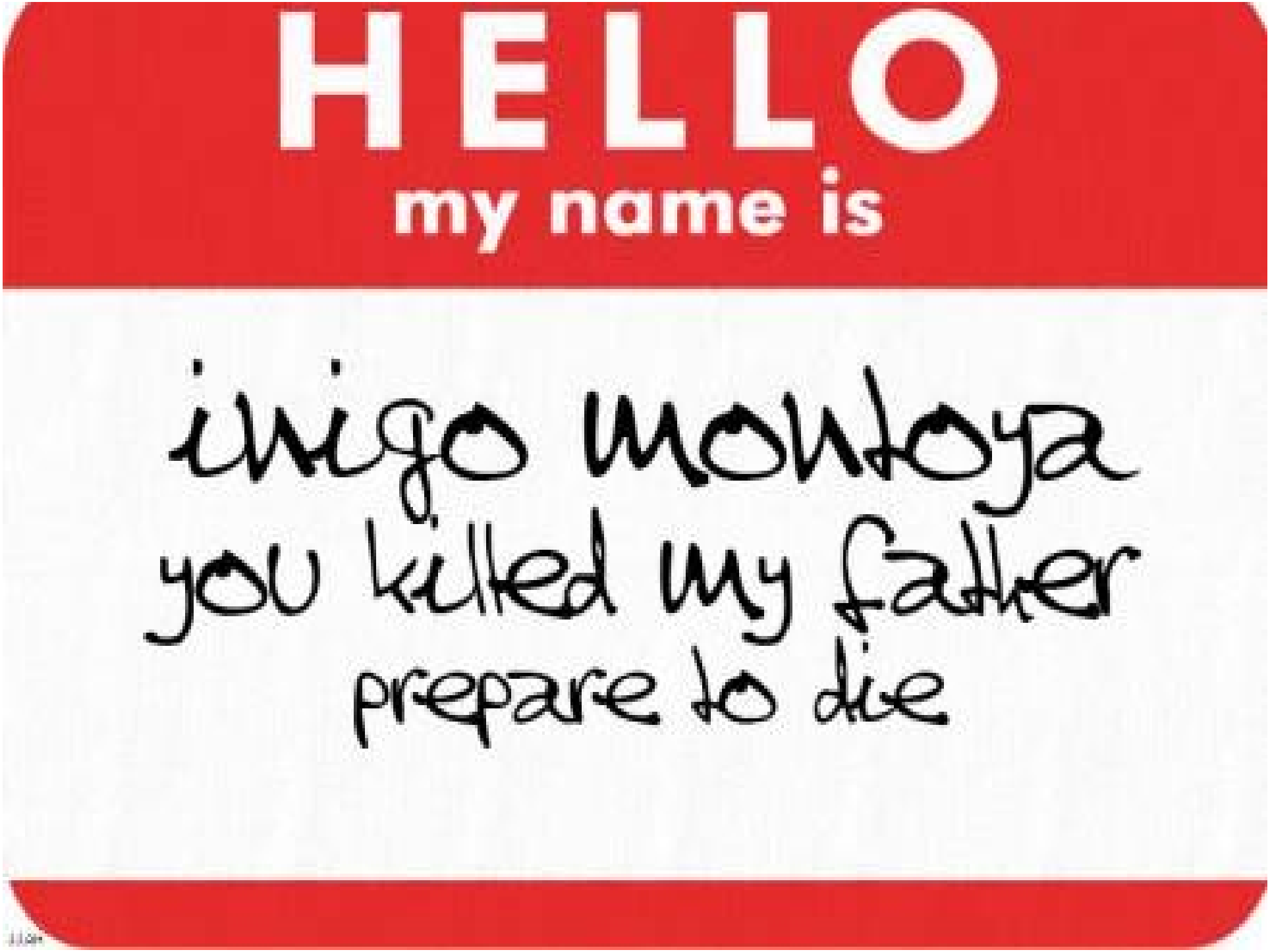
Wifi Security

-or-

Descending Into Depression and Drink

Mike Kershaw / Dragorn
dragorn@kismetwireless.net


HELLO
my name is
inigo montoya
you killed my father
prepare to die

The plan

- 802.11 networks
- Well-defended APs
- Basic vulnerabilities
- Network spoofing
- Client hijacking
- Layer 2 to Layer 7
- Advanced client misery
- Q&A

802.11

- 2.4 and 5.8 GHz
- Multiple data encodings depending on spec
- All fundamentally spread-spectrum
- This means we can interact with it easily

Packing your bags

- Unlike frequency-hopping protocols, trivial to capture 802.11
- Generic Wifi card (Alfa 11g is cheap to start with)
- Support in the OS (more on this later)
- Total cost of ownage: $50 or so

802.11 networks

- Made up of three packet types:
- Management – Defines & controls network (SSID, crypto, etc)
- Control – Flow control (CTS/RTS), power save
- Data – Actual data frames, where the good stuff lives

802.11 Management Frames

- Define network SSID, crypto (beacons)
- Control client access (probe request, response)
- ***Not authenticated***
- ***Not encrypted***
- New standards seek to address this in the future

802.11 Data Frames

- Contain, well... data
- Layer2 encryption (WEP, TKIP, AES)
- Data layer encryption (SSH, SSL, VPN)

Monitoring Voodoo

- Wifi devices presented as 802.3 Ethernet
- Promisc doesn't work the same since it's not really 802.3
- Only gets data frames, not management, and only some data frames

RFMON

- Monitor mode / RFMON
- Special mode, switches interface to 802.11 DLT (sometimes with custom headers for signaling)
- Requires support from drivers/firmware

RFMON

- Shows all packets seen by radio
- This includes management, data, etc, from all networks
- ***Almost*** all cards support this (notable exception, special mobile chipsets may not include support in firmware)
- Almost all Linux drivers, most *BSD, some OSX drivers, and only one windows driver (AirPCAP)

What we get in RFMON

- All networks, regardless of encryption, cloaking, etc
- Client detection
- Layer2 IDS
- Passive observation
- Data collection for offline encryption attacks

Packet Format

- 802.11 headers (unencrypted)
- Length varies slightly based on type of packet
- Management frames are all 802.11 header
- Data frames have 802.11 headers + (optionally encrypted) data

802.11 Addressing

- 802.3 have source and dest MACs
- 802.11 have 3 (or sometimes 4) MAC fields
- Source; Client or AP
- Destination; Client or AP
- BSSID; Mac address of AP used

802.11 Roaming

- Multiple AP with same SSID
- Client assumes the SSID is a common network
- Roams to the strongest signal
- Data handoff responsibility of backend (controller or common L2 network)
- Only differentiator is MAC addr

Hello, my name is 802.11

- Finding an 802.11 network is really easy
- Networks are *really* noisy
- Beacon 10x a second
- Even weird networks make noise when someone talks
- No way to really hide

Is anyone listening?

- Clients constantly look for networks to join
- And often tell us every network they'd like to see
- Just as easy to find as networks
- Clients can be really noisy when they can't find a network

Sniffing around

- Put the card in monitor mode
- Requires an OS w/ rfmon drivers (Linux, BSD, sometimes OSX, AirPCAP on windows)
- Backtrack/Pentoo livecd
- Fire up wireshark/tcpdump/etc
- Kismet does all of this for us

I come not to bury 802.11...

