



Hardening Enterprise Apache

Sander Temme – Sales Engineer, Thales e-Security

Sander.Temme@thalessec.com, November 10, 2011

Presented by



Produced by



THALES



By Reuters and Nicole Kobie

Posted on 20 Jun 2011 at 08:34

Sega has admitted data from 1.3 million customers was stolen in the latest attack again

ck Shows Dang

Suspect in widespread hacking arrested

Cassandra Vinograd, Associated Press
Wednesday, June 22, 2011

011

F

t

tendo, the manufacturer of th

y Detects Suspicious Behavior, Locks 93,000 Online Accounts

Donohue

Share Like 2 +1 0

9 Comments

ected multiple U.S. def

ame Street's Y n Pom



Sony locked the accounts of some 93,000 individuals on the Playstation Network (PSN), the Sony Entertainment Network (SEN), and Sony Online Entertainment (SOE) services following a mass log-in attempt using username-password combinations obtained from an

Thousands of sites compromised following hosting provider hack

Posted on 28 September 2011.

07:35

Sesam
letters >



What I Will Cover



- Hardening Tips
- Security Background
- Threat Modeling

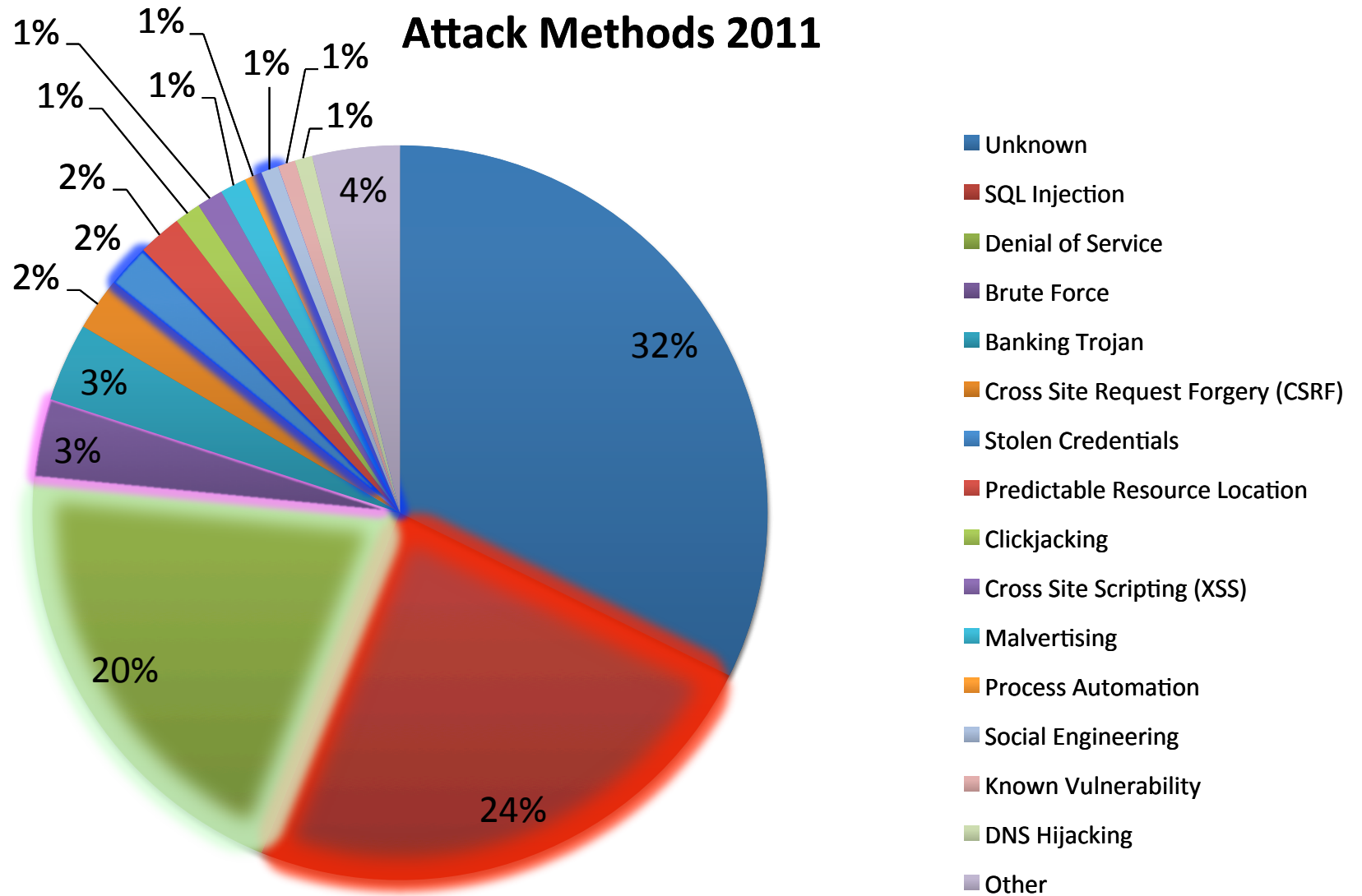


Disclaimer

The information discussed in this presentation is provided "as is" without warranties of any kind, either express or implied, including accuracy, fitness for a particular purpose, reliability, or availability.

It is your web server infrastructure, and you alone are responsible for its secure and reliable operation. If you are uncertain about your approach to hardening and protection, consult a security professional.

Attack Methods 2011



<http://s.apache.org/WHID>



Denial of Service

- Business decision to fight?
- Fight at Routers, Firewalls
 - Work with your ISP
 - Shunt or Sinkhole for DOS traffic
- Apache
 - Not great against trickle attacks
 - MaxClients easily exhausted
 - Event MPM better





Management Password Hygiene

- Use special passwords
- Write them down
- Don't share passwords
 - Role Accounts
 - Sudo



<http://xkcd.com/936/>

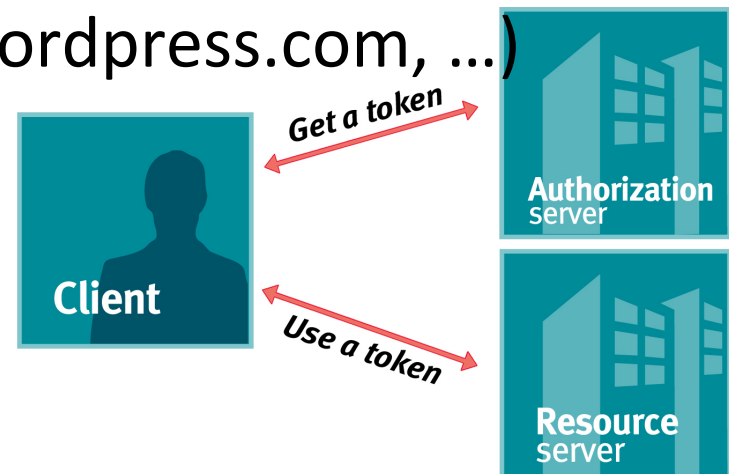
- Define policies
- Force SSL
- One Time Passwords (OTP, OPIE, S/Key)

