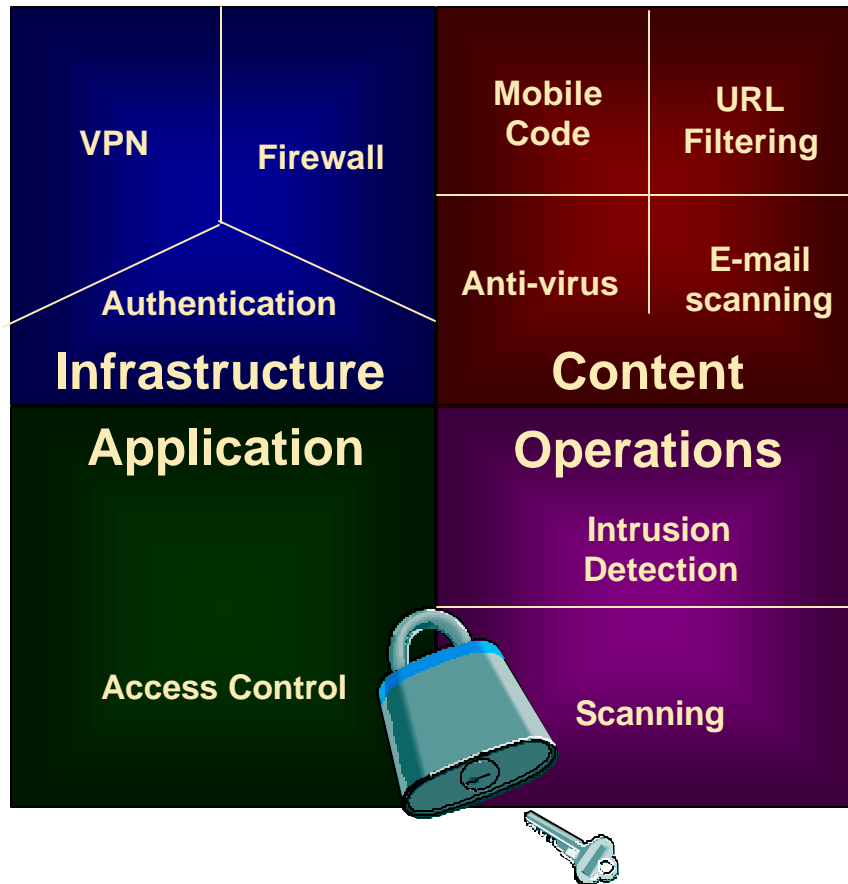


Security systems have always been a key element of information technology. Security systems comprise a host of functions, some of which are shown in Figure 1. With the advent of the Internet and electronic commerce over open channels, security systems are having to adapt to deal with the new requirements being place on networks. This months view provides an overview of how all the pieces of security fit together. The next few articles will analyze the security areas shown in Figure 1 in detail and describe how the Internet is changing the thinking of security architects and creating new approaches for enabling secure environments.

Figure 1
Elements of a Network Security Architecture



The Problem: Old Security Models are Outmoded.

Before the Internet, security was provided by having closed networks running on private lines. Security therefore was limited to worrying about providing differential access to a known base of “trusted” users, and preventing unauthorised access by a few, technically proficient outsiders who might attempt to

break into the system. In those few cases where access to data on typical local area networks were extended into either supplier or customer sites, it was done in a very controlled way, with the assumption that access was limited to all but a few approved users.

The key rules of this traditional environment were:

Restrict Access. The “default” state of any application or data store was to assume no access was allowed. Then via specific permissions contain in an access control list, provide only the minimum level of access to a specific user or user group.

Control is Paramount. Security architecture, policies, and maintenance should be centralised in the hands of a trusted and small security staff. This is true today even in many companies that have a decentralised IT infrastructure, where systems selection and maintenance are delegated to groups of divisions.

Emphasize Prevention. Leave no security hold unplugged. Prevent incidents before they happen, even if the event represents only a minor threat to the network.

Limited Variation in Security Services. Security services in this environment were coarse. In a sense security in these environments was like using an ax to slice a turkey. Security in many cases was perceived as a binary decision: either you had complete, stringent security at all levels or your security was worthless.