- We've got a pretty good idea about 802.11 security by now
- By “we” I mean “security professionals”
- Even “the great unwashed” are clueing in, kind of. Encryption on home nets is up

Secure configurations

- WiFi is secure in proper deployments
- WPA-Enterprise
- Per-user authentication
- Per-user keying
- Mutual auth via certificates

Strong encryption

- We've got a pretty solid crypto system
- AES used in WPA-CCMP as yet unbroken
- TKIP showing flaws, but is already past sell-by date, move to CCMP

“Done Properly”

- WPA-Enterprise secure “done correctly”
- Opportunities for failure exist if users don't validate certs (or are allowed to say 'ok')
- TKIP will eventually fall

802.11 AP Defense

- We've been doing this for a long time now
- Best defense: Strong network architecture (again, WPA)
- Monitoring for conflicting or spoofed access points
- Client protection attempts to defend known good users

Client Protection

- Inter-client traffic can be blocked at the AP
- Defending clients on a strong network is easy since the AP controls crypto
- Defending clients on open AP is very hard

Denial of Service Attacks

- Management frames unprotected
- Spoof AP, tell all clients to disconnect
- Pure channel denial (flood channel with noise)
- “Crowbar” defense – find the person doing it and hit them with a crowbar.

Punching 802.11 in the gut

- ***Absurdly*** easy
- Management frames are totally unprotected
- Open networks are un-authenticateable
- ***It's shared media***

Strangers with candy

- Avoiding hostile networks requires *smart* users
- Users are – typically – bad decision makers
- The OS doesn't help: It likes to join networks it's seen before
- It's hard to tell what's real, assuming the user even looks


FREE CANDY

Going viral

- Users *like* free wi-fi
- Who *wouldn't* want to join "**Free Public Wi-Fi**"?
- Once, long ago, this network probably existed
- When windows can't find a network, it likes to make an ad-hoc version...
- Then someone else tries to join

Sore throats

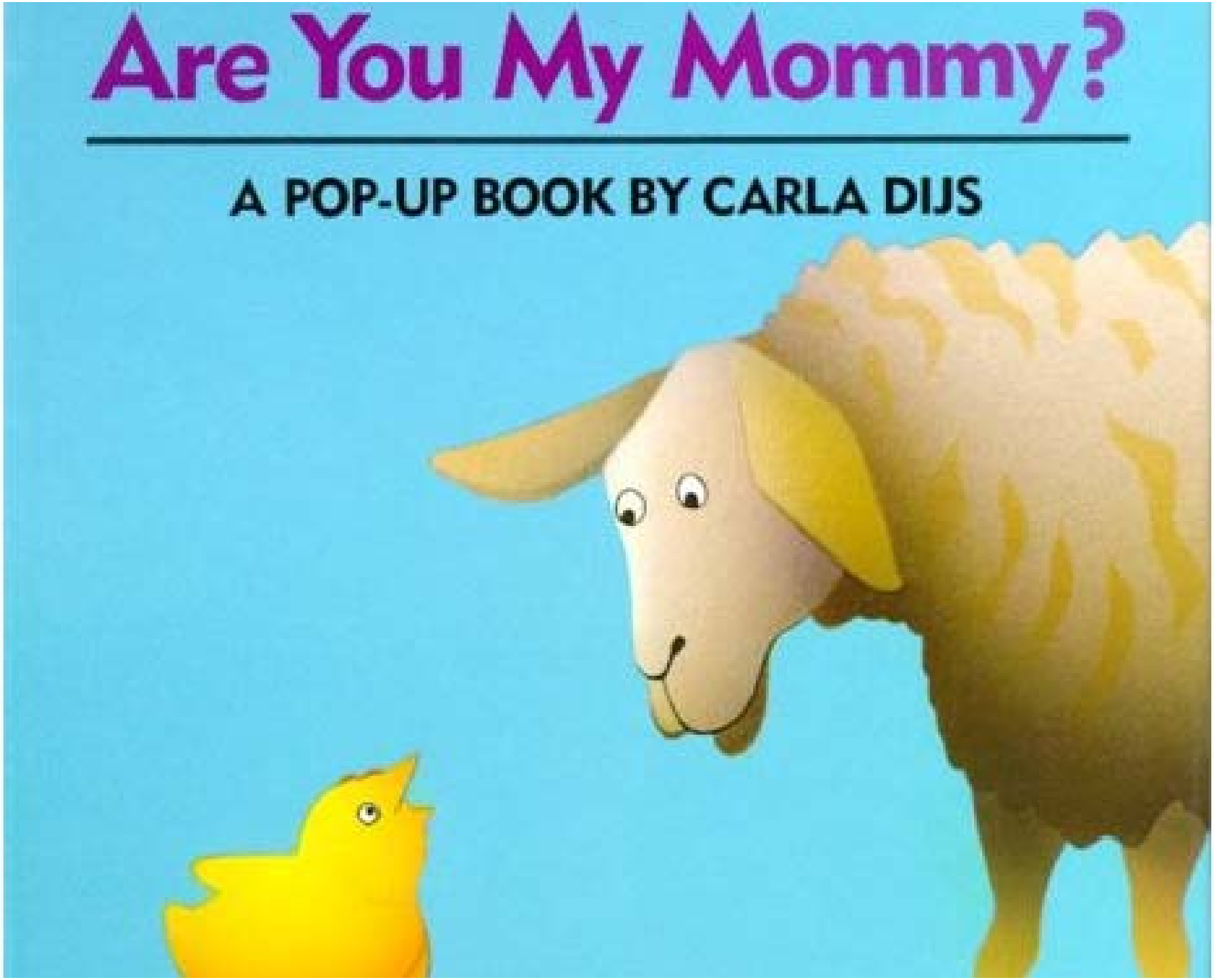
- Of course, this junk ad-hoc network doesn't go anywhere
- Unless of course, someone brought up a network with the same name...
- … And handed out IP addresses...
- Which would get us LAN access to the system

Being too trusting

- Clients are *really* trusting
- If you say you're network *Foo*, you **must** be, right?
- It's very hard to avoid really bad behavior as a user
- Remember before? Roaming sure looks a lot like spoofing

Are You My Mommy?

A POP-UP BOOK BY CARLA DIJS



The packets must flow

- So if an attacker has a stronger radio than the AP...
- You may not be talking to who you think you're talking to
- So long as the packets go through, the user never knows
- Man in the middle = Win

Stuck in the middle with...

- Dual-interface attacker
- Interface 1 connects to legitimate network (any network, or cell data, or...)
- Interface 2 provides spoofed “Free Public Wifi” network.. or “FarDucks”..

Bad karma

- It sounds pretty boring to have to make a fake network for each client
- Plus not ***everyone*** is looking for "Free Public Wifi". Just *almost* everyone.
- Enter ***Karma*** and ***Airbase***
- Answer ***all*** probe requests
- Are you "Free Public Wifi"? Sure am.
- Are you "My Corp Network"? Yup!

Karma ran over your dogma

- When you are the network, you are the internet
- Yes, your IMAP server is here! Give me your password!
- You wanted to update some software? Happy to!
- Please, log in to “twitter”!

Make a bad thing better...

- Karmetasploit!
- Metasploit + Airbase = Massive, evil attack framework + client hijacker
- You wanted facebook? How about a face full of browser exploits instead?

