

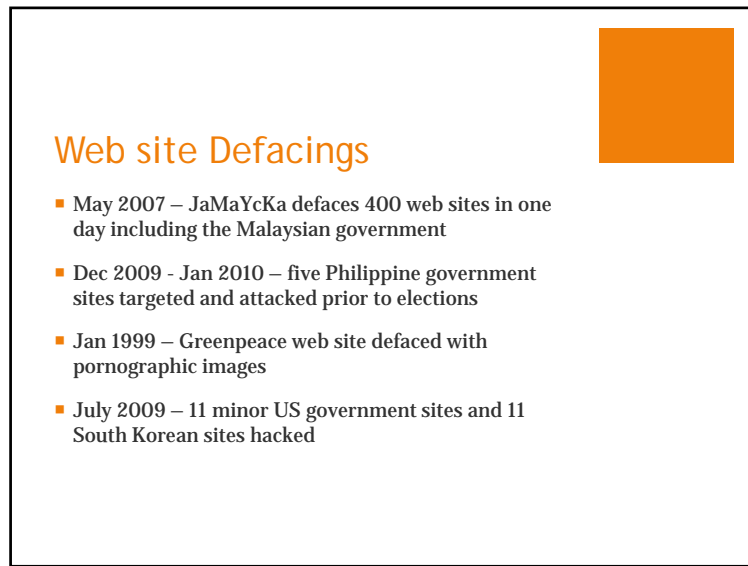


INF400 Web Security

Issues in Web Security

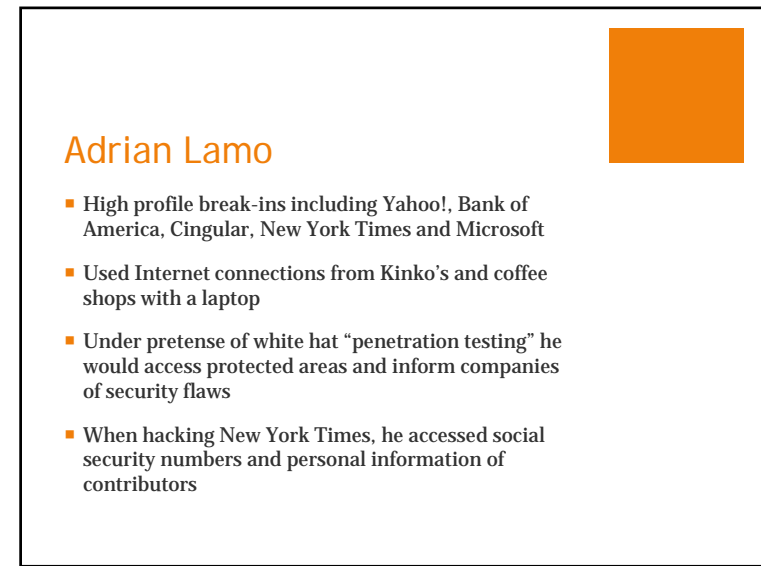


What's The Big Deal



Web site Defacings

- May 2007 – JaMaYcKa defaces 400 web sites in one day including the Malaysian government
- Dec 2009 - Jan 2010 – five Philippine government sites targeted and attacked prior to elections
- Jan 1999 – Greenpeace web site defaced with pornographic images
- July 2009 – 11 minor US government sites and 11 South Korean sites hacked



Adrian Lamo

- High profile break-ins including Yahoo!, Bank of America, Cingular, New York Times and Microsoft
- Used Internet connections from Kinko's and coffee shops with a laptop
- Under pretense of white hat "penetration testing" he would access protected areas and inform companies of security flaws
- When hacking New York Times, he accessed social security numbers and personal information of contributors

Citibank

- Russian hacking group silent for 2 years suddenly attacks Citibank Web site
- Citibank is 27% owned by US government
- Method: Black Energy
 - Software costs \$40 on open market
 - Software designed to block access to SSL Web site and steal access credentials
 - Can be upgraded to invade systems and snatch data
- Loss: Estimated \$10 million+

Data Breaches & Mishaps

- Since 2005, there have been 342,101,335 “records” breached [<http://www.privacyrights.org/ar/ChronDataBreaches.htm>]
- Dec 2009 – RockYou gets SQL injection via Web site exposing 32 million usernames and passwords
- July 2009 – Network Solutions Web servers hacked, compromising 573,000 payment data (credit and debit card accounts) of customers
- Jan 2009 – Indiana Dept. of Administration “accidentally posts” social security data for 8,500+ employees onto public Web site

The Scope

- Financial loss
- Reputation loss
- Identity theft
- Personal information compromise

What's The Problem

Web Sites are open windows

- Servers are only as secure as the number of open ports
 - Web servers always have ports 80 and 443 open
 - Also generally have 21, 25, 81, 8080 and several others
- Web servers run executable or interpreted scripts that can access file systems, databases and other protected areas
- Web servers are only as strong as the security of the operating system and the administrators who set them up

Web Sites are public and have few controls

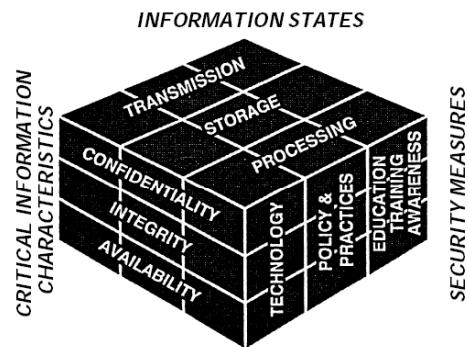
- Extranet Web sites are generally open to the public
- Resource strained Web departments place few controls over pages and data that gets posted
 - Very little filtering and few checks are put in place
 - Those checks that are in place are generally weak or lacking any true verification processes
- It is very easy to change a Web page/site
- Developers frequently leave comments in open code, viewable in the source

Basics of Information Security

Critical Characteristics

- | CIA | CIA+ |
|---------------------------|---------------------------|
| ■ <u>C</u> onfidentiality | ■ <u>C</u> onfidentiality |
| ■ <u>I</u> ntegrity | ■ <u>I</u> ntegrity |
| ■ <u>A</u> vailability | ■ <u>A</u> vailability |
| | ■ Accuracy |
| | ■ Authenticity |
| | ■ Utility |
| | ■ Possession |

NSTISSC Security Model



Balancing Security and Access

Need for Security

- Some information inherently needs to be kept secure and private
- Entities need to have control over how information is disseminated
- Entities need to be able to protect the information held and be flexible in approach

Need for Access

- There is a generalistic public need to have information accessible and available
- Web sites are increasingly the method of data accumulation
- Web sites cost effective methods for providing information

Security is an art

- No hard and fast rules
- Many universally accepted "complete" solutions
- No specific manual for security implementation – it takes practice
- Complex interaction of users, policy and technology

Security is a technology science

- Technology design to perform at highest level
- Conditions cause virtually all actions that occur in computers
- Nearly all faults, security holes and system malfunctions are a result of the interaction of hardware and software
- Developers generally have little time to resolve and eliminate faults or are prevented from doing so for business reasons (cost)

Security is a social science

- Social science examines the behavior of people interacting with computer systems
- Security begins and ends with the people who interact
- End users are generally the weak link
- Administrators inadvertently create weak security profiles which can degrade over time