

Securing Web Application by Symantec



symantec.
Confidence in a connected world.

Securing Web Application

Phattrapha Hongkumdee – CISSP, CISA
Date: March 2007

AGENDA



- 1 Symantec Corporate Overview
- 2 Security Threat Trend
- 3 How to Secure Web Application
- 4 Tool to Help

Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 2


Securing Web Application by Symantec

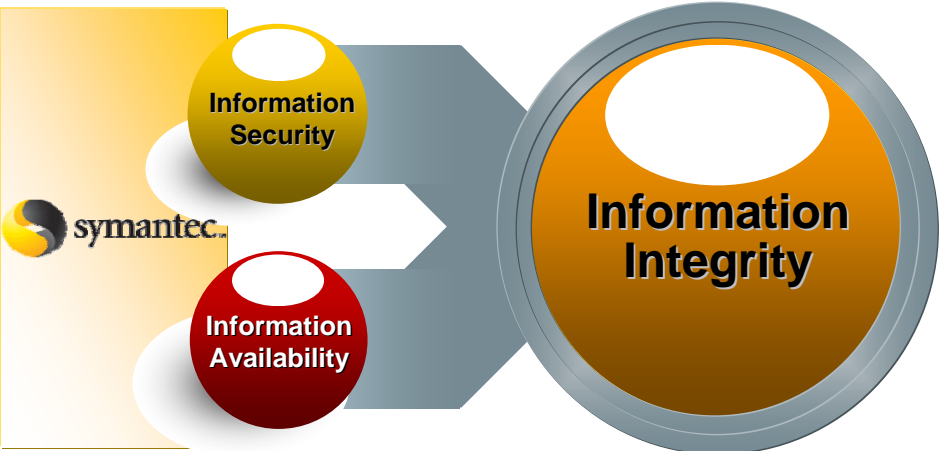
Symantec Corporation Today 



- 4th Largest Software Company In The World
- 200 Million+ Systems Protected Worldwide
- Diverse Customer Base: Consumer, Business, Government And Education
- Global 24x7 Operations: 14,000 Employees In 39 Countries
- 23 Years Of Industry Experience
- Over \$700M Annual Investment In R&D
- Legacy of Protecting Windows
- Our Focus – Your Needs

Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 3

Symantec Corporation Today 



Information Security

Information Availability

Information Integrity

End Point Security **Messaging Security** **Security Management** **Compliance**

Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 4



Attack Trends – Top targeted sectors



- ▶ Home user are often targets of opportunity and provide “cover” for larger, more targeted attacks
- ▶ Targeted attacks against Government, Information Technology, Utilities and Energy are on the rise.

Current Rank	Previous Rank	Sector	Current Proportion of Targeted attacks	Previous Proportion of Targeted attacks
1	1	Home user	86%	93%
2	2	Financial Services	14%	4%
3	6	Government	<1%	<1%
4	3	Education	<1%	2%
5	8	Information Technology	<1%	<1%
6	7	Health care	<1%	<1%
7	5	Accounting	<1%	<1%
8	10	Telecommunications	<1%	<1%
9	4	Small Business	<1%	<1%
10	14	Utilities / Energy	<1%	<1%

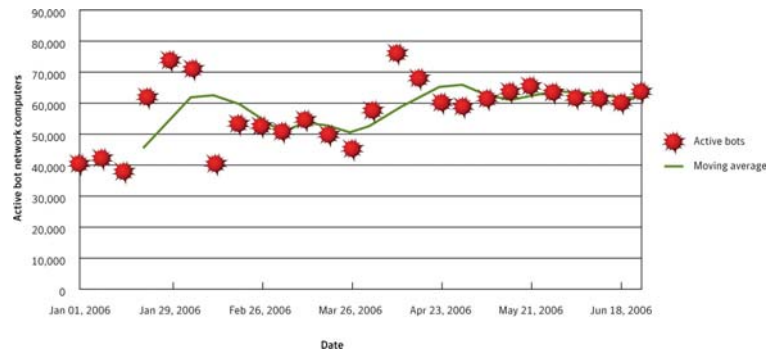
Source: Symantec Internet Security Threat Report (Jan - Jun 2006)

Securing Web Application by Symantec

Attack Trends – Bot Infection Statistics



- ▶ Average daily total of 57,717 active bot network computers per day. Total of 4,696,903 distinct active bot network computers over the six month period. Through our partners, we identified 6,337 command and control servers during the current reporting period.
- ▶ China had the highest percentage of known bot networks worldwide - 20%. The U.S. was second with 19% followed by the U.K. with 7%.



