

## A Perspective on Practical Security

a report by

**Jonathan G Gossels**

### Transition to Defence-in-Depth

Over the past 10 years, technological change and evolving business models have made the very idea of an enterprise perimeter obsolete. Virtual private network (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 organisations are better served by thinking in terms of zones of risk or zones of trust.

In a trust zone model, organisations 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 on which the organisation 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, such as authentication, encryption and authorisation, are required to allow various entities within the zone to interact with one another securely. For example, many organisations 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 organisation is concerned with attacks originating from the 'protected' network or the network is connected to untrusted networks.

The concept of zones of trust can be useful in implementing a defence-in-depth strategy. Defence-in-depth suggests that instead of depending on a single mechanism to protect an environment (e.g. perimeter firewalls), defences are layered. These layers, made up of network segregation, authentication, intrusion detection and authorisation mechanisms, serve to prevent or detect intrusions even when a particular layer is breached. By creating zones close to the perimeter that either minimise trust altogether or establish trust only via strong authentication, it may be

possible to establish other zones that are isolated from the perimeter, which require less stringent controls but still provide adequate protection.

While most organisations recognise the inevitability of implementing defence-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 though the outside is hostile and the inside is safe.

### 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 organisations 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 visualise and manage that security state over time. Many companies have had success in using a colour-coded dashboard approach.

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

The secret to success of this method is to not allow the organisation to get caught up in addressing individual items at the expense of the big picture. Too many organisations respond to red items with projects that do not address the real threat. Another mistake organisations 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 realised. For example, if an organisation 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, organisations 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. Organisations 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. They should ask why the state is red and what it necessary to make it green.

### Acceleration of Time-frames

The Internet has had a number of profound impacts on the world of information technology (IT). One of the most notable is the acceleration of time-frames. Web applications are usually conceived, developed and deployed quickly. In many cases, organisations 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 it was formerly 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 organisations 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 organisations use these reviews to improve their development processes. The biggest enemy to secure code is lack of discipline. Organisations 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.

### Regulatory Compliance

The past several years have 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 (Directive 2002/58) and 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; and
- integrity of reported information.

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

### Changing Threat Environment

Leading organisations have begun to realise that their security programs were never designed to provide protection from the threats they are facing today. Historically, most organisations, when they thought about security at all, thought about protecting themselves from a technically skillful young 'hacker' (the authors actually prefer the term 'determined intruder'). While simplistic, that characterisation 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, organisations are finding that the determined intruders are sponsored by organised 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 recognise 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 organisations 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.

### 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 personal identification number (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 it is hoped that future versions of software will be less susceptible to such attacks, education and vigilance seem to be the watch-words for defending the business against these new threats. Users and employees need to understand the risks of using untrusted sites, responding to unauthenticated requests and installing software to ensure that correct protections are in place.

### 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 this is noted is that many organisations who had jumped on the outsourcing bandwagon expecting to achieve substantial cost savings are now realising 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 to do, the cost saving is far less. Other organisations, while still outsourcing application development, have become much more selective in the countries they consider for the work.

### Securing Wireless Devices

Most organisations recognise 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 organisations 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 centralised corporate processes to establish and maintain the security of these devices in a consistent way; and
- 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.

### 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 Website for vulnerabilities (like Nikto or whisker) and Filters, an IO sanitiser (parameter checker). Its documentation results include a list of the 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.

### Securely Connecting to Business Partners

Organisations are increasingly relying on application service providers (ASPs) to perform critical functions in their environments. It is not uncommon for large organisations to have relationships with dozens of ASPs – the authors have worked with some clients that have hundreds. The services these entities provide range from internally consumed services, such as payroll and benefits management, to externally consumed capabilities such as credit verification and payment processing on Websites.

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 organisations and their clients. Does the ASP safeguard a company's confidential data to the same degree that the company does? How would they know? Does the connection to the ASP represent an open back-door into the company network? Can another customer of that same ASP get at any confidential data? These are obvious questions, but most organisations cannot answer them. This means that they do not 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 easy-to-monitor IT environment with ASPs integrated throughout. ■