INFORMATION SECURITY SearchSecurity.com INFORMATION SECURITY DECISIONS

Case Studies: Mapping Products to Compliance

Vik Phatak
CEO
NSS Labs

Vik Phatak, CEO, NSS Labs

- Expert on vulnerability management and threat protection.
- Served as CTO for Trustwave (ATW), the world’s largest PCI assessor.
- Founded Lucid Security and developed one of the leading IPS appliances for enterprises.
- Global Manager of Enterprise Internet and Security Services at Teleflex, a publicly-traded global manufacturing company.
- Co-founder of Intermedia Sciences Group, Inc., a security consulting firm.

NSS Labs

- A leading independent security product testing and certification lab.
- Performs product feature validation testing for PCI DSS requirements
- Tests & certifies firewalls, Network & Host IPS, UTM, Wireless, PKI / Encryption, DLP, Vulnerability Scanner, more.
- Largest security & performance testing lab in the world.

Agenda

- **Approaches Review – Mapping compliance to technology choice**
- **Case studies**
  - Retail organization - PCI
  - Healthcare - HIPAA + PCI
  - Manufacturing - SOX

Approaches Review

- Aim for security and achieve compliance (gap analysis, multiple compliance reqs?)
- Know where your data is
- Determine protection requirements
- Limit scope (data flows, retention)
- Products, People or Processes
- Seek answers from vendors

Selecting The Right Products

Information Security Products are tools

- **Different products solve different problems**
  - Products fulfill specific purposes – You don’t expect your screwdriver to saw wood
  - Multi-function tools (i.e. Swiss army knife) do lots of things, but are not usually best at solving a specific problem
  - It is okay to have a favorite tool… just don’t expect it to be the only tool you will need

RM1

Selecting The Right Products

No product can MAKE you compliant…

…but the wrong products can impede your compliance efforts

Slide 6

RM1 Like the gist, hate the text.
what concretely are we saying.

be able to DEFEND your choices?

Rick, 3/10/2008

Case Study – PCI DSS

PCI Compliance

- **Retail Organization**
  - Privately Held
    - 200 storefronts
    - 3 regional centers
    - 1 Corporate HQ
  - Technologies Required:
    - Firewall
    - IDS/IPS
    - AV
    - Encryption (data-in-motion)
    - Encryption (data-at-rest)
    - Identity Management
    - Log Management

Selecting The Right Products

- **Firewalls**
  - Separate Inside (trusted) from outside (un-trusted)
  - Traditionally Routing between Internal, External & DMZ networks
  - Used to limit Access to/from a network or systems on the network = Access Control
  - Operate at lower layers (IP, TCP, UDP, etc.)
  - Good at enforcing access. Not good at catching attacks.
  - Low maintenance & upkeep
  - Low granularity of control (control of protocols, not content)

Selecting The Right Products

- **What firewall requirements are we faced with?**
  - PCI DSS v1.1 Requirement #1 = Install & Maintain a firewall to protect cardholder data
- **Do they all "Segment"?**
  - Some firewalls only segment Internal from External despite multiple NICs, while others allow you to create logically separate segments (one per NIC).
  - Per-domain administration?
  - How are you planning on using the firewall?
- **Does the firewall encrypt all non-console administrative access?**
- **Does the firewall log all changes and provide a robust audit trail?**

Selecting The Right Products

- **IDS/IPS**
  - “Deep Inspection” = look into the payload of the traffic
  - High Maintenance & Upkeep
  - Good at catching known attacks (exploits) against systems with vulnerabilities
  - Different brands/manufacturers have different strengths
    - Client Protection (Web Browsers, E-Mail Clients, etc.)
    - Server Protection (Web Servers, E-Mail Servers, etc.)
    - Internal Applications (File & Print, DB, etc.)
    - Application Vendors (Microsoft, Sun, Open Source)
    - Protocols – HTTP, HTTPS, SMTP, IMAP, Exchange, LDAP, DNS, RPC, NetBios, etc.
  - Some Manufacturers: ***BlueLane, Cisco, IBM/ISS, Juniper, McAfee, SecureComputing, Sourcefire, TippingPoint, Third Brigade, TrustWave***

PCI Compliance

- **Large Financial Institution & IDS/IPS**
  - PCI DSS v1.1 – Requirement 11.4:

“Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.”

