Security Testing
For Financial Institutions

915-1784-01 Rev B July 2012

Contents

Introduction

Major security breaches resulting in loss of data, service downtime, and brand damage cost businesses an average of $7.2 million dollars per breach according to Ponemon Institute.[1] Ponemon's 2012 Confidential Documents at Risk survey of IT and security professionals found a whopping 90% of respondents' organizations had experienced leakage or loss of sensitive or confidential documents during the previous12 months.

Security breaches resulting in loss of data, service downtime and brand damage cost businesses an average of $7.2 million dollars per breach according to Ponemon Institute.

While failures occur at every level from applications to network infrastructures, the number of data breaches resulting from malicious attacks increased in 2011 accounting for 37% of the total. These breaches carried an an average cost of $222 per record compared with the overall per-record cost of $194.[2]

From a technology standpoint, companies are increasingly combining existing commercial and open source software, servers, and converged networks and systems to provide new services to their customers. Today's financial infrastructures consist of hundreds, if not thousands of servers. Each hardware and software component has unknown quality, robustness and security. When combined through standard and proprietary interfaces, the risks associated with each component are multiplied.

With considerable time-to-market pressure and the lack of trained security staff, thorough security, and robustness assessment – the ability of a system to handle unexpected input – is often omitted. This results in applications and systems that are insecure and fragile, leaving organizations open to the very real and expensive risks associated with:

- Brand damage
- Service degradation
- Downtime
- Legal exposure

The costs associated with brand damage can be bad and potentially fatal for a company. "Any breach has the tendency to dampen greatly whatever you are spending around your brand," said Kirk Herath, chief privacy officer, assistant vice president and associate general counsel at Nationwide Insurance in Columbus, Ohio.[3]

Service degradation is a hard to measure quantity, but can be very expensive. Services that are poorly engineered fail to scale well. This results in unhappy customers who experience delays while using web sites, or the need for more and more hardware to compensate for the degradation. A small failure in one part of the network can result in significant loss in performance of a critical service.

Downtime is the ultimate insult to the customer, and carries a high risk of of generating customer churn. Legal exposure can also cause severe financial damage, and even be a life-ending event for an organization.

1 Ponemon Institute 2010 Annual Study
2 Ponemon Institute 2011 US Cost of a Data Breach Study
3 Information Security Magazine, July 2007

Governments, financial, and healthcare institutions have unique security and privacy concerns and face stringent industry requirements. Financial institutions are particularly susceptible to large-scale losses due to the nature of their transactions, and having even a few customers compromised can trigger a mass exodus. A single data breach within processing firm Global Payments recently placed as many as 1.5 million credit and debit card numbers from all major card brands at risk.[4]

NBCnews.com reported that large financial institutions faced more online attacks in 2011 than during the previous two years, with hackers attempting to break into and transfer funds from hacked accounts 314 times according to a survey of 95 financial institutions and five service providers conducted by the American Bankers Association.[5] This represents a dramatic increase from 239 reported attempts in 2010 and only 87 in 2009.

Conventional security tools are not completely effective because they deal with the symptoms, not the causes – software flaws that allow attackers to find cracks in the armor and cause Internet applications to fail or under-perform, system crashes, information leakage, and theft. Security and robustness analysis is critical in eliminating software flaws.

As shown in Figure 1, the cost associated with finding and fixing problems increases exponentially as we move from component development to component integration to system integration to deployment. The costs associated with finding and fixing a software flaw in a major Internet service can easily run into the millions of dollars.

Financial institutions are particularly susceptible to large-scale losses, due to the nature of their transactions. Just a few customer compromises are needed to trigger a mass exodus of customers.

