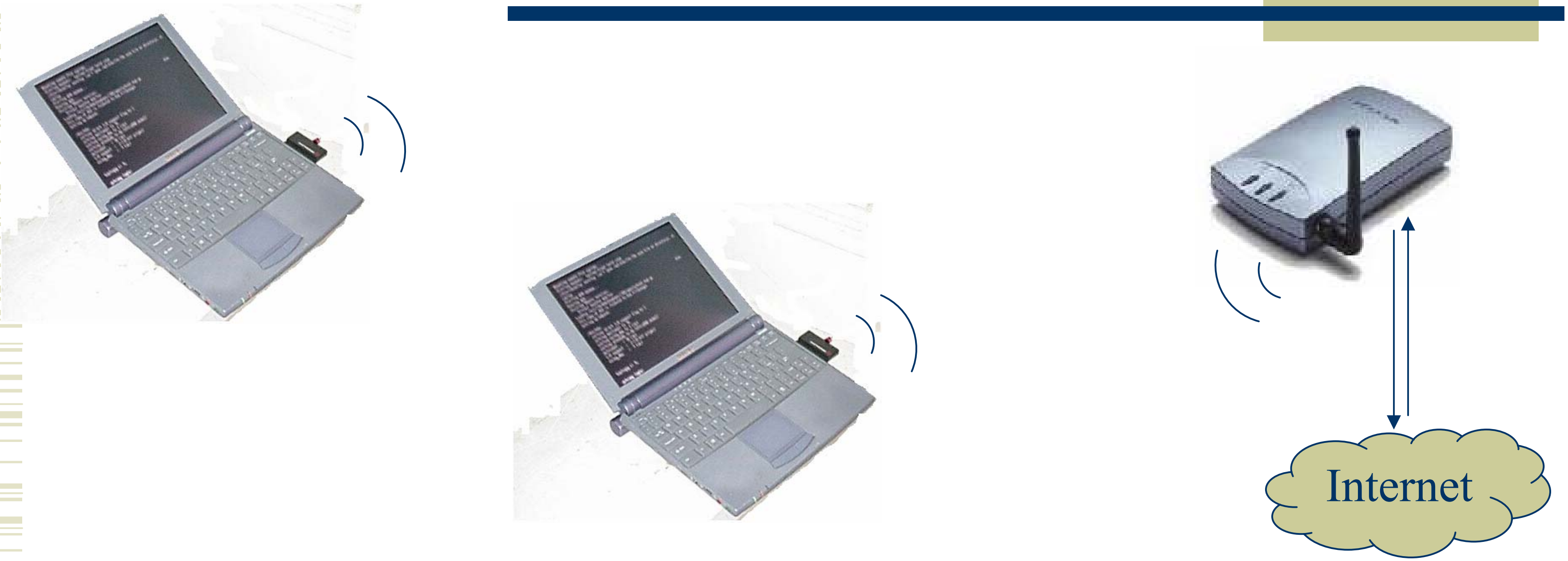
Wireless Security

David Wagner
University of California, Berkeley

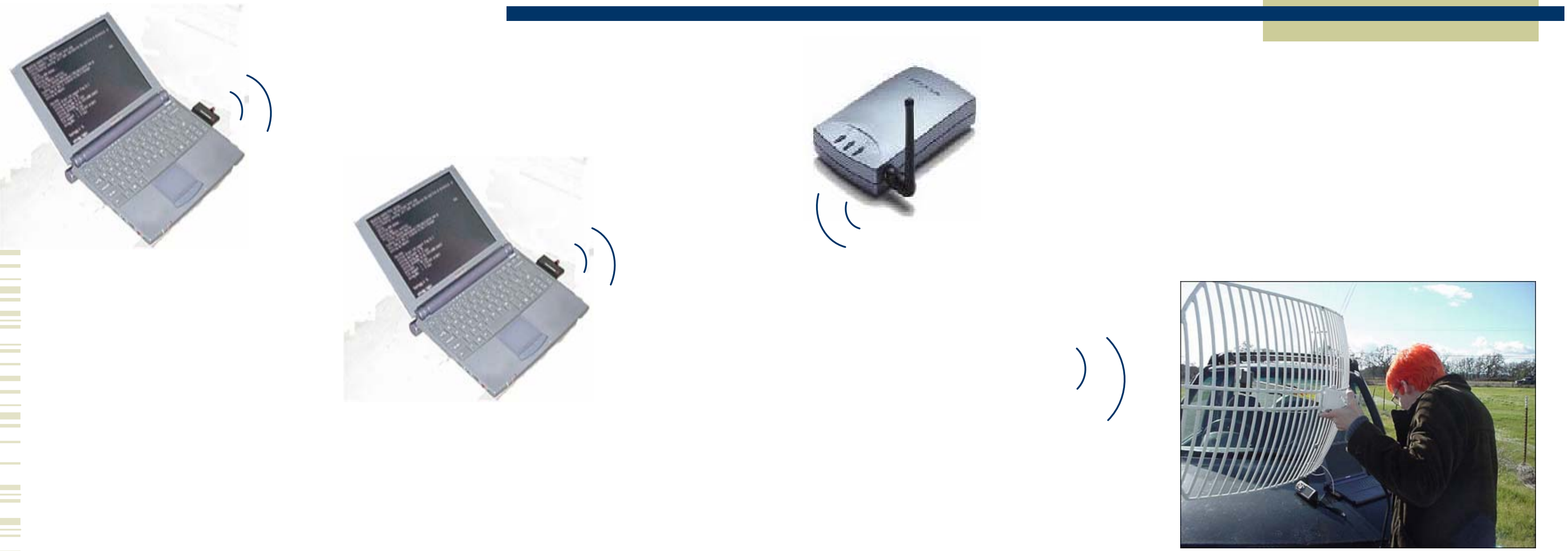
The Setting



An example of a 802.11 wireless network

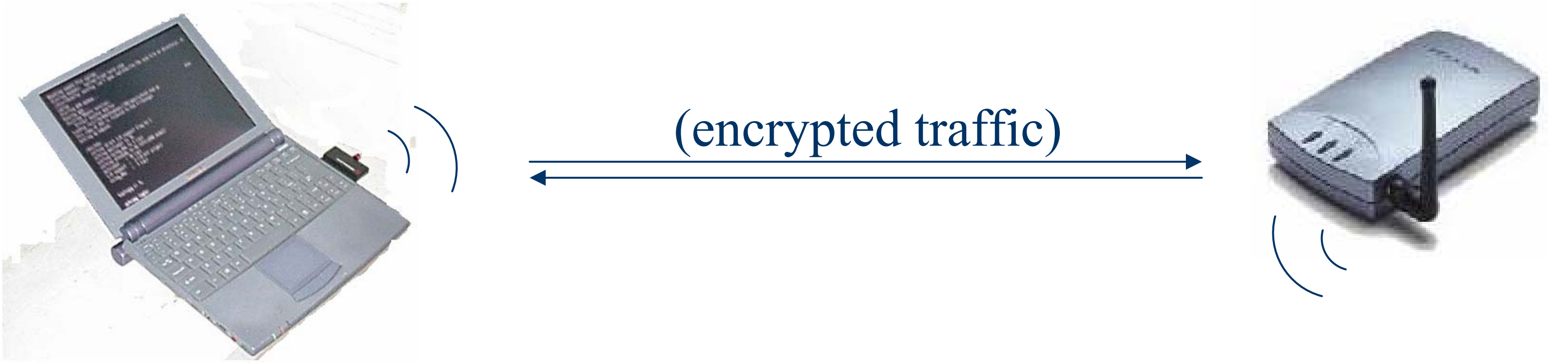
(current installed base in the millions of users)

The Problem: ***Security***!