  - Claimed Firewall with “deep inspection” fulfilled IDS/IPS requirement because product vendor told them it would…
  - It was determined that the firewall with “deep inspection” did not meet compliance requirements because it did not adequately protect the systems in question (E-Commerce Servers)

11.1: Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

PCI Compliance

Lesson Learned?

It is about a product’s ability to perform the necessary functions based upon how / where it is being used.

“Appropriate Usage”

The same firewall with deep inspection may have been appropriate to protect a retail storefront IF it was good at protecting against client attacks (IE, Firefox, Adobe, etc.)

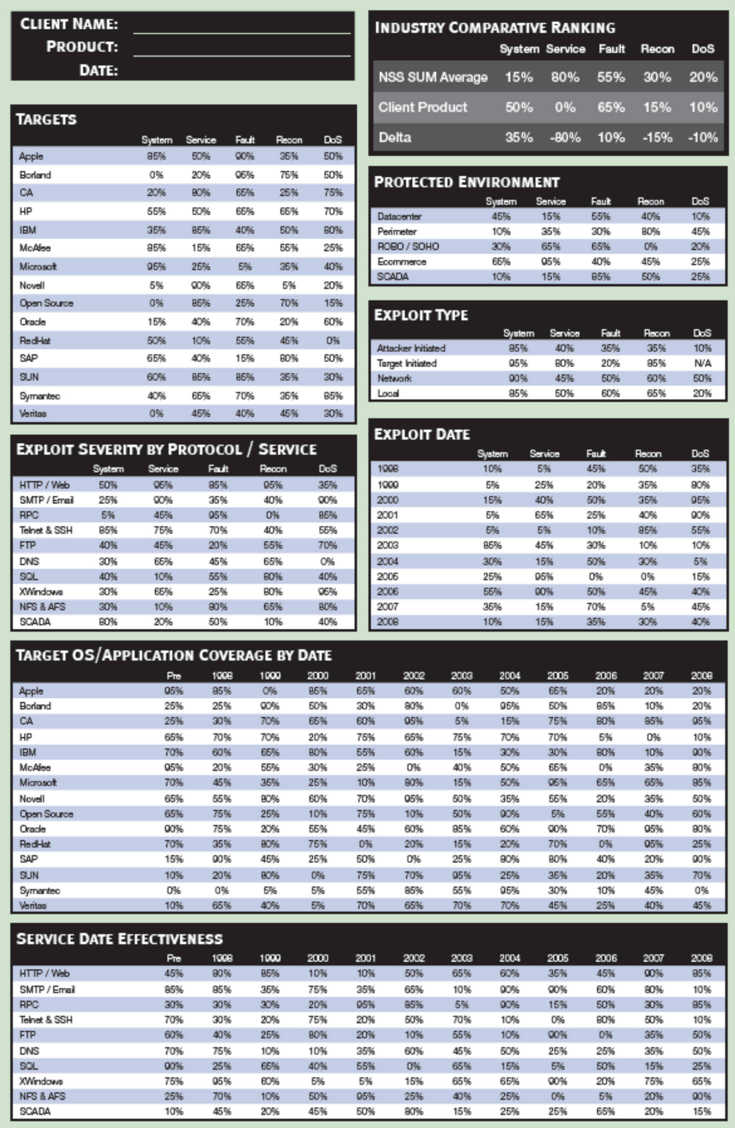
Selecting The Right Products

- **IDS/IPS**
  - Host IPS
    - Strength is in stopping complex attacks that may get past other security
    - System Resource Intensive
    - Cannot stop attacks that compromise OS at a lower layer/before HIPS (i.e. NIC Drivers)
  - Network IPS
    - Good at stopping worms and fast moving attacks
    - Good at protecting against known vulnerabilities
    - Not good at stopping attacks against custom (web) apps

Selecting The Right Products

Common Protection Requirements

	Attacker Initiated	Client/Target Initiated
Retail Storefront		✓
Corporate Perimeter	✓	✓
E-Commerce Datacenter	✓	
Internal Datacenter	✓	



Client Name: ______________________
Product: ______________________
Date:

Industry Comparative Ranking

	System	Service	Fault	Recon	DoS
NSS SUM Average	15%	80%	55%	30%	20%
Client Product	50%	0%	65%	15%	10%
Delta	35%	-80%	10%	-15%	-10%

