

Web 2.0 – Security Recommendations

Ken Kaminski

Security Architect – Northeast US Enterprise

CISSP, GCIA, GCFA

Cisco Systems



Agenda

- Reputation Services
- Web application security – Secure Coding and Web Application Firewalls
- Perimeter Web Gateway
- End-user security (social engineering)
- Client Security
- Monitoring and Botnet Detection

Solutions



Fighting the Last War



A decorative footer area with a circular, abstract pattern in shades of yellow, green, and blue. The pattern consists of overlapping circles and lines, creating a textured, organic feel. In the bottom right corner, there is a horizontal line of small, colorful dots. Below this line, the text "welcome to the human network." is written in a clean, sans-serif font. To the right of the text is the Cisco logo, which includes the word "CISCO" in a bold, sans-serif font and the word "welcome" in a smaller font below it. The overall design is modern and tech-oriented.

But I've Got Firewalls, IPS, Anti-Virus and URL Filtering?!

- Firewalls don't stop port 25 or user requests for protocol-compliant HTTP(S)
- IPS does not stop social engineering
- New vulnerabilities continually
- Anti-virus is shockingly ineffective due to mutating viruses
 - 390 LdPinch security signatures since original in 2003
 - More than 30,000 Bagel variants
- URL filtering can't categorize an infinite number of sources
- URL filtering can't protect from legitimate sites being hacked
- End-users roam
- End-users choose to install, override security
- Once infected, malware hides

welcome to
the human network.



Malware Defeats Anti-Virus Signatures

- Criminals have developed tools to mutate malware to defeat signature-based detection
- At DefCon teams of researchers proved their success yet again
- Seven viruses and two exploits, all well-known, were mutated to defeat anti-virus engines
- Winning time: 2 hours, 25 minutes

Virus Sophistication Beats AV

- 182 virus tools at VX Heavens website vx.netlux.org
Example: NGVCK (Next Generation Virus Creation Kit)
- Poly/Metamorphic tools create random variants
- Viruses download fresh copy every 24 hours
- Viruses use buddy program to reinstall virus if disinfected

VX Heavens
[Home](#)

Virus Creation Tools (182)
Page: [0][1][2][3][4][5][6][7][8][9]
["INVICTUS" VX Library](#)
[\\$MOOTHIE::s Macro Virus Creator 2000](#)
[Access Macro Generator](#)
[Acid Flowing Trojan Generator](#)
[Advanced Batch Mutator](#)
[Advanced Steam Trojan Generator](#)


<<prev index next>>

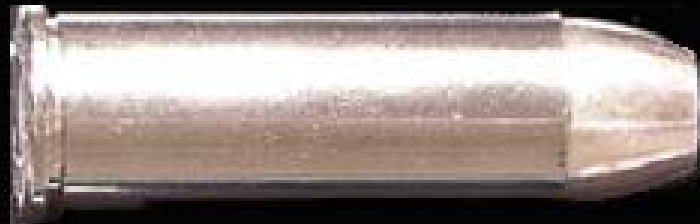
A Quick & Easy Trojan Developing System

Author: Walt DiZnEy

Author's notes: EasyTrojan is a program that enables *ANYONE* to write Ready To Run-Trojan Horses, using a very-easy-to-learn Trojan-Writing-Code. EasyTrojan is not intended to replace "real" programming in the developing of Trojan Horses, but it offers an invaluable help to those who don't know anything about computer languages and want to make Trojans, and also to programmers who are in a hurry and need a Quick-Ready-To-Run Trojan!

Download

Filename	Size	Desc	Date	MD5
 easyt110.zip	23047	[QETDS 1.10]	Dec 1993	a9ca972000641088562807abe152a88c



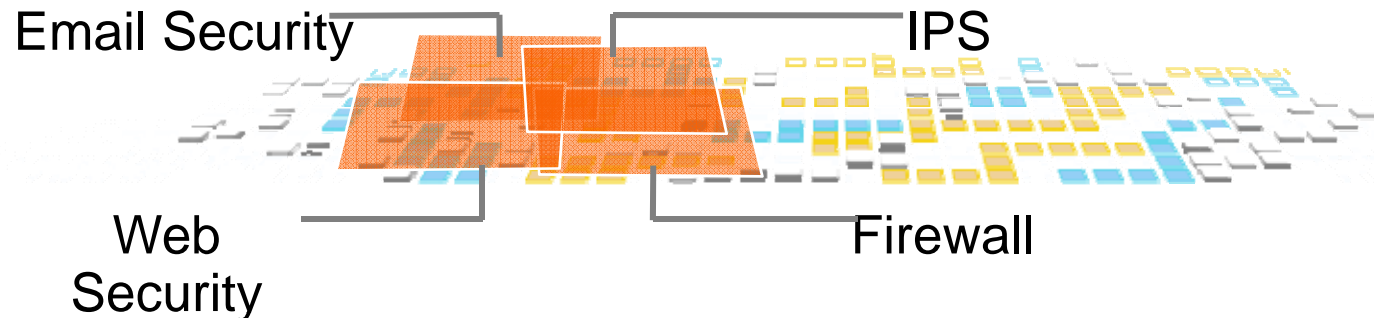
Has anyone seen my silver bullet?