More Man-in-the-middle

- Why just attack the browser?
- Many sites encrypt login, but not session
- Session cookies, data, etc vuln
- “The Middler”, SSLSniff, Cookie Monster
- Hijack sessions via MITM

This bores me

- All of these attacks are really pretty boring
- Why? They're really obvious.
- Might still get some users, but it'll be pretty blatant
- Points ARE awarded for style. Or at least, for stealth.

So wait...

- Didn't we say 802.11 is ***shared media***!?

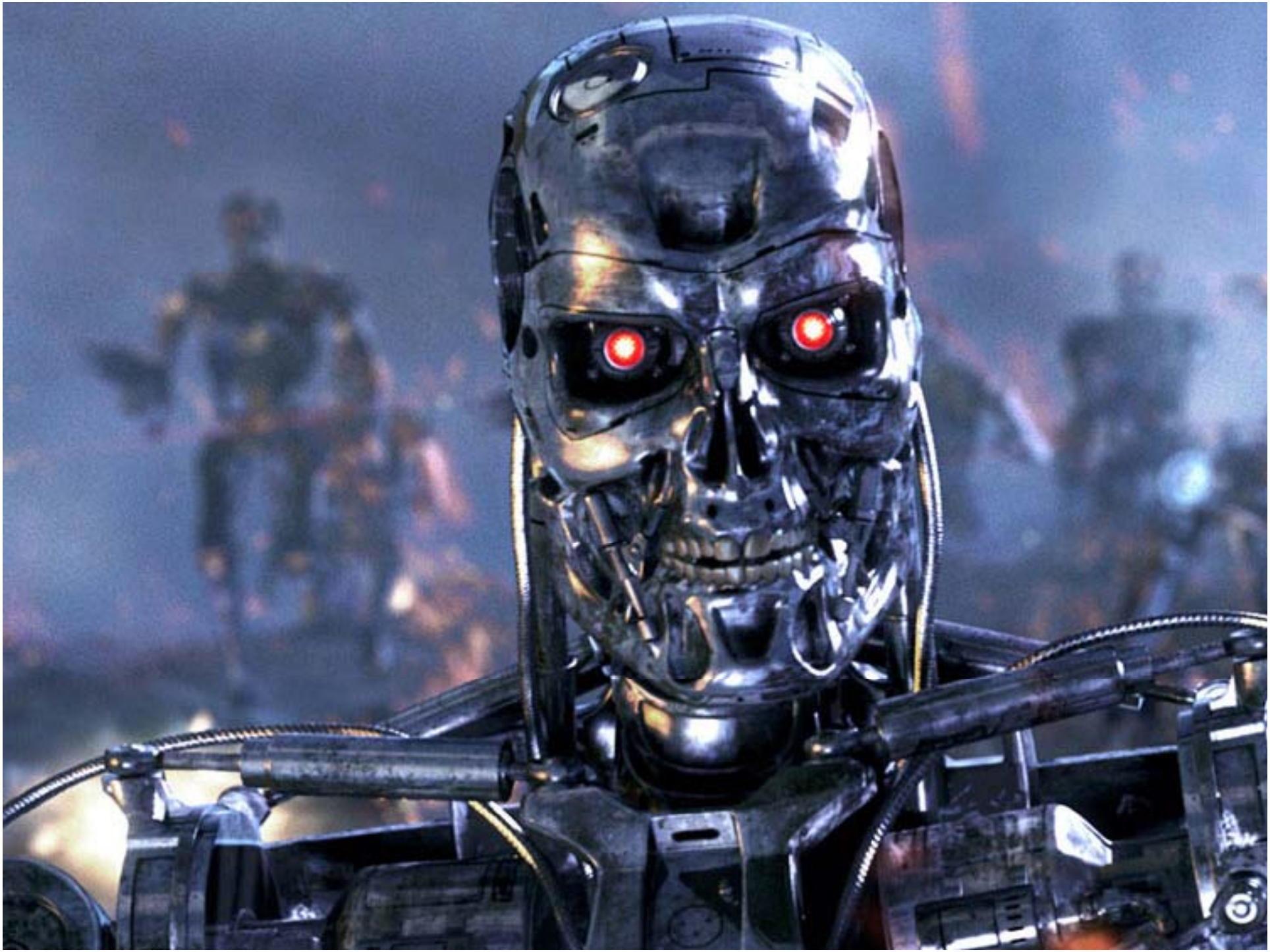
- We just found **the best time machine ever*!***


BAW 51
DMCGLEN

And not some hippy do-gooder time machine, either


POLICE PUBLIC CALL BOX
POLICE PUBLIC CALL BOX

But one where we get to bring back weapons from the future



The bad old days

- Hair metal, grunge, ripped jeans
- Unswitched shared media Ethernet...
- Sniffing the entire segment

…

- TCP session hijacking...

That's too easy

- It'd never be *that* easy, right?
- ***Right***?
- People *have* to have gotten smarter by now...
- You'd *never* take a system from a secure network to an insecure network, *right*?


STARBUCKS COFFEE
STARBUCKS COFFEE
STARBUCKS COFFEE
STARBUCKS COFFEE
STARBUCKS COFFEE
STARBUCKS COFFEE

Mmm, latte

- … and airports
- The gym
- A hotel
- Bookstores
- McDonalds
- Conferences

Making a mess

- Management frames have no protection
- Open networks have no client protection
- Nothing stops us from spoofing the AP and talking directly to a client!

No protection

- AP may filter inter-client communication by blocking packets when they hit the AP
- By generating an 802.11 header FROM the AP and TO the client
- The client thinks the packet is legit
- The AP has no opportunity to act on it
- We can communicate directly with “protected” clients on open networks

Shooting up

- Most modern cards use “soft” MAC control layers
- Most of the control offloaded to the OS
- Only certain timing critical stuff handled in the firmware
- This means we can send anything we like (usually)

The shakes

- Unfortunately there aren't really any standards for injection
- Every OS does it differently
- Different drivers do it differently
- Sometimes needs custom headers per packet

Making it easy: LORCON

- Writing the same injection code for every app sucks
- Writing custom code for each driver sucks
- Writing apps for each OS sucks
- Hopefully LORCON doesn't suck

LORCON2

- Unfortunately... the LORCON1 API... kind of sucked
- New API modeled off of PCAP
- Designed to be easy to use
- C, Ruby API
- Will soon support all the cards LORCON1 did, for now, Linux
- http://802.11ninja.net

Super simple

- Automatically determines the driver
- Automatically configures virtual network interfaces and sets up modes for injection
- Send arbitrary bytes -or- use packet assembly API

The most basic

```
lorcon_driver_t *dri;
lorcon_t *ctx;
uint8_t packet[...];

dri = lorcon_auto_driver(“wlan0”);

ctx = lorcon_create(“wlan0”, dri);

lorcon_open_injmon(ctx);

lorcon_set_channel(ctx, 6);

lorcon_send_bytes(ctx, sizeof(packet), packet);
```

The inspiration

- Wifi session hijacking
- About 5 years ago, Toast debuted Airpwn at defcon
- TCP stream hijacking on 802.11
- *Why hasn't everyone been using this*!?
- Not just for shock-porn anymore!

