

IT Auditing From the Hackers Perspective



Secure360
May 10, 2010

LarsonAllen[®]
LLP

CPAs, Consultants & Advisors

Introductions

Randy Romes

Brian Johnson

Chris Knight



Logistics

The Lab

Breaks

Restrooms



Topics

- What do we see today?
- Outside → In
 - Web Application Vulnerabilities
 - Email Phishing
- Inside → In
 - Identifying Internal Network Vulnerabilities
 - Common Security Issues



Two Security Reports

- Trends: Sans 2009 Top Cyber Security Threats
 - September 2009
 - Data from over 6,000 Intrusion Prevention Systems
 - Data from over 9,000,000 systems (Qualys scans)
 - <http://www.sans.org/top-cyber-security-risks/>
- Intrusion Analysis: TrustWave
 - January 2010
 - Analysis of 200 investigations
 - Analysis of 1,800 penetration tests
 - <https://www.trustwave.com/whitePapers.php>



SANS 2009 Top Cyber Security Risks

- Analysis of global cyber attack patterns
- Two Primary Issues:
 - Priority One: Client-side software that remains unpatched
 - Priority Two: Internet-facing web sites that are vulnerable



SANS - Client Side Vulnerabilities

- Client side vulnerabilities
 - Missing operating system patches
 - Missing application patches
 - ◇ Apple QuickTime
 - ◇ Java Vulnerabilites
 - ◇ MS Office Applications
 - ◇ Adobe Vulnerabilites (PDF, Flash, etc...)
- Objective is to get the users to “Open the door”



