount of traffic by setting thresholds for certain alerts - for example, instead of generating thousands of alerts “root log in” the threshold is set to three messages per minute.
2. It makes sense of seemingly unrelated anomalies and tries to establish a relationship among them - for example, a Domain Name System (DNS) poisoning attack launched simultaneously in different parts of the network. The event correlator determines that the attacks have the same source IP and orders boundary routers and firewalls to modify their ACL and rule sets to block the address.
3. It translates complex data to detect whether traffic is safe.

If SIM stands for security information management, then what is SEM (security event management)? Are the technologies the same?

If Linux, Solaris, Windows, Cisco IOS, mainframes, firewalls, intrusion detection and prevention systems with proprietary operating systems (IDS/IPS), and other platforms make it impossible to feed events directly to a correlation engine (CE; explained later). If all these platforms employed the UNIX “syslog” format, it would make it much easier for the SIM’s CE to understand and decipher the messages; but, clearly, that is not the case. Checkpoint uses its own proprietary format, and then there are SNMP traps. In this case, “normalization” of logs is an absolute requirement. Normalization is the process of reducing the complex structure of data into a simple form without losing all its attributes and characteristics. Once the data is normalized it is then fed into the correlation engine (SIM vendors employ many different architectures; however, the underlying premise remains constant).

With today's complex networks, multiple data centers, global hubs, disaster recovery sites, and many flavors of platforms, the information security well-being of organizations depends on how well the millions of events generated by these systems are collected and analyzed. Centralization of data allows the otherwise disparate and seemingly unrelated information to be gathered, analyzed, and presented as a single source. This is crucial in building a successful SOC. An organization with a well-designed and deployed SIM funnels events from everywhere in the network into a central console that is being monitored by level I or level II support personnel. The advantage is that information sharing becomes much more robust and the speed by which incidents are responded to is improved. Add this to the capability of many SIMs with built-in IPSs and one can have instantaneous shunning of attacks. Of course, a great deal more thought should be given to activating the IPS capabilities of SIMs as they can block legitimate production traffic as well.

The term real-time forensics is new; the concept, however, is not. The technology has been on the wish list of many security personnel. In the traditional forensics world, after an incident has occurred, one would gather logs and events, collect hard drives, bring production systems to a halt, freeze applications, interview employees, call in the experts to tear apart TCP/UDP packets, and perform a slew of other dizzying tasks that could take up tremendous human and financial resources.

This linear approach to forensics analysis could take days or even weeks to complete the analysis; by then, the organization may have lost valuable proprietary data and the perpetrator would have been able to clean up their footprints. The new "parallel forensics processing" is a combination of intelligence, correlation, and real-time processing of security events that do not take place sequentially. It is important to note that, even with the sophistication of SIMs today, a comprehensive and robust incident response policy is absolutely critical to the overall effectiveness of incident handling.

Correlation is an integral part of modern SIM systems. As a matter of fact, one of the most important criteria that I recommend for the evaluation of an effective SIM is how well the CE responds to disparate attacks, which can be simulated using common tools (such as Nmap).

To maximize the effectiveness of SIMs one must make sure that all platforms are covered. For proprietary platforms and applications, one must consider SIM vendors who are willing to work with their clients to develop the right agents. Make sure that your contract includes service level agreements with regard to this issue.

Many SIMs employ a combination of behavior-based modeling and rules to catch anomalies. The systems are generally shipped with a set of canned rules, signatures designed to catch many of the common forms of attacks. Some SIMs, such as netForensics, offer a set of rich graphical tools that allow the user to devise new rules without the use of complicated script languages. As SOC personnel and security engineers become familiar with the system and the environment that it monitors, they can build custom rules targeting a set of specific events. However, even with the existence of these tools, writing effective correlation rules is very challenging. I would recommend attending the SIM's technical training (almost all SIM vendors off er extensive off -site training that includes a day or two on the subject of rules).

Perhaps the most complex and challenging of all implementation tasks; as I have mentioned several times, network components generate gigabytes of data that funnel into the SIM's databases. The correlation and rules engines pour through this data attempting to make sense of them. In the process, thousands of alarms are generated that include "false positives" and "false negatives." False positives are alerts that indicate a potential issue when in fact there is none. A false negative (which happens to be an even bigger concern) is when an anomaly is missed by the SIM. Initially, after deployment, it

would be safe to assume that at least 50% of the generated alerts are false positives. These could be normal chatter among various network components such as the Virtual Router Redundancy Protocol between firewalls for failover. It takes weeks, if not months, for dedicated and knowledgeable security staff to pore over these messages, identify their sources and destination, perform research, contact the SIM vendor, and work with system administrators to eliminate them.

Below are some guidelines for message filtering:

1. Stop message flow from the source - a responsible system administrator will turn off messaging for a specific event at the source.

2. Stop message flow at SIM - rules can be written to ignore the message. Action can be "drop," which eliminates the message altogether from the database, or "store," which means ignore the message but keep it in the database for future use. Future use could include forensics and compliance.

3. Examine the "canned" rules and write rules customized for your environment.

Conclusion

It took nearly one year and the efforts of two people dedicated to the evaluation and testing of SIMs before we were ready to announce the product that best fit our environment. Choosing a SIM is not easy; but it is not magic either. There are many considerations and issues that must be well studied. I found that developing a "matrix" with our requirements seemed to work best.

For example, we wanted a system that supported all of our platforms. In the end, although such a product did not exist, we found a vendor who was willing to develop an agent needed to support the platform.

Bibliography:

[1] Hulme G., "Under Attack", Information Week, July 5, 2004

[2] Munteanu A., "E-Marketplaces Business-to-Business E-Commerce", Analele Universitatii din Oradea-Stiinte Economice, tom XVI, vol.2, 2007, pag. 859-862

[3] Smith, M. K. (2001) "Theories of action, double-loop learning and organizational learning", www.infed.org/argyris.htm

[4] The SANS School Store, "The SANS Security Policy Project", February 6, 2006, http://www.sans.org/resources/policies/

[5] Terena's Guide to Network Resource Tools, "Smart Card Types", February 6, 2006, http://gnrt.terena.nl/content.php?section_id=131

[6] Bezakova, I.; Pashko, O.; Surendran, D., "Smart Card Technology and Security", February 6, 2006, http://people.cs. uchicago.edu/~dinoj/smartcard/security.html