Changes in Computing Make Traditional Security Outmoded

The rise of the Internet and Internet-based commerce has now made the old model of security outmoded. In fact, attempting to build an Internet-based solution on the old security model yields a bad architecture that, if left in place, will ultimately limit the growth of an organization’s on-line business. This is because the old security model first and foremost has an unattainable goal. It is impossible (both technically and economically) to plug every hole in an open network environment. The number of likely attacks is much more extensive and varied than in a closed network environment, and the types of attacks will constantly change as security breaches are identified and corrected. Flexibility, adaptability, and an ability to quantify the various exposures, rank the risks they pose, and establish appropriate *risk mitigation procedures* is more critical than completeness. As my security people constantly tell me, it doesn’t pay to

build an iron wall when the doors are always made of straw. The goal is to build iron walls where economically and technically feasible, determine which weak links (doors) provide the most exposure, try to minimize their size and visibility, and move them around as much as possible so they can't be found.

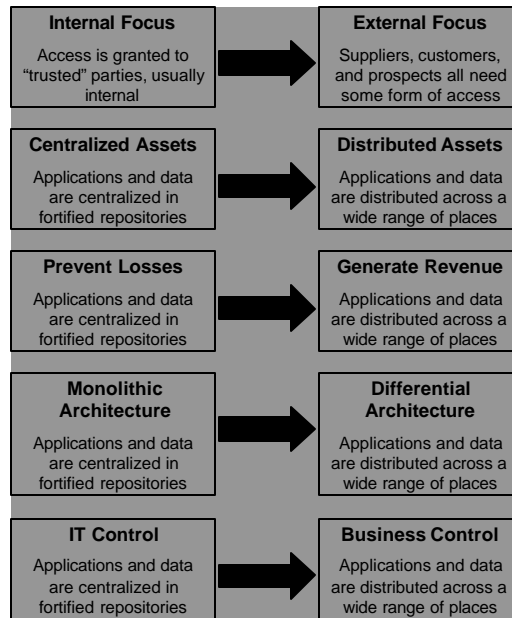
Second, the old model is too inflexible, too expensive, and too manpower intensive to deal with a network environment where

- the boundaries of the corporate “perimeter” may need to change in real-time
- large numbers of unknown and untrusted users will sign up for the network on a regular, but unpredictable basis
- the levels of trust and access provided to a group of users today may change radically tomorrow as the business model evolves
- large groups of individuals (e.g. members of a supplier organization that is part of a supply chain) may need to be join the network in real-time with a variety of privileges and access rights.

Moreover, given that transmissions are now occurring on an “open channel”, eavesdropping, spoofing, and content authentication issues have taken on a higher precedence in security requirements. This is in comparison with closed environments, where users were generally assumed to be “trusted” (meaning that they were not eavesdropping on their own organization), and maintaining appropriate access control to data and applications was an extremely high priority.