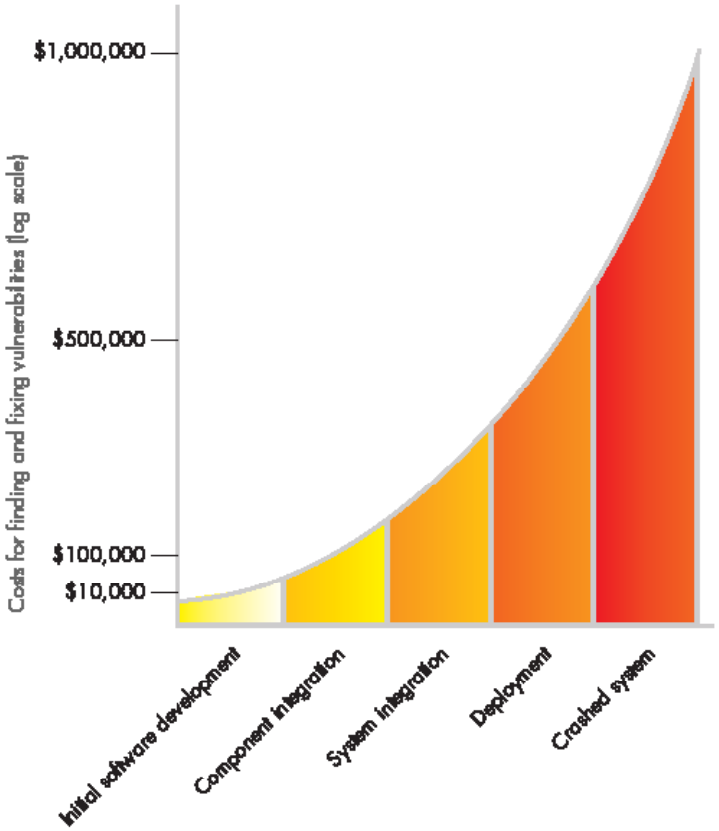

Figure 1. Costs related to security flaws

4 Security on NBCnews.com, "Online Attacks Against Banks on the Rise" by Matt Liebowitz, Security News, June 15, 2012. http://www.msnbc.msn.com/id/47835885/ns/technology_and_science-security/t/online-attacks-against-banks-rise/#.UBBTvbTwunk

5 CNN Money, "1.5M Card Numbers at Risk from Hack" by Juliane Pepitone,@CNNMoneyTech, April 3, 2012. http://money.cnn.com/2012/04/02/technology/global-payments-breach/index.htm

The Need for Security Testing

All this is not to say that organizations are not testing – they are. Products and services are first tested to ensure proper "normal" operation. This is sometimes complemented by vulnerability-specific tests mandated by ISO compliance, secure programming initiatives and risk management best practices. Vulnerabilities are most often exploited by manipulation of network protocols at all levels – from user input in URLs and web page form fields, all the way down to the bits and bytes in protocol packets.

A set of network testing tools is needed that can be used at every stage of development, and at every network level and interface.

The number of protocols involved in modern Internet applications and their complexity make it impractical to ensure secure and robust behavior through purpose-built tests or random testing. A set of network testing tools is needed that can be used at every stage of development, and at every network level and interface.

Internet applications don't exist in a vacuum; they're surrounded by a sea of routers, content servers, firewalls, anti-virus filters, authentication servers, etc. These devices, which supply the infrastructure for the application, must be considered as part of a complete system. Experience with performance testing has shown that realistic scale and traffic requirements are required to stress these devices to the point where they are most vulnerable to failure.

Security Threats

Figure 2 shows the multiple networks between clients accessing financial services and the hosting of those services. The financial exposure associated with security threats increases as we move from individual clients to aggregation networks to the services themselves, due to number of transactions that cross the path. The number of targets, however, decreases – potentially millions of clients on the one hand connecting to a single hosting service location.

