Data Privacy In a World Without Perimeters

By Oscar Mitchell

Data Privacy: A Critical Component of Network Security

Today's organizations are challenged by the complexities of protecting information as well as the critical issues that surround ensuring business continuity while maintaining privacy. But too often, companies leave data exposed.

As companies use the Internet to link up with partners, suppliers and customers, the traditional network perimeters have begun to disappear, prompting greater scrutiny of technologies for protecting data.

This need to share information across today's networks must be superseded by security measures to ensure data privacy. From ubiquitous mobile devices and supply chain partners to electronic business processes and outsourcing partners, sharing data and securing that data are two mutually exclusive issues that all businesses must address.

Data privacy challenges take place at all levels within an organization with each business unit having its own unique set of data security challenges. Given this increased need to securely move data within organizations and the increased frequency of both malicious internal breaches and external attacks, IT managers are looking for ways to protect the data on their networks.

In a recent poll of Fortune 500 IT managers, the biggest obstacle to making the company's network safer is securing the budget for security solutions.

Balancing Security And Privacy

Headlines containing phrases like 'Data Privacy Breach,' 'Vulnerable Networks Hacked,' or 'Confidential Information Lost' have become all too common. The ever-increasing dependence on electronic data has raised the security stakes. As organizations continue to rely heavily on the digital transfer of messages, files, confidential information and even money, the issue of data theft looms larger than ever.

Security threats to confidential information are on the rise. In fact, according to the Federal Trade Commission, more than 10 million consumers fall victim to some form of identity theft annually. And the costs are staggering; identity theft crimes alone are estimated at $53 billion.

Increasing concerns over data loss and compromise are pushing companies to consider new measures for securing unprotected data. Companies are moving beyond the traditional approach of deploying purely network- and perimeter-oriented defenses.

New privacy regulations are also requiring companies to demonstrate due diligence when it comes to protecting data, such as the Health Insurance Portability and Accountability Act (HIPAA) and California's SB 1386 database-breach notification law.

Ensuring security across networks is an ongoing challenge. Networking engineers, security experts and IT departments regularly address security issues, but many corporate networks—including Internet access—remain largely unsecured and porous. IT managers are confronted with a tough balancing act as they address security concerns while also maintaining business continuity and they must look for new ways to effectively protect the data on their networks.

SSL: The Industry Standard for Encryption

SSL (Secure Sockets Layer) is the predominant method of securing transactions over the Internet and it is included within all commonly used Web browsers. In addition to securing e-commerce transactions, SSL is also the preferred way to transmit sensitive data of any type.

The ever-increasing volume of SSL-encrypted traffic presents significant challenges to network architects and systems designers who are tasked with supporting this data in transit while maintaining network and application performance.

Implementing SSL can be difficult and complex. And its pervasive use has been driven by a number of factors, including:

- Data privacy concerns
- National defense initiatives
- Financial regulations
- Compliance initiatives

The complex cryptographic algorithms used within SSL impose a heavy processing load to computing platforms and software. As such, enterprises must often times contend with slow performance, increased latencies, and networking equipment that wasn't designed to handle high volumes of encrypted information.

Cryptographic coprocessors deliver only incremental performance improvements, consume considerable host CPU processing cycles, and don't address other tasks required to completely process SSL traffic. As SSL traffic continues to grow and encryption methods become more advanced, processing the increased load is only going to worsen.

Software vs. Hardware? Choosing the Best Method for Data Security

In the same poll of IT managers, over half (54%) of the respondents mentioned that they would prefer a hardware-based solution (a pre-bundled, standalone, hardware appliance or an embedded feature) in their network equipment to a software-based solution.

Enterprises have traditionally relied on software-based solutions for security, but software inherently comes with drawbacks. In a software-based solution, the encryption keys and certificates remain within reach of an experienced hacker who gains access to the underlying operating system.

Software-based solutions are vulnerable to attacks, require continuous updates and patches, and can negatively impact the performance of servers. Throughput and latency are almost always compromised. And while hardware co-processors can provide some relief, they are also difficult to implement.

A software-based security solution coupled with a co-processor continues to burden the overall system. Co-processors that offload the security processing from CPUs still require the main processor, memory and the system to help them do their job, so delays are still unavoidable.

Meanwhile, constant maintenance to the underlying operating system is always required. Software patches must remain up-to-date to eliminate vulnerabilities, which sometimes can mean repeating the integration with the security software or co-processor card. And then there is the need to re-test the business application. Not to mention, a contingency plan must be in place in the event that the operating system patch doesn't work once installed.

For example, an online equity-trading firm was undertaking a strategic initiative to introduce a new complementary service offering for customers. Data centers in two different cities would host this new application service and serve as redundant sites.

Performance (response time) and reliability (up time) would both be critical factors in providing a high-level of customer service. In addition, data privacy and confidentiality would also be critical components in making this initiative successful. One of the key security requirements was to make application changes without also requiring changes to the data privacy solution. The company explored three data security options:

1. Replacing the Load Balancer because the existing load balancer would not able to handle the required SSL transaction load.
2. Installing an SSL Appliance that would sit in between the load balancer and the application servers. However, a single appliance would not able to handle the SSL workload. Installing multiple appliances creates management and workload balancing issues. Benchmark tests also showed poor response time.
3. Installing a hardware-based data privacy offload solution based upon the SSL standard that would provide the highest performance with up to 10,000 TPS per server with no negative impact to the host CPU. It was the only solution that provided sufficient headroom to scale in the future.