Rerouting streams

- Typical layer2 attack
- TCP is only “secure” because the seq/ack is unknown
- Attacker sees your L2, so seqno is known
- Any TCP stream subject to abuse

Anatomy of a session

- Handshake
- Client → Server

  “GET /foo.html HTTP/1.0”

  Seq 123 ack 10
- Server ← Client

  “HTTP headers, content”

  Seq 10 ack 189

So lets add this to MSF

- Lorcon Ruby wrapper
- Racket packet assembly (high speed Ruby packet assembly)
- Ruby PCAP
- And a little TLC

Anatomy of an Evil session

- Handshake
- Client → Server
  "GET /foo.html HTTP/1.0" [seq/ack]
- MSF ← Client
  "Malicious data..." [seq/ack]
- MSF ← Client **FIN!**
- MSF → Server **FIN!** [using client seq/ack]
- Server ← Client
  "Real data!" [old seq/ack]

MSF

```
msf > use auxiliary/spoof/wifi/airpwn

msf auxiliary(airpwn) > set INTERFACE
  alfa0
INTERFACE => alfa0

msf auxiliary(airpwn) > set RESPONSE
  "Airpwn - MSF!"
RESPONSE => Airpwn – MSF!

msf auxiliary(airpwn) > run
```

MSF

```
msf auxiliary(airpwn) > run


[*] AIRPWN: Response packet has no
  HTTP headers, creating some.
[*] Auxiliary module execution
  completed
msf auxiliary(airpwn) >
[*] AIRPWN: 10.10.100.42 ->
  208.127.144.14 HTTP GET
  [/files/racket/src/doc/] TCP SEQ
  542050816
```

Fine-tuning

- Match & replace in regex
- Response can be full JS, image replacement, HTML, a file
- Sitelist YAML file for matching specific requests (poison lists of known files, like jquery)

Autogen

- Airpwn-MSF automatically generates HTTP headers as needed
- Complete attacker control of page content including headers, too

Ill-gotten profit

- What does that get us?
-
- HTTP content replacement

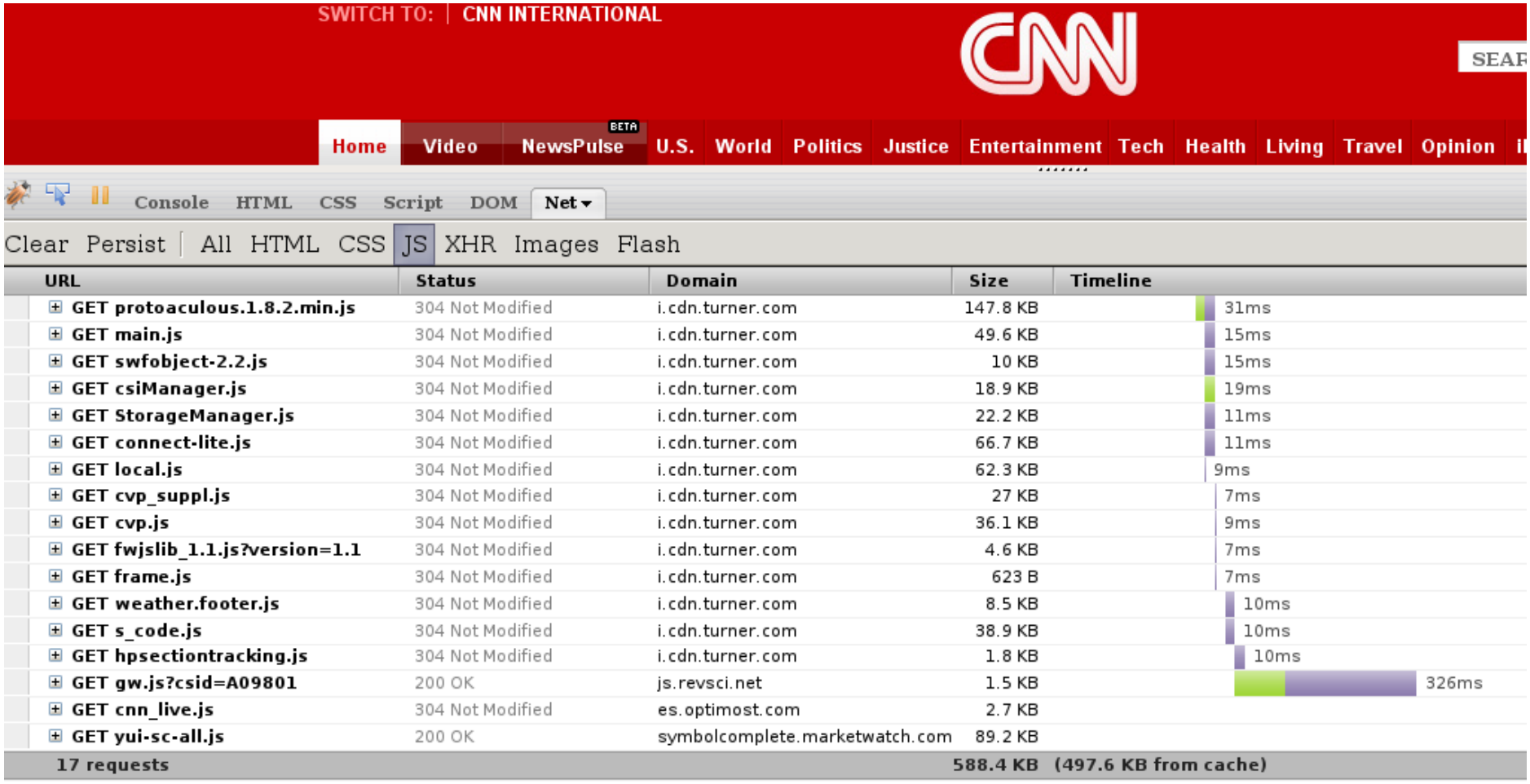
Or in other words...

- Control over the page DOM
- Control over forms
- Control over the browser in general
- Access to anything in the security context of the compromised page

Obviously scripted

- So we can replace content...
- What do we do now?
- Nearly all complex sites include a pile of javascript helper files
- What happens if we replace one of *those*?

It's not news, it's Javascript



JS Fragments

- Especially attractive
- Totally invisible to the user
- Multiple requests = Multiple opportunities to land attack
- Run in same privilege domain as web page

I'm in your browser

- Rewriting your DOM
- DOM = Document Object Model
- Programmatic manipulation of page content
- Once in the DOM we can do *ANYTHING*

updated 9:07 p.m. EDT, Wed June 10, 2009

Make CNN Your Home Page

Updated: ∞

Kismet #1 Wireless Sniffer

Author claims "Open wifi is a HORRIBLE idea" Do you trust your news? Your content? Is that image there exploiting your browser *right now?* Is the *stock market crashing?*

Latest News

- Trump fires Miss California USA Prejean
- New Orleans mayor released from flu quarantine
- 'Black box' could solve plane crash mystery
- Cops: School boss, gun-toting dad fight over flu
- KRQE: 1 found alive as copter search continues
- Chief: Suspect didn't ask how wife, boys died
- Mug shot reveals the true Phil Spector
- CNNMoney: Chrysler and Fiat make it official
- GM 'reinvention' starts with $25M battery lab
- Foggy pileup blocks L.A.-to-Vegas route
- Ticker: I can't speak to Obama, ex-pastor says
- Pregnant woman swims river to flee Mexico
- 3rd-grader steps off school bus, vanishes
- The day I held a sobbing WWII medic in my arms
- Lambert reveals 'crush' on 'Idol' winner
- Dead man talking: 'It's fun to die'
- Man busted in boots, lady's swimsuit

It's not stupid, it's advanced

```
var embeds = document.getElementsByTagName('div');


for(var i=0; i < embeds.length; i++){ if
    (embeds[i].getAttribute("class") == "cnnT1Img") {
    embeds[i].innerHTML = "..."; } else if
    (embeds[i].getAttribute("class") == "cnnT1Txt") {
    embeds[i].innerHTML = "..."; }}
```

DOM is tasty

- What else can we do?
- Rewrite all FORMs to proxy through us? Sure.
- Rewrite all HTTPS to HTTP so we can capture logins and “secure” data? Yup!
- Poison content topical to a conference? Tin foil hat, but yes!