- Wireless networking is just radio communications
  - Hence anyone with a radio can eavesdrop, inject traffic

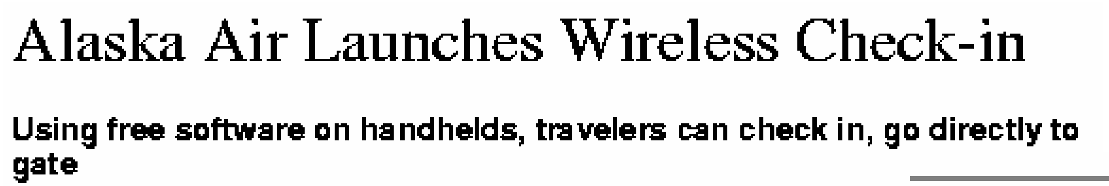
WEP



(encrypted traffic)

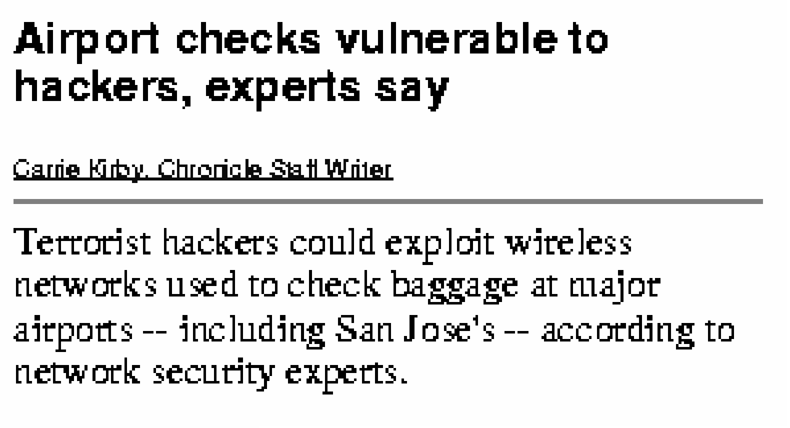
- The industry’s solution: WEP (Wired Equivalent Privacy)
    - Share a single cryptographic key among all devices
    - Encrypt all packets sent over the air, using the shared key
    - Use a checksum to prevent injection of spoofed packets

Why You Should Care



Alaska Air Launches Wireless Check-in

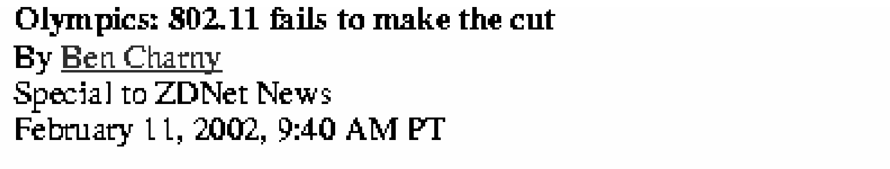
Using free software on handhelds, travelers can check in, go directly to gate



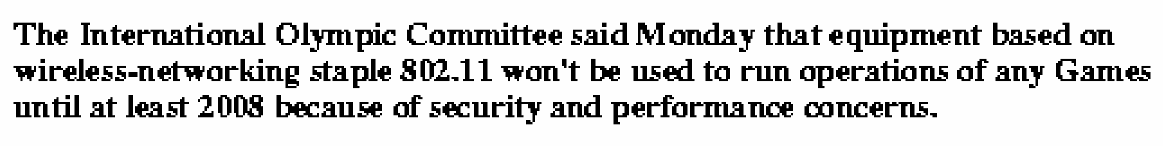
Airport checks vulnerable to hackers, experts say

Carrie Kirby, Chronicle Staff Writer

Terrorist hackers could exploit wireless networks used to check baggage at major airports -- including San Jose's -- according to network security experts.

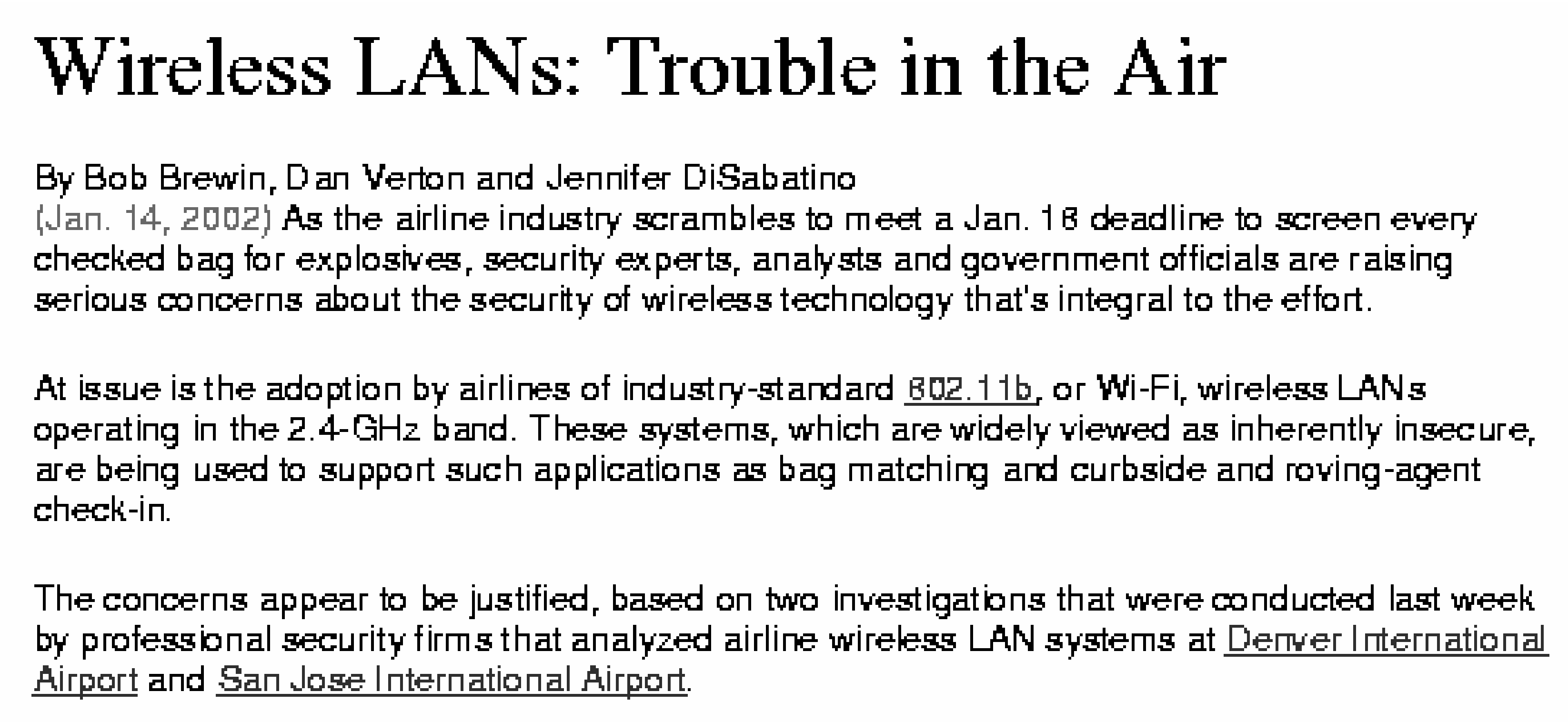


Olympics: 802.11 fails to make the cut
By Ben Charny
Special to ZDNet News
February 11, 2002, 9:40 AM PT



The International Olympic Committee said Monday that equipment based on wireless-networking staple 802.11 won't be used to run operations of any Games until at least 2008 because of security and performance concerns.

