Wireless Security

David Wagner
University of California at Berkeley

Wireless Networking is Here

802.11 wireless networking is on the rise

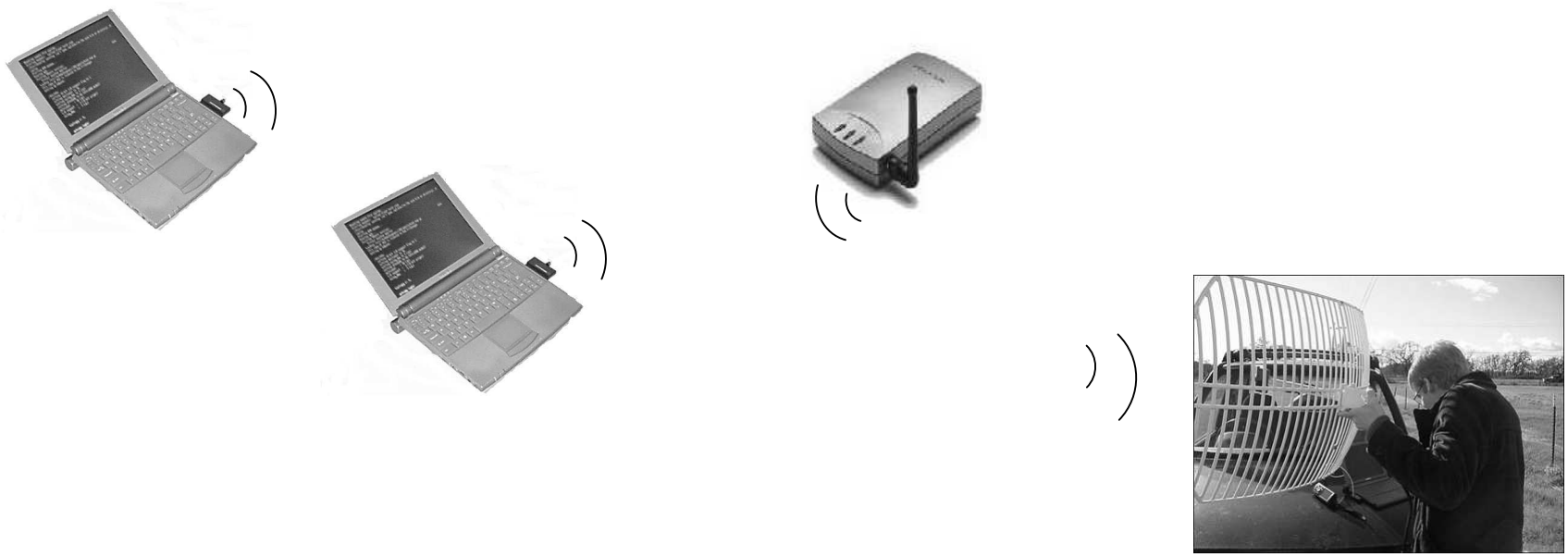
- installed base: ~ 15 million users
- currently a $1 billion/year industry

The Problem: Security

Wireless networking is just radio communications

- Hence anyone with a radio can eavesdrop, inject traffic

The Problem: Security



Wireless networking is just radio communications

- Hence anyone with a radio can eavesdrop, inject traffic

The Security Risk: RF Leakage

The Risk of Attack From Afar

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.

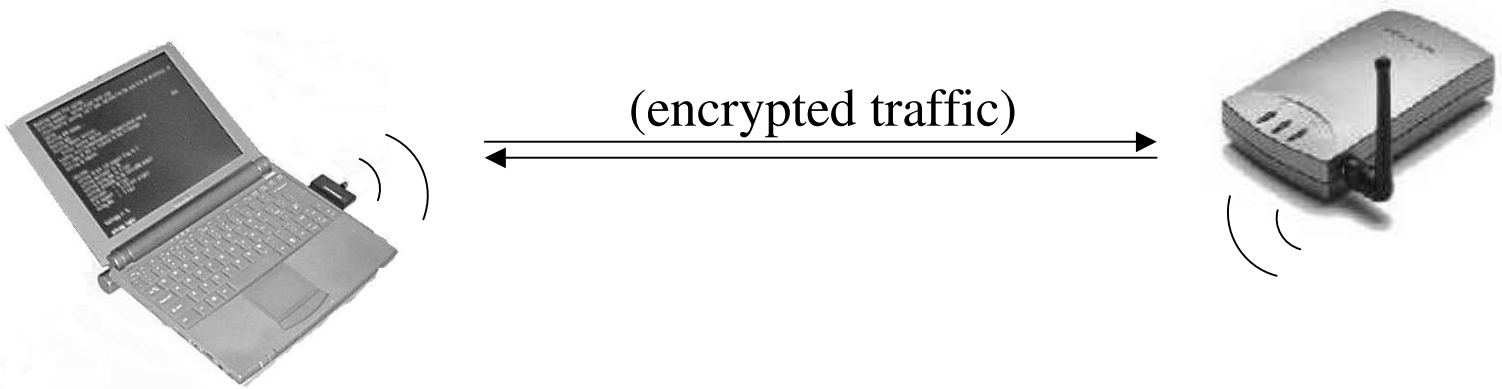
At issue is the adoption by airlines of industry-standard 802.11b, or Wi-Fi, wireless LANs operating in the 2.4-GHz band. These systems, which are widely viewed as inherently insecure, are being used to support such applications as bag matching and curbside and roving-agent check-in.

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

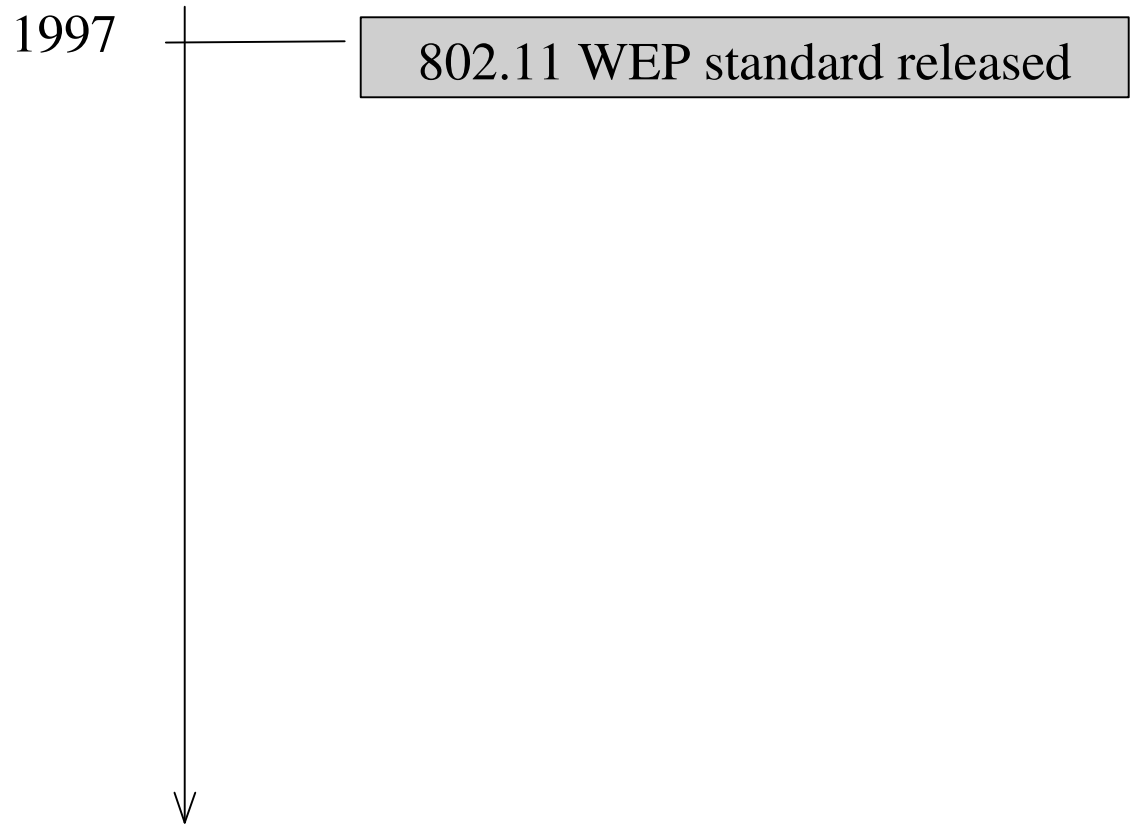
- In this talk:
  - WEP, and its (in)security -- a parade of attacks
  - Theory of modern crypto, or,
    How these problems could have been prevented
  - Where we stand today, in practice