<http://arst.ch/o9q>

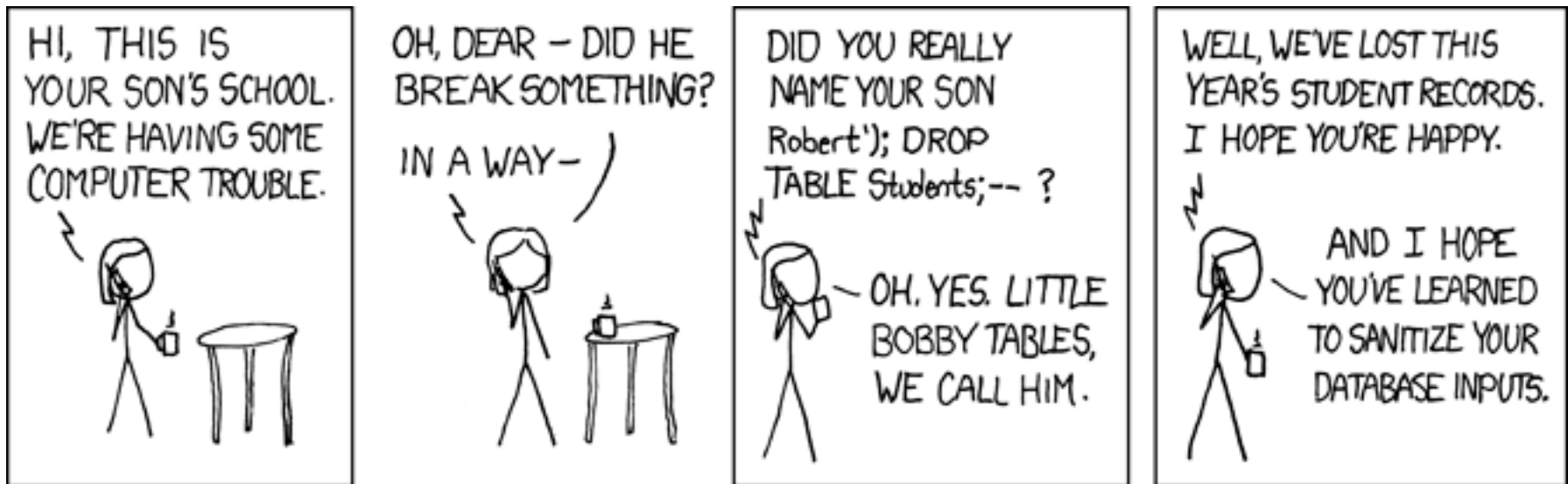


User Password Hygiene

- Use a password vault
- Security Questions
- Federate!
 - OAuth (Facebook, Twitter)
 - OpenID (Yahoo!, Google, Wordpress.com, ...)



SQL Injection



<http://xkcd.com/327/>

SQL Injection Defined


```
"SELECT * FROM grades WHERE (grades.student_id =  
students.id) AND (students.name = '$name');"
```

```
$name = "Robert"); DROP TABLE Students; --"
```

```
"SELECT * FROM grades WHERE (grades.student_id =  
students.id) AND (students.name = 'Robert'); DROP  
TABLE Students; -- ');"
```



SQL Injection Remedies – Code

- Parameterized queries <http://s.apache.org/SQL>
- Validate input
 - Blacklist: arms race
 - Whitelist: bad user experience
 - TAINT Mode (Perl and Ruby, NOT in PHP!)
- Push it to your ORM
- Fail mysteriously 