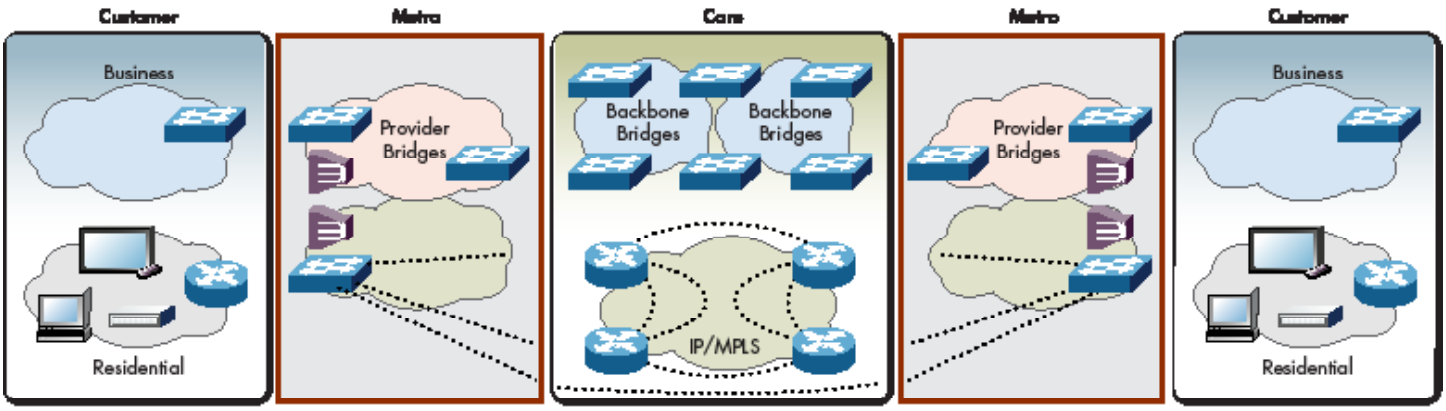

Figure 2. Multiple Networks Connect Clients with Services

Internet usage has expanded dramatically and is expected to continue, as shown below.

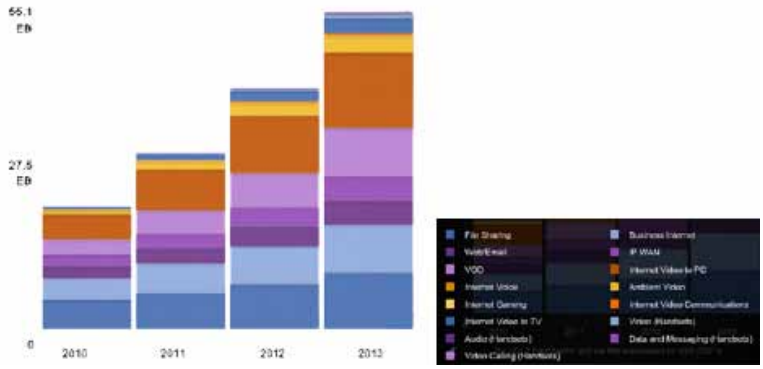

Figure 3. Expansion of Broadband Usage (Cisco VNI – 2009)

The security threats and tools used to combat those tests differ for:

- Clients
- Access, metro and core networks
- Financial service providers

The security threats and tools used to combat those tests differ for, clients, access, metro and core networks, and financial service providers.

Client Threats

Home and enterprise users are subject to a number of vulnerabilities:

- **Exploits delivered by e-mail** – E-mail exploits take the form of malicious attachments and enticements to click on unverified links. A frequent form of the latter is the e-mail note that asks the reader to click on a link that will renew their account information; the link, of course, points to a hacker's site.
- **Exploits embedded in web pages** – Malicious web pages are frequently visited by unwary customers due to e-mails that impersonate a valid institution or as a result of Internet searches. One particular attack, called DNS poisoning, can result in a client using a proper web site address, but being redirected to a malicious web site.
- **Network-level attacks** – Network-level attacks exploit known operating system and application faults. Most of these faults have been fixed by software developers, requiring only that users update their computers. Operating system faults offer attackers full computer and network access; application faults can allow malicious code to sneak into a system.