WEP

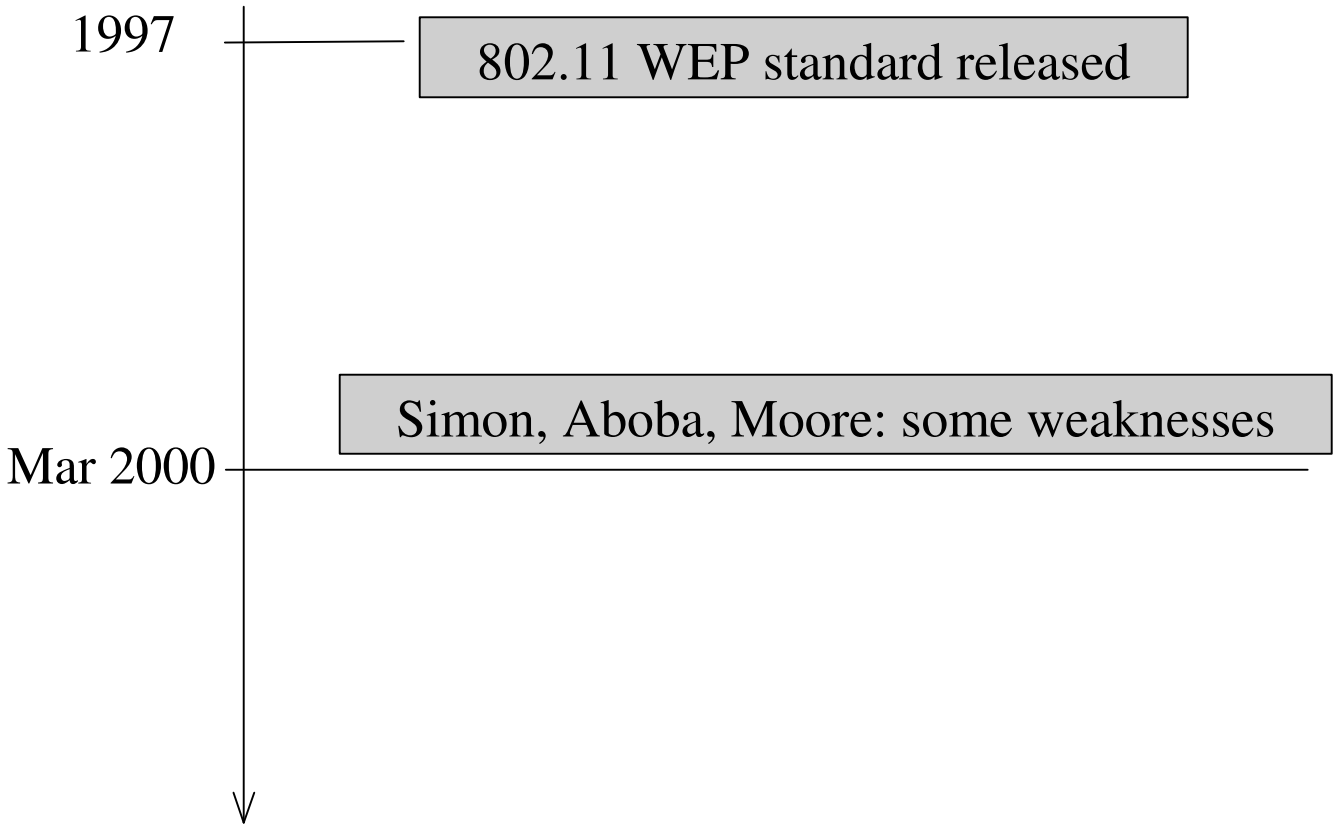


- The industry's solution: WEP (Wired Equivalent Privacy)
  - Share a single cryptographic key among all devices
  - Encrypt all packets sent over the air, using the shared key
  - Use a checksum to prevent injection of spoofed packets