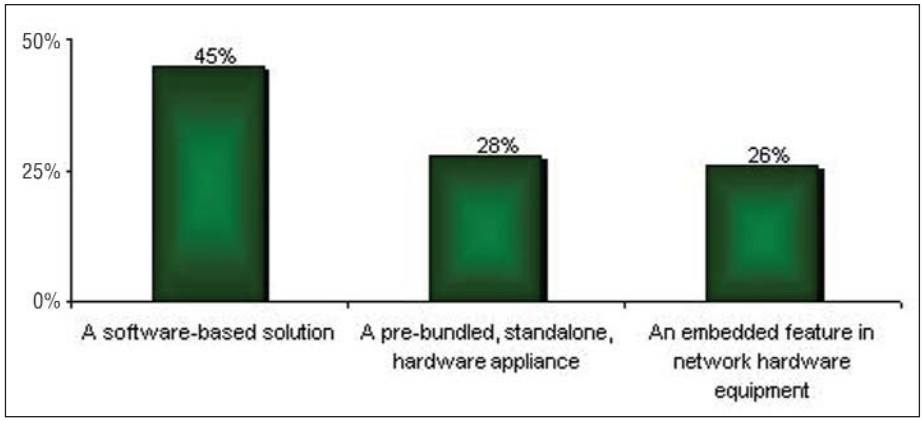

Figure 1: Preferred Method to Deploy Network Security

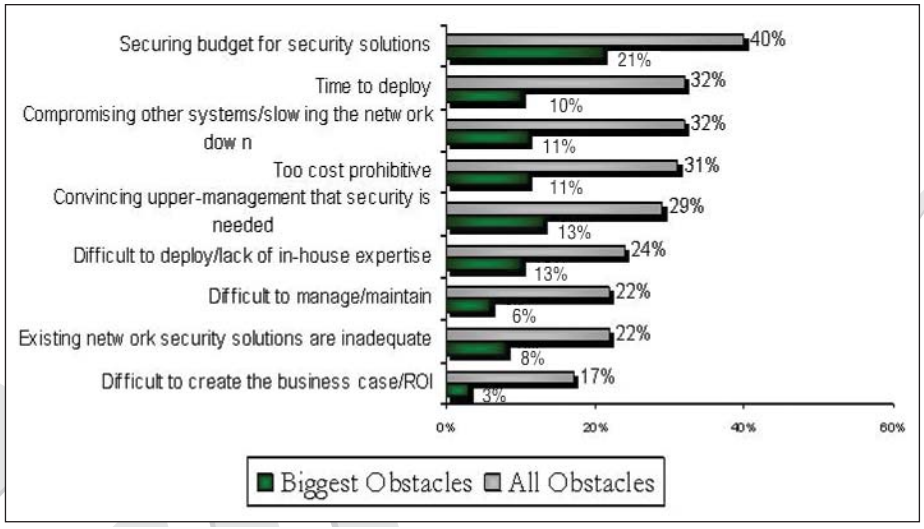

Figure 2: Obstacles to Network Security

The company implemented the hardware offload solution because it had the lowest latency which was almost instantaneous, ease of integration that was not affected by changes to the host application, and the lowest total cost of ownership (TCO) compared to the alternatives.

As a result, the organization experienced a CPU utilization percentage that declined from 95% before the installation to only 15% CPU utilization afterwards. Application memory utilization also improved drastically. Prior to the hardware-based SSL offload solution, 1.3 gigabytes were necessary and afterwards only 300MB of application memory were needed.

This translates into:

- the need for fewer servers to secure the information, which in turn saves money;
- decreased latency, which translates into a better user experience; and
- an increase in overall customer satisfaction.

Hardware-based offload solutions are more secure, more reliable, provide increased performance and offer additional flexibility. Hardware-based offload solutions also allow the encryption key to be stored into the tamper-resistant chip. Only authenticated users can then gain access to the key. Network performance is also preserved using a hardware-based security offload solution. Because the offload hardware actually runs the security applications, the server is free to process other tasks.

A Fortune 100 global financial institution was looking to decrease its network latency and increase customer satisfaction. Their existing network configuration could not support the number of users that the bank required, which impacted their customer satisfaction model and created the potential to lose customers.

The organization's IT environment included a custom-developed online banking application

based on a client-server architecture and required SSL for its applications that included on-line banking, internal security policy (data privacy), and remote access to data and applications.

The organization selected a hardware-based SSL offload solution that allowed it to install on existing qualified equipment without concern that the application would slow down in response time or that the CPU would become overloaded.

As a result, the organization experienced a 500% performance increase for the number of users the application could support and a 100% decrease in latency for the users, increasing overall customer satisfaction.

Conclusion

Hardware-based security offload solutions are becoming the more attractive alternative. In fact, IDC research estimates that 80% of security products will be hardware-based by 2007. Hardware-based offload solutions can offer many advantages.

Because companies have such varied factors to contend with when developing their specific security strategies—budgets, existing equipment, existing applications, operating systems and external pressures like government or compliance initiatives, each organization must develop a comprehensive approach to analyzing their inherent requirements. All the while, they must continue to remain diligent to keep up with the latest technological advancements that can help them save money, improve security, and increase their network's performance.

Oscar Mitchell is founder and CTO of Britestream Networks.