Source: Symantec Internet Security Threat Report (Jan - Jun 2006)

Copyright © 2007 Symantec Corporation. All rights reserved.

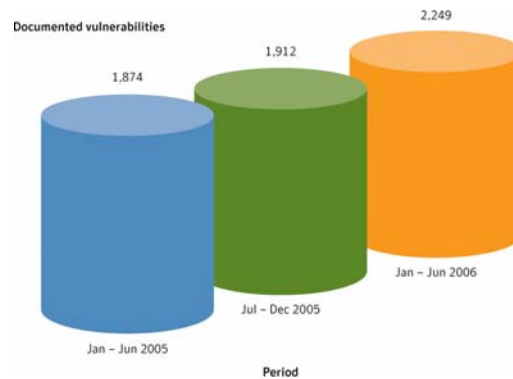
Securing Web Application

7

Vulnerability Trends – Volume



- ▶ Between January 1 and June 30, 2006, the total number of vulnerabilities grew by 18% over the previous reporting period and 20% over the same period last year.
- ▶ Primarily due to the high percentage of Web application vulnerabilities. Once again, this is the highest total Symantec has ever recorded.



Source: Symantec Internet Security Threat Report (Jan - Jun 2006)

Copyright © 2007 Symantec Corporation. All rights reserved.

Securing Web Application

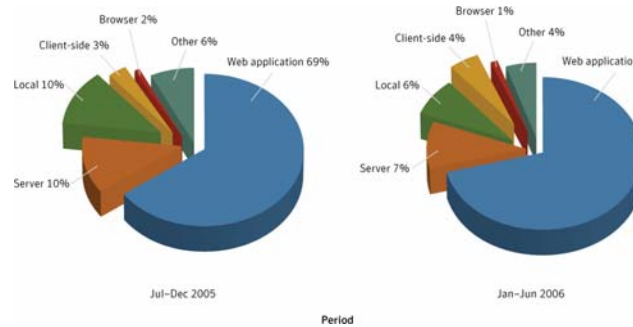
8

Securing Web Application by Symantec

Vulnerability Trends – Easily exploitable vulnerabilities by type - Web applications



- ▶ 69% of all vulnerabilities reported were web application vulnerabilities a slight increase over the previous reporting period.
- ▶ 80% of all vulnerabilities were easily exploitable. Of those, the largest proportion (78%) were web application vulnerabilities. This is due in part to a quicker release cycle, less secure coding practices and low complexity vulnerabilities.



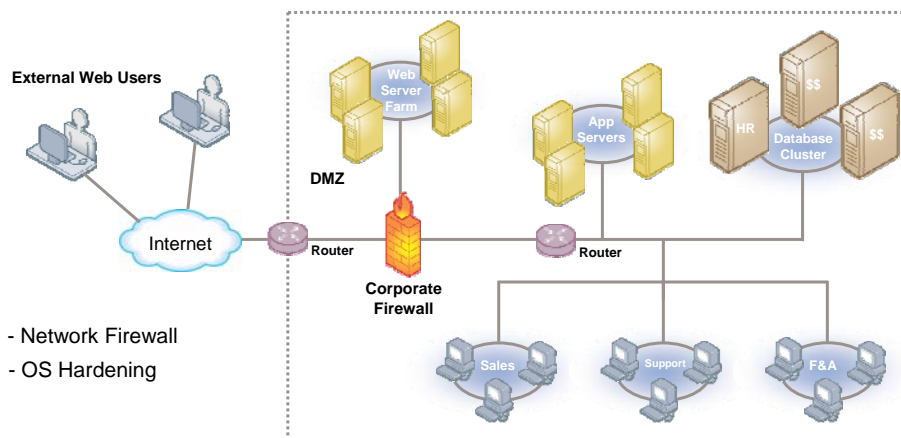
Source: Symantec Internet Security Threat Report (Jan - Jun 2006)

Copyright © 2007 Symantec Corporation. All rights reserved.

Securing Web Application

9

Not only Network and OS Security Application is also a Key



- Network Firewall
- OS Hardening

Copyright © 2007 Symantec Corporation. All rights reserved.