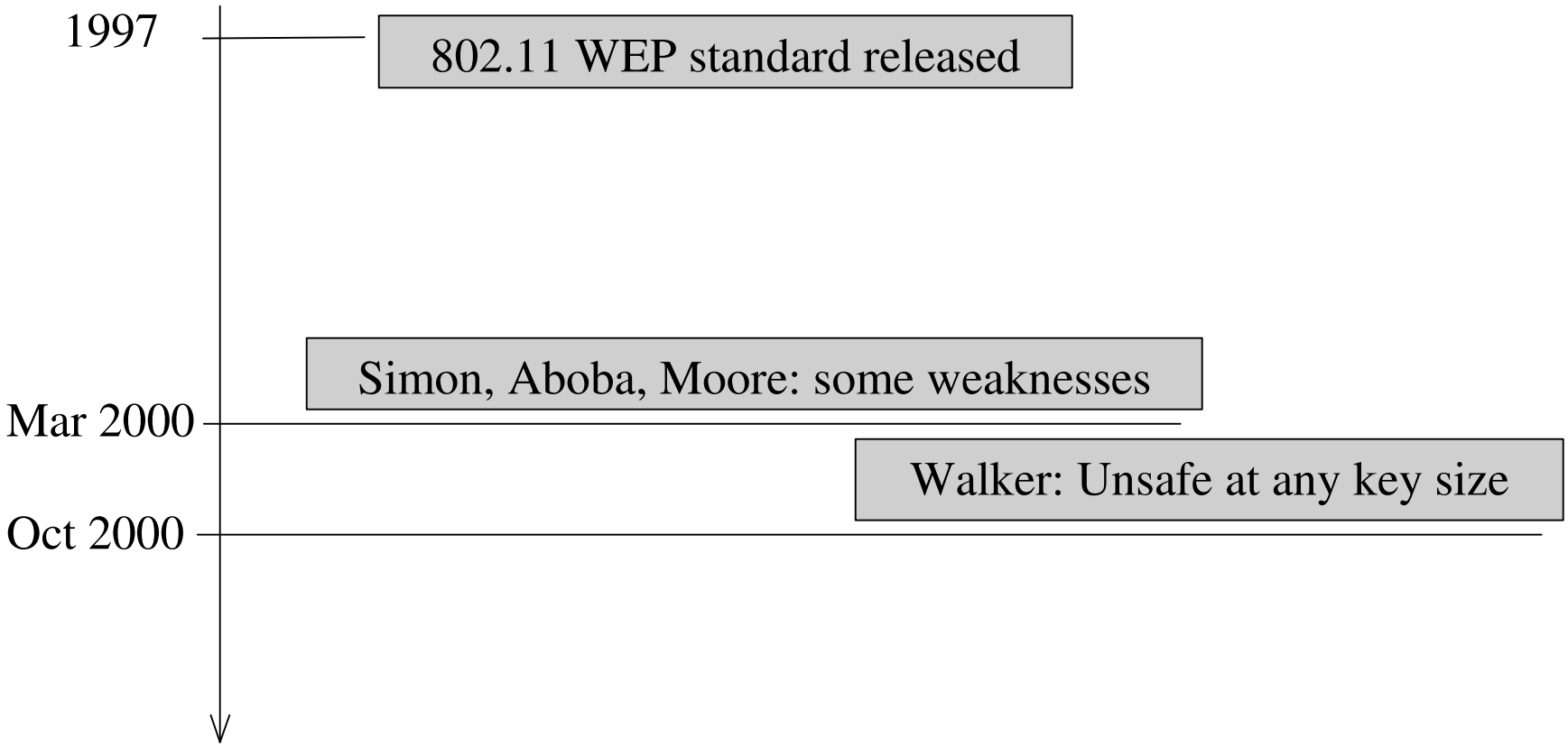
Early History of WEP



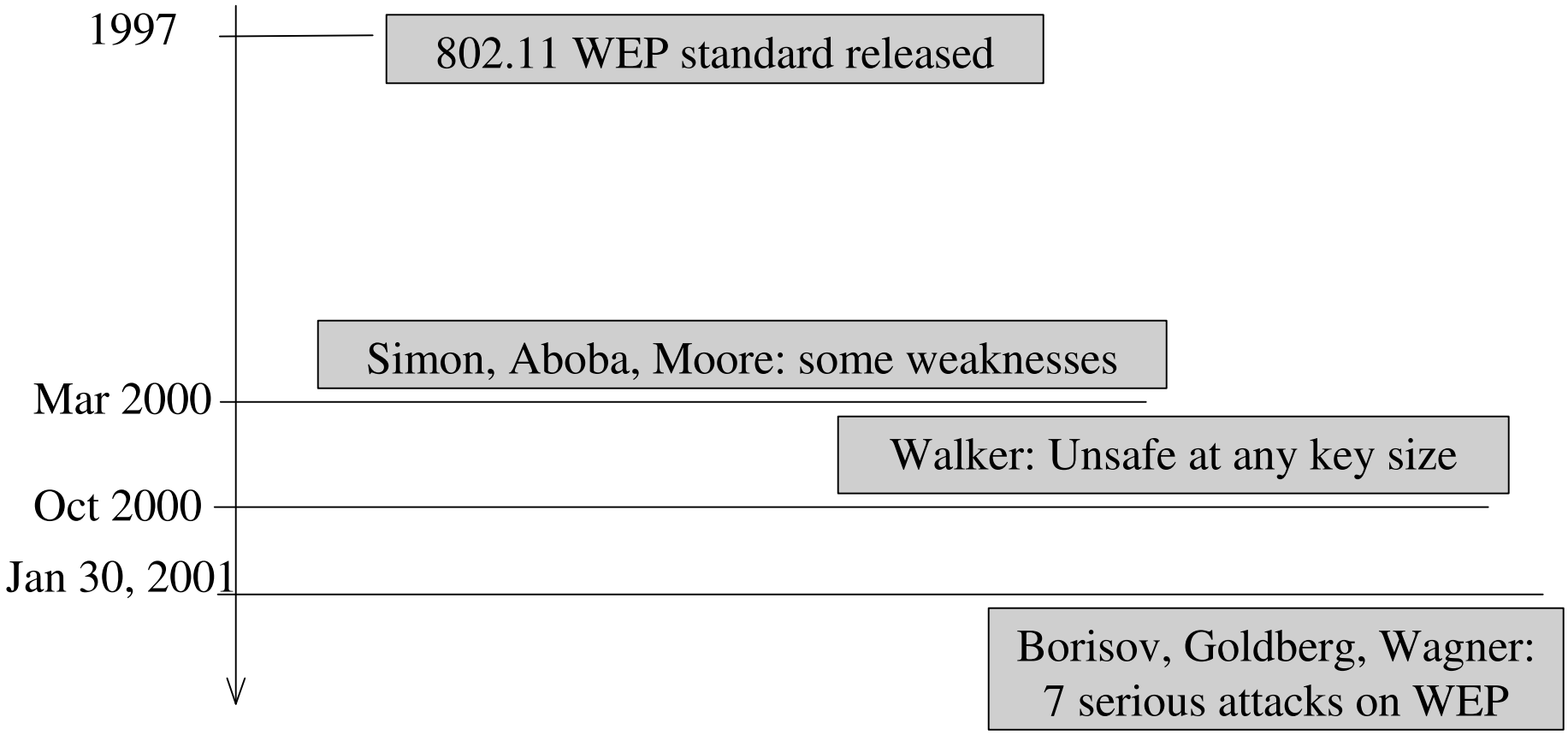
Early History of WEP



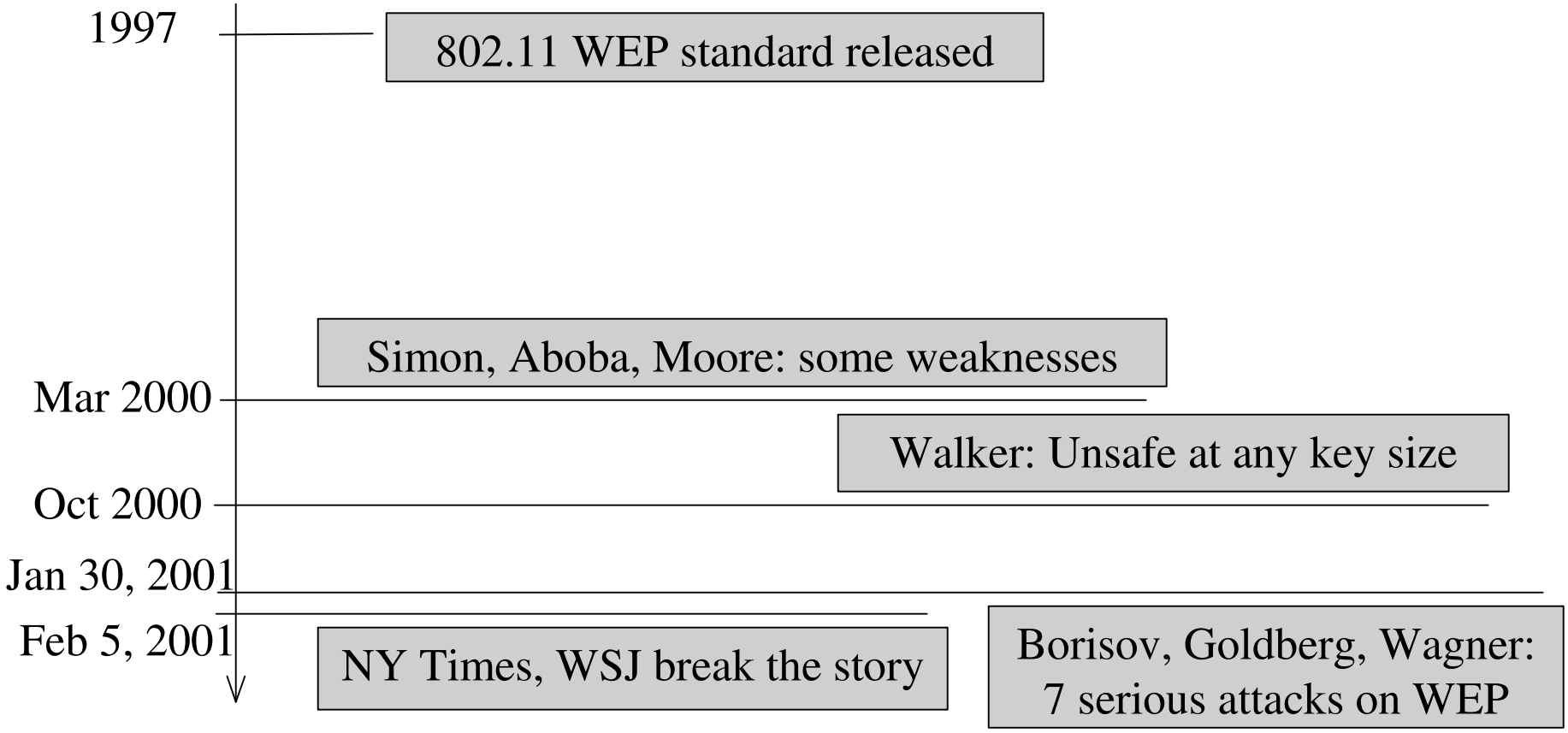
Early History of WEP



Early History of WEP



Early History of WEP



WEP - A Little More Detail

IV, $P \oplus RC4(K, IV)$

- WEP uses the RC4 stream cipher to encrypt a TCP/IP packet (P) by xor-ing it with keystream (RC4(K, IV))

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 $Z = RC4(K, IV)$ be the RC4 keystream
  - Since $C = P \oplus Z$, we can derive the RC4 keystream Z by $P \oplus C = P \oplus (P \oplus Z) = Z$
- This is not a problem ... unless keystream is reused!

A Risk of Keystream Reuse

IV, $P \oplus RC4(K, IV)$

IV, $P' \oplus RC4(K, IV)$

- If IV's repeat, confidentiality is at risk
  - If we send two ciphertexts (C, C′) using the same IV, then the xor of plaintexts leaks ($P \oplus P' = C \oplus C'$), which might reveal both plaintexts
- ➢ Lesson: If RC4 isn't used carefully, it becomes insecure

A Risk With RC4

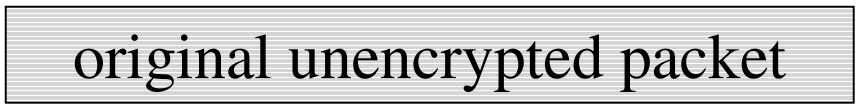
- If any IV ever repeats, confidentiality is at risk
  - Suppose P, P' are two plaintexts encrypted with same IV
  - Let Z = RC4(key, IV); then the two ciphertexts are $C = P \oplus Z$ and $C' = P' \oplus Z$
  - Note that $C \oplus C' = P \oplus P'$, hence the xor of both plaintexts is revealed
  - If 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
- Attackers can eavesdrop on 802.11 traffic
  - An eavesdropper can decrypt intercepted ciphertexts even without knowing the key

