Security Frameworks

Robert "Belka" Frazier
belka@att.net

Security in a Pervasive Computing Environment

There once was a time when it was difficult to convince business leaders that they needed security. That is no longer the case because companies now rely on their information systems more than ever. Business processes have been defined in the hardware and software of systems that support those processes. These systems have become essential to companies. As a result, security is no longer a "nice to have" feature of business information systems. It is essential. Now the question is not whether to have security implemented, but rather how to achieve security that the company needs at a price it can afford.

What do we mean by security? In the past it meant firewalls and routers at the perimeters of our networks, or security devices deployed in layers as "security in depth." But in today's networked and interactive environment, this is no long adequate or even truly secure. Customers, business partners, and remote employees use all of our networks, whether to conduct e-business transactions, do collaborative work, retrieve e-mail, and access critical files. These types of transactions use the entire network, from the DMZ to the database to the desktop.

In today's pervasive computing environment, ALL of the network must be secured. All the hardware, software, applications, and data – all of the network is exposed to processing and is potentially at risk. To achieve security in this environment, you must have hardware such as routers and firewalls, but also reactive elements such as intrusion detection, as well as proactive elements such as security scanning, and pen-testing. These measures must be founded on a sound security regimen of policies and procedures. Perhaps most important of all, security operations need to be monitored 24 hours a day. And last of all, security must match the goals of the organization and the information systems that support those goals.

What is Effective Security?

Effective security is NOT security hardware and software operating in a disjointed vacuum. Security, like e-business, has to adhere to a coordinated architecture. In an e-business architecture, webs servers accept transactions that are forwarded to back-end systems that turn those transactions into fulfillment, invoices, money transfers, inventory changes and product shipments.

In security architecture, firewalls, routers, intrusion systems, vulnerability scans, pen-tests, policies and procedures work together like the e-business systems, to deliver information processing securely. Just as enterprise systems have to be monitored to ensure efficient operation, security systems must be monitored to detect and react to

security problems. The information systems enterprise architecture is designed to help a company achieve its business goals; the security architecture has to match the company's security goals.

To meet these challenges, a security framework extends end to end, from the DMZ to the database, protecting information systems, infrastructure, and networks along the way. The security framework maps to the enterprise architecture to achieve an overall security solution.

The end-to-end security solution is designed to protect information systems, but more importantly, it protects the most valuable and irreplaceable asset – reputation, privacy and brand. The security architecture uses a combination of commercial and open source tools. By leveraging existing security architectures, security managers achieve a higher level of security in a short time for less money than they could by deploying point security solutions.

Goals of a Security Framework

In an enterprise environment, security is critical to success because of all the variety of environments, types of equipment, and applications that have to operate together to successfully support organizational processes. To accomplish this goal effectively, security has to be evaluated and executed consistently. Security controls have to be constantly run and monitored, and cover everything in the enterprise.

A security framework, to be effective has to be reliable and able to protect the systems in the enterprise. Security controls must be robust and capable of coping with dynamic networks, architecture – and attackers. The controls must be repeatable, able to be applied to new applications, business processes and emerging technologies.

Ultimately, for a security framework to be truly effective, its controls and mechanisms have to be monitored. The security systems and controls have to be effectively managed and maintained to keep the framework up-to-date and current with emerging threats,

Mapping the Security Framework to the OSI Model

How does the security framework work? The security architecture is mapped to the customer's enterprise architecture using the Open Systems Interconnect (OSI) networking model. The security framework has security solutions for all the pieces of the enterprise infrastructure that supports the goals of the organization. The Security Framework operates and protects that infrastructure at each of the operational levels of the OSI model.

As transactions take place from end-to-end of the enterprise architecture, these transactions utilize technologies that operates at all the levels of the OSI model as well. Since security extends into policies and procedures, and supports business driven goals, the Security Framework has added two additional layers to the model, the financial and

Political layers. These layers began as a tongue-in-cheek joke at the National Security Agency in the mid-nineties. However, security of information systems really does have to match the budget and the business objectives of an organization and these layers have achieved legitimacy in their own right.

Layer One – Physical Layer

Layer one of the OSI model is the physical layer – the wire over which electronic impulses run to create the magic we know as computing. At this layer, the security framework protects the cable plant, the wiring, and telecommunications infrastructure. The physical layer is protected by redundant power and WAN connection. It also means protecting the physical hardware in network closets, server farms, and systems in raised floor spaces. Protecting the physical layer entails locks, alarms on entrances, climate controls, and access to data centers.

Layers Two and Three – Data Link and Network Layers

At the Data Link and Network layers, the security framework protects systems with a number of technologies. VPNs protect information by encrypting it and sending it through encrypted tunnels through networks or the internet. Network intrusion detection systems or NIDS watch traffic flowing over the wires looking for bit-stream patterns that could indicate attacks or malicious intent. Host Intrusion detection systems monitor bit streams entering the host machines at the Network Interface Card (NIC) level, also looking for suspicious patterns. Virus scanning at this level looks for patterns that indicate malicious code that fits signatures for know viruses.