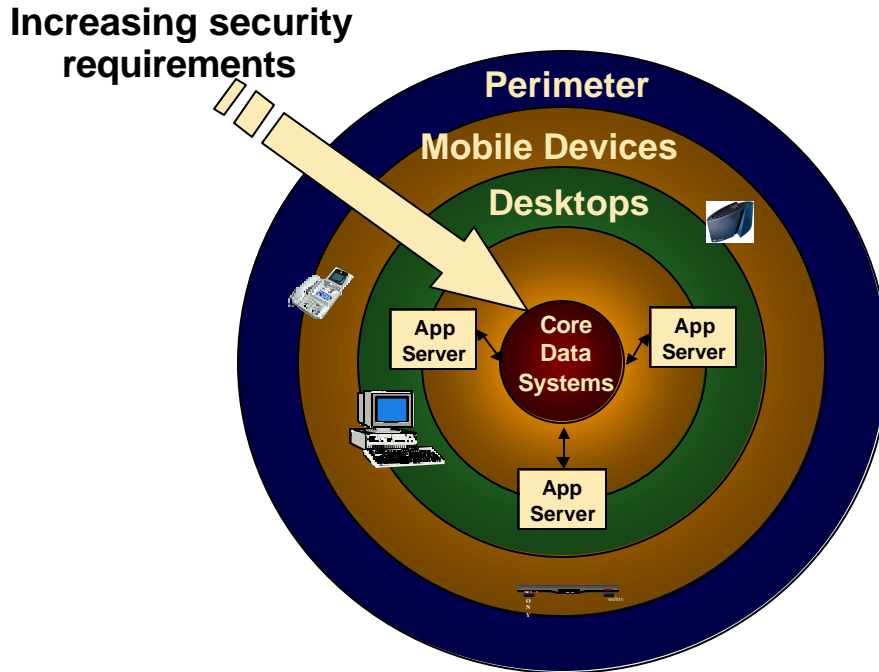
The New Paradigm: Inside-Out Security

Exhibit 2
Changing Security Demands are Changing the Architectural Approach



The new paradigm of security begins with five major changes in approach to security architecture (Figure 2). Instead of access restriction being the default, relatively open access to any third party is assumed to be the default. Second, data and applications are assumed to be distributed instead of centralized, meaning that a balance must be struck between data must be protected at a variety of locations and yet collected and collated to respond to user requests for information with reasonable performance. Third, the goal of security, in this situation, is not to prevent losses, but rather to create a secure platform that enables new services that create revenue. Fourth, the security architecture should not be monolithic. It should allow different assets in a distributed environment to be provided with the appropriate levels of security needed relative to the risk posed by an attack. Lastly, the business manager should be able as needed to control who will gain on-line access to his resources, rather than this being in the control of a centralized IT staff. The business manager should have available to him a structured security environment that ensures that his department follows appropriate security policies but that gives him the flexibility to easily extend his services outside the firewall to large numbers of customers.

Figure 3
The Security Target



In order to deliver this more risk-based security architecture, we have developed a differential risk model called the *security target* (Figure 3). Generically the target shows that different elements of a system have differential requirements for security. For example, a breach of the *perimeter* is the least costly form of breach. While it is important to know that someone has made an unauthorised entry into the network, such entry does not in itself create a loss. It is only when the unauthorised entry leads to some further act against applications or data that it becomes a true threat. Therefore, in a differential risk model, the goal is to put the appropriate security around those elements of the network that most need them.

Figure 4
Security Requirements by Layer of System

| Feature | Layer | | | | | | Product Type |
|--|----------------|--------------|----------------|------------------|-----------|-----------------------|-----------------|
| | I Perimeter | II Mobile | III Desktop | IV App Server | V Core | "Meta" System Mgmt | |
| Intruder Scanning and Detection | ● | ● | ● | ● | ● | ● | Firewalls |
| Attribution | ● | ● | ● | ● | ● | ● | Secure OS |
| Device-Chain Integrity | | ● | ● | ● | ● | | PKI |
| Single Sign On | ● | | | ● | | | PKI |
| Session Ticketing | ● | | | ● | | | PKI |
| Compartmentalization | | | | ● | ● | | Secure OS |
| Non-Repudiation | | | | ● | ● | ● | Middleware |
| Message/Data Stream Integrity | | | | | | ● | PKI |
| Application Access/Attribution | | | | ● | | | OS, PKI |
| Data Repository Security | | | | | ● | | Secure OS, Apps |
| Activity Log Security | | | | | ● | ● | Secure OS, Apps |
| Security Compliance Modeling/ Risk Analysis | | | | | | ● | Hole |

In the target shown in Figure 3, a breach of core data stores poses the largest real risk (e.g. a hacker steals a credit card database). Therefore security should be highest for the data stores. Everything else has relatively higher or lower requirements for security (as shown in Figure 4) in between the two extremes of data store and perimeter. This target has 5 security levels plus a meta level that applies to systems managers looking to the system as a whole; the target for your organization could have more or less depending on the needs of your business.

Conclusions

The Internet has put new demands on security architectures and technologies that cannot be solved in a cost-effective manner using traditional approaches to security systems. Previously these systems created monolithic “one size fits all” approach to securing network assets that assumed as its default that no access would be permitted. However, these assumptions fail to take into account the requirement for open access needed for on-line business, the need for differential protection of computing assets in an open, distributed network environment, and the need for flexibility to adapt security capabilities in near “real-time” as on-line businesses evolve. A new model – one that works “inside-out” - providing differential security to assets requiring quantifiably different risk mitigation from attacks in an economic and flexible

manner and becoming an enabler for revenue generation, represents the type of security system that will underly successful on-line businesses of the future.