Securing Web Application

10

Securing Web Application by Symantec

Not only Network and OS Security Application is also a Key

The diagram illustrates a network architecture where an SQL injection attack originates from External Web Users on the Internet. The attack path is shown as a red line passing through a Router in the DMZ, a Corporate Firewall, and another Router to reach a Database Cluster. The Database Cluster includes HR, Database Cluster, and SS components. Other servers shown include Web Server Farm, App Servers, and desktops for Sales, Support, and F&A departments.

- Network Firewall
- OS Hardening

Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 11

Top 10 – Web Security Issues

- 1 Unvalidated Input**

Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
- 2 Broken Access Control**

Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
- 3 Broken Authentication and Session Management**

Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
- 4 Cross Site Scripting**

The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

Source: <http://www.owasp.org>

Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 12

Top 10 – Web Security Issues



5 Buffer Overflow

Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.

6 Injection Flaws

Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.

7 Improper Error Handling

Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

8 Insecure Storage

Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.

Source: <http://www.owasp.org>

Top 10 – Web Security Issues



9 Application Denial of Service

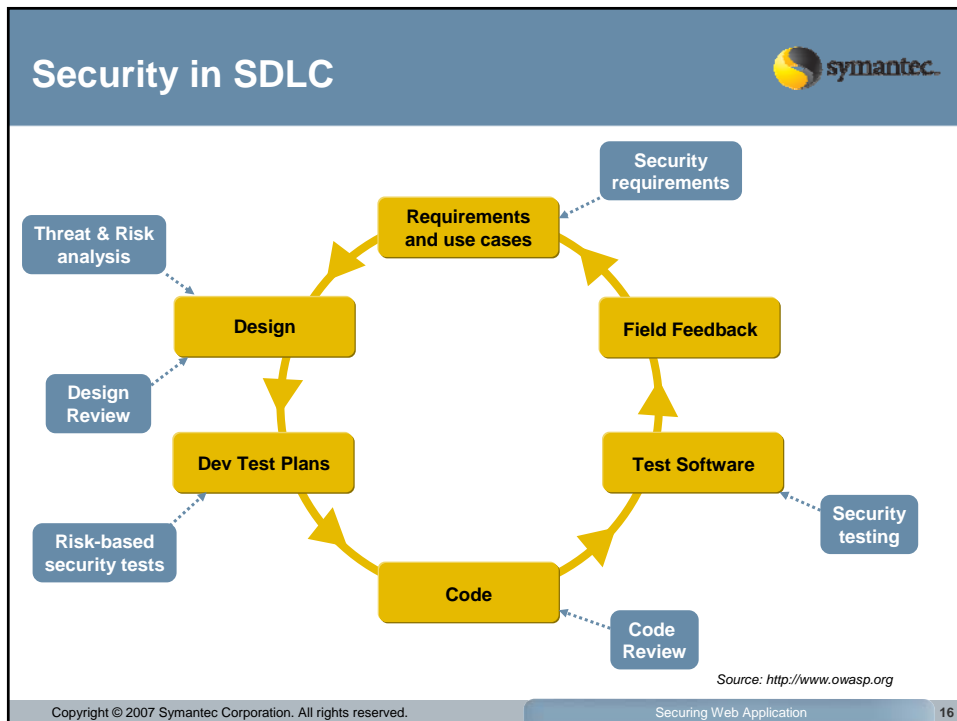
Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.