Reputation Services



1. What is Reputation?

or “Is all reputation the same?”



- Reputation is the history of both actions and qualities of a specific IP address or network. This is calculated using some of the hundreds of different types of data found in the Sensor Database.
- For different types of devices, different parameters can mean more or less for the reputation of a device.

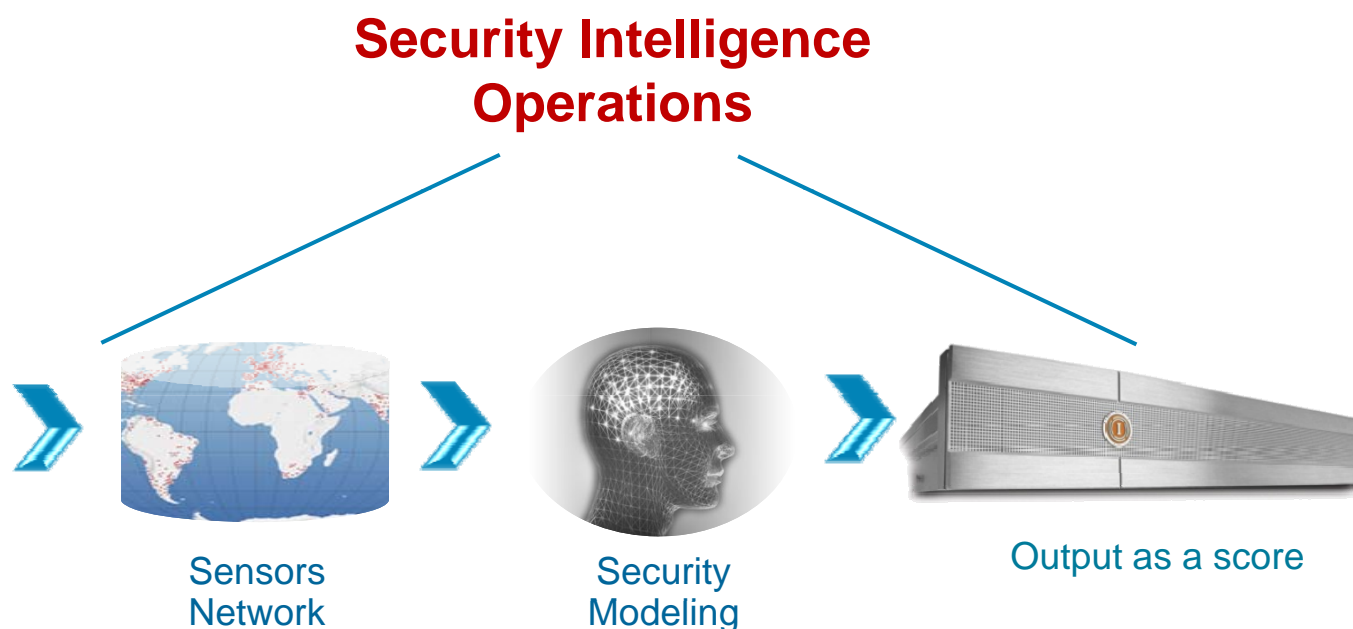
Ex: The fact of sending SPAM is highly relevant to an email reputation device and less so to an IPS sensor.