HTTP not so S

```
var refs =
  document.getElementsByTagName('a');
for (var i = 0; i < refs.length; i++){
var rval =
  refs[i].getAttribute("href");
if (rval == null) { continue; }
refs[i].setAttribute("href",
  rval.replace(/^https:/, "http:");
}
```

This ***really*** matters

- This matters
- A ***lot***.
- No, seriously.

Persistence pays off

- Who has read rsnake's VPN paper?
- Attack HTTP clients via cache control
- Layer 2 attacks against web content can be ***made persistent***
- That means once you leave... ***you're still owned***

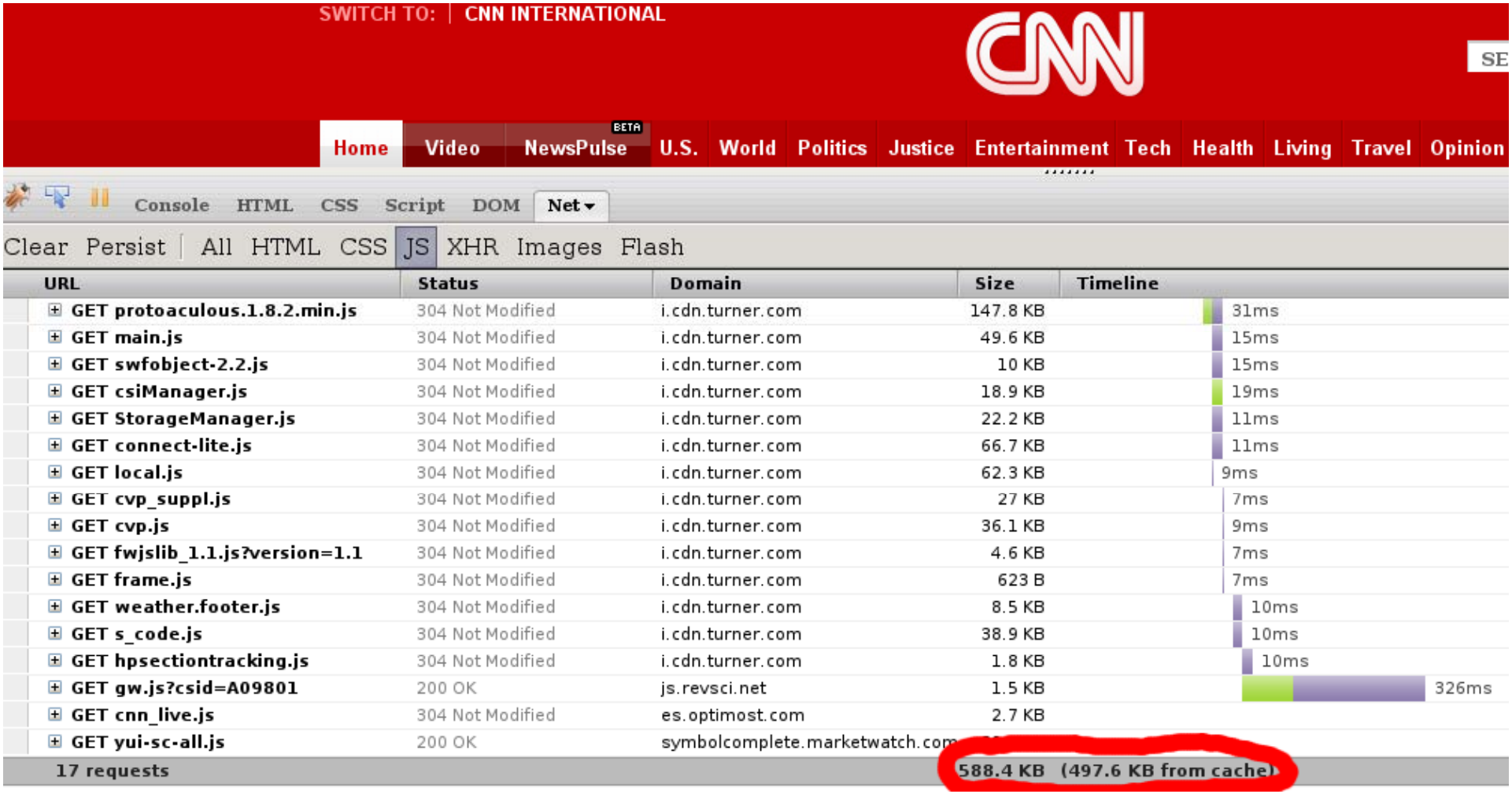
Fast cache

- Short version of the VPN paper:
- Browsers have cache
- Cache, by nature, remains around
- Users don't notice
- If I own your TCP session, I own your cache control

Fast cache

- Client is fed a spiked JS file with cache set to 10 years
- That file remains in their cache
- And is re-used when they revisit that site
- ***From inside the secure office network (or wherever)***

Don't think it's a problem?



Lots of victims

- None of the javascript files are visible to the end user
- Lots of opportunities to poison the files

Making it happen

•Cache-control: max-age=99999999, public

-or-

Expires: Fri, 13 May 2011 13:13:13 GMT

•So we hijack a common JS file

•Spike it with malicious code

•Set it to cache

•Now when the user goes back to work and goes to twitter again...

Watch the spikes

- User now has a spiked, cached javascript
- Browser will keep this and re-use it every time until it expires
- Iframes? Kaminsky socket/sucket? Load new browser exploits?
- But a user would ***never*** go to Twitter at work, right?

Call home to Mom

- Cache modified JS that calls home every time the page is visited
- Maybe no good attacks in the browser this week?
- Wait for a browser 0day then flip the switch to include malware
- Every system that has the cached call-home is attacked as soon as the users visit the poisoned site

Shimming the door

- Cache every page with JS shim
- Shim fetches original content
- DOM manipulation
- Regex replacement
- Future exposure to new browser vulnerabilities

There are no innocents

- No website is “innocent”
- Websites that don't ask for logins are just as capable of feeding browser exploits
- Any website can be poisoned with browser-owning code

Never underestimate fools

- But won't SSL solve it?
- Not really, users still have to be smart enough to not accept a bad cert
- And users would ***never*** do something insecure, right?
- *OBVIOUSLY* that pop star wants me to see her naked!