SQL Injection Remedies – Ops

- Web Application Firewall
 - ModSecurity
 - Breach, Imperva, ...
- Least Privilege

<http://modsecurity.org/>

Database Privileges

Bugzilla: GRANT SELECT, INSERT, UPDATE, DELETE, INDEX, ALTER, CREATE, LOCK TABLES, CREATE TEMPORARY TABLES, **DROP**, REFERENCES ON bugs.* TO bugs@localhost IDENTIFIED BY '\$db_pass';

Wordpress: GRANT **ALL PRIVILEGES** ON databasename.* TO "wordpressuser@hostname" IDENTIFIED BY "password";

Joomla 1.7: you'll need access to a MySQL database, as well as the following credentials (...)

Moodle 2.0: 4. Now use the **Add Users to Databases** button and give this new user account **ALL** rights to the new database.

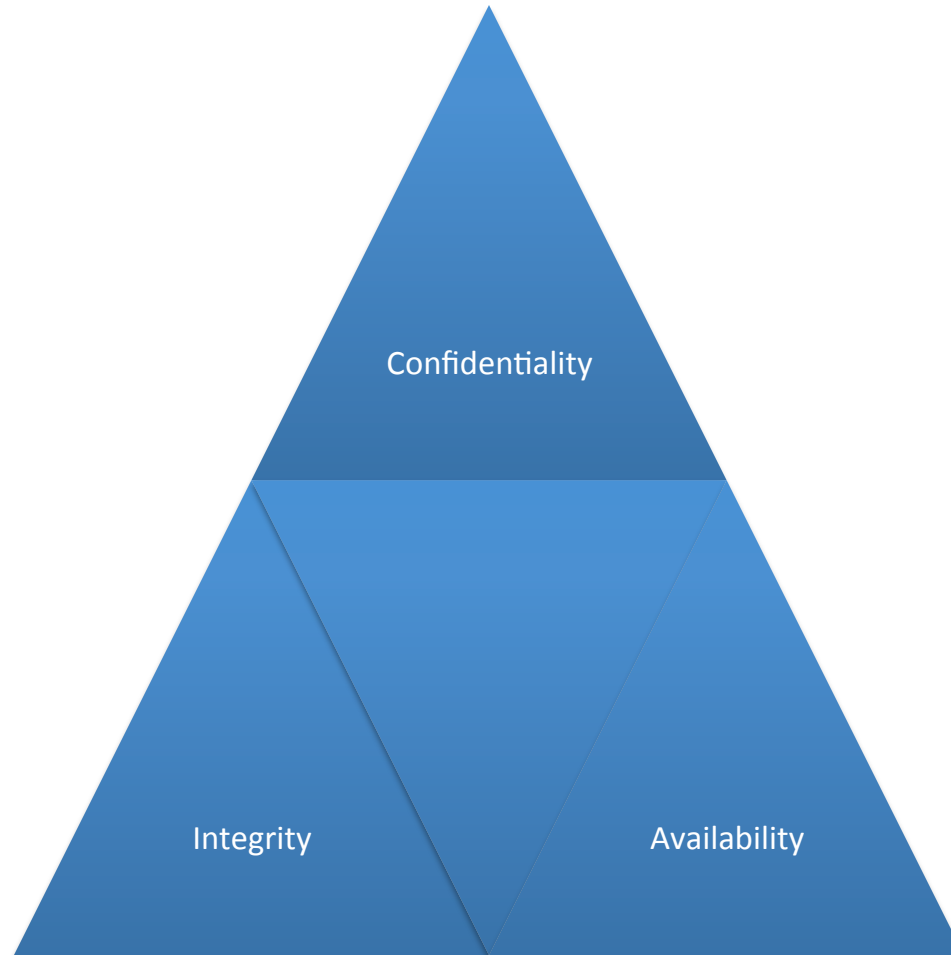
Drupal: SELECT, INSERT, UPDATE, DELETE, CREATE, **DROP**, INDEX, ALTER, LOCK TABLES, CREATE TEMPORARY TABLES