1. Web Reputation Filters

Predictive, Real-Time Threat Prevention

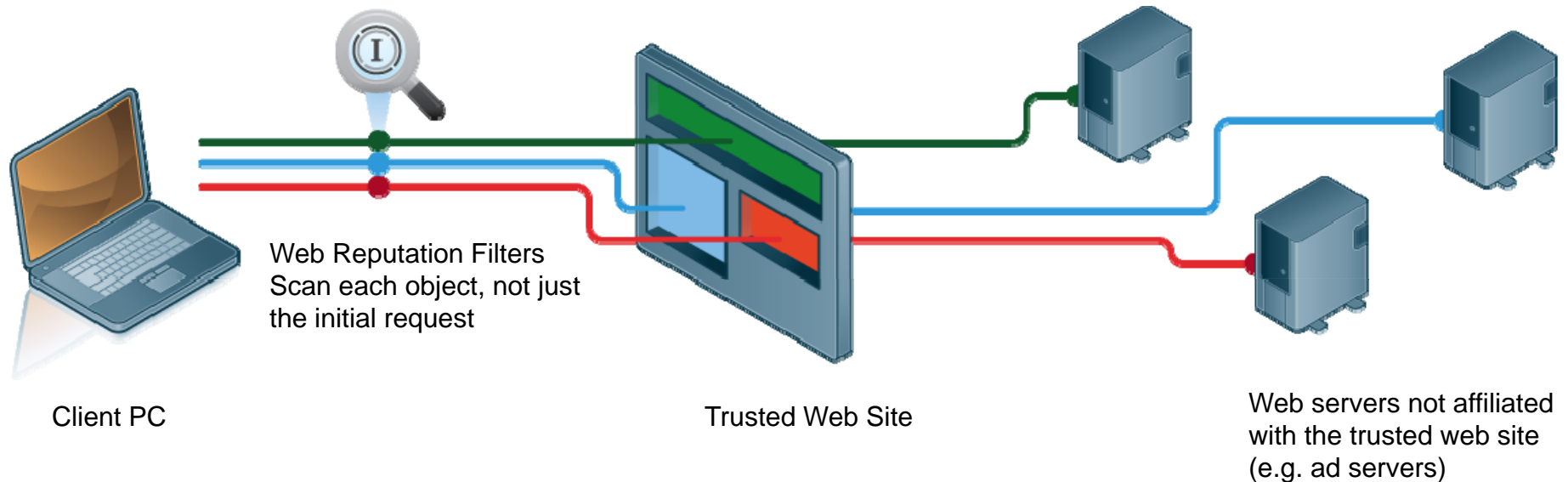
Parameters – The More the Better

- URL Blacklists
- URL Whitelists
- Dynamic IP Addresses
- Bot Networks
- URL Behavior
- Global Volume Data
- Domain Registrar Information
- Compromised Host List
- Real-Time Cloud Analysis
- Network Owners
- Known Threat URLs



Protection For a Dynamic Web 2.0 World

Visibility Beyond the Initial Threat



- Web pages are made up of objects coming from different sources
- Objects can be images, executables, JavaScript...
- Compromised websites often grab malicious objects from external sources
- Security means looking at each object individually, not just the initial request

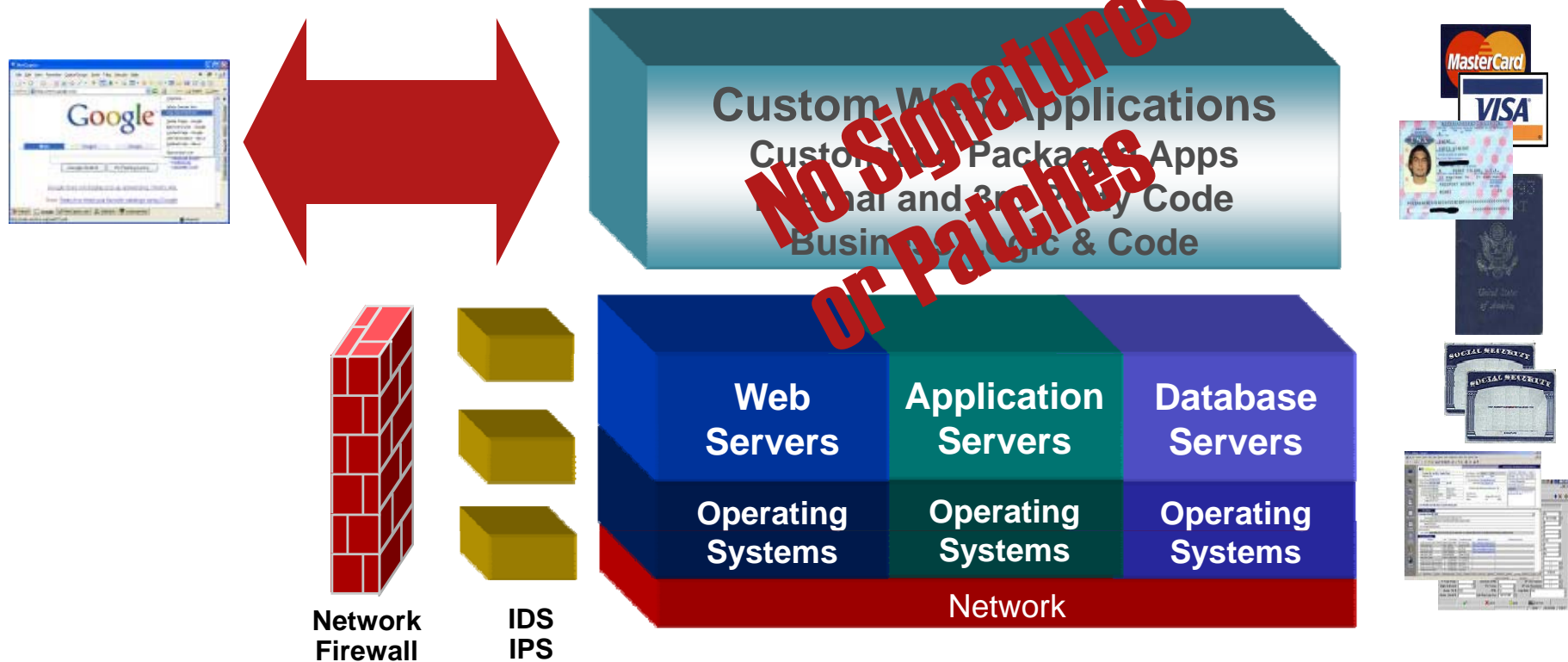
Web Application Firewalls

- Secure Coding
- Web Application Firewalls



Focus of Today's Attacks

2/3rd of Attacks Focused Here



No magic signatures or patches for your custom PHP script

2. Web Application Security

- Inventory pages, servers, development environments, groups
- Secure Web Development Methodology