The Register®
Biting the hand that feeds IT

High spam response powers junk mail economy

Lunkhead junk mail buyers come clean

By **John Leyden** · **Get more from this author**

Posted in Spam, 16th July 2009 15:17 GMT

Almost a third of consumers admit responding to messages that might be spam emails. Some acted out of curiosity or by mistake but a puzzling 96 from a sample of 800 (12 per cent) said they clicked because they interested in the product or service advertised in junk mail messages.

A survey by the Messaging Anti-Abuse Working Group (MAAWG), released on Wednesday, also found that four in five consumers thought it unlikely they were at risk from malware

Security Alert

Practical advice for protecting your PC and your privacy

Subscribe to this blog

Erin Andrews Video Attacks Target Macs and PCs

Erik Larkin

Jul 21, 2009 2:31 pm

Internet crooks love to create attack sites and e-mails that use lures based on popular news items and Internet porn. When the two come together, as with the recent news of an online "peephole" video of ESPN sportscaster Erin Andrews, the malware is sure to swarm.

Swine flu malware poses as pig plague update

Telling porkies

By **John Leyden** · **Get more from this author**

Posted in Spam, 21st July 2009 10:03 GMT

Wrongdoers have created a new strain of swine flu-themed malware.

A Trojan, containing backdoor and keylogger functionality, poses as a Word document from the US Centre of Disease Control giving information about the disease.

The infectious file - Novel H1N1 Flu Situation Update.exe - appears with an icon that makes it look like a Word document file. Users tempted to open the booby-trapped file are presented with a document.

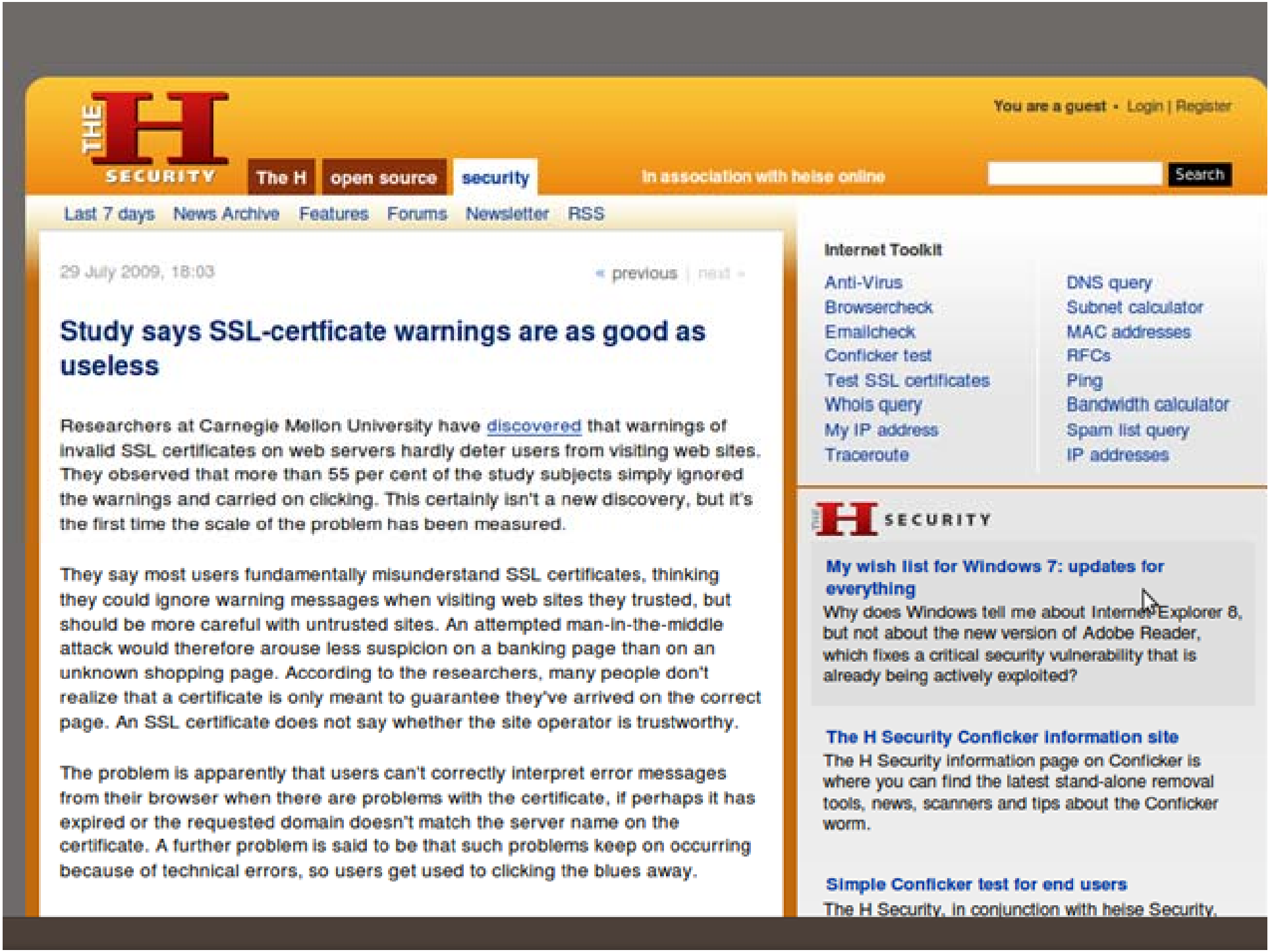
White Paper

Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior

EXECUTIVE SUMMARY

To study remote worker behavior, Cisco Systems® commissioned InsightExpress, a third-party market research firm, to surv from a variety of industries. The surveys were conducted in parallel in 10 countries: the United States, the United Kingdom, Germany, Italy, Japan, China, India, Australia, and Brazil. More than 1,000 remote workers were surveyed. The survey reve remote workers believe they are working securely, yet they continue to engage in risky online behavior.

- **Online shopping:** Nearly 40 percent of remote workers in the same respondent pool said they use their work comput shopping. Half said they make personal online purchases because their "company does not mind them doing so."
- **Sharing computers:** 21 percent of users admitted that they allowed others to use their work computers. More than o stated that they "don't see anything wrong with it." And believed computer sharing "does not increase security risks.
- **Risky wireless behavior:** One in 10 users surveyed stated that they have used a neighbor's Internet connection whe


THE H SECURITY
You are a guest · Login | Register
The H
open source
security
In association with heise online
Search
Last 7 days
News Archive
Features
Forums
Newsletter
RSS
29 July 2009, 18:03
« previous | next »
Study says SSL-certficate warnings are as good as useless
Researchers at Carnegie Mellon University have discovered that warnings of invalid SSL certificates on web servers hardly deter users from visiting web sites. They observed that more than 55 per cent of the study subjects simply ignored the warnings and carried on clicking. This certainly isn't a new discovery, but it's the first time the scale of the problem has been measured.
They say most users fundamentally misunderstand SSL certificates, thinking they could ignore warning messages when visiting web sites they trusted, but should be more careful with untrusted sites. An attempted man-in-the-middle attack would therefore arouse less suspicion on a banking page than on an unknown shopping page. According to the researchers, many people don't realize that a certificate is only meant to guarantee they've arrived on the correct page. An SSL certificate does not say whether the site operator is trustworthy.
The problem is apparently that users can't correctly interpret error messages from their browser when there are problems with the certificate, if perhaps it has expired or the requested domain doesn't match the server name on the certificate. A further problem is said to be that such problems keep on occurring because of technical errors, so users get used to clicking the blues away.
Internet Toolkit
Anti-Virus
Browsercheck
Emailcheck
Conficker test
Test SSL certificates
Whois query
My IP address
Traceroute
DNS query
Subnet calculator
MAC addresses
RFCs
Ping
Bandwidth calculator
Spam list query
IP addresses
THE H SECURITY
My wish list for Windows 7: updates for everything
Why does Windows tell me about Internet Explorer 8, but not about the new version of Adobe Reader, which fixes a critical security vulnerability that is already being actively exploited?
The H Security Conficker information site
The H Security information page on Conficker is where you can find the latest stand-alone removal tools, news, scanners and tips about the Conficker worm.
Simple Conficker test for end users
The H Security, in conjunction with heise Security,