Layers Three and Four – Network and Transport Layers

At the Network and Transport layer, the security framework uses firewalls to do stateful inspection of packets entering and leaving the network. Routers, using Access Control Lists or ACLs filter IP packets, preventing traffic from going to systems that have no need for it. Utilizing IP address schemes, network engineers can plan and implement routing tables that protect networks with router ACLs, making firewall rules easier to write and deploy, and thwarting attacks such as address spoofing. At the network and transport layers, virus scanning software opens attachments in messaging packets such as e-mail, looking for embedded viruses or malicious code.

Layers Five Six and Seven – Session, Presentation, and Application Layers

At the Session, Presentation, and Application layers, the security framework uses a number of techniques and tools to secure systems. Some of these techniques are policies for system management such as hardening the operating systems, keeping patch levels and OS revisions up to date, running with only the services needed to support the business processes and turning off all other process, running processes with limited system privileges, etc. All of these management techniques contribute to security at the

session, presentation and application layer and are the kind of system controls that automatically enforce security policies.

Utilizing Security Health Checking software is part of the Security Framework at layers five, six, and seven. Security health checking is a software client that resides on systems that checks whether security policies are being followed and adhered to on the system. The health checking client will look at things such as passwords length and composition, processes running to ensure only allowed processes are running, open ports to detect if disallowed ports are open, etc. The results of the health checking are reported to a central server and a report is sent to the system administrators for action.

Vulnerability scanning subjects target machines to automated attacks to test if the systems are misconfigured and vulnerable to attacks, or are missing bug patches or have software susceptible to known exploits, etc. The data for the attacks comes from various vulnerability lists, CERT, Mitre CVE list, etc. and from other security research. Vulnerability scanning is an automated way to check on new and known security holes in systems, OS, and applications.

Penetration testing is a simulated attack by a team of trained security experts, also known as "white hat" or ethical hackers. The team tests the configuration and management of the security architecture by attacking it as a real hacker would, looking for lapses in security or exploitable vulnerabilities to take over a target system. Vulnerability testing is analogous to security architecture as performance and stress testing is to networks and applications. Performance and stress testing check to see if the infrastructure and applications can meet the processing demands of the network in times of high volume. Vulnerability testing test the security of the security architecture to determine if it can meet the security demands of an active and determined attack.

Layers Six and Seven – presentation and Application Layers

At the Presentation and Application Layers, the security framework utilizes user account management to control access to the network, systems and applications. The security framework relies on system managers to control access to their machines, network administrators to manage user access to their networks, and application managers such as Data Base Administrators (DBA) to control access to applications and data. At this level, the security framework includes virus scanning applications to scan hard drives and system memory for malicious code, updating scan engines and virus signatures. Host Intrusion Detection Systems (HIDS), active in the lower levels of the model, work at the presentation and application layer to watch for changes to critical system files and other system behavior that might indicate an attacker trying to gain control of the system.

The security framework can also control user access centrally using a role/rule-based access control (RBAC) engine, that uses a directory such as LDAP or Active Directory that contains information about users and the systems and resources to which the users are authorized access. PKI and digital certificates can be used at this level to provide digital signatures, encryption, and non-repudiation at the application level.

Layer 8 – Financial Layer

At the financial layer, the Security Frame work uses existing infrastructure to reduce cost and provide services at a lower total cost than providing all the services as individual devices. By capturing the costs of the Security Framework and its components, it is easier to estimate the cost of providing security to an organization.

Layer 9 – Political Layer

At each level of the network, and at each zone of the business logic of the e-business architecture, the security framework can extend it self to meet the security needs of the enterprise. Business processes are analyzed and compared to the IT services that carry out those processes. The processes are then analyzed to determine how the processes and transactions are carried out across the OSI model. From the results of that analysis, the appropriate components of the security framework can be employed to secure that process.

From securing legacy systems and NT domains, to hardening operating systems of UNIX and Windows systems, to proactive managed services such as security scanning and pen-testing, the security framework extends to cover all of the enterprise at every level and every instance.

Combining all the security pieces of the enterprise, the security framework can meet any an organization's particular environment, matching the components of the enterprise to the security framework.

The flexibility of the security framework allows for new security technologies to be integrated into the security framework. Role/Rule Based Access Control (RBAC), PKI, and other technologies can be added based on customer needs. This is facilitated because within a framework model, new technologies are added in the context of the framework, which helps define interaction and relationships with other security technologies. Security does not happen in a vacuum – every element has a reason to be in the infrastructure, has a role, and complements and extends the other security components.

Summary

Security is more than technology. It is people, policies, and procedures as much as it is technologies. The Security Framework takes this into account by leveraging existing security infrastructure, and providing a platform to manage security services. The security manager uses the security policies and procedures, and security framework to match security needs of the objectives of the company. The policies and procedures, the security services and frame work act together to securely support the goals of the organization.