10 Insecure Configuration Management

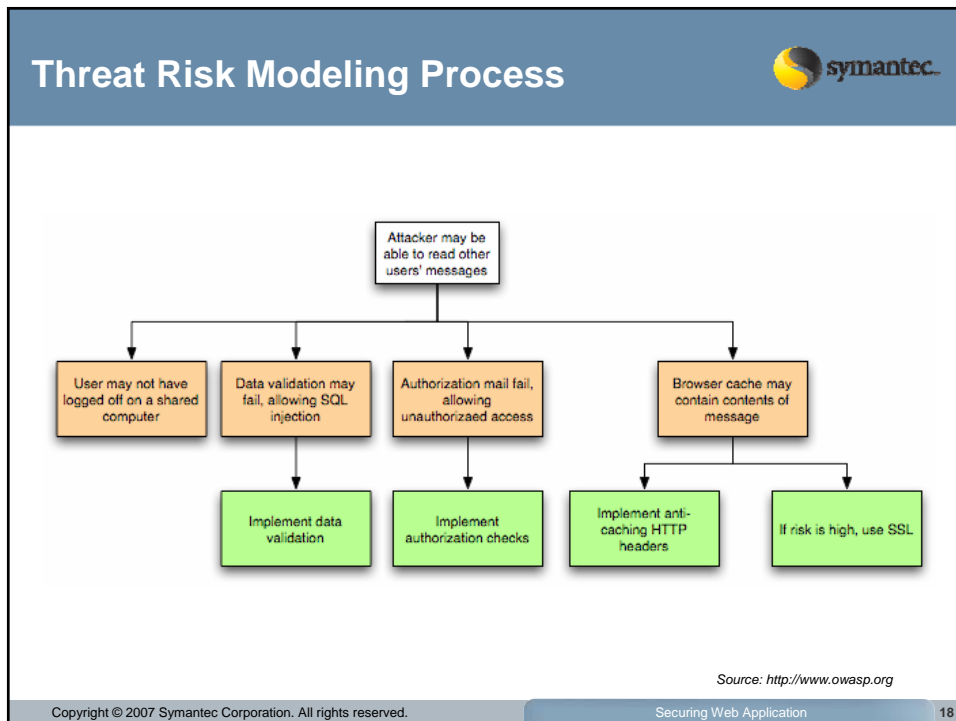
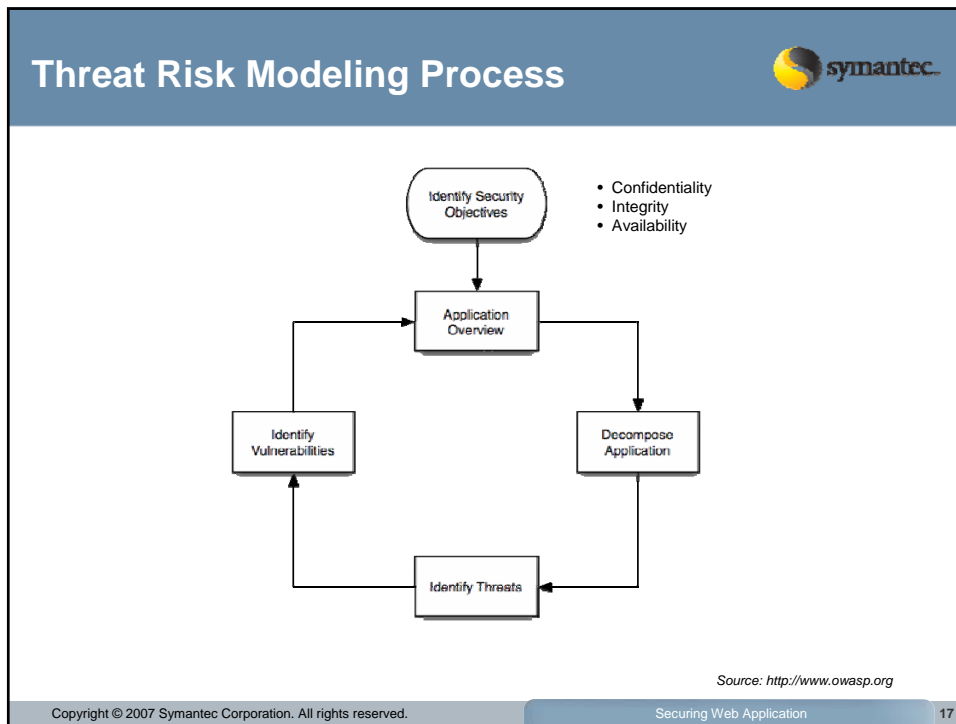
Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

Source: <http://www.owasp.org>

Securing Web Application by Symantec



Securing Web Application by Symantec



Secure Coding Principles



- **Minimize Attack Surface Area**

Every feature that is added to an application adds a certain amount of risk to the overall application.

- **Secure by defaults**

For example, by default, password aging and complexity should be enabled. Users might be allowed to turn these two features off to simplify their use of the application and increase their risk.

- **Principle of Least Privilege**

- **Principle of Defense in Depth**

The principle of defense in depth suggests that where one control would be reasonable, more controls that approach risks in different fashions are better.

- **Fail Securely**

Source: <http://www.owasp.org>

Secure Coding Principles



- **External System are Insecure**

Implicit trust of externally run systems is not warranted. All external systems should be treated in a similar fashion

- **Separation of Duties**

For example, someone who requests a computer cannot also sign for it, nor should they directly receive the computer.