Self-made cert

- Self-signed certificates are “obvious”
- But we're technical people
- “Signed by VeriSign” vs “Signed by Verisign”
- Assuming a user even *looks* and doesn't just click “OK”
- Users just want the web
- “Click OK until porn”

Fail Whale

- Uneducated users will always find a way to expose themselves
- But we're all smart, we're fine, right?
- Even hackers can get fooled...

Moxie Marlinspike

- Moxie Marlinspike released SSL null-byte attack at BH09
- SSL certs validated for HTTP by matching CN (common name)
- Wildcards are allowed - *.foo.com is valid for any host in foo.com
- C strings are terminated with a null byte...

Bob can vouch for me

- You trust that the CA validated foo.com before giving out the cert
- CA only gives out certs for owners of a domain
- What if we got them to sign a cert for *<null>foo.com?
- And then C code saw that null and stopped?

It's got Moxie

- Other things that use SSL for auth may be vulnerable too...
- Has to use common name, and has to allow wildcards
- VPN authentication?
- Custom apps?
- LDAP? (OpenLDAP did...)
- If it uses the MS SSL APIs...

Maybe fixed...

- Sure, the Moxie bug is fixed
- What about the next one?
- Even smart people fall to 0day
- Once your cache is poisoned, it's going to stay there...
- How often do YOU use public wifi?

Well aren't you clever...

- I'm smart!
- I use a VPN!

  -or-
- I ***force*** my users to use a VPN via user management!
- This won't work against me!

Yuh huh but...

- You're right, it wouldn't...

  …
- Except your browser has no concept of security domains
- What was cached in an insecure domain will remain for a secure domain

“Click OK to agree...”

- Many hotspots have a landing page to agree to EULA or sign in
- Many first-stage landers are not encrypted
- Unencrypted page on open network? Perfect target

Magic (h)8 ball

- If attacker controls your pre-vpn landing page...
- Then the attacker can control your browser...
- Iframes? Pop-under windows? Ajax queries dumped to nowhere?

Top 10 countdown

- All the attacker needs to do is inject code to go to the top *N* pages the victim may be likely to visit
- Request page in the background
- Cache spiked page (which the victim never saw)

Smart JS

- Attacker landing page can request content multiple times
- Compare content with signature for attack
- Request again if attack didn't land
- Now we own arbitry sites in cache ***PRE-VPN***

Frequent Landings

- Take it one step further: VPN allows access to internal pages, right?
- So if the attacker controls L2...

*D*umb *N*etwork *S*tuff

- If we own L2, can we attack other protocols?
- Sure can!
- Race the DNS server!
- Wait for a DNS query, then...
- Set a QR flag on the request and supply our own response

DNS-pwn in MSF

- Same model as Airpwn
- YAML config to match multiple queries with different responses
- Races DNS server to give user a “custom” IP

Your intranet is showing

- So if we control the browser
- We control DNS resolution
- We can re-try as quickly as we want thanks to a JS script that watches for success...
- What stops us from caching http://intranet/

(hint: Nothing)

- Nothing!
- How about a shim that ships your internal pages off to a remote server once you're on VPN?
- Or just rewrites all your form DOMs to proxy out?

Browsers cache other stuff too!

- Browsers are great!
- Speed of user experience is the biggest concern...
- So lets cache DNS in the browser, too!
- So this means...?

Trust me, it's over here

- Pre-VPN browser DNS poisoning
- Post-VPN site control thanks to guessed internal DNS names being cached as external servers

What else can we do?

- What else has cache?
- Fun fact – Flash maintains it's own cache
- Even when a user clears browser cache, Flash cache can remain
- TrustMe-ItsCool.swf

“Mobile Convergence”

“Smart” phones are dumb?

- So-called “smart” phones are really general-purpose computers now
- Complex browsers
- Lower bandwidth networks
- Yup, very happy to cache data

Not talking to you

- Of course, all the smartphones are on cell networks, right?
- I'll just use 3G!
- You can't see me there!
- True...

AT&T collects iPhone user complaints about poor service

By **Marguerite Reardon,** CNET
December 8, 2009 1:52 p.m. EST

With free app, iPhone users can report service problems. Data is collected to look for trends, AT&T says.

(CNET) -- Would you like to let AT&T know when your iPhone has dropped a call? Well, now there is an app for that.

AT&T on Monday released a new application called "Mark the Spot," which lets iPhone users submit complaints about dropped calls, poor service coverage, and less-than-perfect voice quality.

The application is free and available in the iTunes App Store. It uses GPS technology in the iPhone 3G and the iPhone 3GS to pin point where the user is when experiencing the problems. For first generation iPhones, it uses cell tower-triangulation to get a fix on problem areas.

Once the application is launched, users have several complaint options. They will see a screen that has buttons that let them report a dropped call, poor voice quality, or poor service coverage.

STORY HIGHLIGHTS

- 'Mark the Spot' app lets iPhone users submit complaints about poor coverage
- AT&T says app part of company's commitment to

NewsPulse »
Most popular stories right

Toyota recalls top 5.3 million vehicles

Police release security photo of couple

Reactions to Obama's speech

Stock selloff accelerates

Las Vegas: Most foreclosures of any city in 2009

Explore the news with News

Why Won't AT&T Admit to Its Wireless Network Problems?

By Om Malik | Mar. 16, 2009, 4:05pm PST | 88 Comments

Last summer, when Apple introduced its 3G iPhone device, I brought up the issue of AT&T not being ready for the data usage brought on by the data-centric touchscreen phone. Company officials of course denied having such problems, assuring me that they were ready.

Ready or not, a lot of people signed up for AT&T's service, and many were soon disappointed by the lack of backhaul bandwidth. For me personally it got so bad, that I switched away from the iPhone (which I love, by the way) to T-Mobile's 8900 BlackBerry and a plain old phone from Verizon.

AT&T keeps denying that it has any network bandwidth problems and continued its state of denial in an article in the New York Times this past weekend. Kristin S. Rinne, senior VP of architecture and planning for AT&T, blamed the phones and the chipsets on handsets for some of the problems.

Om Malik

OM'S POSTS

My Early Impressions of Apple's Hands-on Review

Introducing Our Newest Ace: Da

SUBSCRIBE BY EM

Email address

MOST RECENT

CELL PHONES / VOIP August 13, 2008 2:15 PM

iPhone 3G: Complaints Mount About Data Service Speeds

By Melissa J. Perenson, PC World

How often are users receiving true 3G for their data transmission speed with the iPhone 3G? After all, Apple and AT&T promote the phone as being "twice as fast" as its predecessor.