Web applications treat all input as malicious and validate accordingly

Target OWASP top ten (owasp.org) and SANS top 20 (sans.org)

Applications should always consider user input malicious and filter out what it doesn't need

Applications should use session ID generation libraries that rely on well-known hash or randomization functions

Application should not print out verbose error messages to regular users

Coders must pay attention to "developers-only" comments in page source

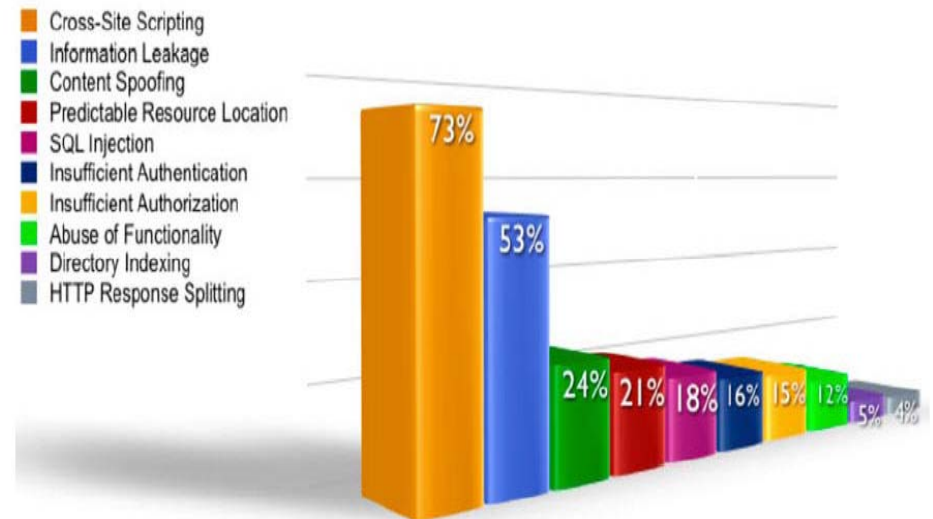
- Consider Web Application Firewall

You Said OWASP?

OWASP = Open Web App Security Project

<http://www.owasp.org>

- A1 – Cross Site Scripting (XSS)
- A2 – Injection Flaws.....
- A3 – Malicious File Execution
- A4 – Insecure Direct Object Reference
- A5 – Cross Site Request Forgery (CSRF)
- A6 – Information Leakage and Improper Error Handling
- A7 – Broken Authentication and Session Management
- A8 – Insecure Cryptographic Storage.....
- A9 – Insecure Communications
- A10 – Failure to Restrict URL Access.....



Top 10 vulnerability classes by percentage likelihood.

Source: WhiteHat Security, 2007

Web Application Firewall (WAF)