- **Do not trust Security through Obscurity**

The security of an application should not rely upon knowledge of the source code being kept secret. The security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

Source: <http://www.owasp.org>

Secure Coding Principles



- **Simplicity**

Developers should avoid the use of double negatives and complex architectures when a simpler approach would be faster and simpler.

- **Fix Security Issues Correctly**

Once a security issue has been identified, it is important to develop a test for it, and to understand the root cause of the issue.

Source: <http://www.owasp.org>

Copyright © 2007 Symantec Corporation. All rights reserved.

Securing Web Application

21



Confidence in a connected world.

Tools to Help

- Vulnerability Management
- Database Security

Securing Web Application by Symantec

Vulnerability Management

Security Configuration Database

Standards & Regulations

- CobIT
- Coso
- ISO17799-2005 (ISO27001)
- NIST-800
- SOX
- HIPPA
- GLBA
- ...


Servers and Applications

Copyright © 2007 Symantec Corporation. All rights reserved.
Securing Web Application
23


Vulnerability Management

Copyright © 2007 Symantec Corporation. All rights reserved.
Securing Web Application
24

Securing Web Application by Symantec


Enterprise Databases Security Issues 

Identity Info: SSN
Health Records
Financial Data




Corporate & Government databases

→

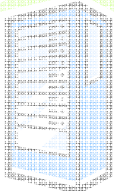


Crown Jewels of the Organization

Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 25

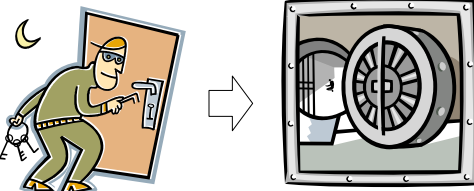
Enterprise Databases Security Issues 

Identity Info: SSN
Health Records
Financial Data

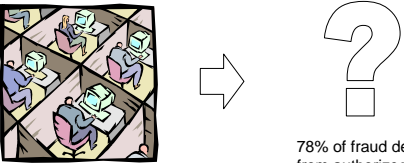


Corporate & Government databases

How do you protect against attack?



But we need use the information.



78% of fraud derives from authorized users
US Secret Service Study.

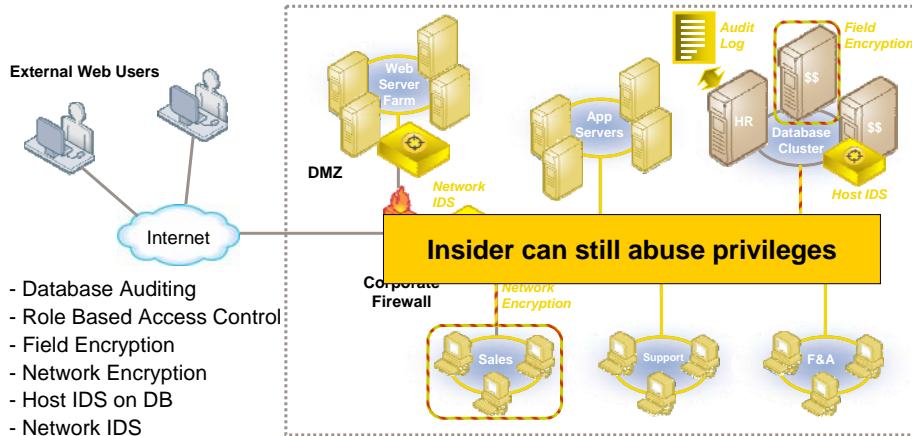
Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 26

Securing Web Application by Symantec

How can this be happening?



Let's look at the techniques in use today...



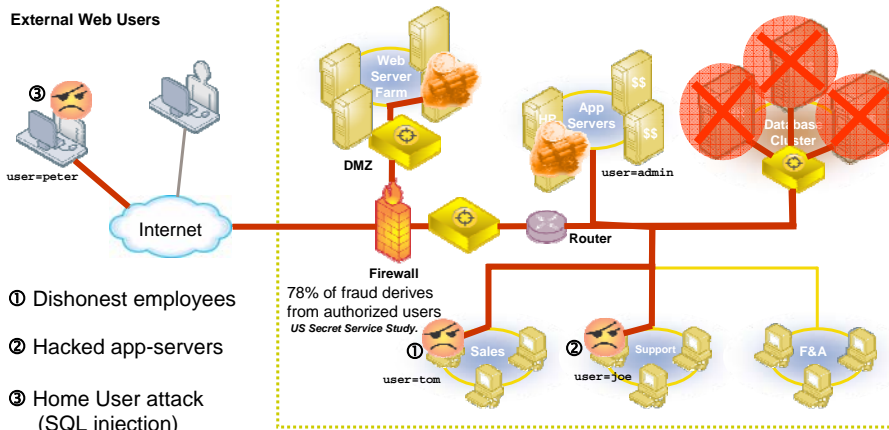
- Database Auditing
- Role Based Access Control
- Field Encryption
- Network Encryption
- Host IDS on DB
- Network IDS