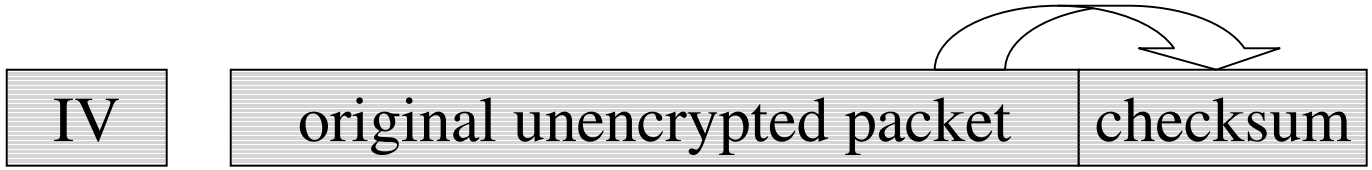
WEP -- Even More Detail

WEP -- Even More Detail

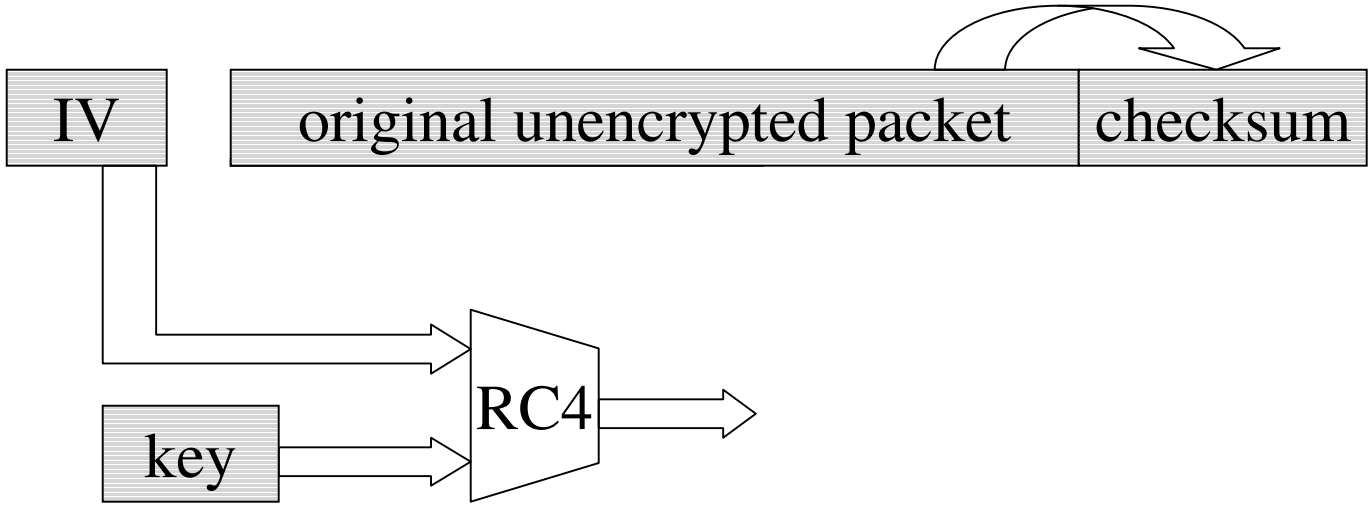


WEP -- Even More Detail

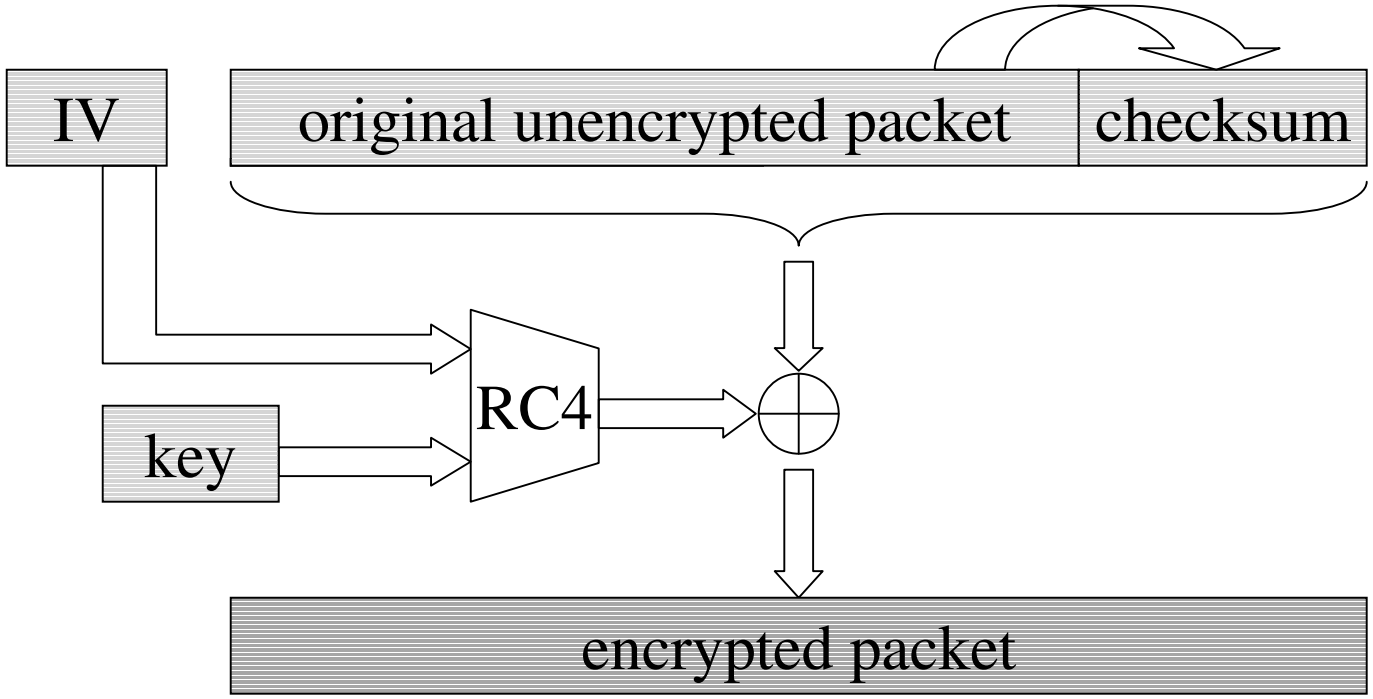
WEP -- Even More Detail



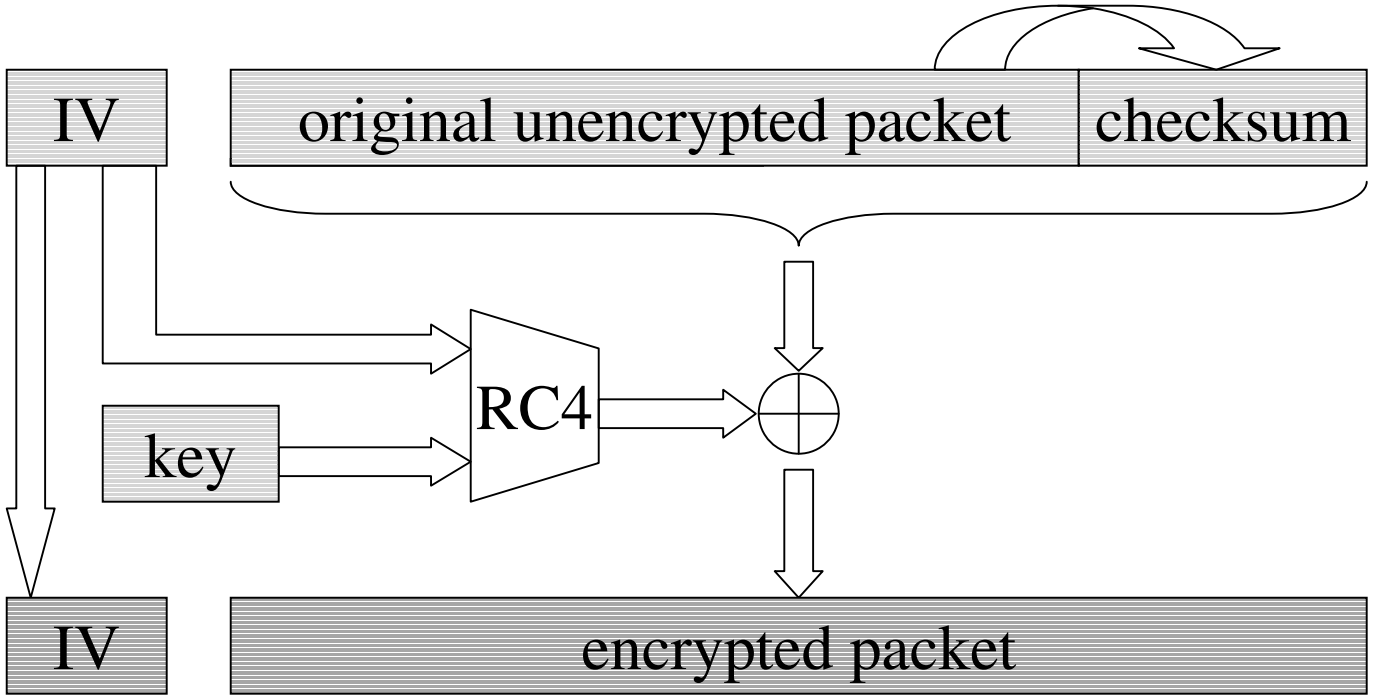
WEP -- Even More Detail



WEP -- Even More Detail



WEP -- Even More Detail



Attack #2: Spoofed Packets

- Attackers can inject forged 802.11 traffic
  - Learn RC4(K, IV) using previous attack
  - Since the checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

