WiFi Identification & Authentication

[redacted]

Terms and Concepts

- AP - “Access Point”
  - A device capable of accepting client WiFi connections
- SSID - “Service Set Identifier”
  - Human-readable network name (“Brown-Guest”)
- BSSID - “Basic Service Set Identifier”
  - Identifies the AP (usually the device’s MAC address)
- Can be multiple APs serving a single SSID
- Thus, can be multiple BSSIDs per SSID

SSID Issues

- SSIDs are all that identify a network
    - Can’t tell two networks with same SSID apart
- “On iPhone, beware of that AT&T WiFi hot spot”
    - “Rogue AP” problem

SSID Issues

- SSIDs are all that identify a network
  - Can't tell two networks with same SSID apart
- "On iPhone, beware of that AT&T WiFi hot spot"
  - "Rogue AP" problem
- Client devices actively broadcast trying to connect to known SSIDs
  - Sniff these broadcasts, pretend to be the SSID

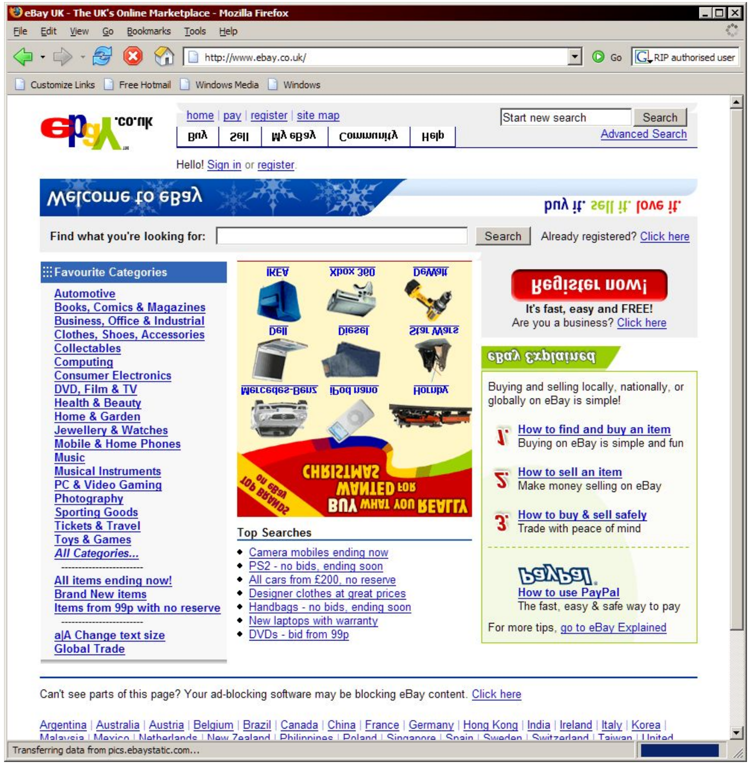
SSID Issues

- What can you do with a rogue AP?

SSID Issues

- What can you do with a rogue AP?
- Sniffing, but you could do that anyway
- Active MitM
  - Fake captive portal (phish credentials)
    - "Phishing in Public WiFi Connections Plagu China's Major Cities"
  - Upside-Down-Ternet

SSID Issues - Upside-Down-Ternet



eBay UK - The UK's Online Marketplace - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.ebay.co.uk/
Go
RIP authorised user
Customize Links
Free Hotmail
Windows Media
Windows

home | pay | register | site map

Buy | Sell | My eBay | Community | Help

Start new search Search

Advanced Search

Hello! Sign in or register.

Welcome to eBay

buy it. sell it. love it.

Find what you're looking for: Search Already registered? Click here

Favourite Categories

- Automotive
- Books, Comics & Magazines
- Business, Office & Industrial
- Clothes, Shoes, Accessories
- Collectables
- Computing
- Consumer Electronics
- DVD, Film & TV
- Health & Beauty
- Home & Garden
- Jewellery & Watches
- Mobile & Home Phones
- Music
- Musical Instruments
- PC & Video Gaming
- Photography
- Sporting Goods
- Tickets & Travel
- Toys & Games
- *All Categories...*

- All items ending now!
- Brand New items
- Items from 99p with no reserve

- a|A Change text size
- Global Trade

IKEA Xbox 360 DeWalt
Dell Diesel Star Wars
Mercedes-Benz iPod nano Hornby

CHRISTMAS WANTED FOR BUY WHAT YOU REALLY
Top Brands on eBay

Top Searches

- Camera mobiles ending now
- PS2 - no bids, ending soon
- All cars from £200, no reserve
- Designer clothes at great prices
- Handbags - no bids, ending soon
- New laptops with warranty
- DVDs - bid from 99p

Register now!