Copyright © 2007 Symantec Corporation. All rights reserved.

Securing Web Application

27

Traditional security will not stop or even detect ...



- ① Dishonest employees
- ② Hacked app-servers
- ③ Home User attack (SQL injection)

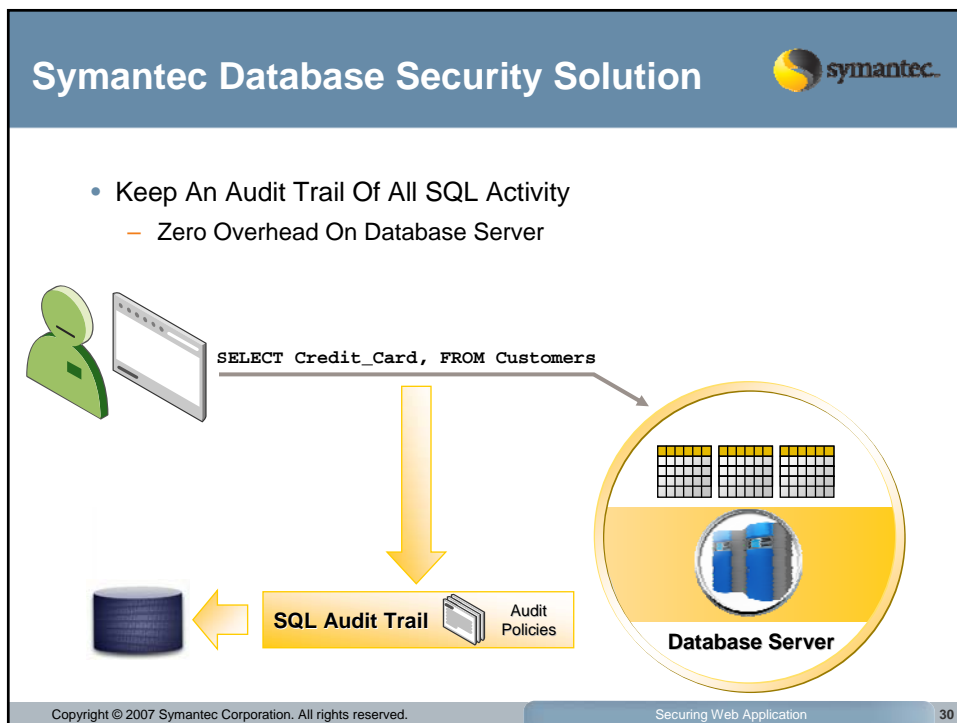
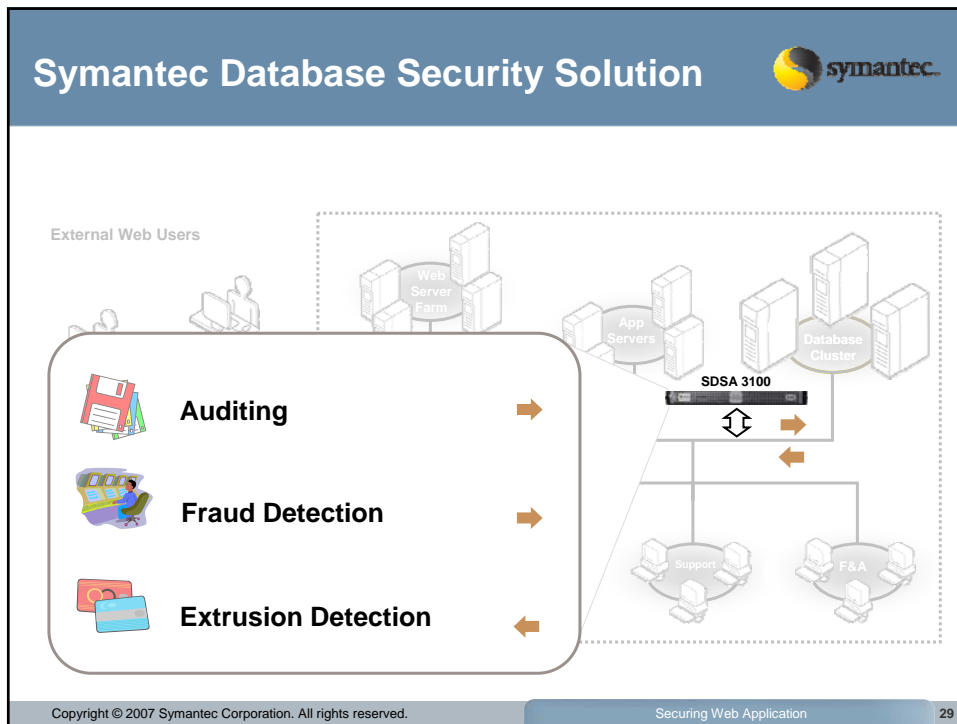
78% of fraud derives from authorized users
US Secret Service Study