Gallery 3: Create a MySQL database for your Gallery 3 installation and note down the username and password for the Database (if required). Usually this is done in the control panel for your website.



SECURITY PRINCIPLES

Security Triad

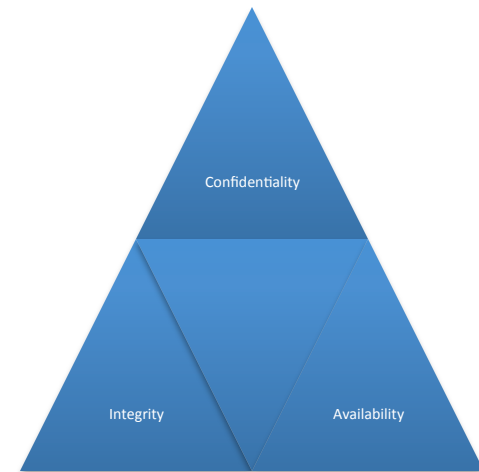


THALES

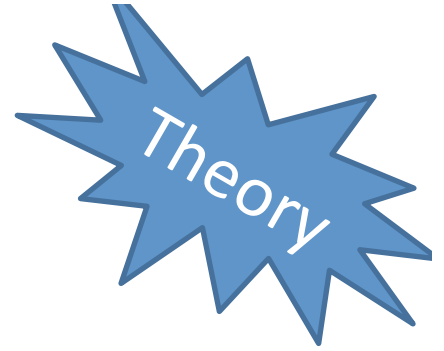
Security Objectives



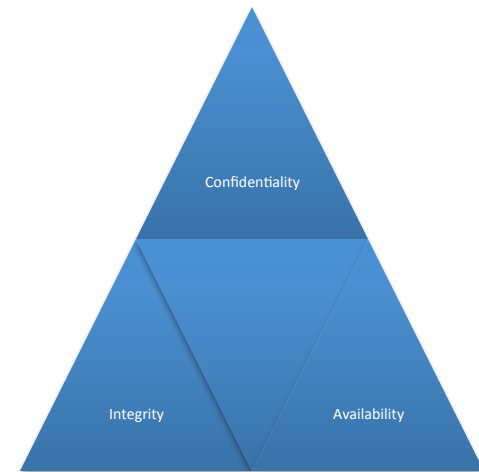
- Harder
- More expensive
- More likely to get noticed



Controls



- Any Countermeasure
 - Application Code
 - Configuration
 - Data Processing





Information Systems Security Association
The Global Voice of Information Security

<http://www.issa.org/>

THALES



MORE TIPS

THALES



Operating System Hardening

- Writable directories
 - Mount /tmp with noexec, nosuid
- chroot, FreeBSD jail, Solaris Zones
- Unnecessary services
- Unused packages
- Create a skinny installation
- SELinux, FreeBSD secureLevel