Targets

	System	Service	Fault	Recon	DoS
Apple	85%	60%	90%	35%	50%
Borland	0%	20%	95%	75%	50%
CA	20%	80%	65%	25%	75%
HP	55%	60%	65%	65%	70%
IBM	35%	85%	40%	50%	80%
McAfee	85%	15%	65%	55%	25%
Microsoft	95%	25%	5%	35%	40%
Novell	5%	90%	65%	5%	20%
Open Source	0%	85%	25%	70%	15%
Oracle	15%	40%	70%	20%	60%
RedHat	50%	10%	55%	45%	0%
SAP	65%	40%	15%	80%	50%
SUN	60%	85%	85%	35%	30%
Symantec	40%	65%	70%	35%	85%
Veritas	0%	45%	40%	45%	30%

Protected Environment

	System	Service	Fault	Recon	DoS
Datacenter	45%	15%	55%	40%	10%
Perimeter	10%	35%	30%	80%	45%
ROBO / SOHO	30%	65%	65%	0%	20%
Ecommerce	65%	95%	40%	45%	25%
SCADA	10%	15%	85%	50%	25%

Exploit Type

	System	Service	Fault	Recon	DoS
Attacker Initiated	85%	40%	35%	35%	10%
Target Initiated	95%	80%	20%	85%	N/A
Network	90%	45%	50%	60%	50%
Local	85%	50%	60%	65%	20%

Exploit Severity by Protocol / Service

	System	Service	Fault	Recon	DoS
HTTP / Web	50%	95%	85%	95%	35%
SMTP / Email	25%	90%	35%	40%	90%
RPC	5%	45%	95%	0%	85%
Telnet & SSH	85%	75%	70%	40%	55%
FTP	40%	45%	20%	55%	70%
DNS	30%	65%	45%	65%	0%
SQL	40%	10%	55%	80%	40%
XWindows	30%	65%	25%	80%	95%
NFS & AFS	30%	10%	80%	65%	80%
SCADA	80%	20%	50%	10%	40%

Exploit Date

	System	Service	Fault	Recon	DoS
1998	10%	5%	45%	50%	35%
1999	5%	25%	20%	35%	80%
2000	15%	40%	50%	35%	95%
2001	5%	65%	25%	40%	90%
2002	5%	5%	10%	85%	55%
2003	85%	45%	30%	10%	10%
2004	30%	15%	50%	30%	5%
2005	25%	95%	0%	0%	15%
2006	55%	90%	50%	45%	40%
2007	35%	15%	70%	5%	45%
2008	10%	15%	35%	30%	40%

Target OS/Application Coverage by Date

	Pre	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Apple	95%	85%	0%	85%	65%	60%	60%	50%	65%	20%	20%	20%
Borland	25%	25%	90%	50%	30%	80%	0%	95%	50%	85%	10%	20%
CA	25%	30%	70%	65%	60%	95%	5%	15%	75%	80%	85%	95%
HP	65%	70%	70%	20%	75%	65%	75%	70%	70%	5%	0%	10%
IBM	70%	60%	65%	80%	55%	60%	15%	30%	30%	80%	10%	90%
McAfee	95%	20%	55%	30%	25%	0%	40%	50%	65%	0%	35%	80%
Microsoft	70%	45%	35%	25%	10%	80%	15%	50%	95%	65%	65%	85%
Novell	65%	55%	80%	60%	70%	95%	50%	35%	55%	20%	35%	50%
Open Source	65%	75%	25%	10%	75%	10%	50%	90%	5%	55%	40%	60%
Oracle	90%	75%	20%	55%	45%	60%	85%	60%	90%	70%	95%	80%
RedHat	70%	35%	80%	75%	0%	20%	15%	20%	70%	0%	95%	25%
SAP	15%	90%	45%	25%	50%	0%	25%	80%	80%	40%	20%	90%
SUN	10%	20%	80%	0%	75%	70%	95%	25%	35%	20%	35%	70%
Symantec	0%	0%	5%	5%	55%	85%	55%	95%	30%	10%	45%	0%
Veritas	10%	65%	40%	5%	70%	65%	70%	70%	45%	25%	40%	45%