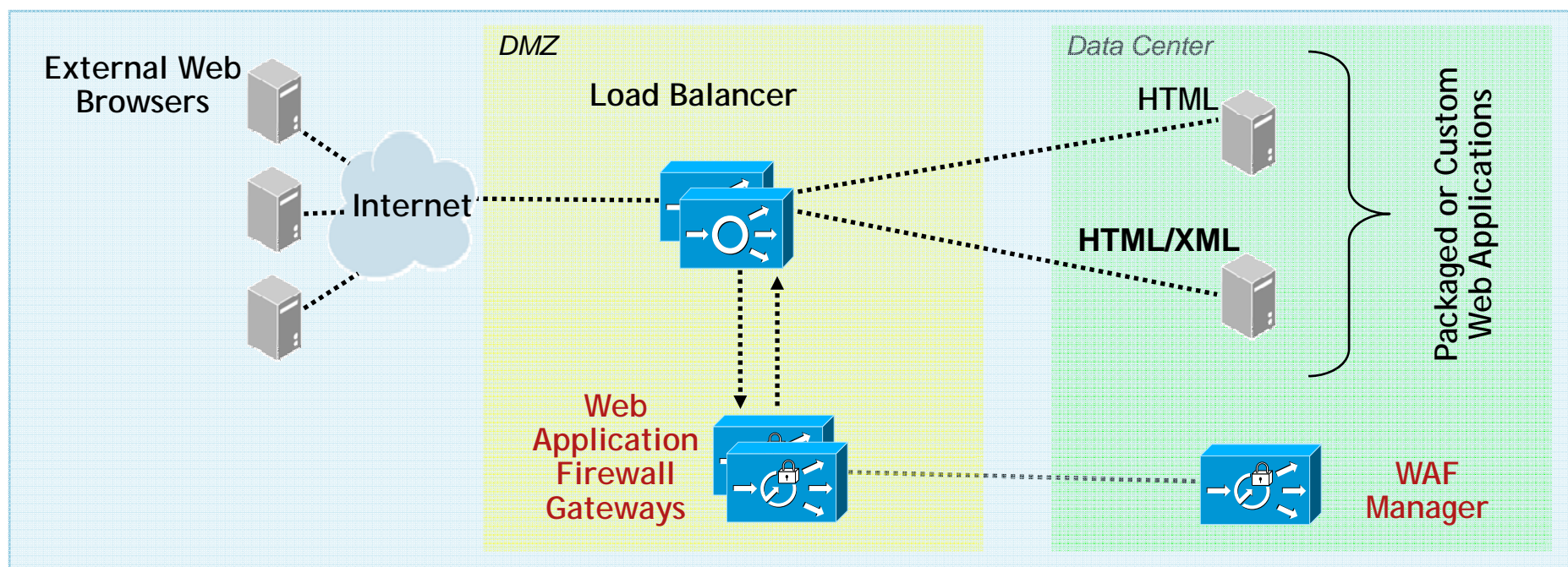


The WAF is a drop-in solution that protects web-enabled applications from attacks

PCI Compliance, Virtual App Patching,
Data Loss Prevention

- **Secure** – Deep packet protection of the most common vulnerabilities
- **Drop-in** - Does not require recoding applications, deployable in under an hour
- **PCI 6.5/6.6 compliance is just a few clicks away**

WAF Network Deployment



- Typically deployed in the DMZ or WWW Server Farm access
- Cluster of 2 appliances behind Load Balancer for Failover
- Distributed solution:
 - Manager = GUI
 - Gateways = Policy Enforcement Points

Perimeter Web Gateway

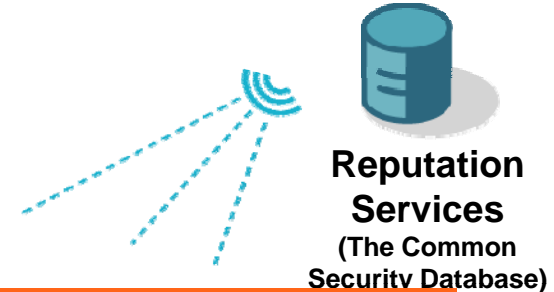
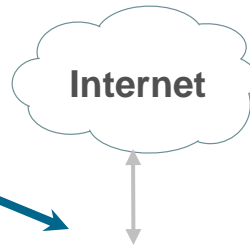


3. Perimeter Web Gateway

Application-Specific Security Gateway

BLOCK Incoming Threats:

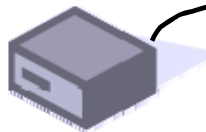
- Viruses, Trojans, Worms
- Spyware, Adware, Phishing
- Unauthorized Access



APPLICATION-SPECIFIC SECURITY GATEWAY

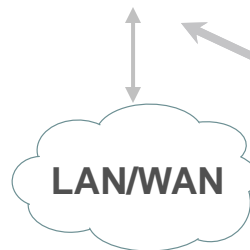


MANAGEMENT Controller



CENTRALIZE Admin:

- Per-user policy
- Per-user reporting
- Quarantine
- Archiving



ENFORCE Policy:

- Acceptable Use
- Regulatory Compliance
- Intellectual Property
- Encryption
- URL Filtering