It's fast, easy and FREE!
Are you a business? Click here

eBay Explained

Buying and selling locally, nationally, or globally on eBay is simple!

1. How to find and buy an item
   Buying on eBay is simple and fun
2. How to sell an item
   Make money selling on eBay
3. How to buy & sell safely
   Trade with peace of mind

PayPal
How to use PayPal
The fast, easy & safe way to pay

For more tips, go to eBay Explained

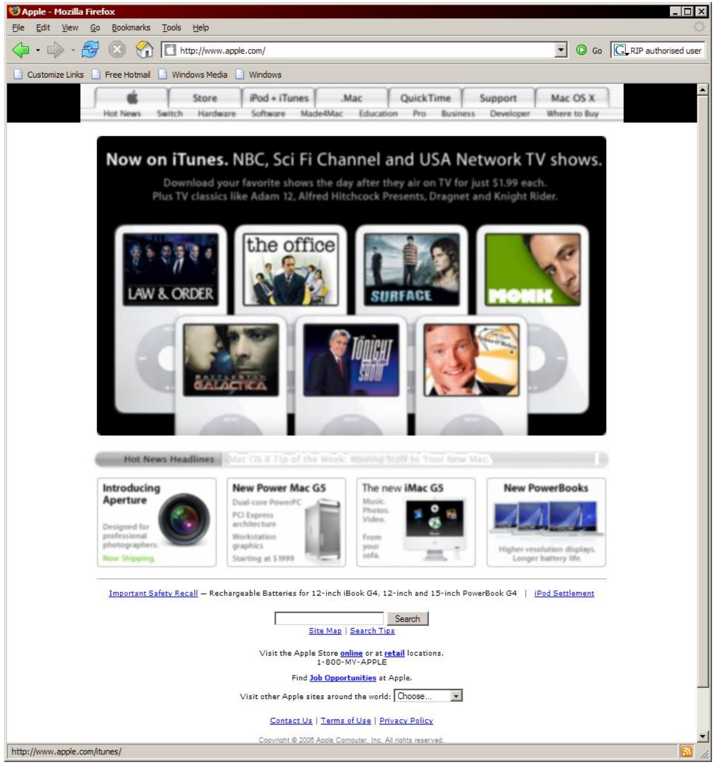
Can't see parts of this page? Your ad-blocking software may be blocking eBay content. Click here

Argentina | Australia | Austria | Belgium | Brazil | Canada | China | France | Germany | Hong Kong | India | Ireland | Italy | Korea |
Malaysia | Mexico | Netherlands | New Zealand | Philippines | Poland | Singapore | Spain | Sweden | Switzerland | Taiwan | United

Transferring data from pics.ebaystatic.com...

http://www.ex-parrot.com/pete/upside-down-ternet.html

SSID Issues - Upside-Down-Ternet



Now on iTunes. NBC, Sci Fi Channel and USA Network TV shows.

Download your favorite shows the day after they air on TV for just $1.99 each.
Plus TV classics like Adam 12, Alfred Hitchcock Presents, Dragnet and Knight Rider.

Mac OS X Tip of the Week: Moving Stuff to Your New Mac.

Introducing Aperture
Designed for professional photographers.
Now Shipping.

New Power Mac G5
Dual-core PowerPC
PCI Express architecture
Workstation graphics
Starting at $1999

The new iMac G5
Music. Photos. Video.
From your sofa.

New PowerBooks
Higher-resolution displays. Longer battery life.

Important Safety Recall — Rechargeable Batteries for 12-inch iBook G4, 12-inch and 15-inch PowerBook G4 | iPod Settlement

Site Map | Search Tips

Visit the Apple Store online or at retail locations.
1-800-MY-APPLE

Find Job Opportunities at Apple.

Visit other Apple sites around the world:

Contact Us | Terms of Use | Privacy Policy

Copyright © 2006 Apple Computer, Inc. All rights reserved.

http://www.ex-parrot.com/pete/upside-down-ternet.html

SSID Issues - Privacy

- Clients broadcast looking for known SSIDs
- What could we learn?