Service Date Effectiveness

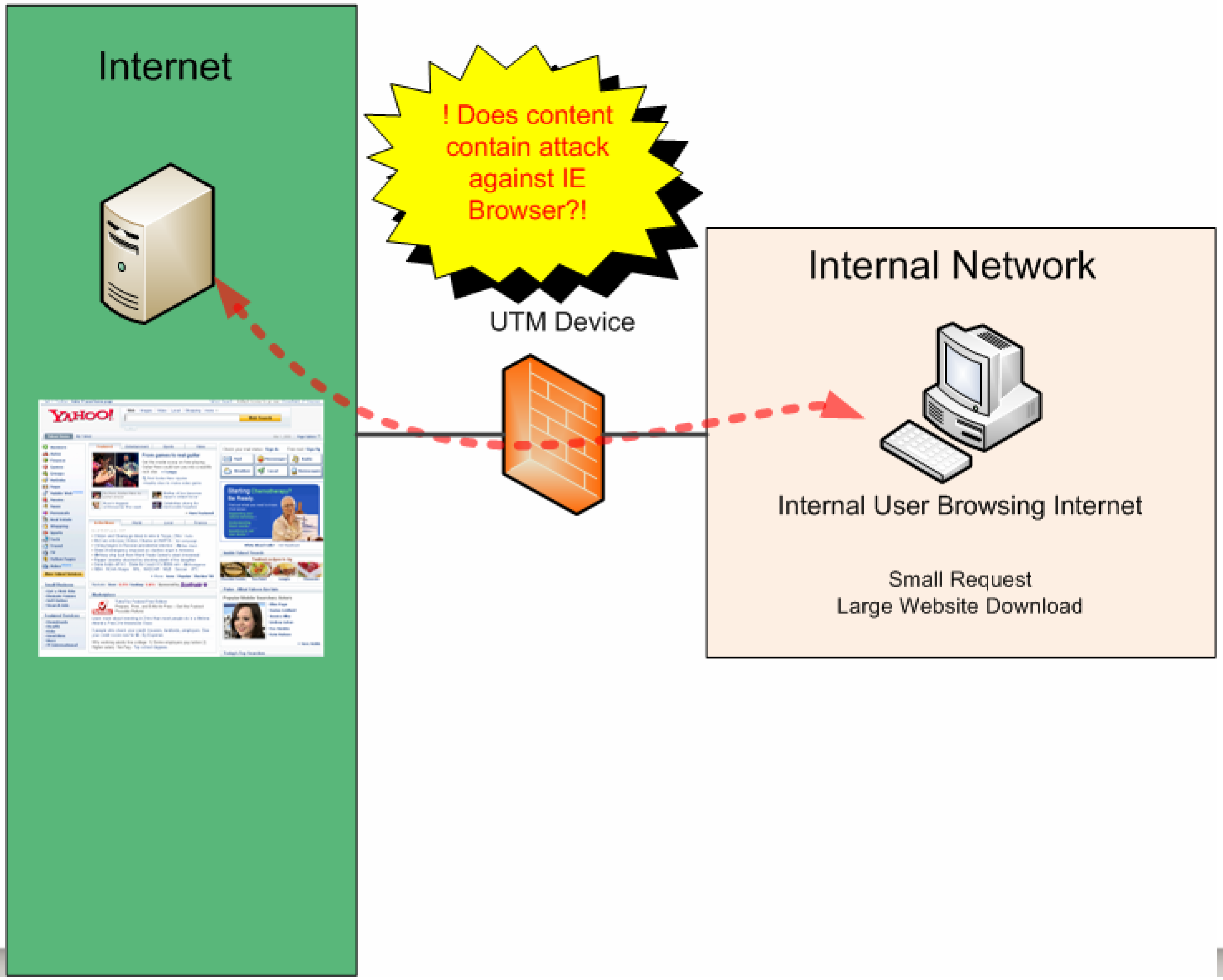
	Pre	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
HTTP / Web	45%	80%	85%	10%	10%	50%	65%	60%	35%	45%	90%	85%
SMTP / Email	85%	85%	35%	75%	35%	65%	10%	90%	90%	60%	80%	10%
RPC	30%	30%	30%	20%	95%	85%	5%	90%	15%	50%	30%	85%
Telnet & SSH	70%	30%	20%	75%	20%	50%	70%	10%	0%	80%	50%	10%
FTP	60%	40%	25%	80%	20%	10%	55%	10%	90%	0%	35%	50%
DNS	70%	75%	10%	10%	35%	60%	45%	50%	25%	25%	35%	50%
SQL	90%	25%	65%	40%	55%	0%	65%	15%	5%	50%	15%	25%
XWindows	75%	95%	60%	5%	5%	15%	65%	65%	90%	20%	75%	65%
NFS & AFS	25%	70%	10%	50%	95%	25%	40%	25%	0%	5%	20%	90%
SCADA	10%	45%	20%	45%	50%	80%	15%	25%	25%	65%	20%	15%