Multi-Layered Malware Defense

Protection Against Today's Threats



L4 Traffic Monitor

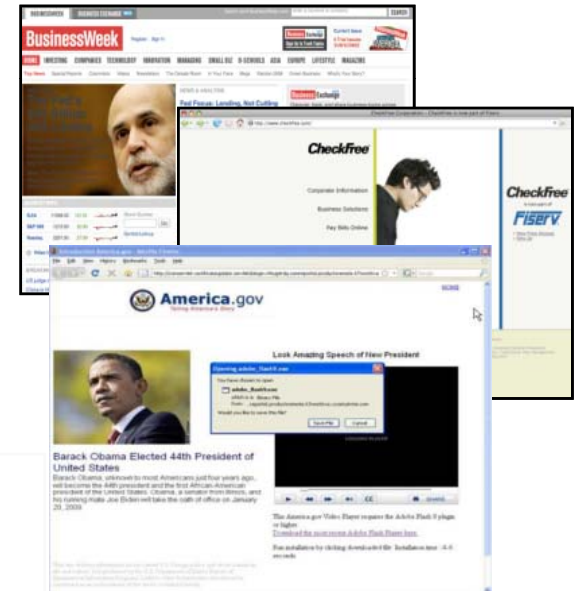
Web Reputation Services

Anti-Virus/Anti-Malware Engines



- Blocks much of unknown/known malware traffic at connection time

- Blocks malware based on deep content analysis



HTTPS Use Cases

SSL Trojans
and Malware



Secure
Anonymizing
Proxies



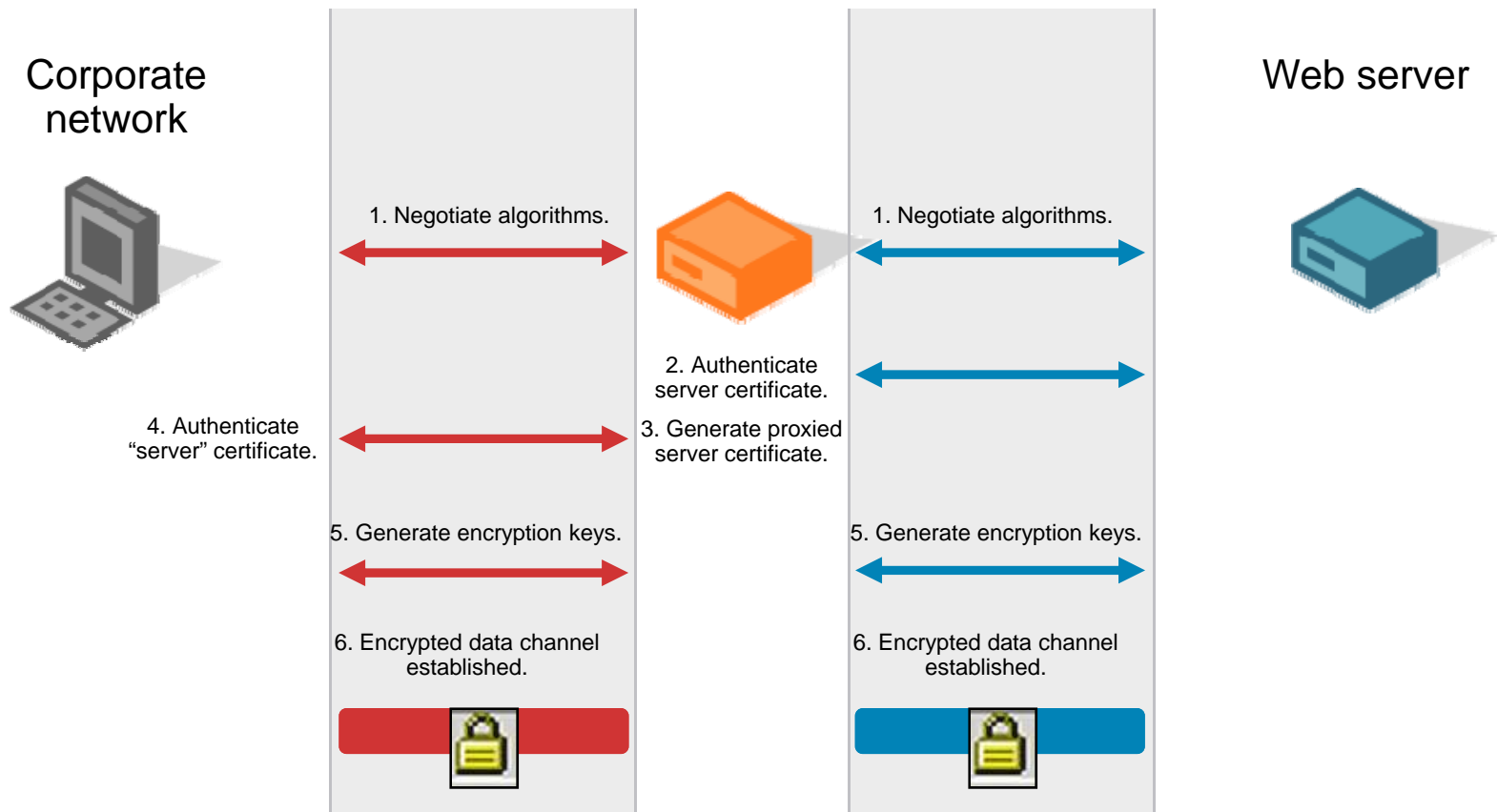
Secure
Webmail
Attachments



The screenshot shows a web browser window titled "Anonymous Web Surfing through ProxyWeb.net - Mozilla Firefox". The address bar shows the URL "https://www.proxyweb.net/antilog.php". The browser's proxy settings are visible, showing "Proxy: None". The main content of the browser is an article from InfoWorld titled "An SSL trojan unmasked" by Ryan A. Grimes, dated 2006. The article's title and a portion of its text are highlighted with a red box. Below the browser window, a Gmail inbox is visible, showing a list of emails with their subjects and dates.