By and large, enterprise users are better protected than home users due to corporate policies and security devices, including firewalls and intrusion protection systems. Once a virus enters a corporate network, however, the network is an open field for exploit due to the trusted nature of the corporate LAN. Home users, on the other hand, are responsible for their own security – often requiring purchase of security tools and paying attention to updates.

The tools available to combat client threats include:

- **Education** – users need to be continuously reminded of the threats associated with e-mail, the need to update their computers, and the need to be constantly suspicious.
- **Anti-virus/security software** – each and every computer requires that security software be installed and that updates for that software be purchased and applied. The existence of corporate firewalls and other measures does not diminish this requirement.
- **Operating system/application updates** – home users frequently ignore reminders, while corporate users expect that others have taken care of the problem for them.
- **Secure web sites** – financial service providers must ensure that their web sites are inherently secure and easily recognized by their users.

Access, core and metro networks are the great unknown for the financial service provider, largely out of their control.

Access, core and metro networks

This part of the network is the great unknown for the financial service provider, largely out of their control. Faults in the network infrastructure, however, can exploit the client-server connection. Some of the more common threats include:

- **DNS poisoning** – the domain name service (DNS) is responsible for translating Internet names, such as *www.yahoo.com* to the IP addresses that are used to find computers on the Internet. Although there are central servers that contain the master copy of the translation, servers throughout the Internet maintain short-term copies of the mapping. If an attacker succeeds in changing, or poisoning, one of these servers they can direct a large audience of users to go to an alternate web site, or send their e-mail through a server that copies client information.
- **Router control** – routers are used throughout the Internet to forward traffic. Routers, however, are sophisticated computers complete with operating systems, application software and passwords. A number of these routers are publicly accessible and use the well-known default password installed on the device by the manufacturer. Hackers can take control of these routers in order to disable them or redirect traffic.
- **Zombie'd computers** – home and enterprise users that fall victim to attacks discussed in the previous section may become zombie computers that are available to hackers to mount massive attacks. Among these are distributed denial of service (DDoS) attacks, which can initiate large numbers of connections and send huge amounts of traffic against financial service providers.
- **Man in the middle attacks** – physical access or one of the other attacks discussed above can result in the placement of an intermediate system between the client and service – one that copies and forwards information including financial information.

The tools available to combat these threats include:

- **Server security** – in the same way as client computers must be protected from attack, so must the servers that support DNS and other network infrastructure services. Firewall protection, multi-factor authentication, and anti-virus tools are often used and are discussed in the next section.
- **Router security** – network service providers must keep careful control over of their network components, applying strict security controls. Routers often include secure, encrypted methods of user authentication and control that should be utilized.
- **Traffic shaping** – network service providers ensure the fairness of their services by inspecting the traffic that they are forwarding in order to identify traffic flows. Voice and video flows, for example, require low latency and jitter while peer-to-peer traffic can be reduced in priority. The technique, called deep packet inspection (DPI), can be used to identify and halt security threats such as DDoS.
- **End-to-end encryption** – we'll discuss this in the next section.

Financial service providers

Financial service providers are subject to attacks that steal money or affect the delivery of client services; both can result in serious losses. The principal threats to financial service providers include:

Financial service providers are subject to attacks that steal money or affect the delivery of client services; both can result in serious losses.

- **DDoS attacks** – consisting of significant connections and traffic designed to overload the service. The traffic can consist of arbitrary packets or normal-looking web site usage, for example – an attempt to login with fictitious accounts names and passwords.
- **Known vulnerability attacks** – that exploit software flaws in network stacks, operating systems and applications. Such exploits utilize many network protocols on many levels – IP, TCP, UDP, e-mail, FTP, web, and proprietary protocols. These attacks often use randomized data, making it hard for security precautions to counter.
- **Encryption attacks** – most financial transactions are encrypted. Determined hackers attempt to decrypt the traffic. Modern encryption techniques render this type of attack impractical, but some financial services may use shorter key lengths that can be decoded using brute force calculations.
- **Impersonations** – compromised client computers can provide hackers with valid user names and passwords and can be used to transfer funds.

