Protecting Web-Based Applications:
A META Security Group White Paper

Summary

Despite the “dot bomb” stock market debacle, most organizations continue to roll out new web-based business applications at a feverish pace. This phenomenon is not tied to a single vertical market. In fact, the trend toward web-based or true network computing spans both governmental and commercial organizations, and is evident in industries as diverse as insurance, banking, and finance to manufacturing, health care, pharmaceutical, and computers. Unfortunately, while there has been real progress in protecting corporate network infrastructure over the last few years, many organizations’ web-based applications remain at very high risk.

This white paper defines the application security problem in some detail, while providing practical guidance and prioritized recommendations. META Security Group is a pioneer in the web-based application security field; our team works with a diverse set of customers in all aspects of web-based application security. Our dedicated R&D team continues to explore the latest tools, techniques, and solutions to help organizations mitigate these risks and to protect critical customer and corporate information assets.

Problem

If you listened to the financial news, you could easily assume the demise of the Internet is well underway. However, in reality, the use of the Internet by companies and individuals continues to grow, and is forecast to expand at 20 percent rates for the next four years. Businesses are calling on their IT and security departments to help develop internet-based applications to improve their competitive position. The “net” is not going away.

A relevant indicator is the number of Internet hosts, which soared from 44 million in January 1999, to 88 million in August 2000, to almost 120 million in April 2001, according to Telcordia Technologies. Web commerce is now mainstream commerce. According to Nielsen//NetRatings, some 48 percent of all Americans over 18 have purchased products online. Moreover, businesses and government organizations of all sizes are rapidly deploying web-based applications to offer or improve a myriad of services. Corporate competitors are increasingly gaining market share by using the Internet.

Rather than going the way of the dinosaur, the Internet has become the underlying architecture for countless business applications. These new web-based applications range from retrofitted legacy mainframe systems or even, dare we say it, “legacy” client-server systems. They also include new, “pure” web-based applications and extend to wireless applications accessible via a plethora of novel mobile computing devices. The applications span vertical industry segments as well as front- and back-office business functions. Some of the key business drivers for these products and services include:

- Expense reduction:
  - Lower the cost of selling.
  - Lower the supply chain costs.
  - Reduce the cost of supporting business.
- Improved Linkage with Customers, Partners, and Constituents:
  - Improve product development process and time to market.
  - Improve the customer experience.
- Improved Access -- To provide “anywhere, anytime” access to customers, employees, and stakeholders who increasingly want greater Internet access and speed:

- Improve on-time deliveries.
- Improve employee service through intranets and self-service.

At the same time, META Security Group customers are continuing to seek assistance in reducing the Information Security risks resulting from all these new applications and business demands, and the related rapid transition to web- and network-based computing.

Numerous organizations have begun to make real progress in protecting their networks from attack. However, web-based applications -- and the critical customer, employee, constituent data they contain -- often remain at high risk for:

- Integrity Issues – For example, alteration of pricing information, contract terms, and conditions.
- Breaches of Confidentiality – Exposure of personal customer data, credit card information, or important intellectual property such as formulas and business plans.
- Systems Availability – Examples include denial of service attacks or other, inadvertent interruptions in service that leave customers, partners, employees, and constituents dissatisfied.

Much of the activities of "crackers" – known to the public at large as hackers -- are still oriented at breaking in through the infrastructure layers. However, a significant amount of energy is being devoted to exploring new ways to break business applications themselves. The new class of application exploits includes buffer overflows designed to overwhelm and crash applications, thus enabling easy access to important data. They also encompass techniques for exploiting the integrity of data stored in "cookies" used in e-commerce transactions, which can lead to such consequences as hackers "shoplifting" systems that have shopping cart functionality.

Because of the Internet's inherent risks, as well as crackers' focus on breaking the application itself, organizations need to do a better job of thinking through security as it relates to their entire system architecture, and pay special attention to the application-level components of the system. The business consequences of these application-level breaches can range from minimal annoyances to catastrophic, highly publicized losses in revenue, brand image, and customer trust. The career consequences for those responsible for failing to prevent the breaches are often equally severe.

Solution

The critical issue for many organizations is the deployment of secure web-based applications. The high-level solution to the issue has three key components:

1. Secure *infrastructure* such as routers, firewalls, and operating systems.

2. Secure *applications*, including secure programming practices for languages like Java and Perl, and specific application-level security controls such as application firewalls.

3. Security *policies* and *processes* including:

    a. IT-oriented policy and processes, for example, secure system design and development practices, sound configuration and change management, vulnerability testing, threat assessments, and ongoing vulnerability and incident monitoring and response.

    b. Business-level policy and processes, such as secure methods for bringing new customers on board, and mitigating the security issues that result from insecure customer service and help desk activities.

To date, most security activity has emphasized securing the IT infrastructure. Certainly a secure network and systems infrastructure are critical to delivery of a secure web-based application. These include properly and securely configuring the base infrastructure elements such as servers, routers, switches, etc., and instituting changes and patches over time to remove new vulnerabilities. It also requires putting in place protective measures such as traditional firewalls, ensuring network- and system-level access controls, and appropriately protecting data and transactions through virtual private networks (VPNs) or other cryptographic measures. Infrastructure-level security also involves such measures as monitoring for potentially malicious activity or for denial of service conditions.