HTTPs Decryption

Solution: The Active Man-in-the-Middle



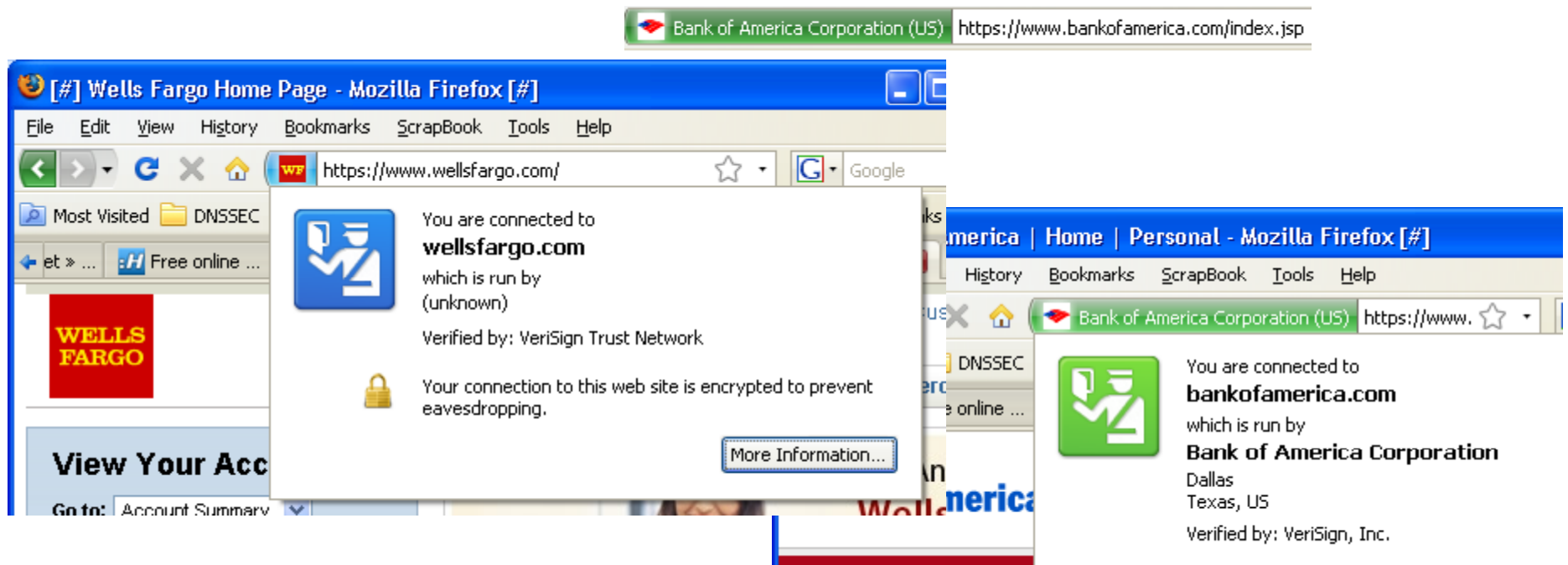
End User Security



4. End User Security

- Train users with real-world examples
- Streamline security policies to include essentials
- Train users to understand web works and parse URLs

Firefox 3 and IE 7 have improved UI



Browser Security

- Browsers have built-in phishing/malware updates
- Internet Explorer 8 (currently in beta 2 status)
 - adds XSS filters
 - blocks “><script>... types of attacks on both GET and POST
 - can be controlled by server-set HTTP header
- Firefox add-on called NoScript
 - detects more vectors/encodings than IE8.0 ...
 - ... but probably less user friendly (more geek-oriented)


Google Browser Security

- Google anti-malware search results effective
 - Interstitial page warning of infection pops up



Safe Browsing

Diagnostic page for tejary.net

Advisory provided by 

What is the current listing status for tejary.net?

Site is listed as suspicious - visiting this web site may harm your computer.

Part of this site was listed for suspicious activity 1 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 194 pages we tested on the site over the past 90 days, 164 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2009-04-14, and the last time suspicious content was found on this site was on 2009-03-25.

Malicious software includes 3138 scripting exploit(s), 4 trojan(s). Successful infection resulted in an average of 12 new process(es) on the target machine.