More Motivation



Wireless LANs: Trouble in the Air

By Bob Brewin, Dan Verton and Jennifer DiSabatino

(Jan. 14, 2002) As the airline industry scrambles to meet a Jan. 18 deadline to screen every checked bag for explosives, security experts, analysts and government officials are raising serious concerns about the security of wireless technology that's integral to the effort.

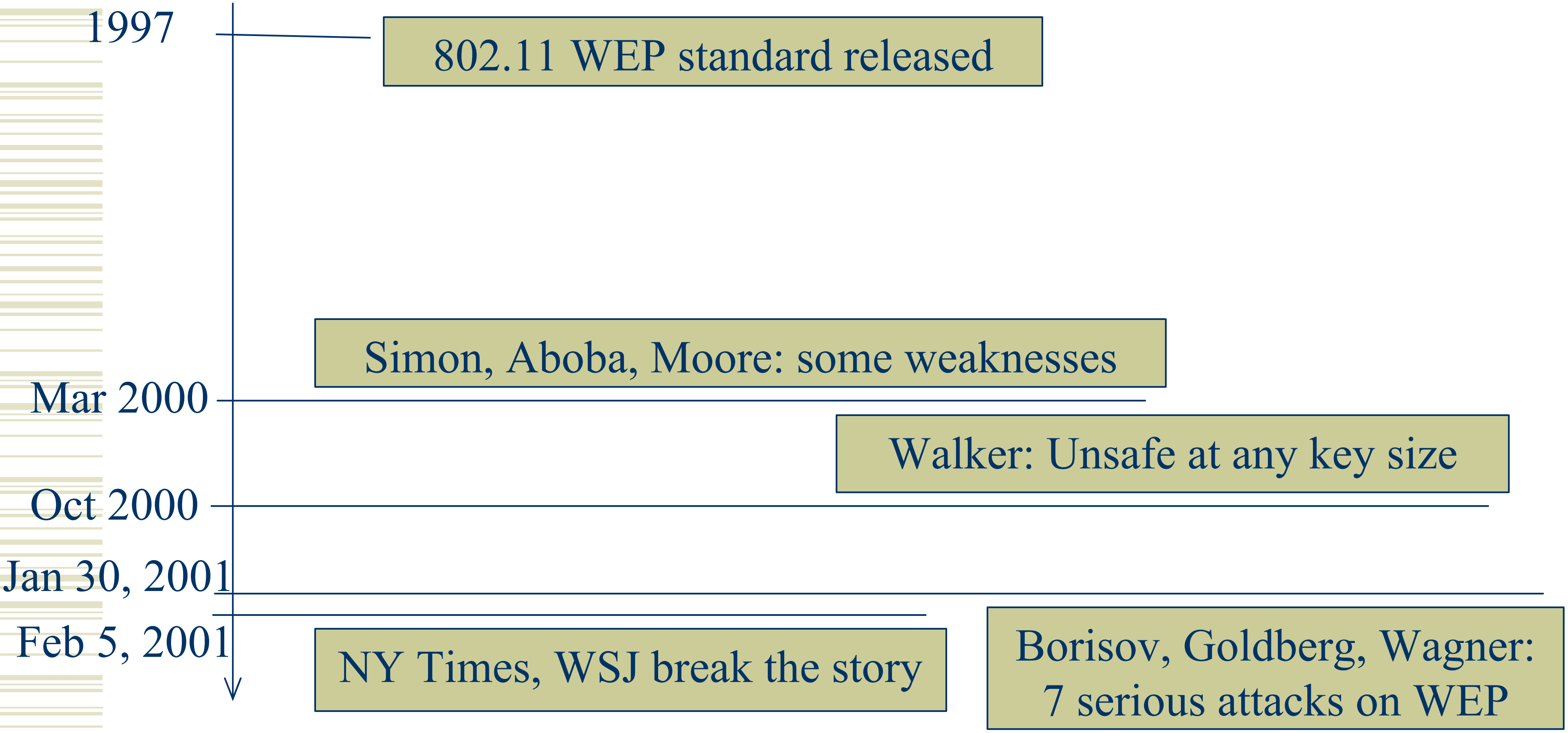
At issue is the adoption by airlines of industry-standard 802.11b, or Wi-Fi, wireless LANs operating in the 2.4-GHz band. These systems, which are widely viewed as inherently insecure, are being used to support such applications as bag matching and curbside and roving-agent check-in.

The concerns appear to be justified, based on two investigations that were conducted last week by professional security firms that analyzed airline wireless LAN systems at Denver International Airport and San Jose International Airport.

Overview of the Talk

- In this talk:
  - Security evaluation of WEP
  - The history, where we stand today, and future directions

Early History of WEP



1997

802.11 WEP standard released

Simon, Aboba, Moore: some weaknesses

Mar 2000

Walker: Unsafe at any key size

Oct 2000

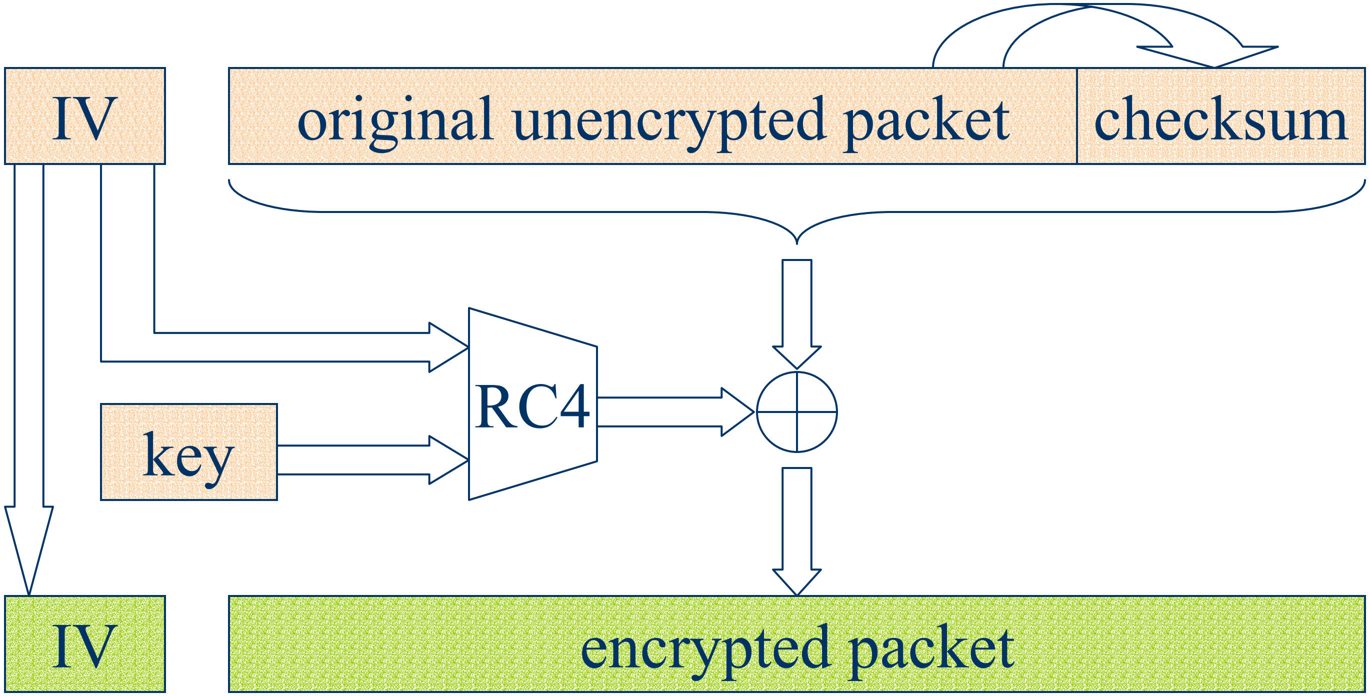
Jan 30, 2001

Feb 5, 2001

NY Times, WSJ break the story

Borisov, Goldberg, Wagner: 7 serious attacks on WEP

How WEP Works



A Property of RC4

- Keystream leaks, under known-plaintext attack
  - Suppose we intercept a ciphertext C, and suppose we can guess the corresponding plaintext P
  - Let Z = RC4(key, IV) be the RC4 keystream
  - Since $C = P \oplus Z$, we can derive the RC4 keystream Z by $Z = P \oplus C = P \oplus (P \oplus Z)$
- This is not a problem ... unless keystream is reused!

