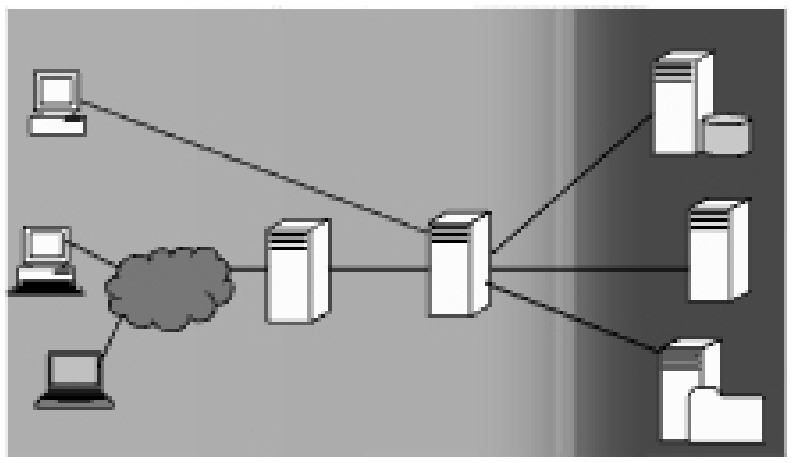
Web Site Security

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: Kal Schlichting <kal@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."