A number of tools are used to implement security for financial service providers:

- **Pre-deployment testing** – components and networks should be tested before being deployed in live networks. Principal among the security tests are:
  - **Conformance** – packaged tests that ensure that all supported network protocols conform to industry standards. Such tests include both positive and negative cases that help close security holes and ensure inter-operation between network components purchased from multiple vendors.
  - **Fuzzing** – packaged tests that explore protocol implementation flaws in great detail. Fuzzing tests perform targeted randomization on protocol packets, exploring all possible exploits.
  - **Known vulnerability testing** – potentially large number of tests that ensure that services and applications have been updated and improved to resist historical attacks.
  - **Performance** – it is essential to determine the maximum real-world performance of the financial service to ensure that each client is serviced with sufficient quality. It's also necessary to determine how the service performs under overload – rejecting new users, slowing down sessions, or failing.
- **End-to-end encryption** – because intermediate networks are out of financial service's control, techniques must be applied to guard the client-server communications. This most often takes the form of browser-based encrypted connections using SSL or TLS. Financial services use certificates that are presented to the user for verification if they don't match the web site being used or have expired; service providers should never let this happen. Authentication of the client commonly takes the form of a user name and password, or if viewed as insecure, a physical authentication device.
- **Firewalls** – and related servers as shown in figure 4. Firewalls admit or reject connections, handle DDoS and other attacks, filter outgoing information for confidential data, detect sophisticated intrusions, SPAM and viruses. They frequently terminate SSL connections, enabling them to view the content of encrypted sessions. In many cases, auxiliary processors are used for the separate functions.

Firewalls admit or reject connections, handle DDoS and other attacks, filter outgoing information for confidential data, detect sophisticated intrusions, SPAM and viruses.

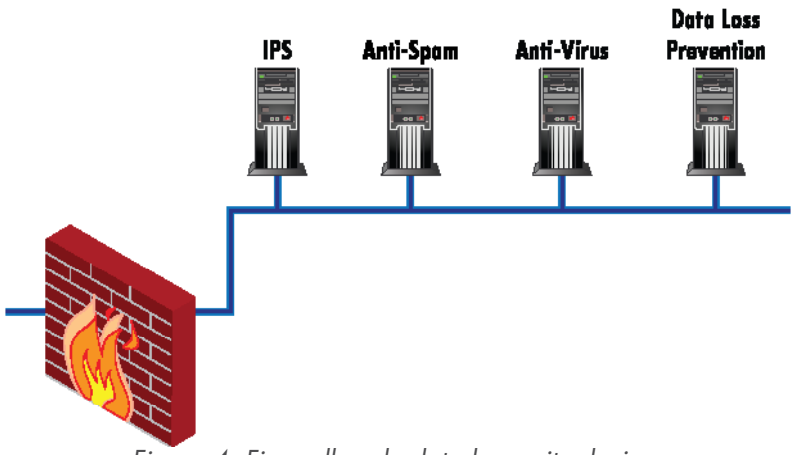

Figure 4. Firewall and related security devices

The Payoff

The benefits of early and frequent security analysis are substantial. Return on investment is maximized because secure products operate better and require less maintenance. Total cost of ownership is minimized because robust products exhibit high reliability.

- A secure, robust and reliable system exhibits:
- Lower development costs
- Reduced time to market
- Quick problem resolution
- Reduced susceptibility to security attacks
- Increased availability
- Fewer recalls
- Minimal legal exposure
- Lower compliance risks
- Preserved brand identity

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 818.871.1805
www.ixiacom.com

Other Ixia Contacts
Info: info@ixiacom.com
Investors: ir@ixiacom.com
Public Relations: pr@ixiacom.com
Renewals: renewals@ixiacom.com
Sales: sales@ixiacom.com
Support: support@ixiacom.com
Training: training@ixiacom.com