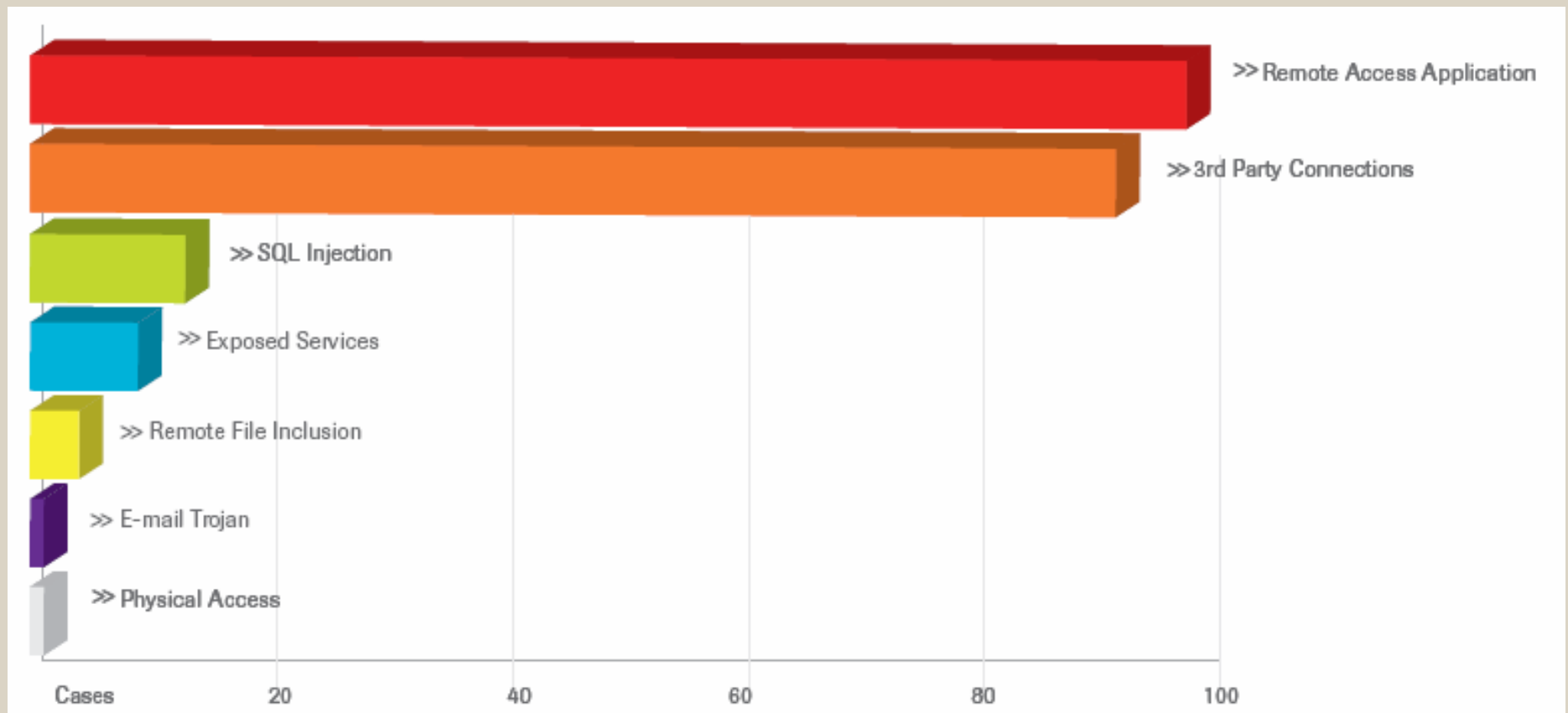
SANS - Vulnerable Web Sites

- Two main avenues for exploiting web applications:
 - Brute force password guessing
 - ◇ MS SQL, FTP, and SSH
 - Web application attacks
 - ◇ SQL Injection, Cross-site Scripting, and PHP File Include
- Objective is to:
 - Compromise weak credentials...
 - Compromise the website to gain control, OR
 - Place malicious code for later “drive-by downloads”



TrustWave – Intrusion Analysis Report

Top Methods of Entry Included:



TrustWave – Intrusion Analysis Report

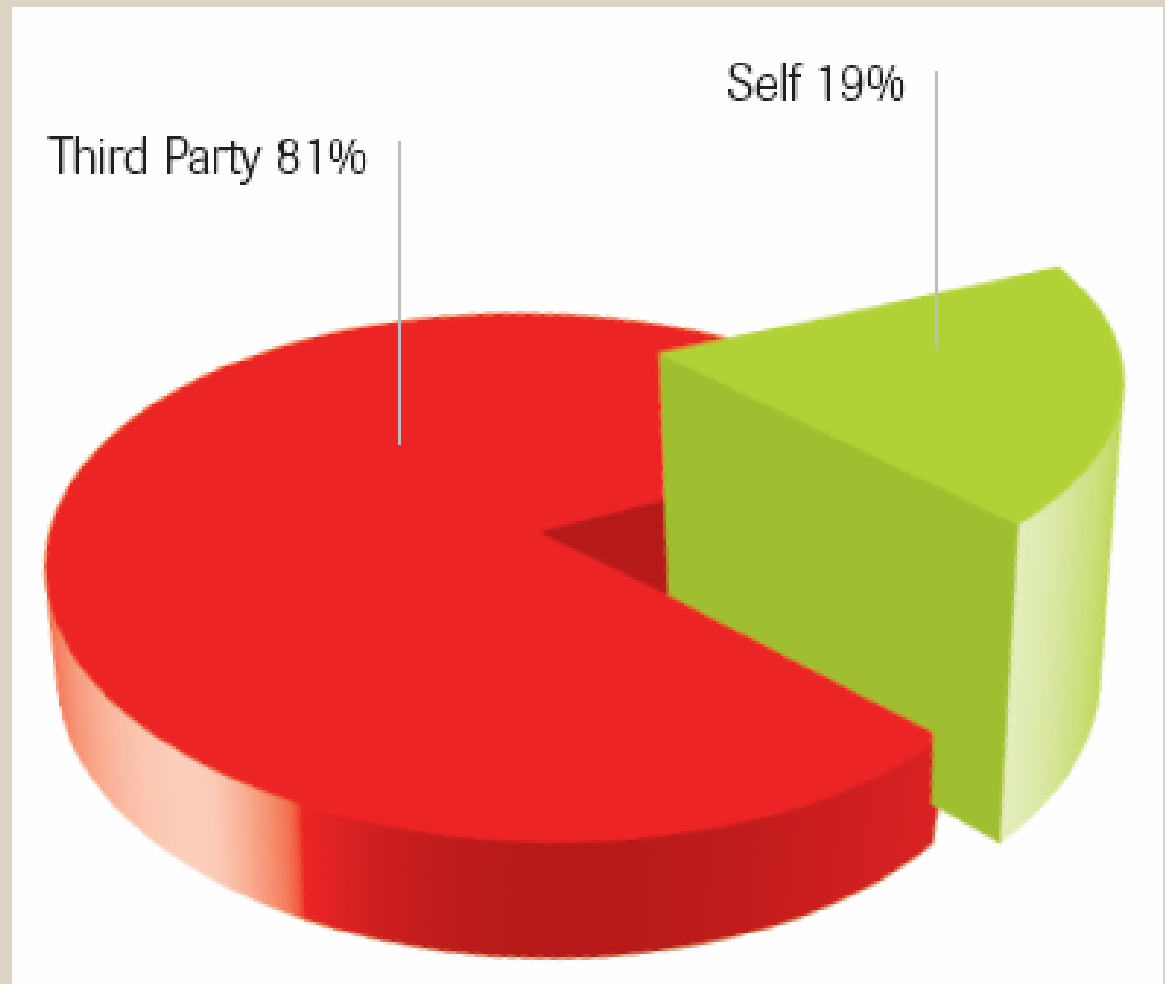
Top Methods of Entry Included:

- Remote Access Applications [45%]
 - **Default vendor supplied or weak passwords [90%]**
- 3rd Party Connections [42%]
 - MPLS, ATM, frame relay
- SQL Injection [6%]
 - Web application compromises [90%]
- Exposed Services [4%]
- Remote File Inclusion [2%]
- Email Trojan [<1%]
 - 2 recent Adobe vulnerability cases
- Physical Access [<1%]



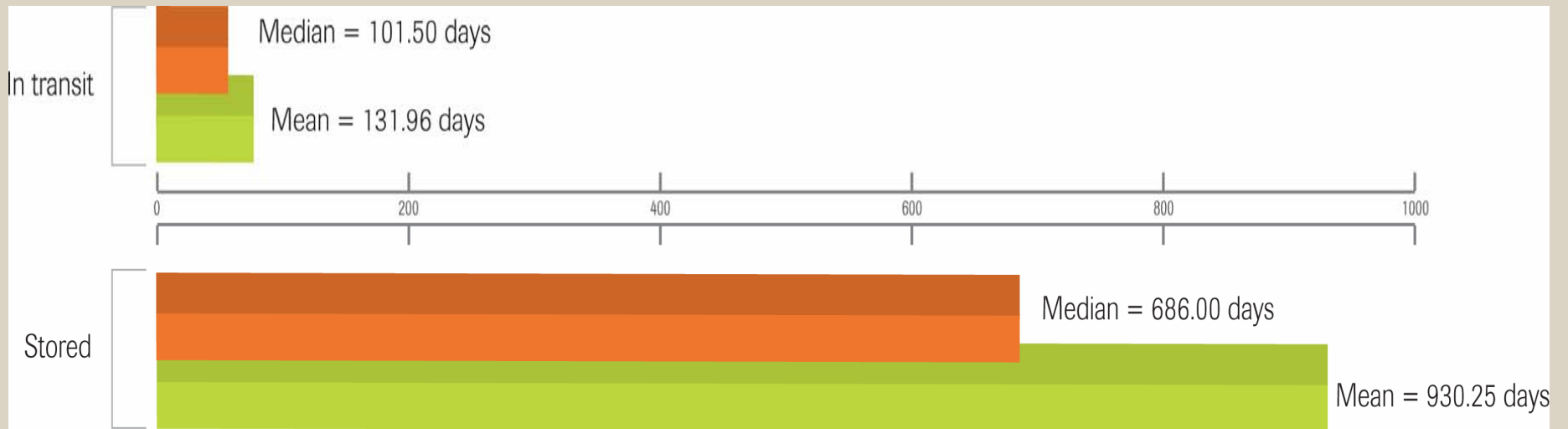
TrustWave – Intrusion Analysis Report

- Most of the compromised systems were managed by a third party...



TrustWave – Intrusion Analysis Report

- Incident Response – Investigative Conclusions
- Window of Data Exposure



Once inside, attackers have very little reason to think they will be detected...



“Compliance” Risk

- PCI - DSS
- HIPAA/HITECH
- GLBA
- A wide variety of State Laws

http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State

- These affect most organizations either directly or indirectly



Customer Sues Bank

- **Michigan company is suing its bank** after cyber thieves allegedly made **fraudulent wire transfers totaling US \$560,000**.
- Alleges that the bank had inadequate security practices and failed to take note of indications that the transactions were suspicious.
- The cyber thieves obtained the banking account credentials through a phishing email sent to an employee at EMI.
- The transactions **wired funds to bank accounts in Russia, Estonia, Scotland, Finland, China and the US** and were withdrawn soon after the deposits were made.
- Alleges Comerica's security practices made EMI vulnerable to the phishing attack. The bank allegedly routinely sent its online customers emails with links asking them to submit information to renew digital certificates.
- Also alleges that the bank failed to notice unusual activity. **Until the fraudulent transactions were made, EMI had made just two wire transfers ever; in just a three-hour period, 47 wire transfers and 12 transfer of fund requests were made.**
- In addition, after EMI became aware of the situation and asked the bank to halt transactions, the bank allegedly failed to do so until 38 more had been initiated.