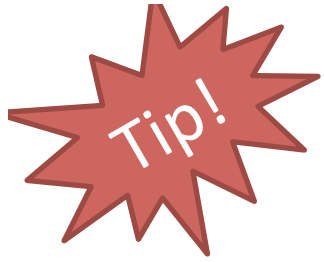
Don't Run Your Own Code

Your Own Code

- Purpose-built one-off
- Written by you
 - Or your predecessor
- Exercised by you
 - Only in your app
- Broken by someone
- Fixed by you

Other People's Code

- Frameworks and Libraries
- Written by Them
- Exercised by EVERYONE
 - In tons of apps
 - In every context imaginable
- Broken by someone
- Fixed by Them



Picking Code

- Technical Fit
 - Can you Contribute?
- Team Viability
- User Community
- Responsiveness to Issues



Start Apache as Root



- Parent as root
 - Binds to low ports
 - Opens log files
 - Doesn't handle network traffic
- Children drop privilege
 - Inherit open file descriptors
 - Handle network traffic
 - Write to open log files
 - But nowhere else



An Overview

WEB SITES UNDER ATTACK

THALES



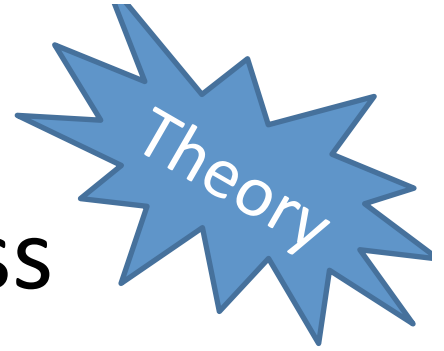




THALES

Apache
Con
North America | 2011

Brick and Mortar: The Cost of Doing Business

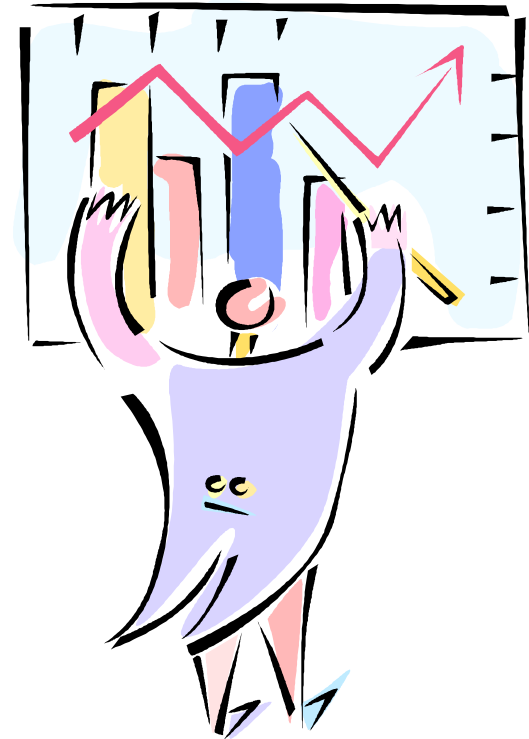


- “Shrinkage” is expected
 - Just manage it
 - Work the margin
- Targeted countermeasures
 - Restrict access
 - Exclude suspects

Business Reasons to be on the Web



- Increase sales
- Decrease costs



What's the Big Deal?




- Data is valuable
 - Regulatory pressure
- Exposed 24/7
- Bad traffic indistinguishable from good
- Attacks are free!
- Vulnerabilities galore!
- Little jeopardy attached



How to Defend



- Fail Closed
- Manage out-of-band 
- Keep it offline
- Plan response, recovery



Writing to the File System

- Network listener == attack vector
- Write permissions == open door
 - Rootkits
 - Planted malware
- Exceptions exist



Writing to Document Root

Joomla! 1.6.0 Installation

Steps:

- 1 : Language
- 2 : Pre-Installation check
- 3 : License
- 4 : Database
- 5 : FTP Configuration
- 6 : Configuration
- 7 : Finish

Pre-Installation Check

Pre-installation check for Joomla! 1.6.0 Beta13 [Onward] 01-Nov-2010 23:00 GMT:

If any of these items is not supported (marked as **No**) then please take actions to correct them. Failure to do so could lead to your Joomla! installation not functioning correctly.