A Risk With RC4

- If any IV ever repeats, confidentiality is at risk
  - Suppose P, P' are two plaintexts encrypted with same IV
  - Let Z = RC4(key, IV); then the two ciphertexts are $C = P \oplus Z$ and $C' = P' \oplus Z$
  - Note that $C \oplus C' = (P \oplus Z) \oplus (P' \oplus Z) = (Z \oplus Z) \oplus (P \oplus P') = P \oplus P'$
  - Hence the xor of both plaintexts is revealed
  - If there is redundancy, this may reveal both plaintexts
  - Or, if we can guess one plaintext, the other is leaked
- So: If RC4 isn't used carefully, it becomes insecure

Attack #1: Keystream Reuse

- WEP didn't use RC4 carefully
- The problem: IV's frequently repeat
  - The IV is often a counter that starts at zero
  - Hence, rebooting causes IV reuse
  - Also, there are only 16 million possible IV's, so after intercepting enough packets, there are sure to be repeats
- Implications: can eavesdrop on 802.11 traffic
  - An eavesdropper can decrypt intercepted ciphertexts even without knowing the key

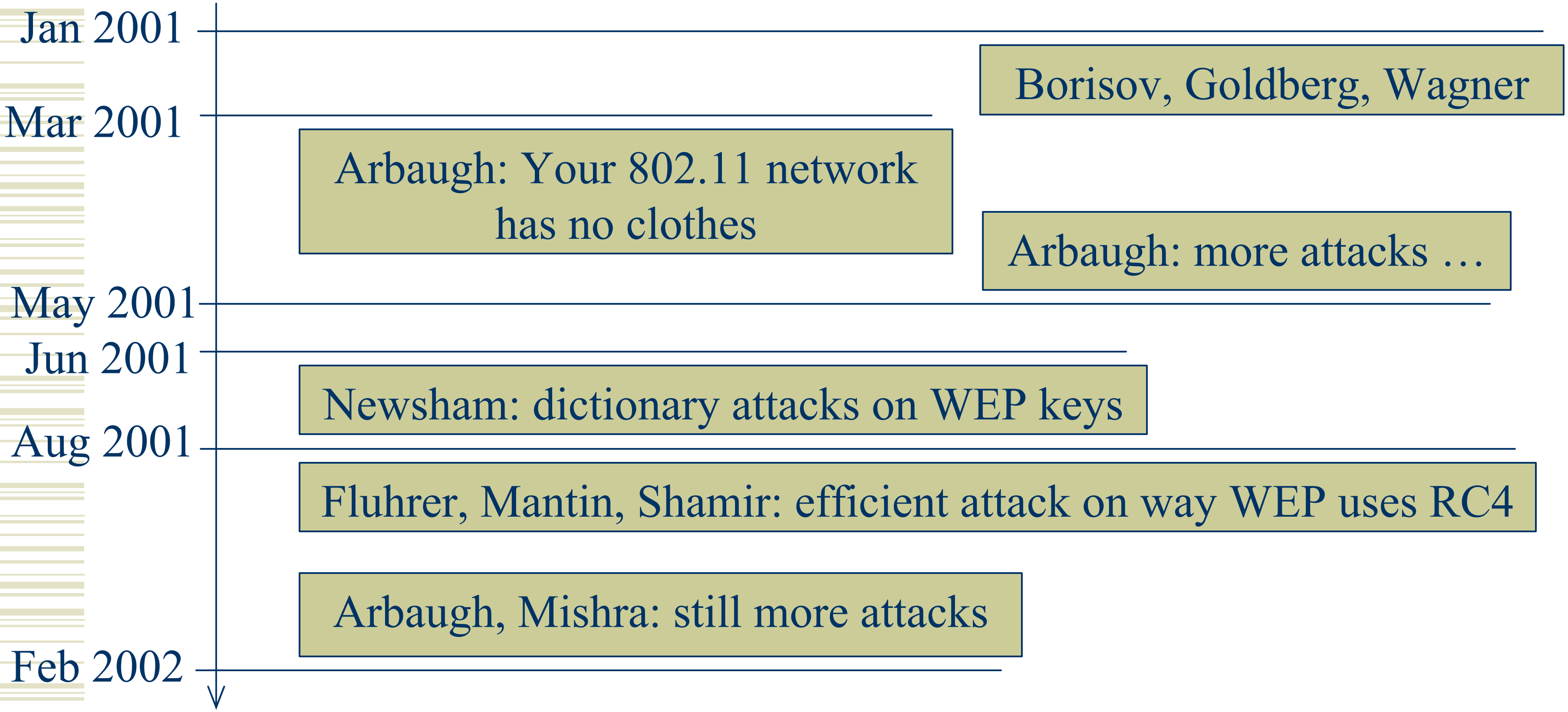
Attack #2: Spoofed Packets

- Attackers can inject forged traffic onto 802.11 nets
  - Suppose I know the value *Z* = RC4(key, IV) for some IV
    - e.g., by decrypting a single packet
  - This is all I need to know to encrypt using this IV
  - Since the checksum is unkeyed, I can create valid ciphertexts that will be accepted by the receiver
- Implication: can bypass access control
  - Can attack any computer attached to the wireless net

Summary So Far

- None of WEP’s goals are achieved
  - Confidentiality, integrity, access control all broken
- And these are only 2 of the 7 attacks we showed in our paper…