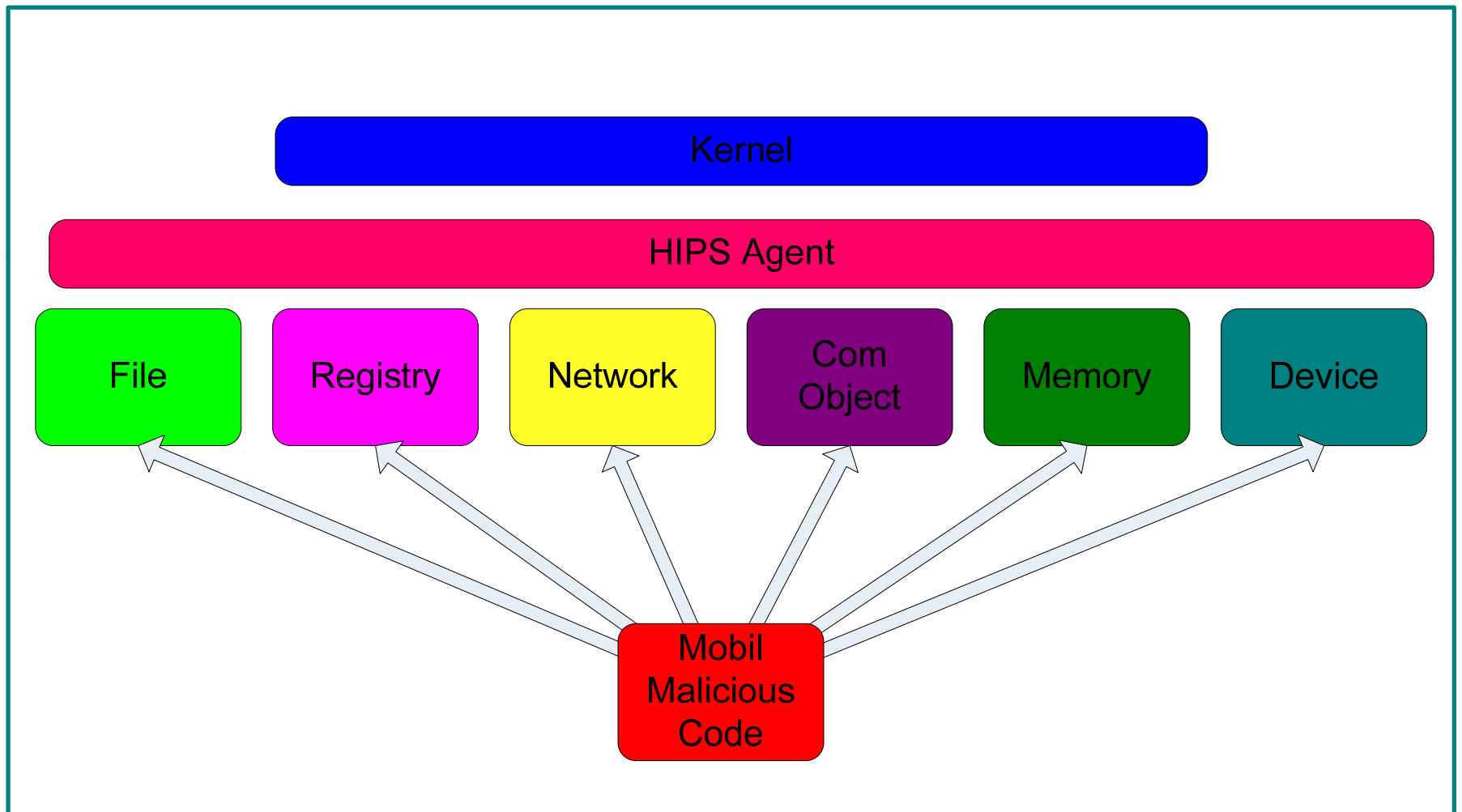
Client Security



5. Client Security

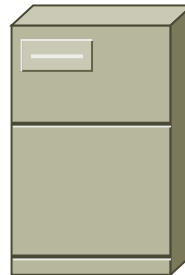
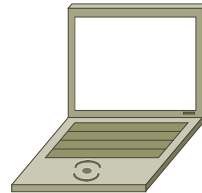
- Vulnerability scanning and patching (including web browser ecosystem)
- Assess anti-virus and consider behavior-based system
 - Host Intrusion Prevention System (HIPS)

Behavior-Based Rules



HIPS Agent Consolidates Multiple Endpoint Products

- ✓ Only one agent to purchase, deploy and manage



Desktop and Server Protection:

- **Distributed Firewall – Port Blocking & Packet Inspection**
- **Host-based Intrusion Prevention**
- **Day Zero Virus/Worm Protection**
- **File Integrity Checking**
- **Application Blacklist/Whitelist**
- **Policy Enforcement**
- **Spyware/Adware**
- **Operating System Hardening**
- **Web Server Protection**
- **Data Leakage Protection**
- **Wireless Interface Controls**

Complementary with Anti-Virus

HIPS Pro's and Cons

- Pro:

- The best HIPS products, using only the default policies, have never been compromised by anything that appeared in the wild

- CSO Surveys - #1 Security Technology with the Most ROI

- Proven ROI – savings in system admin time

- Con:

- Large project – up front time and effort across multiple groups

- Tuning required to reduce amount of Information and tune policies

Monitoring



6. Monitoring

- Assume your security will fail and look for symptoms
- IPS, Botnet Traffic Filters, Netflow will show infections and security weaknesses
- SRI bothunter is free tool
- Netflow can require significant work
- IPS systems indicate attack profile as well as internal hosts attacking other hosts

Q and A