PHP Version >= 5.2.4	Yes
Zlib Compression Support	Yes
XML Support	Yes
MySQL Support	Yes
MB Language Support	Yes
configuration.php Writeable	No

You can still continue the installation as the configuration settings will be displayed at the end. You will have to manually upload the code. Click in the text area to highlight all of the code and then paste into a new text file. Name this file 'configuration.php' and upload it to your site root folder.


Recommended settings:

These settings are recommended for PHP in order to ensure full compatibility with Joomla! However, Joomla! will still operate if your settings do not quite match the recommended.

Directive	Current	Recommended
Safe Mode:	Off	Off
Display Errors:	Off	On
File Uploads:	On	On
Magic Quotes Runtime:	Off	Off
Register Globals:	Off	Off
Output Buffering:	Off	Off



Defending your Writable DocRoot

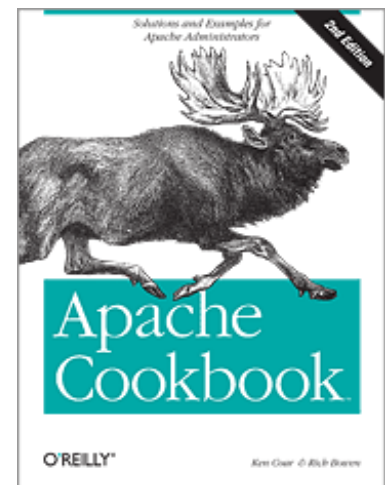
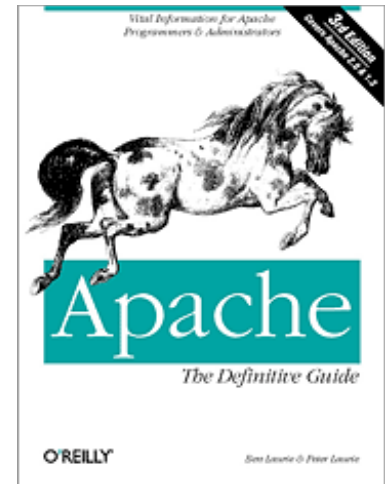
- Responsibility of application
 - No safety net
- Out-of-band management 
 - ssh, (s)ftp, another Apache?
- Assurance Case



Apache Configuration

- Write your own
- Avoid `<IfModule>`
- Disable unused modules
- `mod_info` to view results