Subsequent Events



Jan 2001

Borisov, Goldberg, Wagner

Mar 2001

Arbaugh: Your 802.11 network has no clothes

Arbaugh: more attacks …

May 2001

Jun 2001

Newsham: dictionary attacks on WEP keys

Aug 2001

Fluhrer, Mantin, Shamir: efficient attack on way WEP uses RC4

Arbaugh, Mishra: still more attacks

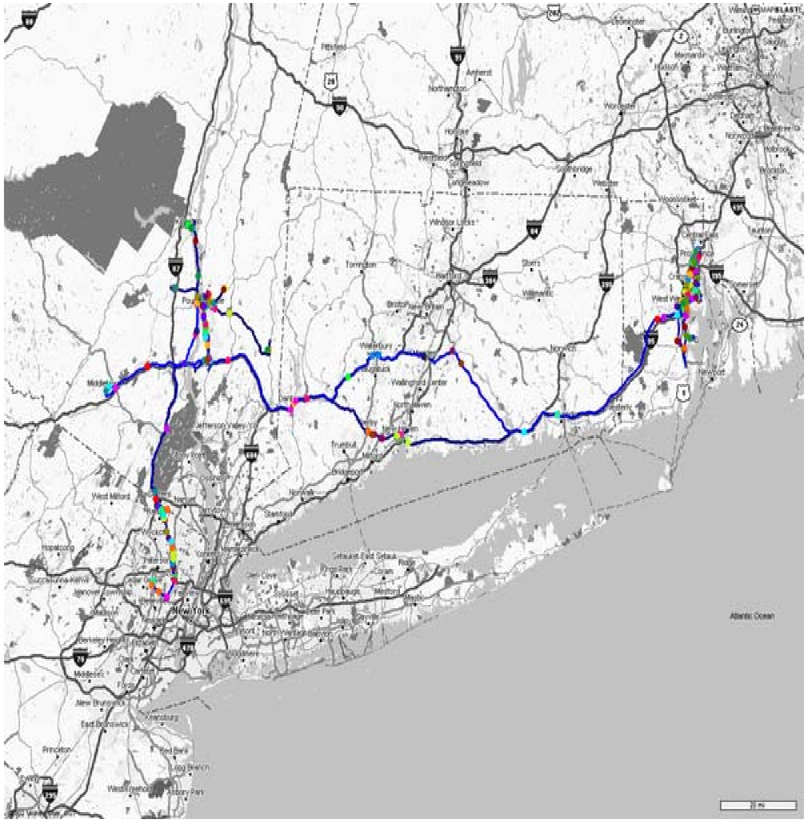
Feb 2002

Evaluation of WEP

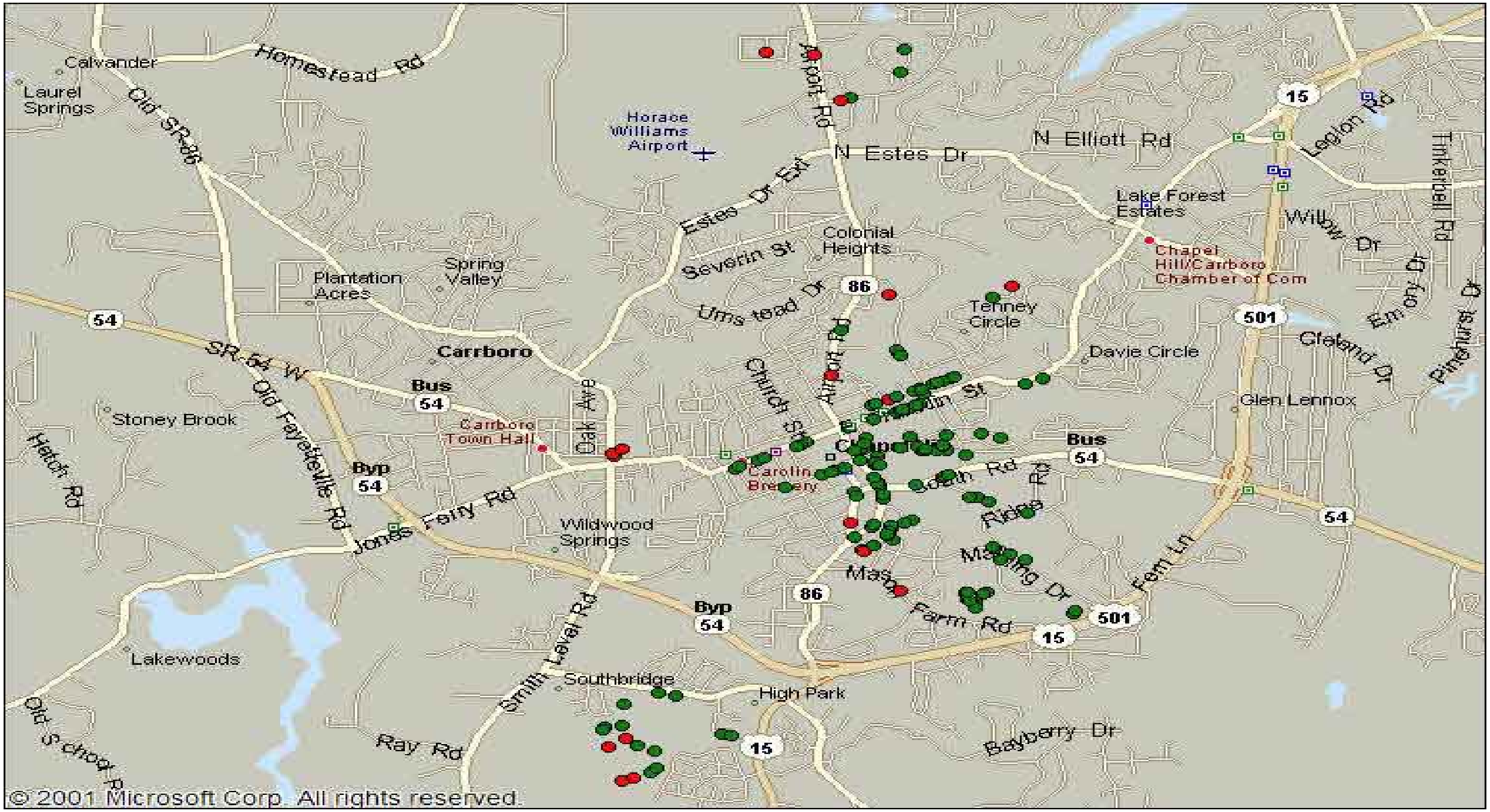
- WEP cannot be trusted for security
  - Attackers can eavesdrop, spoof wireless traffic
  - Can often break the key with a few minutes of traffic
- Attacks are very serious in practice
  - Attack tools are available for download on the Net
  - Hackers sitting in a van can watch all your wireless data, despite the encryption

War Driving

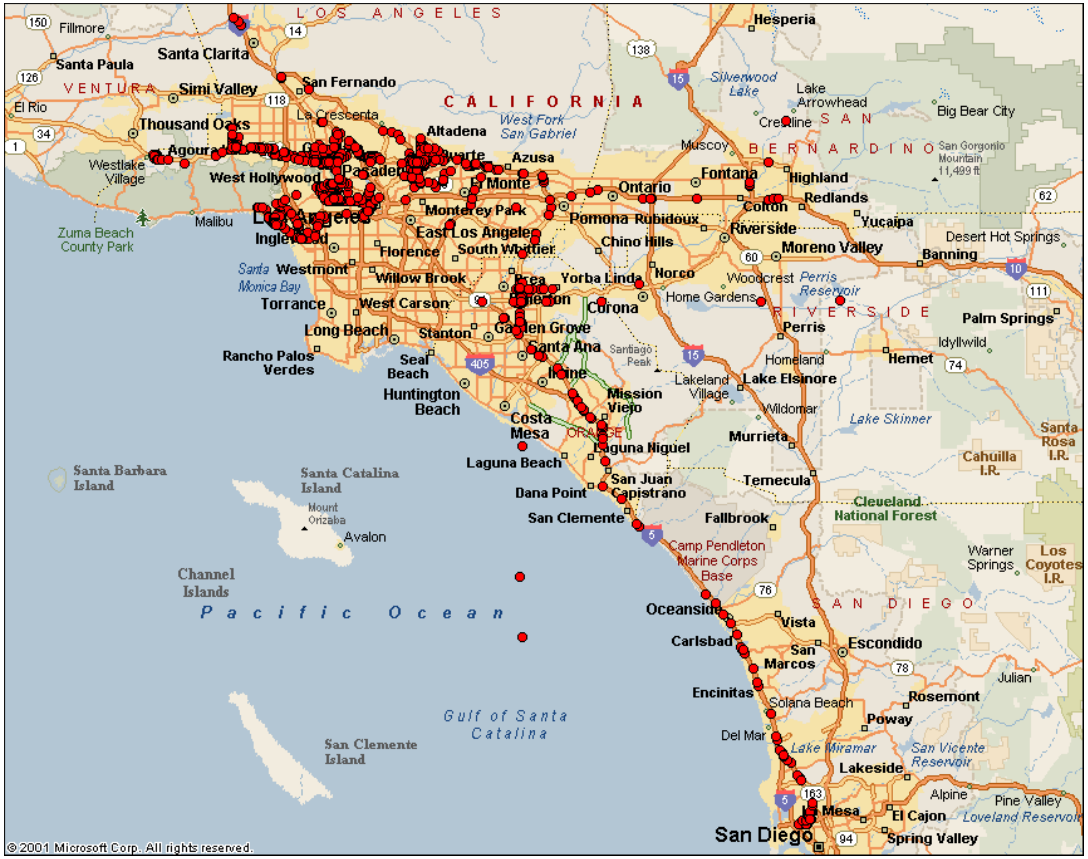
- To find wireless nets:
  - Load laptop, 802.11 card, and GPS in car
  - Drive
- While you drive:
  - Attack software listens and builds map of all 802.11 networks found