Still, organizations need to put as much effort into securing the *whole* system, not only the base infrastructure components such as servers and routers, but application-level components as well, such as programs, databases, and other middleware elements (see Figure 1).

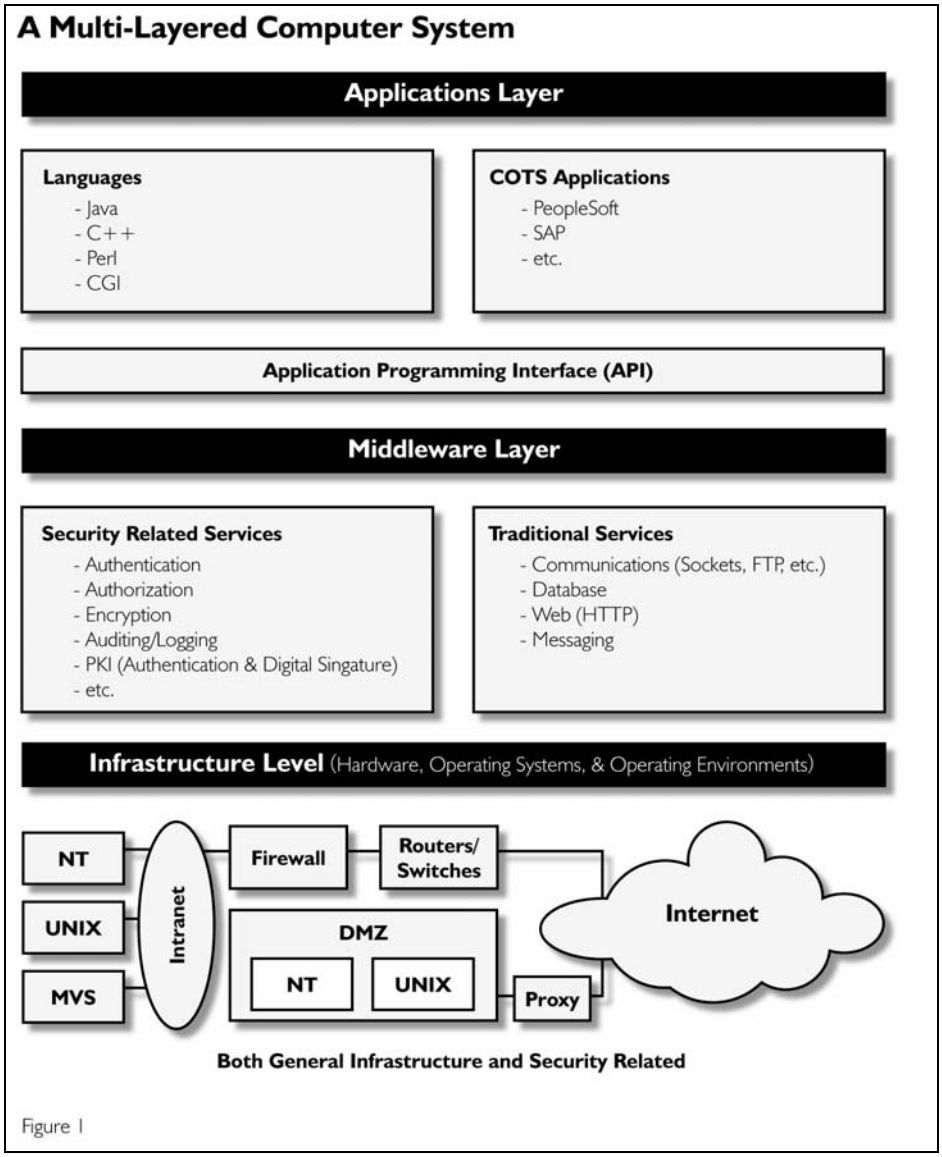

Figure 1: A Multi-Layered Computer System

Ensuring the application itself is protected is as important as protecting the base infrastructure. Optimally, application-level security is achieved by using secure coding practices to create appropriately hardened applications. However, even in smaller organizations, it is difficult to ensure that all application developers are adequately trained in secure coding practices, and kept up on new vulnerabilities. In larger organizations, this can be a daunting challenge. A new class of application protection, which includes application firewalls, can significantly improve security by blocking application hacking techniques. While training development and integration personnel in secure coding techniques is still a good idea, implementing an application firewall that blocks malicious activity constitutes an excellent stopgap.

It is vitally important to put non-technical security controls on an equal footing with technical controls. Non-technical security controls, such as security policy, training and education, and processes and procedures, are just as important as technical controls, which include strong passwords and firewalls. Non-technical controls also pertain to such items such as adopting a secure systems development life cycle and ensuring security is put into systems from the beginning rather than bolted on as an afterthought. Other examples of non-technical controls are creating processes and procedures for vulnerability testing, ongoing vulnerability management, incident monitoring and response, as well as integrating such controls with traditional IT processes, for example, network management, change management, configuration management, and disaster recovery.