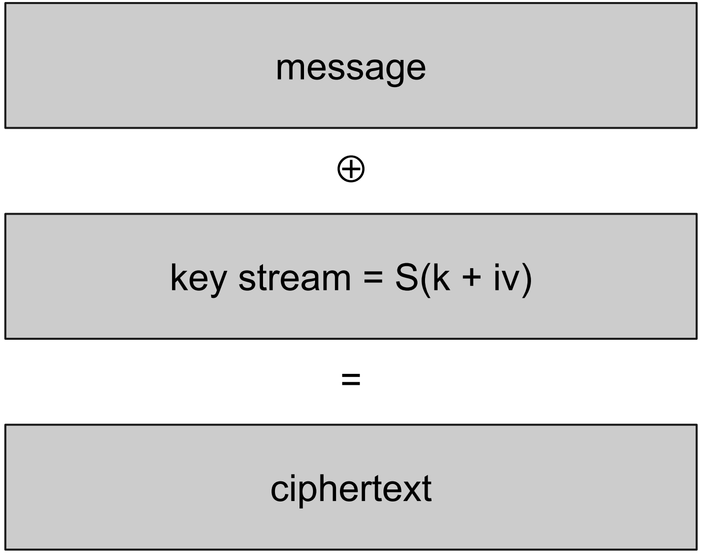
SSID Issues - Privacy

- Clients broadcast looking for known SSIDs
- What could we learn?
  - Lots, but let's look at location
- Skyhook
  - "No GPS? No problem!"
- Google Street View
  - Joffe v. Google (Google violated the Wiretap Act)
- WiGLE (Wireless Geographic Logging Engine)

Ivy + WEP

[redacted]

Ivy Problem Recap



message

⊕

key stream = S(k + iv)

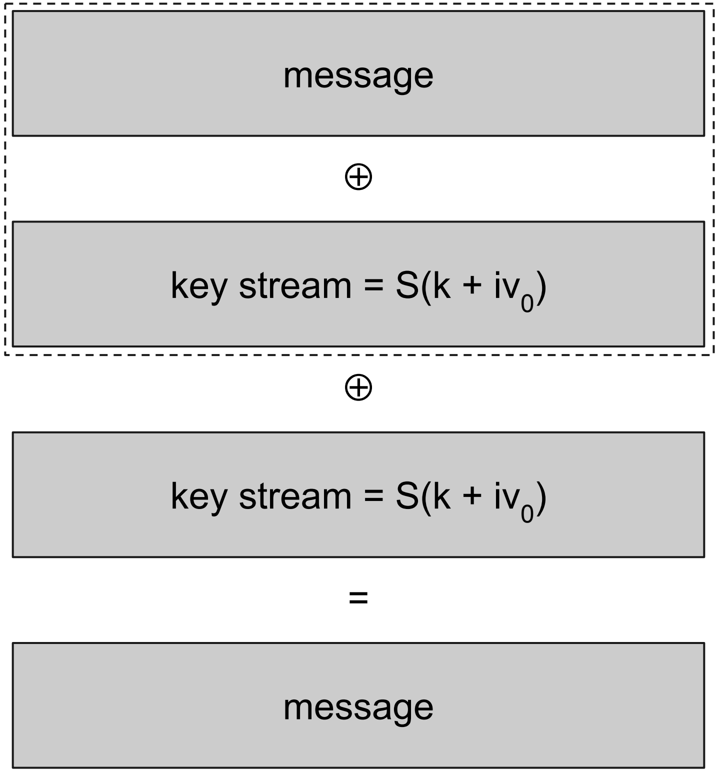
=

ciphertext

Ivy Problem Recap

- Randomly-generated IVs
- Problem: Same IV means same key stream
- Get key streams to cancel

Ivy Problem Recap



message

⊕

key stream = S(k + iv_0)

⊕

key stream = S(k + iv_0)

=

message

WEP

- Very similar to Ivy
- 24-bit IVs
- RC4 PRNG
- RC4 seed = shared secret key + iv

WEP - RC4 Weakness

- Fluhrer, Mantin, and Shamir, 2001
- RC4 has “weak [seeds]” (usually called keys)
- Given ciphertexts, can recover full RC4 seed

- WEP has RC4 seed as *key* + *iv* (*iv* is public)
- Last 24 bits of seed (IV) is enough to know whether the seed will be a weak seed

WEP Attack

- Step 1. Sniff many packets
- Step 2. Filter for IVs that indicate weak seeds
- Step 3. Recover full RC4 seed
    - High-order bits are the shared secret WEP key
- Step 4. Profit

WEP Attack

- Problem: need *many* IVs to find enough weak seeds. For a 104-bit key:
  - 40K IVs = ~50% probability of success
  - 85K IVs = ~95% probability of success
- Might take a while...

WEP Attack

- Solution: injection
- Idea: force network to send more packets

WEP Attack

- Step 1. Capture packets
- Step 2. Wait for an ARP request
  - Always 28 bytes long (WEP preserves plaintext length)
  - Once you have a candidate ARP request, send it to the AP. Does it send an ARP reply?
- Step 3. Replay the ARP request over and over
- Step 4. AP will respond to each with an ARP