War Driving: Chapel Hill

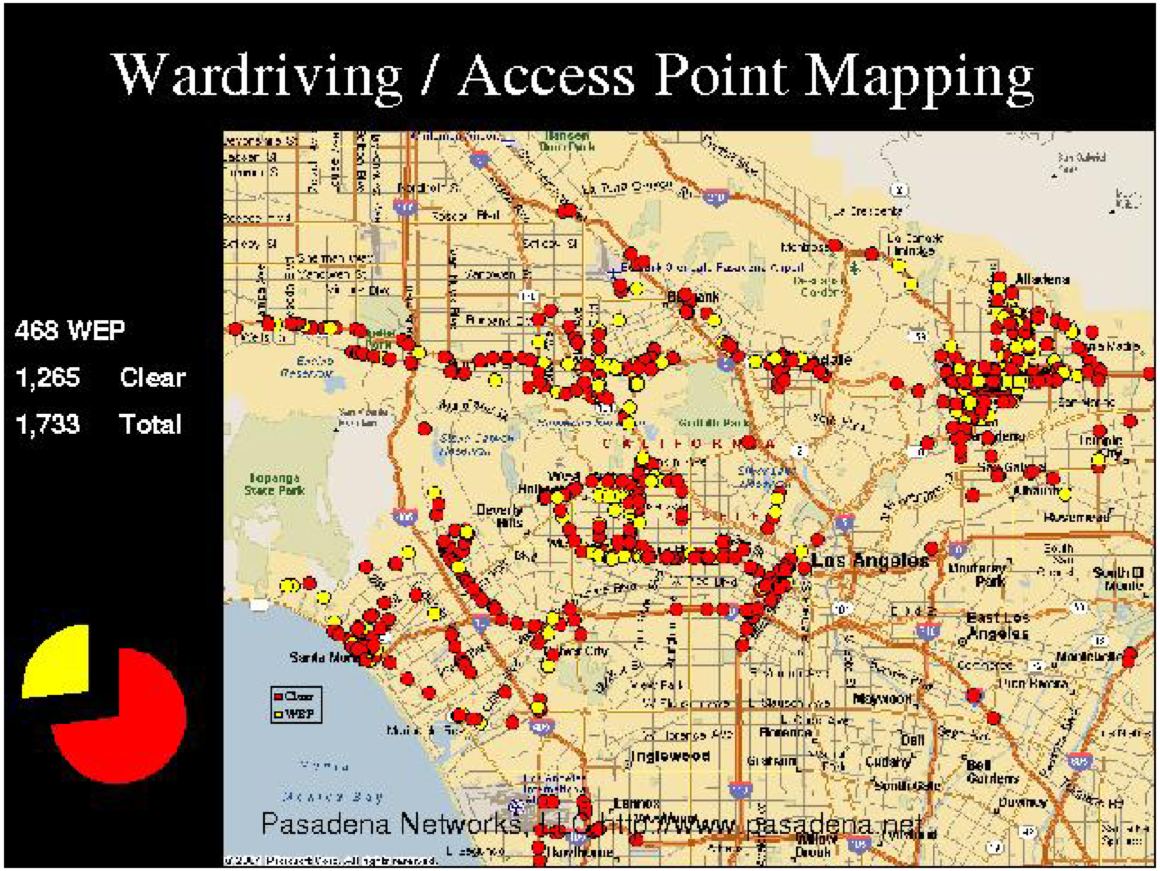


Driving from LA to San Diego



© 2001 Microsoft Corp. All rights reserved.