Bank Sues Customer

- A Texas bank is suing one of its commercial banking customers following an incident in which the customer lost \$800,000 through [fraudulent ACH transactions](#).
- PlainsCapital Bank, a \$4.4 billion bank headquartered in Dallas, has filed suit against Texas-based Hillary Machinery Inc., following a series of incidents that began last November, **when cyber thieves made a series of ACH transactions that totaled \$801,495 from Hillary Machinery Inc.'s bank account.**
- The bank was able to retrieve about \$600,000 of the money, but **when Hillary subsequently sent a letter requesting that the bank refund the remaining \$200,000**, PlainsCapital responded by filing [the lawsuit](#) in U.S. District Court for the Eastern District of Texas.
- The lawsuit requests that the court certify that PlainsCapital's security was in fact reasonable, and that it processed the wire transfers in good faith. **Documents filed with the court allege that the fraudulent transactions were initiated using the defendant's valid online banking credentials.**



Morning Agenda

- Common Security Issues
“The Low Hanging Fruit”
- Identifying Vulnerable Systems on the Internal Network
“Your Hackers Tool Chest”



Afternoon Agenda

- Identifying Vulnerable Systems on the Internal Network (cont.)
- Web Application Vulnerabilities
“Modern Remote Attack Vectors”

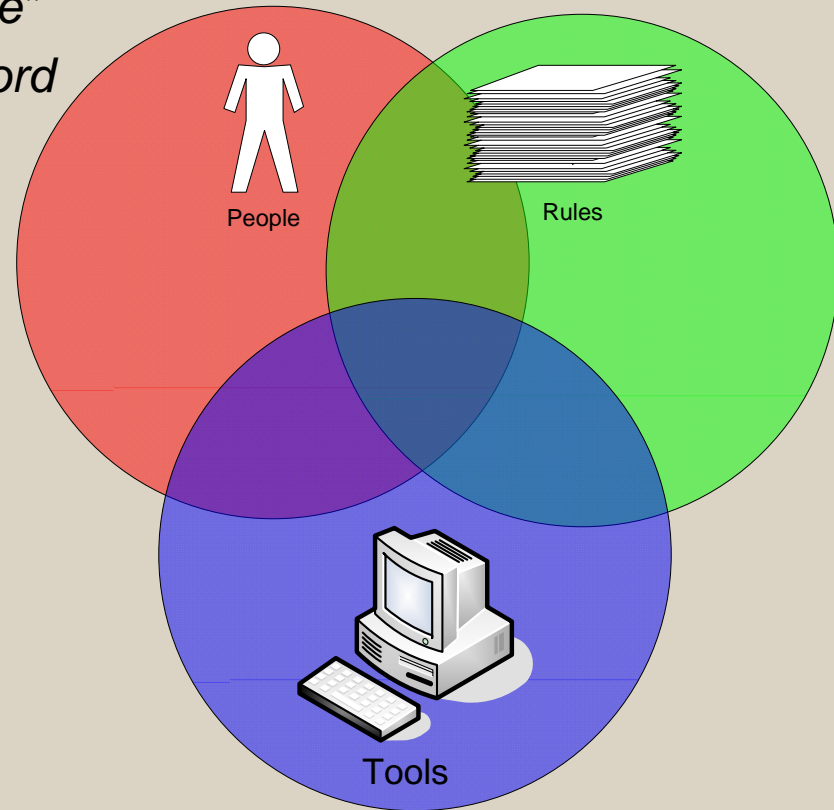


Secure System Defined

“A secure system is one we can depend on to behave as we expect.”

Source: “*Web Security and Commerce*”
by Simson Garfinkel with Gene Spafford

- Confidentiality
- Integrity
- Availability



Security = Culture!!

Security is a **BUSINESS** issue, NOT a technical issue!!

- *Administrative Policies / Procedures*
- *Physical Access Controls*
- *Technical Security Controls*



Questions

Thank You!

Randy Romes, CISSP, MCP

Principal, Information Security Services

612-397-3114

rromes@larsonallen.com

