SC MAGAZINE HOME
SC Online Magazine

June 2002

Perimeter Defense Model for Security

by Adam Lipson

There has to be a better way!

Is there a reasonable technology solution for enterprise security?

The overwhelming majority of corporate enterprises employ a perimeter security model: hard exterior, soft interior. Typical perimeter defenses include technologies like firewalls, intrusion detection systems (IDS), application proxies and virtual private network (VPN) servers.

When properly configured, the perimeter defenses only permit those activities that are required to conduct business. Using the perimeter defense security model, the perimeter technology prevents, absorbs or detects attacks, thus reducing the risk to critical back-end systems.

In theory, if a severe incident occurs:

- The firewall or application proxy absorbs the impact rather than the back-end systems.
- IDS detect attacks and alert security staff in sufficient time for them to analyze and respond to an attack before the back-end system is affected.
- VPN solutions can authenticate and provide a secure channel to legitimate users.

General acceptance of this perimeter defense model has occurred because it is far easier (and seemingly less costly) to secure one perimeter than it is to secure a large volume of applications or a large number of internal networks. Given today's state-of-the-art security technology, chief security officers (CSOs) confronted with the alternative of spending $200,000 per year on securing one perimeter or spending millions of dollars securing a battery of applications, choose the former without proper attention to the back-end infrastructure. Until the current state of end-to-end security technology improves, CSOs will continue to make the tactical cost decision.

This is an old problem, and this solution has proven to be an ill-advised long-term strategy. Today, there is no good technology solution. However, solving this problem requires a new approach to aspects of security that have often been ignored: people and processes.

Absolute Reliance on Perimeter Defenses is a Grave Weakness

Security can be no better than the weakest link!

Sound security posture requires confidence in many things: people being available, motivated, alert, aligned with the

mission, and technically current in the context of a constantly changing threatscape. Intrusion detection is complex and requires continual vigilance and up-to-date knowledge. Too many firewalls are not configured and maintained expertly. Proxy design is difficult and often relies on maintaining the security of the underlying (typically general purpose) operating system. Even with perfect IDS, firewalls and proxies, there is always some application data that cannot be interpreted except by the back-end systems that the perimeter is intended to protect.

If you believe that security is only as good as the weakest link, then an adequate security model must include elements that go beyond perimeter security. To create a reasonable level of assurance, any security model must consider not only the perimeter technology, but also the internal and external factors as well as people and processes (see Table 1 below - Nine Security Domains).

Table 1: Nine Security Domains (*3 x 3 Matrix*)

---	TECHNOLOGY	PROCESS	PEOPLE
INTERNAL			
PERIMETER	*Traditional perimeter defense model*	*Traditional perimeter defense model*	*Traditional perimeter defense model*
EXTERNAL			

Although sound architecture, good design and proper implementation may attempt to use perimeter defense in depth to bolster some potential weaknesses, this only buys time. If that time is not used for analysis and response, there is no real assurance: it is an illusion on which the service has relied.

CSOs need to ensure that critical business applications and data are available (at the quality of service that they expect), that the end-users trust using the service, that the service adequately maintains confidentiality (where required) and user authorization (which requires adequate authentication of identity).

The Role of Technology in the End-to-End Application Model

What will the future security technology model look like?

Regardless of technological improvement, security will always require people and process. However, what could future security technology do to increase security assurance, while decreasing the magnitude of reliance on people and process?

In a perfect world, future technological advances in security could make end-to-end application security affordable and practical. Such technology would provide local proofs within modular subsystems on purpose built operating systems and smart networks with layered security. Agents with the responsibility for lending credentials or signatures would not lend them to a compromised module/process. Communications between client and server would rely upon client and server credentials that would be strongly authenticated, communicated with integrity, and demonstrated to be impossible to forge and unrepeatable. The local proofs would not be communicated to the

other end systems. However, in some instances with mission critical or high-value system-to-system communications between two comparable organizations, there could well be value in presenting the locals proofs remotely.