PEOPLE WHO READ THIS ALSO READ:

- What If Steve Jobs Ran One of the Big Three?
- Macworld Expo Responds to Apple Exiting Expo
- Living With an iPhone 3G, Part 2

2,093 PEOPLE VIEWED THIS

Not often enough, apparently. Most users don't seem to be experiencing the near Wi-Fi-like performance that the 3G spec promises.

In informal testing, I had mixed results. My iPhone 3G has some difficulties living up to the promised speed boost, which AT&T says should "typically" range from 600 to 1400 kilobits per second on its 3G network. You also can use AT&T's EDGE service with any iPhone--that network

Now on Technologizer...

Looking back at the future

The iPhones that weren't

Those Apple event invites

AT&T's Network Problems Aren't Just in Big Cities Anymore

By Ed Oswald | Posted at 2:10 pm on Tuesday, June 9, 2009 See all: News

The AT&T hate is strong these days, especially following the carrier's inability to deliver two of the most highly anticipated features to the single largest iPhone market in the world. But now even I am beginning to hate AT&T, and I still unfortunately have 16 more months to deal with these folks.

I've been hearing a lot of reports from people about network quality issues. I never experienced them, and I guessed it had something to do with the fact that I live in a relatively small

Technologizer
The Future of De
One) Five Things
A Smart Skeptic

Asus EEE Seash
Dell Inspiron M
Toshiba Mini Nl
HP Mini 5101: C
Browse and sear

Latest From P

PC Pitstop News

Technologizer: 1

Used to fail

- Smartphone users are used to going to wifi
- Some prefer it – power / speed / data limits
- Besides, we could “help” them along...

P13 Compact GSM/CDMA/DCS/PHS/3G Cell Phone Signal Jammer

Share your own customer images

Price: **$26.90** FREE SHIPPING

satisfaction guaranteed
or your money back

SKU 24229

Qty 1 ADD TO CART

EMAIL THIS PAGE

45 diggs digg

No payments 90 days when you spend $50 or more with PayPal Pay Later. Details
(USA Customers)

Add to Wish List | Product Updates | Price Match | Report Error

Overview | Buy 3+ and Save ($25.00 ~ $25.20) | Community Tools

In Stock: ships in 2 to 4 days (5 to 8 during new year season) Worldwide

Free Shipping

- Jams/Isolate Signals from mobile phone only. Does not affect the normal operation of other electronic devices
- Mobile Phone Signal Jammed: CDMA:850-894MHz, GSM:930-960MHz, DCS:1805-1850MHz, PHS:1900-1980MHz, 3G:2110-2170MHz
- Range: 3~15 meters
- Build-in 2500mAh lithium battery
- Package includes:
- 1 * Jammer

No, you shouldn't

- You absolutely should ***NOT*** go to import sites
- Should ***NOT*** buy illegal cell phone jammers to force victims to use wifi
- And ***of course*** someone trying to own your company wouldn't do something ***illegal***, right?

So how many?

- So how many of your users (or executives!?) carry smartphones between the office and airports?
- How do you clear the browser cache on an iPhone?

Dynamic Host Ownage Protocol

- What else can we do to L2?
- DHCP is a good target
- Smart AP can filter DHCP for authorized servers only
- But if we're talking directly to the client...
- Same trick as DNS

DHCP is fun

- Push the same info but a "custom" DNS server?
- MITM routing?
- NIS login domain?
- Netbios options?
- All perfectly plausible...

Chasing tail

- We can use a similar injection trick to append to streams
- What does a HTTP/1.0 stream look like?

TCP PSH/ACK
HTTP/1.0 200 OK
Headers: Foo
data
FIN

HTTP tail

- So what happens if we beat the FIN?
- We now control the socket
- We can continue writing data
- Script after </html> works fine!
- Defeat server filters by appending conflicting content

Gifarrr

- GIF-AR attack appends JAR to GIF
- ZIP can be appended after other content
- Exact behavior depends on browser
- Lets us sneak content in

Tail fail

- Beating the FIN is ***really*** hard to do
- Only works about 8% of the time
- Makes HTTP 1.1 mad
- Can't control caching
- Still, if it works sometimes

“But I'm encrypted!”

- Lorcon doesn't support injecting on WEP/WPA … ***yet***
- WEP is trivial – one key used for everyone
- WPA is slightly less trivial, but WPA-PSK with a known PSK isn't good...

Sharing is fun

- WPA-PSK uses one shared secret
- PSK used to compute a per-user key on join
- Sounds good... except if we know the PSK, and we watched a user join...
- The only reason WPA-PSK is “ok” for conferences is a lack of tools

Where we go from here

- Future plans:
- Better MSF integration with other L2 attacks
- Dynamic content generation based on target
- Integration with browser autopwn

802.11 fuzzing

- Lots of opportunities for fuzzing
- Already semi-continual flow of driver bugs
- Lots of variable-length and nested variable fields
- LORCON Packet Forge simplifies packet building

Joe vs the Volcano

- Very hard to detect these attacks
- Attacker is not spoofing an AP (Most IDS detect on beacons)
- IDS system must know every packet being sent legitimately to spot these
- IDS must see the packet in the air

Loosing battle

- If the IDS can even see it
- Low power highly directional antenna lets attacker snipe a single user
- Wireless IDS has no chance
- Wired IDS never sees the malicious packets

In summary...

- We've more or less figured out how to defend access points
- It's much harder to defend clients
- Especially when they go off into the world onto insecure APs

In summary...

- Using an open network?
- Sites you think you trust, you can't
- Spiked attacks can stay resident in the browser
- Your users might be bringing something back with them

In summary...

- This is bad even for ***smart*** users
- Normal users don't stand a chance
- You may already be screwed

- I warned you this would be depressing...

Trying to fix it

- Use a VPN – at least it's a start despite the problems
- Easy for **US**
- Hard for most users
- Hard to enforce: Users don't like barriers between them and internet

Other options

- SSH SOCKS tunneling (basically just a VPN)
- Mandate updates (easier said than enforced)
- Forbid users from taking laptops onto open networks (policy, UAC, don't give out laptops?)

Tragedy of trust

- Would be nice to say “move open networks to WPA”
- WPA-PSK? Better but not a solution.
- WPA-EAP? Better still, even with the same user/password you get per-user keying

Tragedy of trust

- But WPA-EAP requires SSL
- If cert is signed by a common CA, easy to get another from the same CA
- If cert is signed by self-sign CA user has to accept
- Up to user to determine valididy
- Not what users are good at

Stuck in the rut

- Hard to deploy secure public networks
- Some vendors try to solve it with custom clients
- Ties into specific OS then
- Running foreign binaries
- No really good solution yet

Protecting yourself

- Manually enforce security domains
- Use different browsers for login and normal use
- Manually clear cache
- Never keep windows open between security domains
- Still scary, forget once and you're screwed

Thanks to..

- Rsnake
- HDM
- Toast
- Renderman
- Jesse Burns
- And anyone I've forgotten

Q & A

- Lorcon @ 802.11ninja.net
- Kismet @ www.kismetwireless.net
- MSF @ metasploit.com
- Me @ dragorn@kismetwireless.net