- Attackers can bypass 802.11 access control
  - All computers attached to wireless net are exposed

Attack #2: Spoofed Packets

- Attackers can inject forged 802.11 traffic
  - Learn Z = RC4(K, IV) using previous attack
  - Since the CRC checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

- Attackers can bypass 802.11 access control
  - All computers attached to wireless net are exposed

Attack #2: Spoofed Packets

$IV, (P, CRC(P)) \oplus Z$

- Attackers can inject forged 802.11 traffic
  - Learn $Z = RC4(K, IV)$ using previous attack
  - Since the CRC checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

- Attackers can bypass 802.11 access control
  - All computers attached to wireless net are exposed

Attack #3: Packet Modification

$(P, CRC(P)) \oplus RC4(K)$

Attack #3: Packet Modification

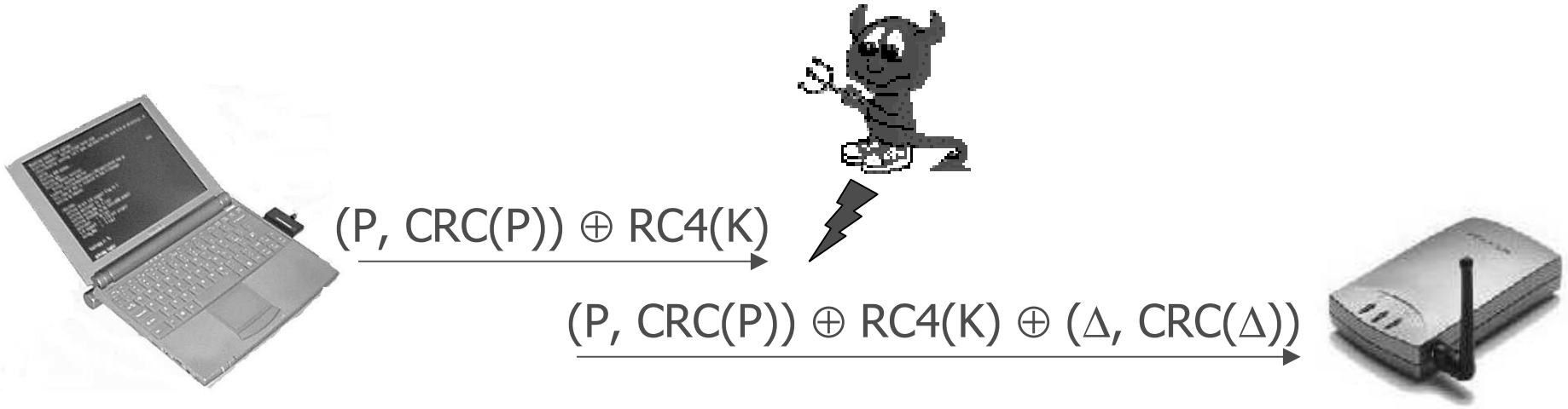
$(P, CRC(P)) \oplus RC4(K)$

Attack #3: Packet Modification

$(P, CRC(P)) \oplus RC4(K)$

$(P, CRC(P)) \oplus RC4(K) \oplus (\Delta, CRC(\Delta))$

Attack #3: Packet Modification



- CRC is linear
  - $\Rightarrow CRC(P \oplus \Delta) = CRC(P) \oplus CRC(\Delta)$
    - $\Rightarrow$ the modified packet $(P \oplus \Delta)$ has a valid checksum
- Attacker can tamper with packet (P) without breaking RC4

Attack #4: Inductive Learning

- Learn $Z_{1..n} = RC4(K, IV)_{1..n}$ using previous attack
- Then guess Z_{n+1}; verify guess by sending a ping packet ((P, CRC(P))) of length n+1 and watching for a response
- Repeat, for n=1,2,…, until all of RC4(K, IV) is known

Credits: Arbaugh, et al.

Attack #4: Inductive Learning

$(P, CRC(P)) \oplus (Z_{1..n}, 0)$

- Learn $Z_{1..n} = RC4(K, IV)_{1..n}$ using previous attack
- Then guess Z_{n+1}; verify guess by sending a ping packet $((P, CRC(P)))$ of length $n+1$ and watching for a response
- Repeat, for $n=1,2,\ldots$, until all of $RC4(K, IV)$ is known

Credits: Arbaugh, et al.

Attack #4: Inductive Learning

$(P, CRC(P)) \oplus (Z_{1..n}, 0)$

$(P, CRC(P)) \oplus (Z_{1..n}, 1)$

- Learn $Z_{1..n} = RC4(K, IV)_{1..n}$ using previous attack
- Then guess Z_{n+1}; verify guess by sending a ping packet $((P, CRC(P)))$ of length $n+1$ and watching for a response
- Repeat, for $n=1,2,\ldots$, until all of $RC4(K, IV)$ is known

Credits: Arbaugh, et al.

Attack #4: Inductive Learning

$(P, CRC(P)) \oplus (Z_{1..n}, 0)$

$(P, CRC(P)) \oplus (Z_{1..n}, 1)$

:

$(P, CRC(P)) \oplus (Z_{1..n}, 255)$

- Learn $Z_{1..n} = RC4(K, IV)_{1..n}$ using previous attack
- Then guess Z_{n+1}; verify guess by sending a ping packet ($(P, CRC(P))$) of length $n+1$ and watching for a response
- Repeat, for $n=1,2,\ldots$, until all of $RC4(K, IV)$ is known

Credits: Arbaugh, et al.

Attack #4: Inductive Learning

$(P, CRC(P)) \oplus (Z_{1..n}, 0)$

$(P, CRC(P)) \oplus (Z_{1..n}, 1)$

:

$(P, CRC(P)) \oplus (Z_{1..n}, 255)$

(pong)

- Learn $Z_{1..n} = RC4(K, IV)_{1..n}$ using previous attack
- Then guess Z_{n+1}; verify guess by sending a ping packet ($(P, CRC(P))$) of length $n+1$ and watching for a response
- Repeat, for $n=1,2,\ldots$, until all of $RC4(K, IV)$ is known

Credits: Arbaugh, et al.