<http://httpd.apache.org/docs/2.2/>



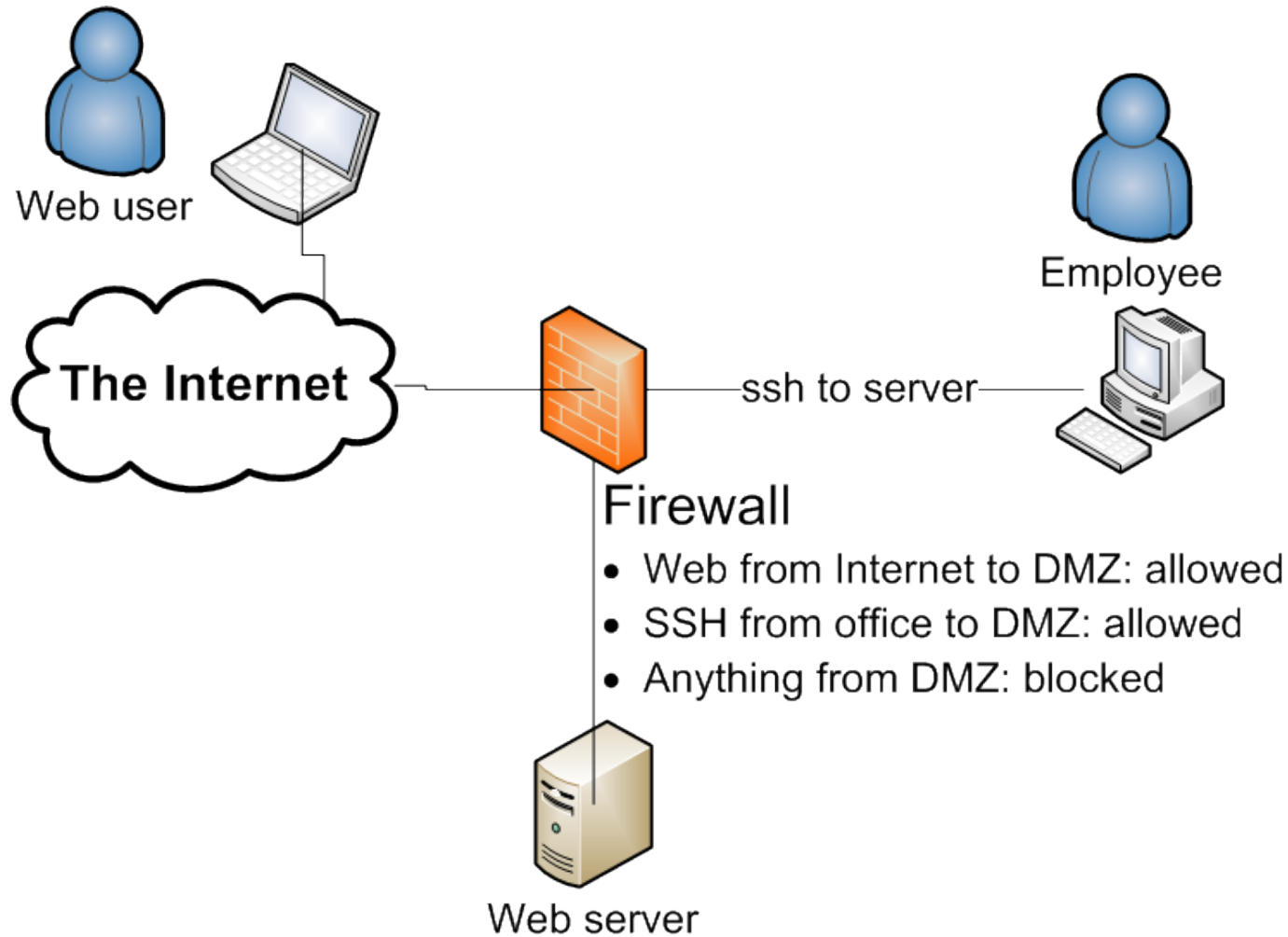


Network

- Block outgoing connections
 - Web Server only serves incoming connections
- Minimize incoming connections
 - Port 80, port 443
 - ssh, sftp, etc. through bastion
- Use firewall



Suggested DMZ Configuration



ASF Security Process

- Report vulnerabilities to security@apache.org
- Forwarded to appropriate Project
- Handled by Project
 - Vulnerability # assigned
 - Fix developed
 - New version released
 - Disclosure coordinated
- The Project is You

Wrap Up

- Tips!
- Security becomes business
- Rationalization of defense

Sources

- Ryan C. Barnett, Preventing Web Attacks With Apache, ISBN 0-321-32128-6
- Ivan Ristic, Apache Security, ISBN 978-0596007249
- Tony Mobily, Hardening Apache, ISBN 978-1590593783
- http://httpd.apache.org/security_report.html
- <http://www.cisecurity.org/>
- Mike Andrews and James A. Whittaker, How to Break Web Software, ISBN 0-321-36944-0
- <http://www.owasp.org/>
- NIST Guidelines on Securing Public Web Servers: <http://bit.ly/41oFmE> (pdf)

Contact

- Sander Temme

- Sander.Temme@thalessec.com
- @keysinthecloud on  [twitter](#)
- <http://www.temme.net/sander/>
- Slides: <http://people.apache.org/~sctemme/ApconNA2011/>

Presented by



Produced by



THALES



THANK YOU!

THALES



Backup Slides

THALES

Why Attacked?



- Data Theft
- Blackmail
- Espionage
- Hacktivism
- Upload Malware




How Attacked?



- (Distributed) Denial of Service
- Crafted requests
- Social engineering
- Stolen credentials
- ...



Windows

- Use what you know!!! 
- Pull Server Root out of install dir 
 - `httpd -n Apache2.2 -d c:\mysite -k config`
- Create *apache* user 
 - Services run as SYSTEM user
 - Can write to many directories
 - Write access only to `c:\mysite\logs` subdirectory
 - Let Apache2.2 Service log on as *apache*

ModSecurity

- Web Application Firewall
- Runs Right Inside Apache
 - Can see SSL session content
- Rule-based request filtering
- ...