A Phased Approach

A comprehensive, systematic approach to implementing security from the very start of a new business application project is now considered to be the “best practice” approach. A standard firewall, for example, will fail to sufficiently protect a web-based application that was not designed with appropriate security in mind, or otherwise adequately protected. Security teams will have to work more closely with the architecture and design, application, infrastructure, IT, and business teams to ensure secure applications. While this is rather easy to state, META Security Group understands that designing and implementing the myriad of technical security controls, policies, processes, and procedures mentioned in summary form above can be an overwhelming task. Therefore we recommend, in keeping with a core META Security Group philosophy, a phased approach. Our recommended phasing takes into account often-present resource and budgetary constraints, and is designed to ensure the earliest initiatives have, from a risk reduction perspective, the highest return on investment (ROI). The phasing is broken into two sets of initiatives occurring at different times:

Stop Gap Application Protection Initiatives (3-6 month timeframe):

- Provide initial application developer/system architect training and awareness.
- Implement a pre-production, application-level vulnerability testing regimen
  - Perform thorough tests of critical applications, using both commercial tools and experienced “ethical” application hackers.
  - Complete minimal, tool-based scans of less-critical applications.
  - Develop a feedback loop to the development teams.
  - Schedule periodic reassessment of new versions.
- Initiate a thorough network perimeter and DMZ vulnerability assessment. Ensure the assessment not only points out vulnerabilities and fixes, but also identifies the root causes of the vulnerabilities and what to do to systemically remove vulnerabilities from the environment.
- Implement application-level firewalls for all moderate-to-critical, web-based applications.

Mid-Term Initiatives and Forensics (6-12 month timeframe)

- Deliver more in-depth application developer/systems architecture security training
- Adopt a secure systems development process to ensure appropriate security requirements and protections are considered throughout the entire systems development life cycle.
- Develop security standards for code/applications development.
- Initiate a thorough internal network vulnerability assessment, and ensure the understanding of root vulnerability causes and fixes.
- Implement ongoing (quarterly or change-based), application-level vulnerability scans
- At a minimum, ensure log files on critical network devices – especially Internet facing devices – are reviewed regularly. Optimally, deploy Intrusion Detection Systems (IDS) on critical network access points, and implement the attendant monitoring and incident response processes.

META Security Group Application Security Services

As mentioned at the start of this white paper, META Security Group is a pioneer in the web and network application security marketplace. We have developed a tremendous base of experience and of intellectual capital, including documented best practices, that enable us to meet diverse customer demands in this arena. We continue to invest heavily in our research and development activities to enhance our thinking and leadership in this arena.

META Security Group provides the industry's most complete range of solutions for protecting web-based critical applications. They include infrastructure services, application services, and policies and processes services.

Secure Infrastructure Services

- Traditional network vulnerability and penetration assessments (a.k.a. "ethical hacking") for network perimeters and internal networks, which ensure a secure base for critical applications.
- Secure network architecture, design, and implementation services to help organizations appropriately architect and deploy critical technical controls:
    - Firewall, VPN, IDS, perimeter and access controls, authentication, Public Key Infrastructure (PKI), encryption, etc.
- Ongoing (monthly/quarterly) vulnerability scanning to ensure new vulnerabilities are uncovered and addressed before hackers find them.
- Managed security services to ensure constant security vigilance. These include:
    - Firewall and VPN monitoring and management
    - IDS monitoring and management
    - Computer forensics and litigation support
- Training and awareness, which include:
    - Executive-level security awareness
    - Management-level courses such as: How to Build a Security Program, How to Develop a Security Policy Framework, Security Vulnerability and Configuration Management, Secure Systems Development, etc.
    - Security for systems/network administrators and developers, which include Network Security Tools, PKI/Encryption 101, Secure Application Coding Practices, Security for Various Infrastructure Platforms, etc.

- Response and investigation, such as Computer Forensics, and Setting up a Security Incident Response Team (SIRT)

Secure Application Services

- Web-based application assessments. Both detailed, hands-on testing and tool-based scanning services specifically geared towards uncovering application-level-vulnerabilities.
- Application-level firewall services. Examples include product selection, architecture, and design and deployment services.
- Secure systems development life cycle process development
- Application security training and awareness programs:
  - Security for application developers
  - Secure coding practices
  - Developing a secure systems development life cycle

Secure Policies and Processes Services

- Security policy assessment and development:
  - Based on META Security Group's Best Practice Security Policy Framework (policies, standards, procedures)
- Command Center. A web-based tool/service that features documented best practice policies, standards, procedures, and research for securing network elements. The service also has profile-base vulnerability alert services to ensure security teams and network administrators are kept abreast of the latest vulnerabilities and fixes.
- Security process assessment and development:
  - Security Incident Response Team (SIRT), vulnerability management, secure change/configuration management, incident monitoring, etc.
- Security organization and governance assessment and development:
  - Best practice organizational models, roles, and responsibilities definition

Conclusion

This white paper is only the tip of the proverbial iceberg. We hope it has provided a good starting point for understanding the problem of and solutions for protecting web-based applications. We continue to develop critical partner relationships and service offerings to ensure we can bring the appropriate solutions that our customers require.