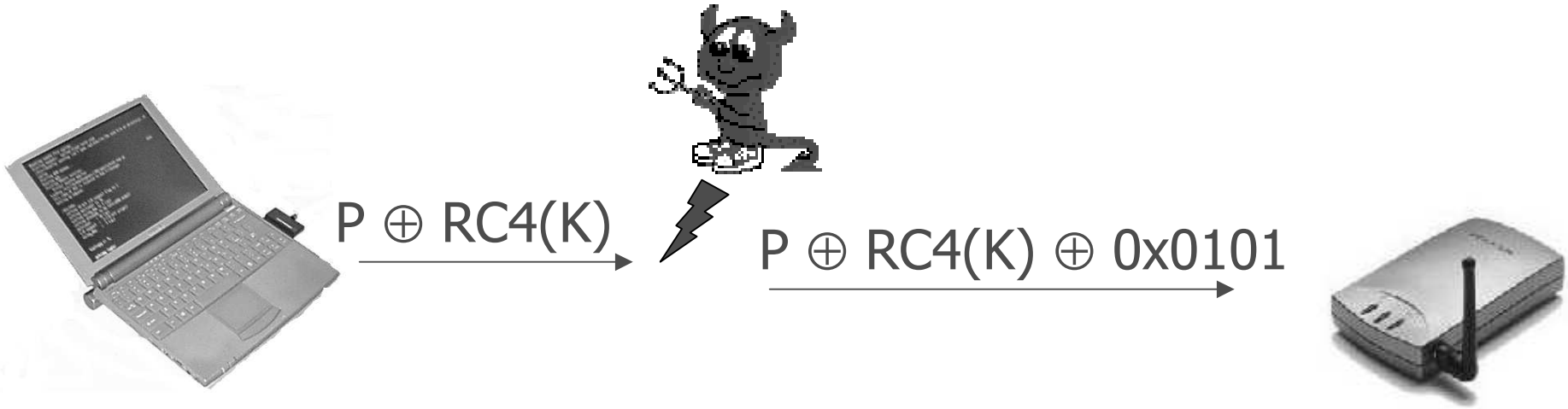
Attack #5: Reaction Attacks

$P \oplus RC4(K)$ →

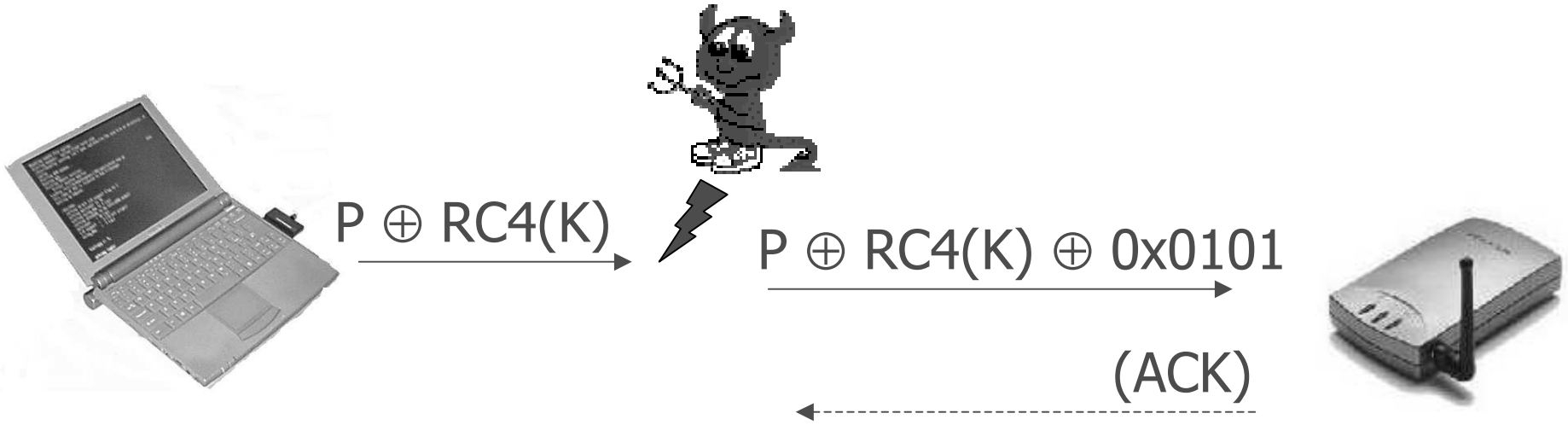
Attack #5: Reaction Attacks

$P \oplus RC4(K)$

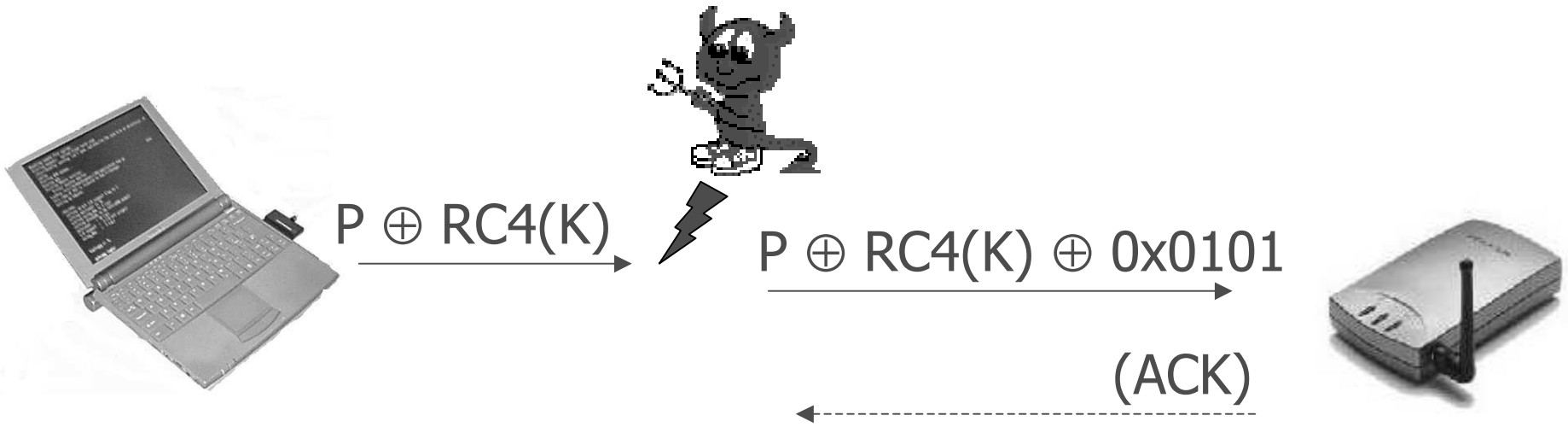
Attack #5: Reaction Attacks



Attack #5: Reaction Attacks

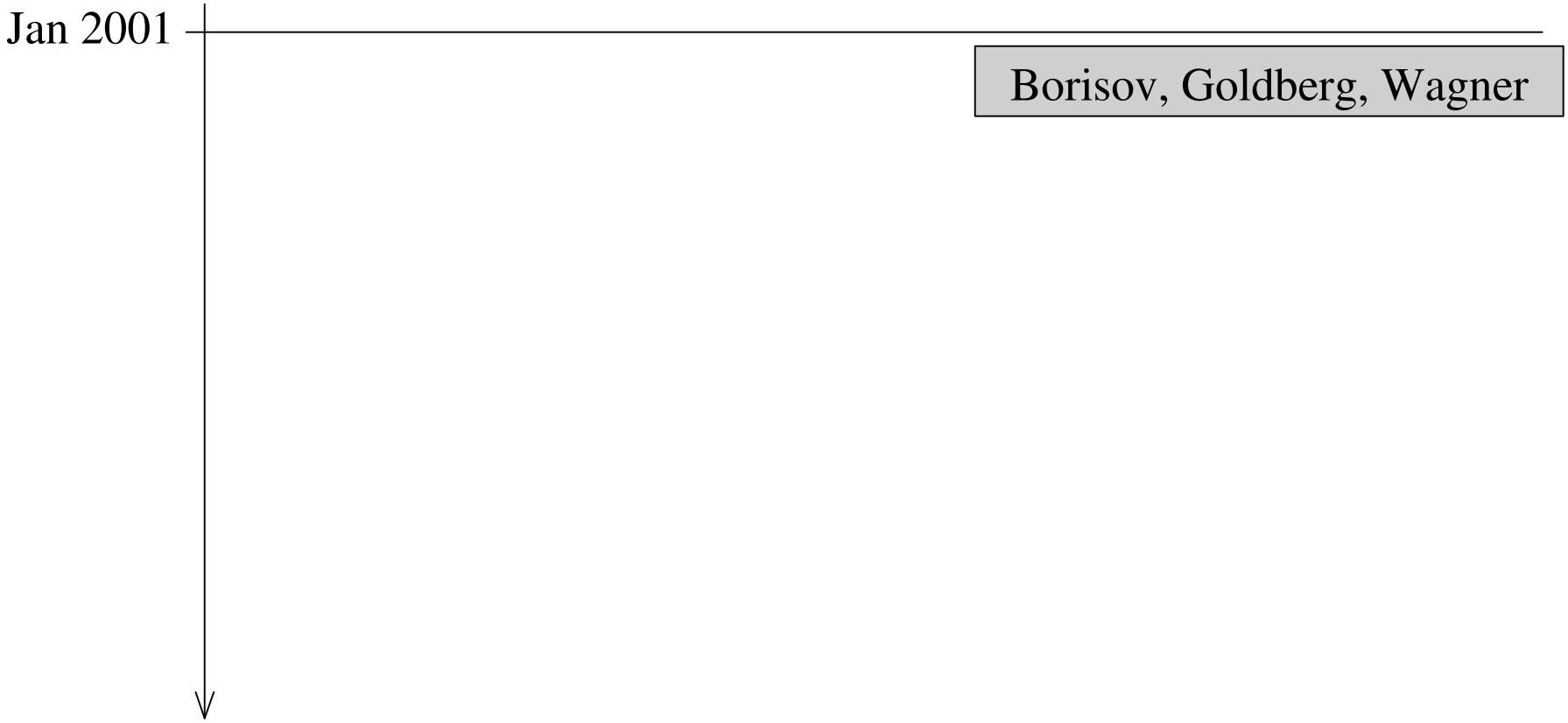


Attack #5: Reaction Attacks

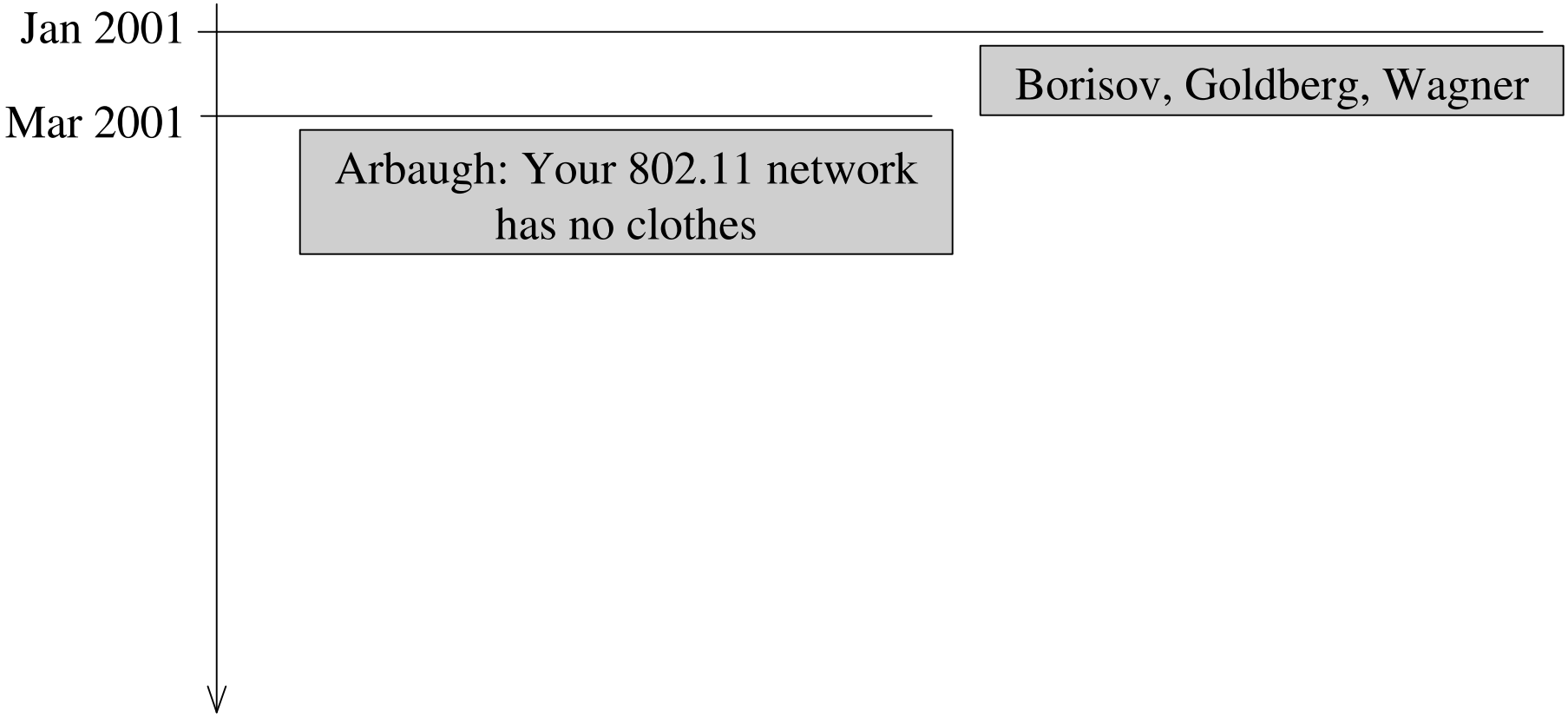


- TCP ACKnowledgement returned by recipient
  ⇔ TCP checksum on modified packet (P ⊕ 0x0101) is valid
  ⇔ wt(P & 0x0101) = 1
- ➢ Attacker can recover plaintext (P) without breaking RC4