The initial production environments for the future end-to-end security technology are likely to be high value (and therefore higher risk) applications. These may include financial services applications that perform electronic transactions by institutional investors, critical national infrastructure such as those managed by utility companies or even military groups that require extremely high levels of assurance. In this case, true end-to-end application security would start at the user's input console and end at the back-end system, with the responsibility for security never being passed to another modular component.

Then what would be the role for perimeter security?

If the blue-sky inter-subsystem proofs, operating systems with secure architecture and end-to-end applications security were to become reality, what would the role be for perimeter security? If future technology can accommodate sound security at the component level (i.e. application, database, host, network device), then the need for perimeter security would be radically changed.

Today, perimeter security is used to protect the back-end systems from unauthorized access. Future security technology might be thought of as an early warning system against quality adversaries. For certain, the role of perimeter security would change significantly.

Today we are far from the assurance levels described. Organizations do what they perceive as reasonable. Today, there are firewalls, VPN, application proxies, IDS, multiple support groups, outsourced services. There are new attacks daily. There is real concern about attackers (often in groups) burrowed quietly in existing environments performing reconnaissance activities. Every new piece of software, new release, new patch, new configuration, poses potential risk. Organizations are unable to allocate sufficient resources to maintain utmost vigilance. It is unrealistic for organizations to do independent code reviews. Commonly used operating systems are not sufficiently secure. Applications and operating systems are typically not built or designed for layered security.

Today's security technologies are so deficient that security is just too hard to do in a casual, inexpert way, on general-purpose platforms. There is NO ASSURANCE today; only illusion!

Today's Practical Reality

True assurance will be costly and hard-won, in the future, led and vetted by true security experts (academics, security agencies and top practitioners), in compact purpose-built subsystems, and only when the stakes are high and assurance a mission critical necessity. Barring technological assurance, most business service executives must settle for their people and process, occasional detected compromise, loss of money and reputation, and the possibility of deep undetected attack.

End-to-end secure application implementations will not become commonplace until the technology becomes easier to deploy and support, better integrated and less expensive, while relying less on people and process.

All is not Lost: Returning to Process and People

Lacking good technological assurance, there are many things that we can do to reduce our enterprise security risk. These measures extend well beyond perimeter security. Some of these include the following:

- Conduct routine assessments of vulnerabilities that go beyond perimeter technology assessments and include all nine of the security domain areas (see Table 1). The first step in creating assurance is understanding your strengths and weaknesses.
- Write policy that is clear, concise, relevant, up-to-date and maintainable. Adhere to and educate your users while maintaining your policies. Without a policy, there is no set of standards upon which to measure yourself.
- Develop, maintain or purchase a set of minimum security best practices for implementation on all your platforms including desktops, servers, routers, firewalls, applications (email, web servers, etc.). Reliance solely on a secure perimeter without hardened systems leads to a false sense of security.
- Understand your risks as well as the threat. Manage the critical changes in the threatscape that appear daily. Stay current on new and emerging threats, including malicious code, vulnerabilities and geo-political cyberthreats. While this will take effort, it will pay for itself in reduced down time.
- Educate your people. Teach your developers how to incorporate sound security practices into applications. Teach your end-users the "do's and don'ts" of good security. Keep your IT staff up to date. Education and awareness are two of the least expensive ways to mitigate enterprise risk.
- Review your processes. Make sure that processes exist where they are needed. Does a process exist for system backup? What about protecting those backups? What about moving those backups off-site? Do all those processes exist? Are they regularly tested?
- Streamline your processes. Processes that are unpleasant to perform or feel unnecessary to the employees are less likely to be followed - despite their importance to ensuring security. Although security processes may never be fun, they should be easy to follow.

Conclusion

Until such time that technology-driven end-to-end application security becomes practical, CSOs must ensure that not only their enterprise perimeter is secure, but also internal and external factors. Those with a fiduciary responsibility for their company need to move away from the "I have a firewall" mindset towards a more holistic view of security.

Lacking mature security technology that properly addresses end-to-end application security, there are many actions that can be taken to manage enterprise risk. These actions, when conducted in a sequential and rational order, can ultimately save money. Good security today does not need to cost more - it needs to be implemented holistically.

SC On-Line
SC Magazine
www.scmagazine.com