Selecting The Right Products

- **UTM**
  - Multi-Function Device: FW + VPN + IPS + WF + AV
  - Evolved out of Firewalls – firewall usually strong
  - Decisions were made about what to emphasize – no product can be all things
    - Perimeter Devices - often cannot protect applications in the Core
    - Good at preventing people from bypassing Gateway AV (HTTP AV)
  - Different brands/manufacturers have different strengths
    - Client Protection (Web Browsers, E-Mail Clients, etc.)
    - Server Protection (Web Servers, E-Mail Servers, etc.)
    - Application Vendors (Microsoft, Sun, Open Source)
    - Protocols – HTTP, HTTPS, SMTP, IMAP, Exchange, DNS, RPC, etc.
  - Some Manufacturers: Cisco, Fortinet, IBM/ISS, Juniper, SecureComputing, 3Com/TippingPoint

Remote Office / Branch Office / Retail Storefront

No DMZ or servers facing the Internet



Internet

! Does content contain attack against IE Browser?!

UTM Device

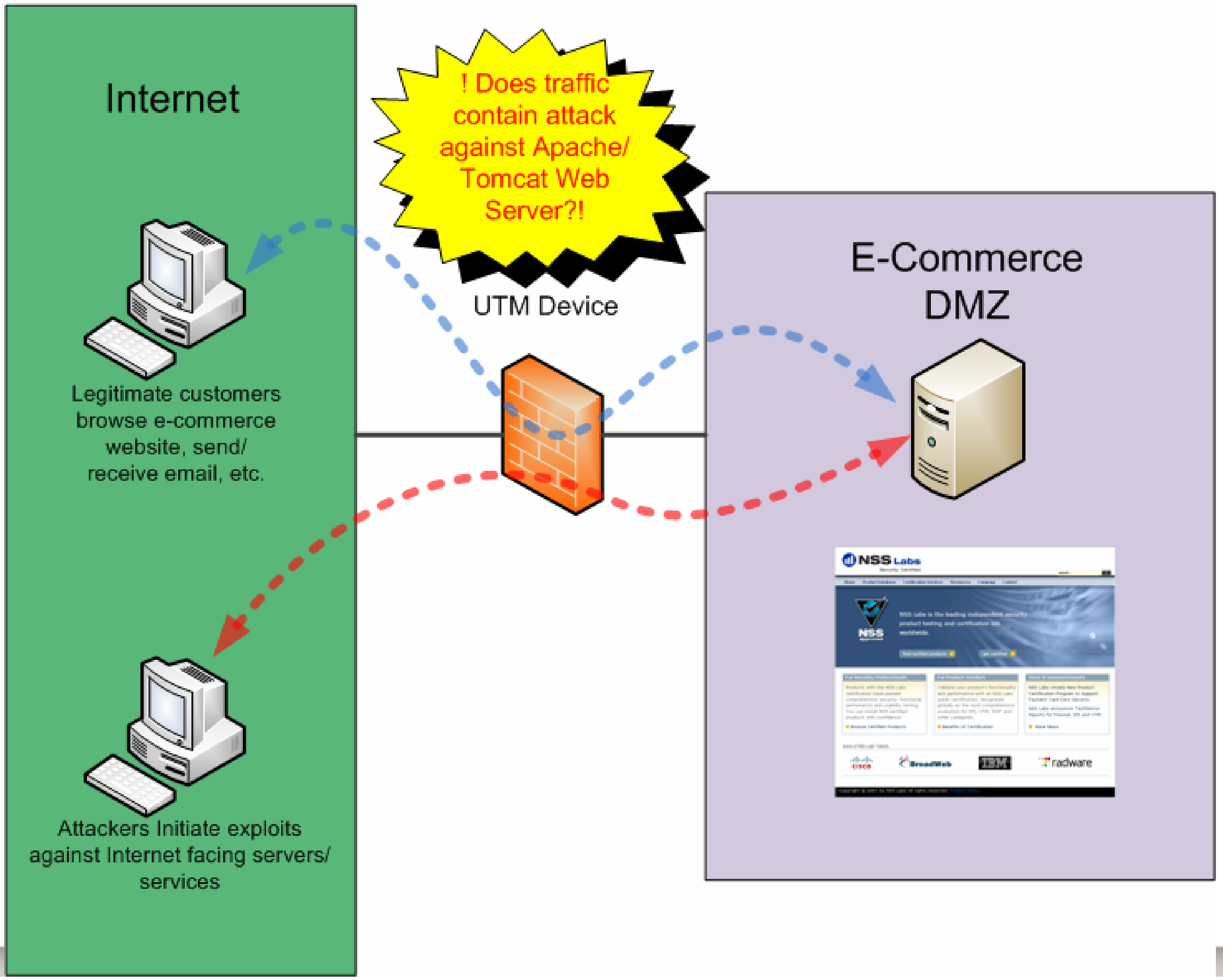
Internal Network

Internal User Browsing Internet

Small Request
Large Website Download

E-Commerce Datacenter

No client traffic initiated from DMZ – All traffic initiated from outside of the network



Internet

Legitimate customers browse e-commerce website, send/ receive email, etc.

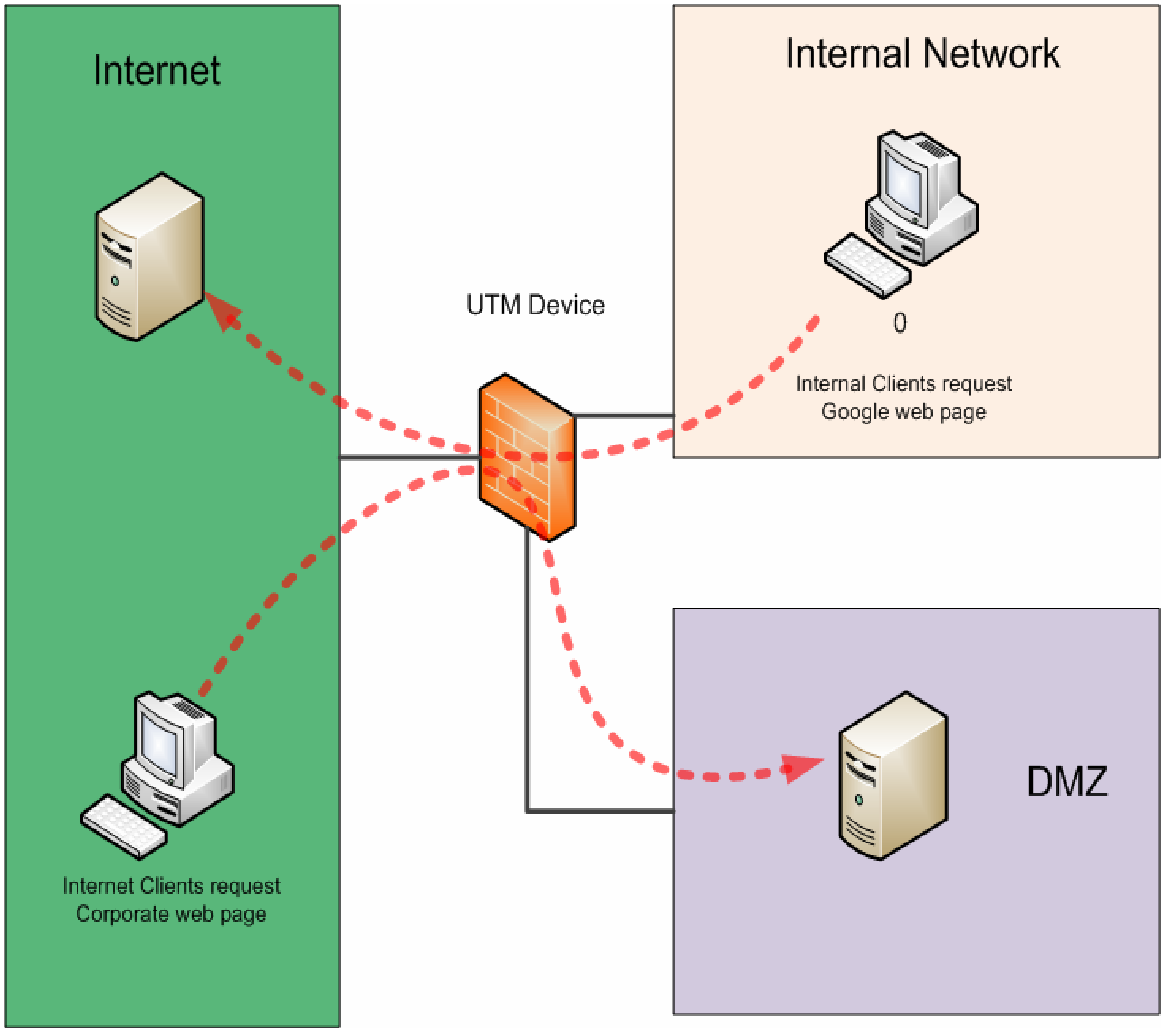
Attackers Initiate exploits against Internet facing servers/ services

! Does traffic contain attack against Apache/ Tomcat Web Server?!