ModSecurity Filter

```
# Accept only digits in content length
#
SecRule REQUEST_HEADERS:Content-Length "!^\d+$" \
    "deny,log,auditlog,status:400, \
    msg:'Content-Length HTTP header is not numeric', \
    severity:'2',id:'960016', \
    tag:'PROTOCOL_VIOLATION/INVALID_HREQ'"
```

Case Study

apache.org, August 2009

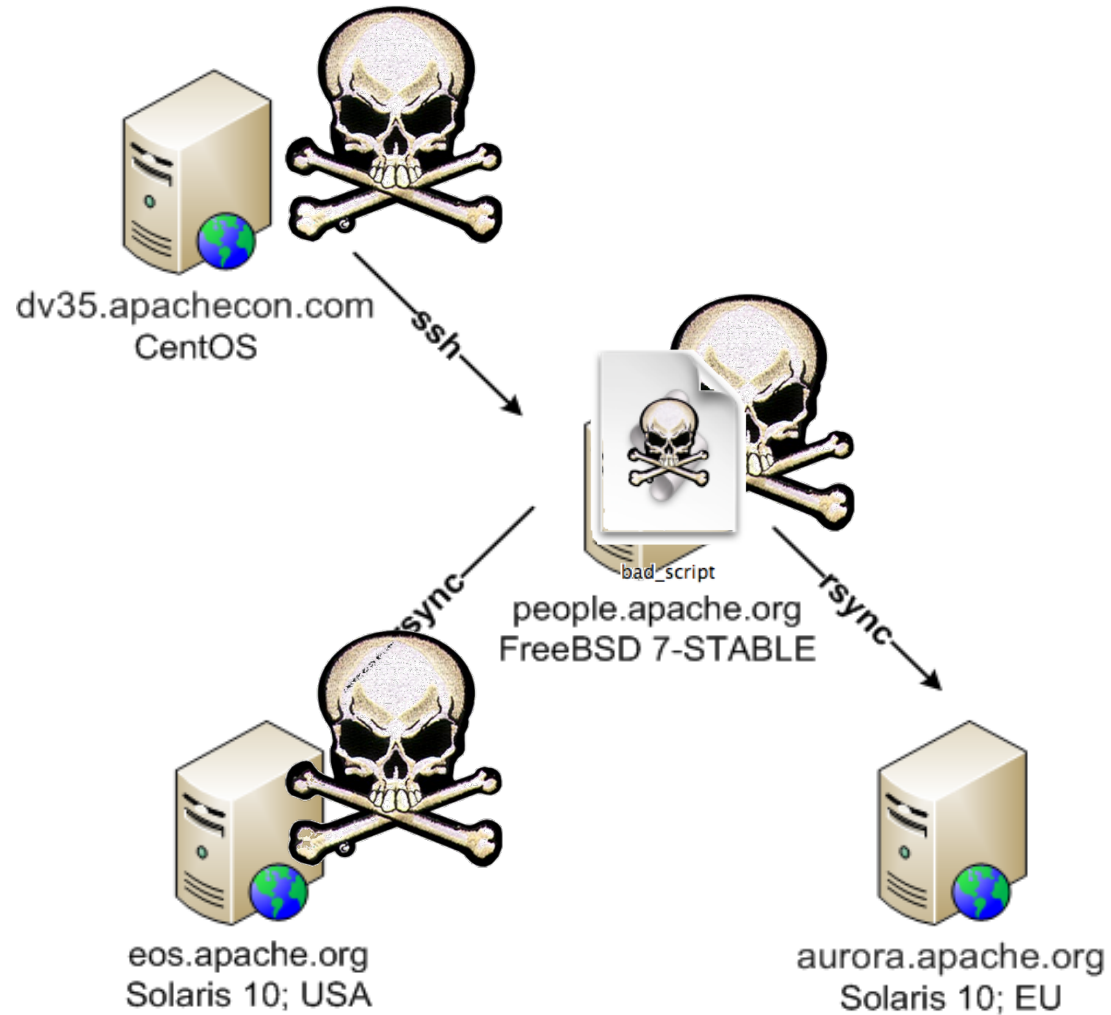
THALES



The Incident

- Apachecon.com rooted
- ssh tunnel to people.apache.org
- Malware served from apache.org servers

apache.org Network



Response

- Shut down affected servers
- Rolled back ZFS Snapshot
- Rebuilt apachecon.com

Changes

- Require One-Time Passwords
- Better ssh key management
- Remove ExecCGI
- Improve content management

https://blogs.apache.org/infra/entry/apache_org_downtime_report

Software and Libraries

- Be on Announcements lists
- Update as needed
- Consider packages