

# Top 10 Hot Topics in Security

By Jonathan Gossels

[jon.gossels@systemexperts.com](mailto:jon.gossels@systemexperts.com)

**T**alk to anyone wrestling with securing an enterprise and before you know it, you'll hear about dozens of projects, initiatives, tools, policies, and challenges covering networks, hosts, applications, personnel, and wireless devices. Security requirements have grown exponentially over the past few years. In this article, I present my top ten list of hot security topics.

## #1 Transition to Defense-in-Depth

Over the past ten years, technological change and evolving business models have made the very idea of an enterprise perimeter obsolete. VPN technology, the use of protocols (like http) that are allowed to pass through firewalls, and the extension of networks to encompass outside service providers and business partners illustrate this point. Rather than thinking about "the perimeter," most organizations are better served by thinking in terms of *zones of risk or zones of trust*.

In a trust zone model, organizations design zones where the boundaries are defined by network mechanisms such as firewall or router controls and policies that define who is allowed physical, network and interactive access to the systems in the zone. The combination of policies and mechanisms provide the basis upon which the organization can assess how well the resources inside the zone are protected from various threats. This assessment can then be used to determine what other mechanisms, like authentication, encryption and authorization, are required to allow various entities within the zone to interact with one another securely. For example, many organizations conclude that internal environments located in isolated network segments allow entities within that network to authenticate each other by IP address. This choice may be acceptable in an isolated and well-controlled internal zone but would be a mistake in an environment where an organization is concerned with attacks originating from the "protected" network or where the network is connected to untrusted networks.

The concept of zones of trust can be useful in implementing a defense-in-depth strategy. Defense-in-depth suggests that instead of depending on a single mechanism to protect an environment (e.g., perimeter firewalls), defenses are layered. These layers, made up of network segregation, authentication, intrusion detection, and authorization mechanisms, serve to prevent or detect intrusions, even when a particular layer is breached. By creating zones close to the perimeter that either minimize trust altogether or establish trust only via strong authentication, it may be possible to establish other zones that are isolated from the perimeter that require less stringent controls but still provide adequate protection.

While most organizations recognize the inevitability of implementing defense-in-depth, many find themselves in the early stages of transition. A small number of people within these enterprises are beginning to think

about security architecture in terms of zones of risk and zones of trust, and they are beginning to put plans in place to instrument what had previously been considered *the inside* to detect security problems. The vast majority, however, still perform their day-to-day roles as if the outside is hostile and the inside is safe.

## #2 Managing Complexity

As security becomes integrated into the fabric of an enterprise, keeping track of all of the security-related activities and aligning project priorities across multiple departments becomes a major challenge. After organizations have figured out how secure they need to be, where they currently stand on that dimension, and what improvements are required to reach the desired security level, they need a way to visualize and manage that security state over time. Many companies have had success in using a color-coded dashboard approach.

The security dashboard enables senior management to understand, at a glance, which programs are green, yellow or red, prioritize spending to mitigate problems, and align security projects with corporate initiatives.

The secret to success of this method is not to allow the organization to get caught up in addressing individual items at the expense of the big picture. Too many organizations respond to red items with projects that don't address the real threat. Another mistake organizations make is to expect the progress of a project to be measured in a smooth transition from red to yellow to green. Often projects need to be complete before any real improvement in risk is realized. For example, if an organization is replacing vulnerable systems with hardened ones, the risk may not change until all have been replaced. Intermediate points may not change the risk at all.

Finally, organizations should keep in mind that the purpose of the dashboard is to help them to look at the big picture. It is not a mathematical formula that determines risk. Organizations need to reason about the state of various systems and processes and determine risk holistically. Further, it is critical that evaluations of risk and state be augmented with what led to the state assessment. Ask why the state is red and what is necessary to make it green.

## #3 Acceleration of Time Frames

The Internet has had a number of profound impacts on the world of IT. One of the most notable is the acceleration of time frames. Web applications are usually conceived, developed, and deployed quickly. In many cases, organizations do not apply their time-tested application development process to these applications (design review, code review, unit and integration testing).

Administrative time frames are compressed as well. While formerly it was acceptable to deploy software patches and updates over a period of weeks and months, that time frame has now shrunk to days and hours. The same holds true for virus protection.

While the old time frames will not come back, many organizations are beginning to formally address the obvious deficiencies. For example, leading financial institutions are once again requiring security design reviews early in the application development process. They are also requiring security code reviews for critical applications.

The best organizations use these reviews to improve their development processes. The biggest enemy to secure code is lack of discipline. Organizations need to reduce the amount of code that controls security, implement common utilities to verify input, and implement strict quality controls on code modifications. Similar activities should take place for administration. Tight configuration control, strong authentication and access control on production devices, and informative logging of administrative activity can have a substantial impact on making systems more secure. It is important to remember that disciplined processes may seem like they add to the time to market, but they actually help to ensure that good, secure products are delivered more quickly.

#### #4 Regulatory Compliance

The past several years has seen the emergence of broadly applicable regulations. Whether talking about Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill No. 1386 (sections 1798.29 and 1798.82 of California Civil Code) or the EU's Privacy and Electronic Communications (Directive 2002/58) and the Data Protection Directive (Directive 95/46/EC), these laws have certain key concepts in common:

- ▲ Accountability
- ▲ Protection of personal private information
- ▲ Disclosure of disclosure policies
- ▲ Integrity of reported information

Many organizations find the need for compliance to be a catalyst to resolve long-overlooked security problems.