UTM Device

E-Commerce DMZ

Typical Traffic Flow



Where is UTM Appropriate?

- **PCI says nothing specifically about UTMs**
- **However, PCI does mention firewall, IDS/IPS, AV, & Encryption of data-in-motion (VPN)**
- **UTMs are not generally not “best of breed”**
- **Must examine the threat & risk dynamics:**
  - UTMs good at protecting Internet Services
    - Retail Storefront (client protection)
    - Corporate Perimeter (both client & server)
    - SIMPLE E-Commerce sites
  - UTMs NOT good at protecting INTERNAL services (SQL, NetBios, etc.)

"Web-facing" Application Security

- **6.5 Secure coding**
  - OWASP Top 10 is a great start but… more than 10 significant vulnerability types in web apps
  - Other resources & tools
- **6.6 Code review or WAF**
  - Mandatory as of June 30, 2008

Application Security Tools

Vulnerability Scanner (ext)	• Systems • Services
Web App Firewall	• Protects Applications, databases • OWASP Top 10 • Usually in DMZ
Web App Vulnerability Scanner	• Scans Web Applications externally for flaws • Highly specific
Application Code Scanner	• Programmatic analysis of source/binary code. Used to speed up a code review.
Code Review	• Manual process of reading source code. Code Scanner used to make process more efficient. • DSS 6.6 – best practice until June 30, 2008

Vulnerability Assessment (Scanner)

- Look for network and “common” application vulnerabilities – IIS, Apache, etc.
- Usually look for circumstantial evidence
  - Don’t run actual exploits – nobody wants their systems to be crashed or compromised
- Used as an information gathering tool
- Not conclusive, but are a good measuring tool nonetheless
- Some Manufacturers: IBM/ISS, N-Circle, Qualys, Saint, Tenable (Nessus)

Web App Vulnerability Scanner

- **Look for flaws in Web Applications**
  - Look deeper and more thoroughly than traditional Vulnerability Scanners
  - Detect unique flaws within Web Applications (i.e. SQL Injection, Form Validation errors, etc.)
- **Used as an information gathering tool**
- **Can be high maintenance - Some products are prone to false positives**
- **Will be required by June 30, 2008**
- **Some Manufactures: Appscan, Cenzic, NT Objectives, SPI Dynamics (HP), Watchfire (IBM), Whitehat**

Web App Firewall

- **Compensating Control for PCI DSS 6.6 (vs. code review). June 30, 2008**
- **Enforce "positive" rules for Web Applications**
  - Firewall for Layer-7
  - Look deeper than traditional Firewalls
  - Prevent flaws within Web Applications from being exploited (i.e. SQL Injection, Form Validation errors, etc.)
- **Unforgiving: Only content you define as acceptable is allowed**
- **Some Manufactures: Barracuda, Breach, Citrix, F5, Fortify, eEye, Imperva, Mod Security, Sanctum**

App Code Scanner (Static analysis)

- **Examine the source code of Applications**
  - Some can even examine binaries (Veracode)
  - Look for coding flaws
- **Used as an information gathering tool**
- **Can be high maintenance**
- **Some Manufactures: Appscan, Cenzic, NT Objectives, SPI Dynamics (HP), Watchfire (IBM), Whitehat**
- **Not required by any Compliance regime, but it’s inefficient to perform a code review and not use an App Code Scanner**

Anti-Malware (Anti-Virus)

- **Host**
  - Strength is in stopping complex attacks that may get past other security
  - Can be System Resource Intensive
  - Cannot stop attacks that compromise OS at a lower layer/before AM/AV (i.e. NIC Drivers)
  - Varying effectiveness (Strengths/Weaknesses) by product
- **Network/Gateway**
  - Email is not time-sensitive
  - May be bypassed by someone using webmail
  - Centralized – good at seeing patterns & being proactive on a macro level

Case Study - HIPAA + PCI

HIPAA + PCI Compliance

- **Healthcare Organization**
  - Privately Held
    - 4 Hospitals
    - 30 medical centers (doctor’s offices)
    - 1 Corporate HQ
  - Technologies Required:
    - Firewall
    - IDS/IPS
    - AV
    - Encryption (data-in-motion)
    - Encryption (data-at-rest)
    - Data Leak Prevention (DLP)