Copyright © 2007 Symantec Corporation. All rights reserved.

Securing Web Application


28

Securing Web Application by Symantec

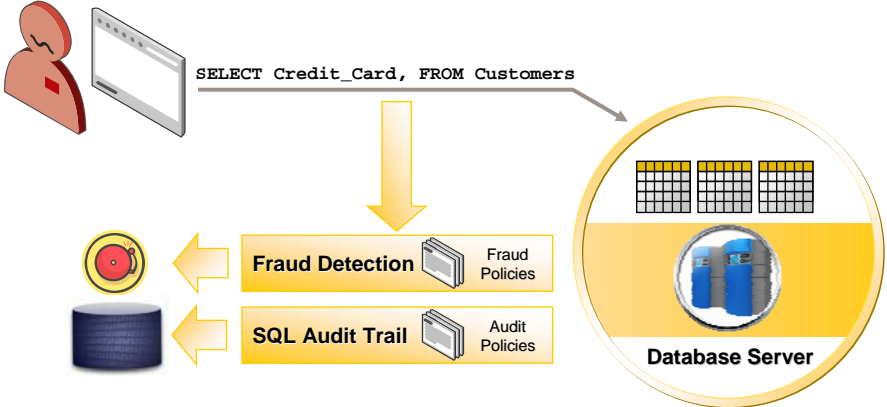


Securing Web Application by Symantec

Symantec Database Security Solution




- Detect Potential Threats From Insiders & Outsiders
 - Using Fraud Policies & Historical Transaction Information

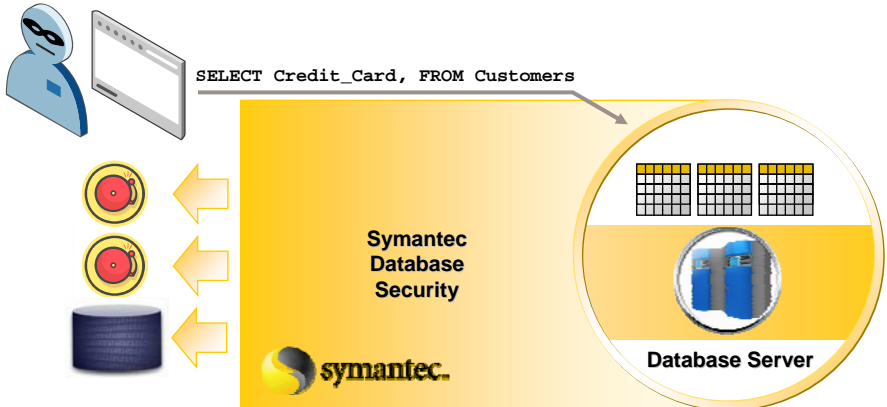


Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 31

Symantec Database Security Solution



- Detect Leakage Of Confidential Information
 - Based On “Extrusion” Policies



Copyright © 2007 Symantec Corporation. All rights reserved. Securing Web Application 32

SUMMARY



- Application security is a critical factor for Information Security
- Secure coding practice is importance
- Symantec Technology for Secure Application
 - Vulnerability Management
 - Database Security



Confidence in a connected world.

Thank You!

Phattrapha Hongkumdee
Phattrapha_Hongkumdee@symantec.com
66-(0)2627-9000

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.