#### #5 Changing Threat Environment

Leading organizations have begun to realize that their security programs were never designed to provide protection from the threats they are facing today. Historically, most organizations, when they thought about security at all, thought about protecting themselves from a technically skillful young hacker (we actually prefer the term *determined intruder*). While simplistic, that characterization was largely correct; most hacks were intended to show off for the hacker's community and did not do serious damage.

The threat environment has changed. Today, organizations are finding that the determined intruders are sponsored by organized crime, terrorists and hostile governments. The attributes that they share are deep pockets and a willingness to spend an *unreasonable* amount of time accomplishing their objectives.

The most forward-thinking companies recognize that these well-funded attacks are likely to come from "the inside" or from trusted partners. Further, hostile nations and terrorists are not looking for the quick score. More likely, they are working to undermine the integrity of the

business, sabotage operations over the long term, or change market direction to their advantage.

The key to combating these types of attacks is for organizations to know their employees and partners and eliminate unnecessary trust. The environment of the future will need to be structured in small trust domains that are particular to an application or a business area.

#### #6 Changing Threats

It is not only the threat environment that is changing but the nature of the threats as well. A clear example of a pervasive new threat is phishing, tricking users into disclosing private information like a bank account number and PIN and then emptying the account. Other examples of new threats include the myriad varieties of adware and spyware. The cost of removing this malware has become a major headache to businesses around the world.

While we hope that future versions of software will be less susceptible to such attacks, education and vigilance seem to be the watchwords for defending the business against these new threats. Users and employees need to understand the risks of using untrusted sites, responding to unauthenticated request, and installing software to ensure that correct protections are in place.

#### #7 Outsourcing Application Development

Outsourcing of software development is not new. What is new is the extent of the practice and the post 9/11 political climate. The reason we note this as a hot topic is that many organizations that had jumped on the outsourcing bandwagon expecting to achieve substantial cost savings are now realizing that by the time they implement suitable security controls (e.g., programmatic and manual code reviews, extensive testing) to ensure that the received code does only what it was intended, the cost savings is far less. Other organizations, while still outsourcing application development, have become much more selective in the countries they consider for the work.

#### #8 Securing Wireless Devices

Most organizations recognize that laptops are every bit as capable and vulnerable as desktop computers. However, they consider hand-held computers, like Palm Pilots and Pocket PCs, in a different light, as if the historical limitations of those devices somehow eliminate the risks associated with their larger, laptop counterparts. Over the past few years, the processing power, system software and connectivity of these small computers have increased to the point where such a distinction no longer applies.

As organizations increasingly rely on hand-held devices to store and manipulate sensitive information, it is imperative that they develop a security program that includes three components:

- ▲ a security policy that deals specifically with hand-held devices
- ▲ a set of centralized corporate processes to establish and maintain the security of these devices in a consistent way
- ▲ a set of security products to protect the integrity of the device (including virus protection), the confidentiality of data stored there, and the authenticity, integrity and confidentiality of hand-held network communications.

#### #9 Developing Secure Web Applications


The vast majority of Web applications would fail a simple security review. Typical problems include allowing users to escalate their capabilities to perform inappropriate actions on their own account, obtaining information about the accounts of other users, performing any actions on the accounts of other users, reaching back-end systems, and impacting the functionality of the server as a whole.

The Open Web Application Security Project (OWASP) ([www.owasp.org](http://www.owasp.org)) is a reaction to the enormous problem of inconsistent and exploitable Web applications. Its software results include WebScarab, a Java program to spider a Web site for vulnerabilities (like Nikto or whisker) and Filters, an IO sanitizer (parameter checker). Its documentation results include a list of top 10 Web application vulnerabilities, a guide to building secure Web applications and Web services, and a guide to testing the security of these applications and services.

## #10 Securely Connecting to Business Partners

Organizations are increasingly relying on Application Service Providers (ASPs) to perform critical functions in their environments. It is not uncommon for large organizations to have relationships with dozens of ASPs—we've worked with some clients who have hundreds. The services these entities provide range from internally consumed services like payroll and benefits management to externally consumed capabilities, like credit verification and payment processing on Web sites.

While the use of ASPs is proving beneficial at a business level, enabling innovative functionality and reducing time to market, integrating these ASPs into the network and processing environment raises obvious security concerns for organizations and their clients. Does the ASP safeguard your confidential data to the same degree that you do? How would you know? Does the connection to the ASP represent an open back door into your network? Can another customer of that same ASP get at your confidential data? These are obvious questions, yet most organizations can't answer them. If you can't, you don't have an effective ASP security program in place.

The single biggest problem with ASP security is that it has been neglected. The answer lies in applying the same type of risk assessment and security review process to ASPs as is typical in most companies for internal applications. Further, reducing complexity is crucial. Developing a small number of secure ASP connection models and using them consistently will provide the foundation for a stable, secure and monitorable IT environment with ASPs integrated throughout. 

---

*Jonathan Gossels is president of SystemExperts Corporation ([www.systemexperts.com](http://www.systemexperts.com)), the leader in computer and network security.*