HIPAA + PCI Compliance

- **Data Leak Prevention (DLP)**
  - Requires a lot of ‘care & feeding’ to minimize false negatives & false positives
  - Good at stopping “Gilligan” but not “the Professor
  - Content:
    - Simple regex?
    - Context aware?
    - Partial fragment recognition?
  - Host: Good granular control, but resource intensive
  - Network: Good for specific data (Credit Card & Social Security numbers)

HIPAA + PCI Compliance

- **Encryption – data-in-motion**
  - Network-level tunneling (L2 and L3)
    - IPSec, some proprietary
  - Application-protocol-level tunneling
    - SSL VPN
  - Application-native crypto
  - Key management challenges – how does solution do provisioning, revocation?
    - Especially if multiple technologies in use
  - How does the solution deploy, protect and store key material / certificates? Concentration of risk → audit risk
  - How is access control / key deployment auditable?
  - Impact on network latency and throughput?

HIPAA + PCI Compliance

- **Encryption – data-at-rest**
  - Full-disk encryption (hardware-level, driver-level)
  - File-level encryption (OS or third-party)
  - Application-native crypto – database, file
  - Key management challenges – provisioning, revocation
  - Key management challenges – how does solution do provisioning, revocation?
    - Especially if multiple technologies in use
  - How does the solution deploy, protect and store key material / certificates? Concentration of risk ➔ audit risk
  - How is access control / key deployment auditable?
  - Impact on I/O latency and throughput
    - Especially in the context of bulk storage – backup tapes

HIPAA + PCI Compliance

- **Encryption deployment example**
  - Healthcare provider implemented DBMS-level encryption
  - Disqualified as a mitigating control due to use of hard-coded keys
  - Key management is the hard part!

Case Study - SOX

SOX Compliance

- **Mid-Sized Telecommunications Provider**
  - Publicly Held
    - 15 corporate offices, 400+ POPs, 1000+ retail stores
    - 8000 employees
  - Technologies Required:
    - Firewall
    - IDS/IPS
    - AV
    - Encryption (data-in-motion)
    - Encryption (data-at-rest)
    - Identity Management
    - Log Management / SIM / SEM

SOX Compliance

- **Log Management / SIM / SEM**
  - SOX 404(a) requirement: “formal program” to retain, consolidate, and review log activity for all in-scope systems and devices including include monitoring of change requests and authorization, user account authorizations and application and system access controls
  - What is breadth of device support (software, network, security? – evaluate relative to unique environment
  - Data acquisition speed?
  - Agentless vs. agent-based?
  - Log storage – local, central, hierarchical/cached?
  - Speed of raw data retrieval?
  - Flexibility of Reporting (canned, custom), and speed of reporting
  - Correlation based on rates/counts/vulns/assets → quality of alerting
  - Actionability of alerting - reduction of false positives
  - Summarization (alert collapsing) – reduction of noise

SOX Compliance

- **Log Management / SIM / SEM**
  - SOX pre-audit situation
    - Log retention and aggregation in place
      - Homebrew solution based on EventLog and Syslog collection
    - Pre-audit testing found adequate control of log *content* to be lacking – no formal process for alerting/review based on real-time or retained log data

SOX Compliance

- **Identity Management**
  - SOX 404(a) requirement: “adequate internal controls” with respect to user access and privileges
  - What is breadth of available Integration Points? (OS/software/network)
    - Authentication?
    - Granular, app-level authorization?
  - User Provisioning – local/central/hierarchical/delegable?
  - Role-based Management?
  - Entitlement Management capabilities - relative to unique application footprint
  - Identity Audit (IdA) capabilities
    - Access controls, authorization / privileges
    - Positive *and negative* reporting relative to HR systems

SOX Compliance

- **Identity Management**
  - Pre-audit situation
  - IdM in place
    - Major vendor solution
  - Pre-audit testing found adequate control of access rights to be lacking
    - No implementation of negative reporting relative to SAP/HR systems: inability to positively confirm that specific users did *not* have access to certain systems

Summary

- Map compliance requirements into security objectives, and RFPs
- Ensure people & processes can support effective use of products
- Track users & data. Segment to limit scope.
- Determine detailed protection requirements to show justification & set expectations
- If you can’t get answers from vendors it may be a fad