Zoom in on Los Angeles



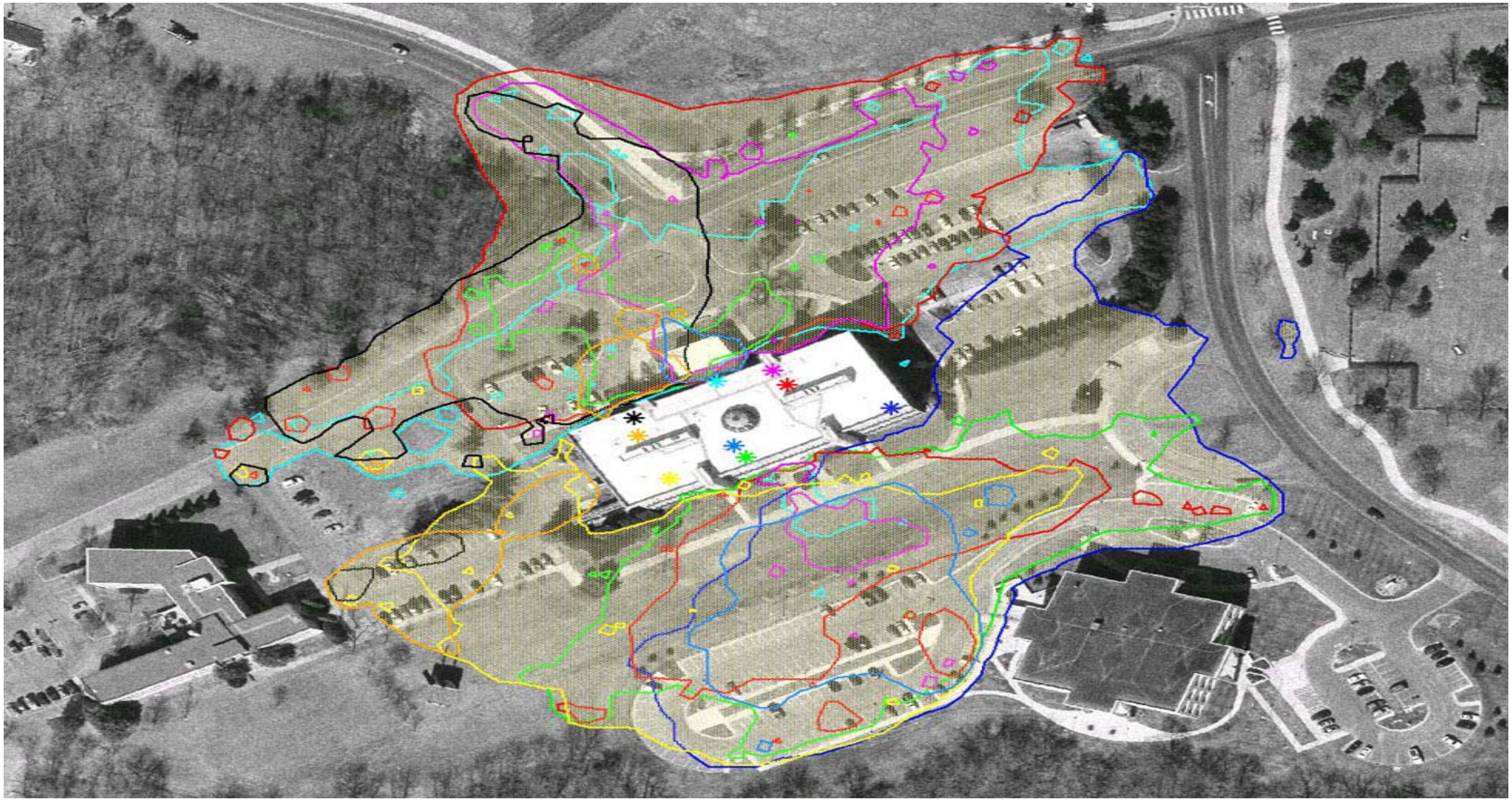
Wardriving / Access Point Mapping

468	WEP
1,265	Clear
1,733	Total

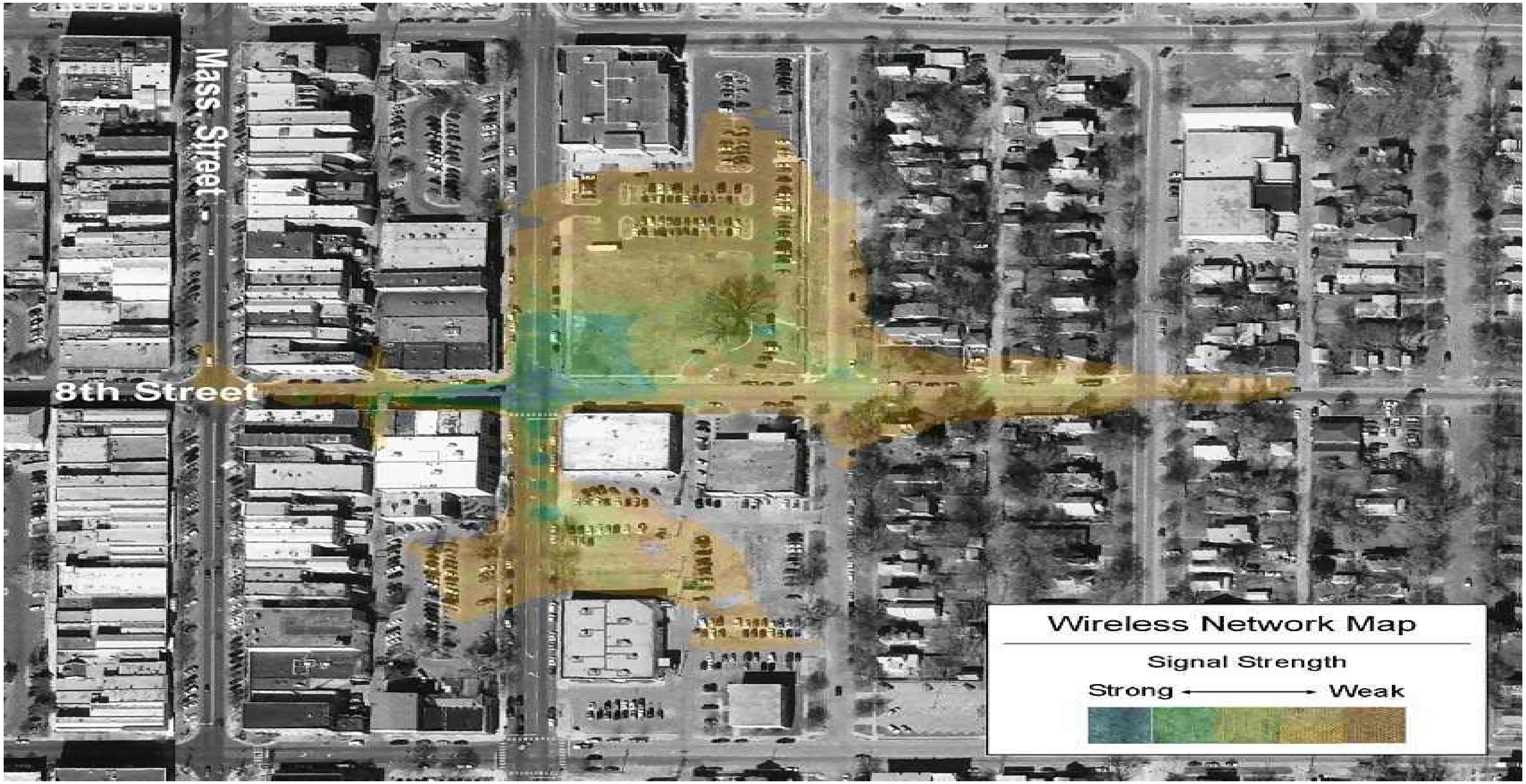
🟥 Clear
🟨 WEP

Pasadena Networks, LLC http://www.pasadena.net

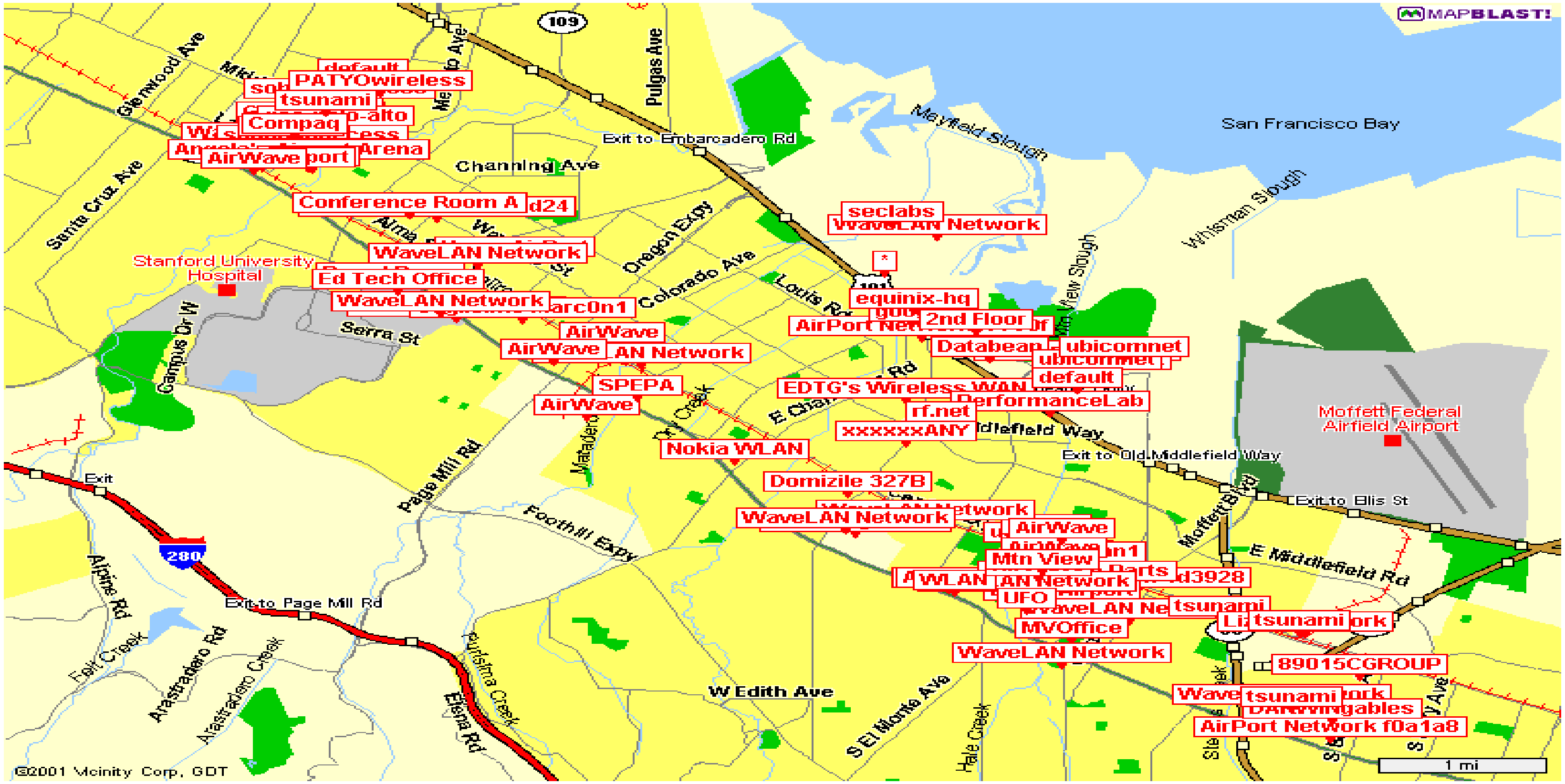
Example: RF Leakage



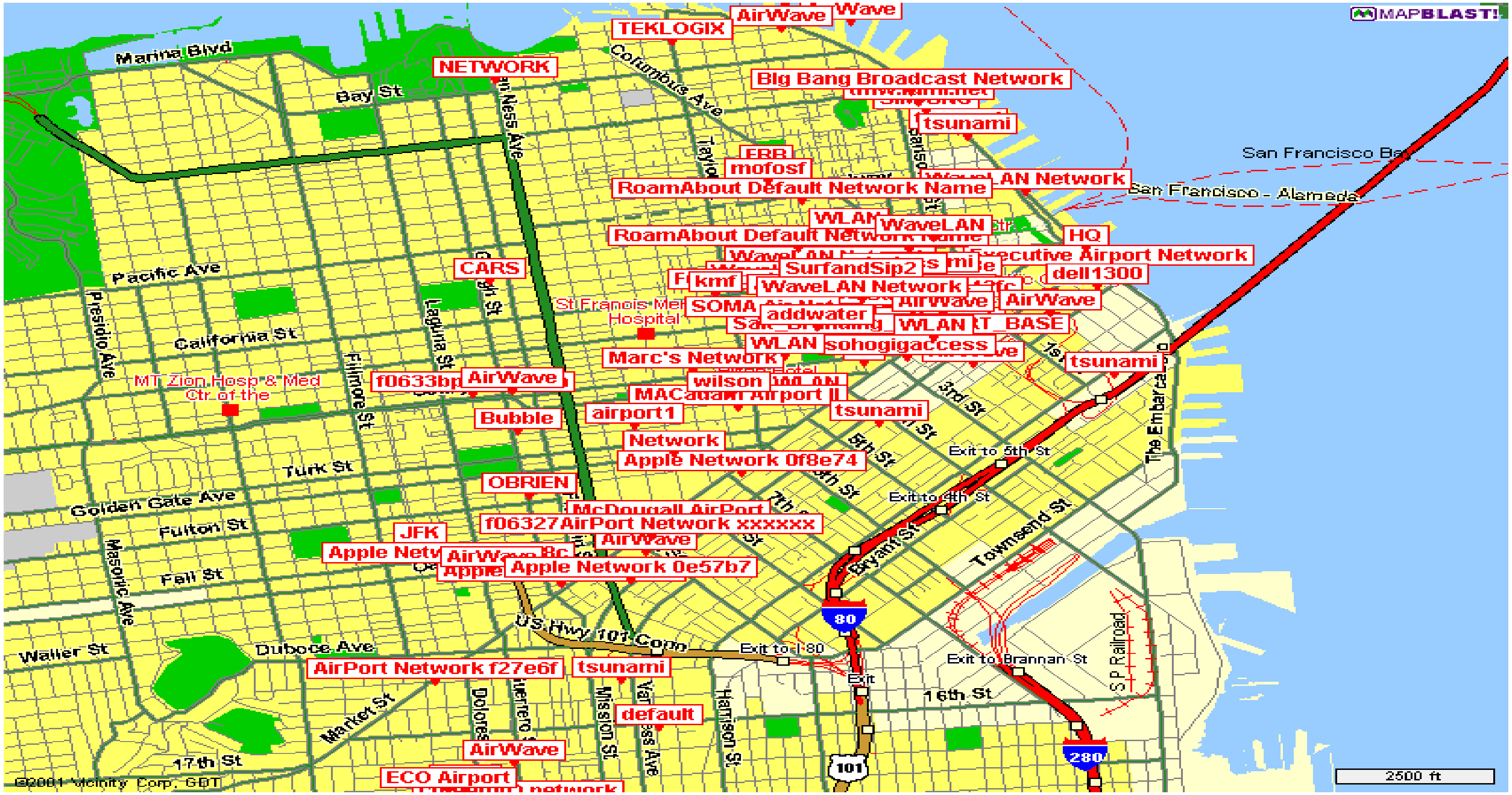
One Network in Kansas City



Silicon Valley

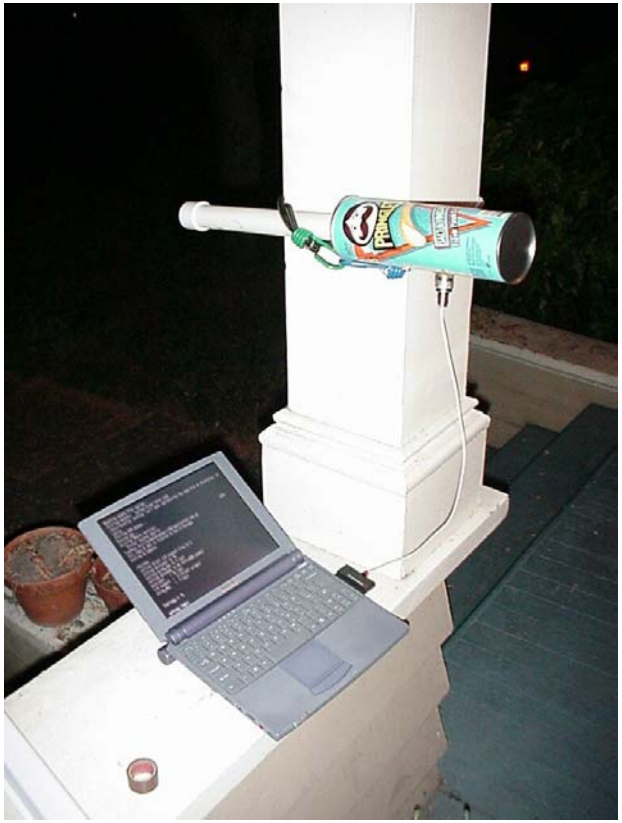


San Francisco



Toys for Hackers

A Dual-Use Product



(28 g / about 14 crisps)
Servings Per Container about 6
Amount Per Serving
Calories 160 Calories from Fat 100
% Daily Value*
Total Fat 11 g 17%
Saturated Fat 1.5 g 8%
Cholesterol 0 mg 0%
Sodium 8%
Total 5%
4%
Vitamin C 6%
Not a significant source of vitamin A, calcium, and iron.
*Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher

Conclusions

- Wireless networks: insecure in theory & in practice
  - 50-70% of networks never even turn on encryption, and the remaining are vulnerable to attacks shown here
  - Hackers are exploiting these weaknesses in the field, from distances of a mile or more
- Lesson: Open design is important
  - These problems were all avoidable
- In security-critical contexts, be wary of wireless!