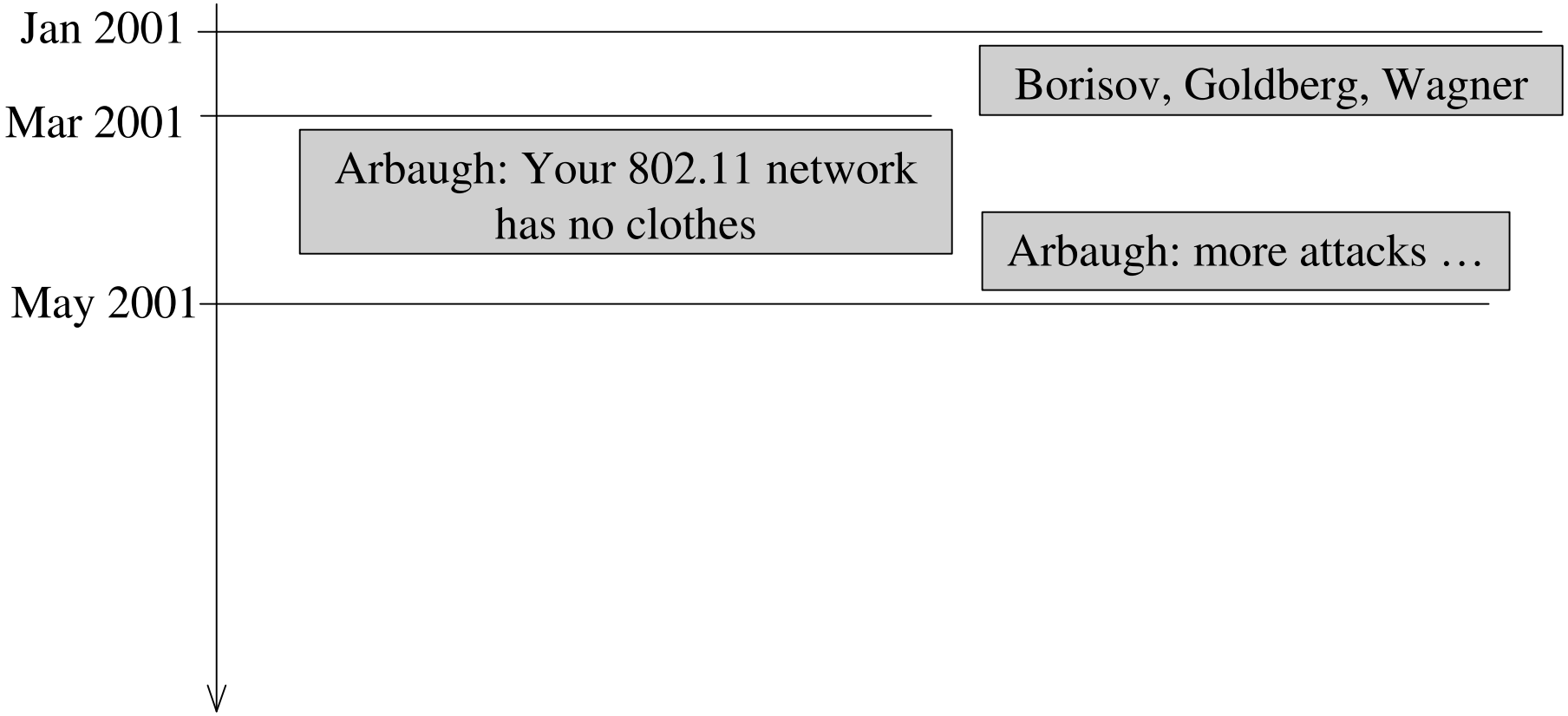
Other Research



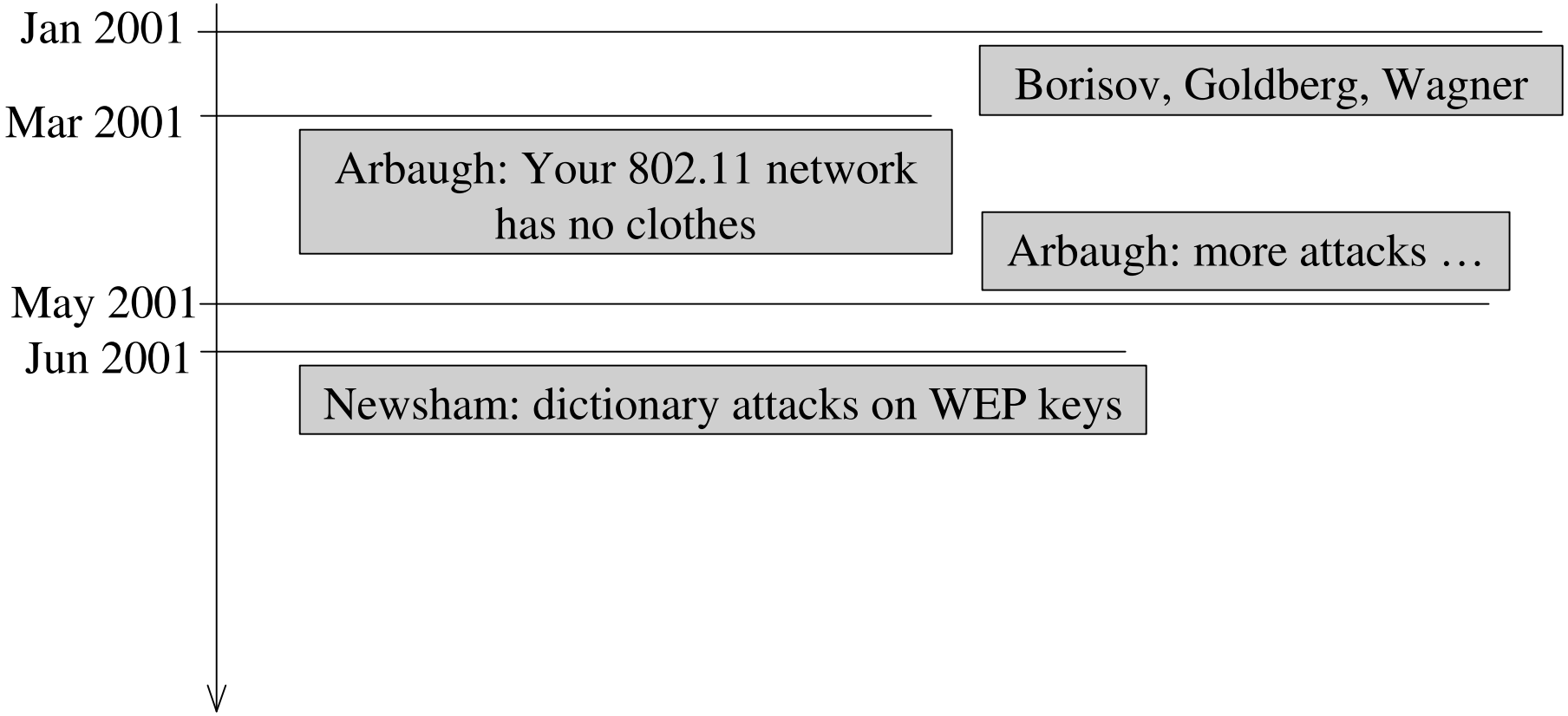
Other Research



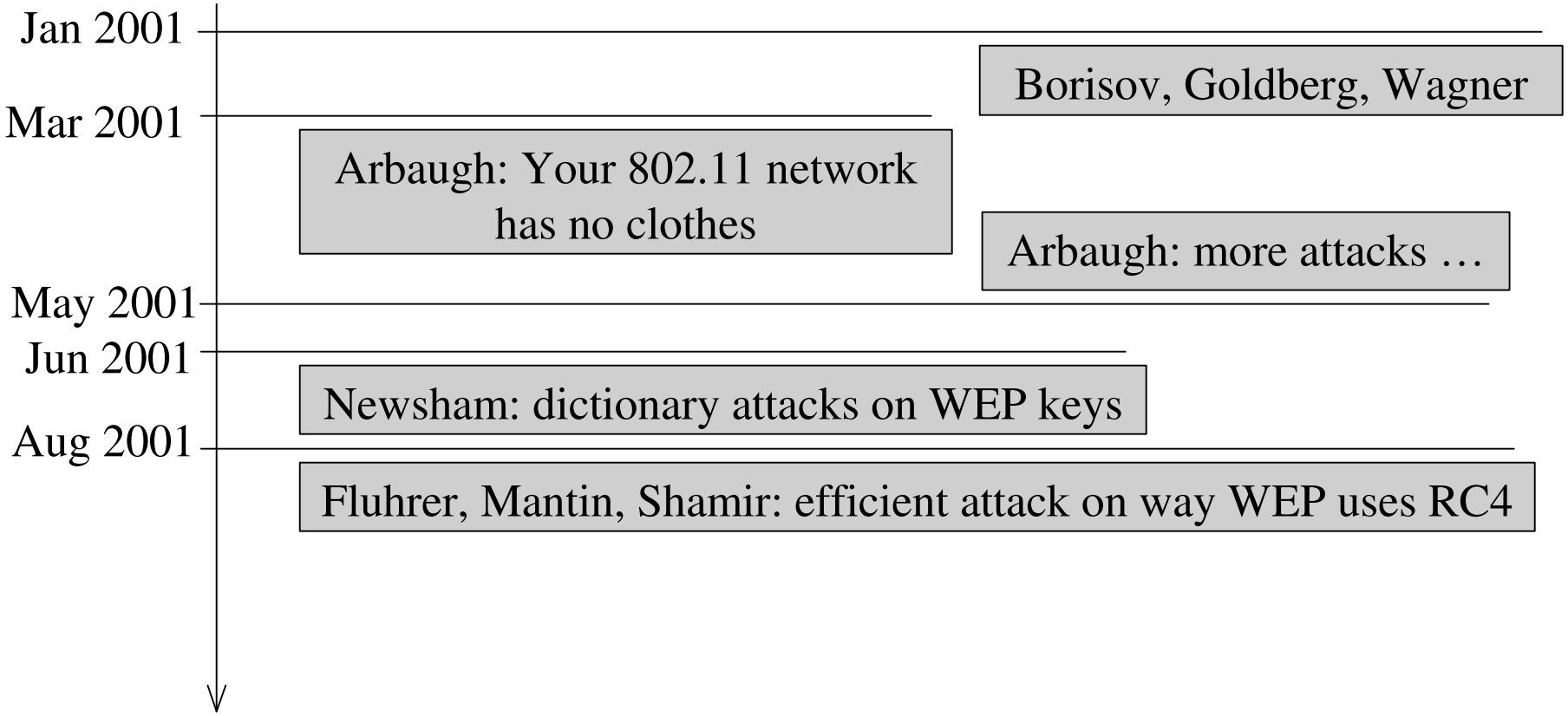
Other Research



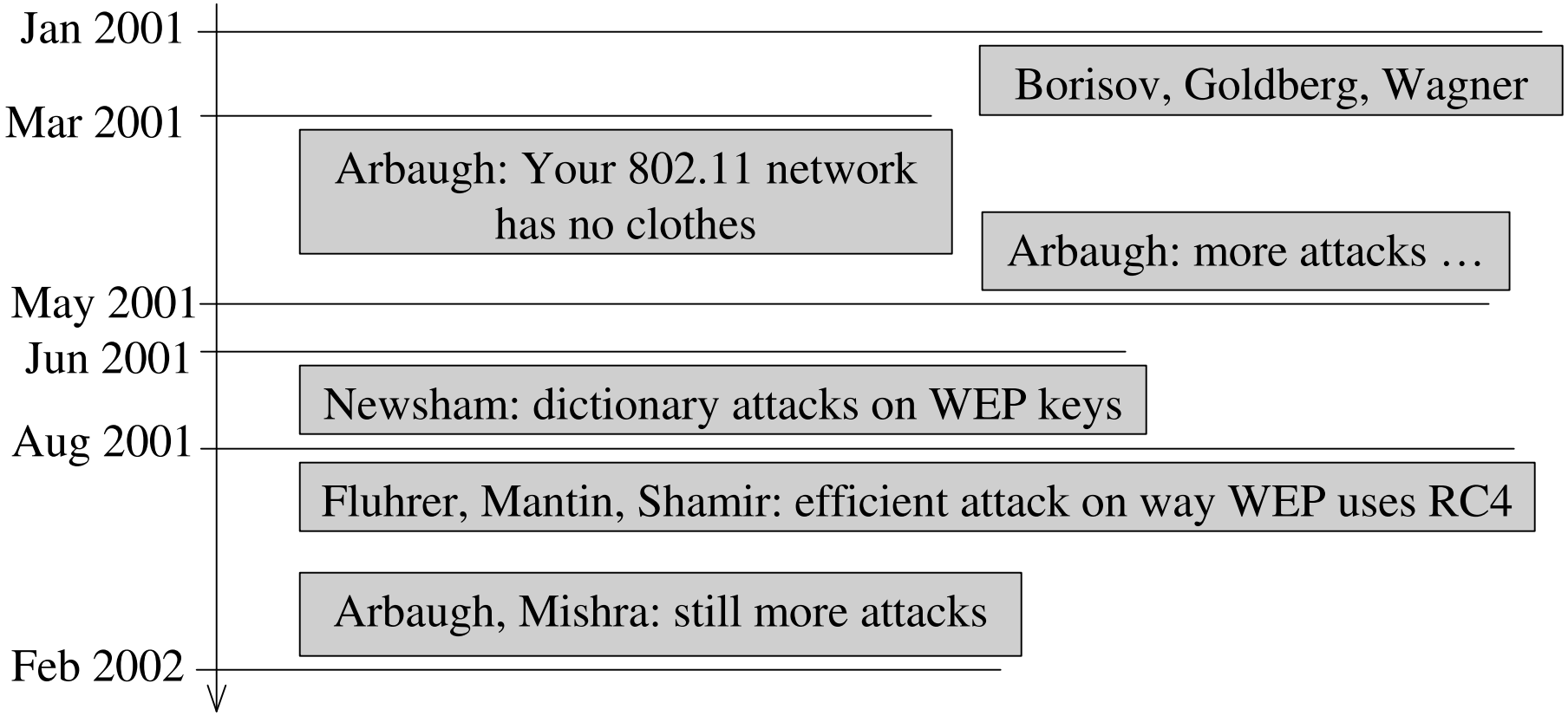
Other Research



Other Research



Other Research



Evaluation of 802.11 WEP

- None of WEP's goals are achieved
- Confidentiality, integrity, access control: *all insecure*

Avoiding These Pitfalls

- How could we have prevented these flaws?

Avoiding These Pitfalls

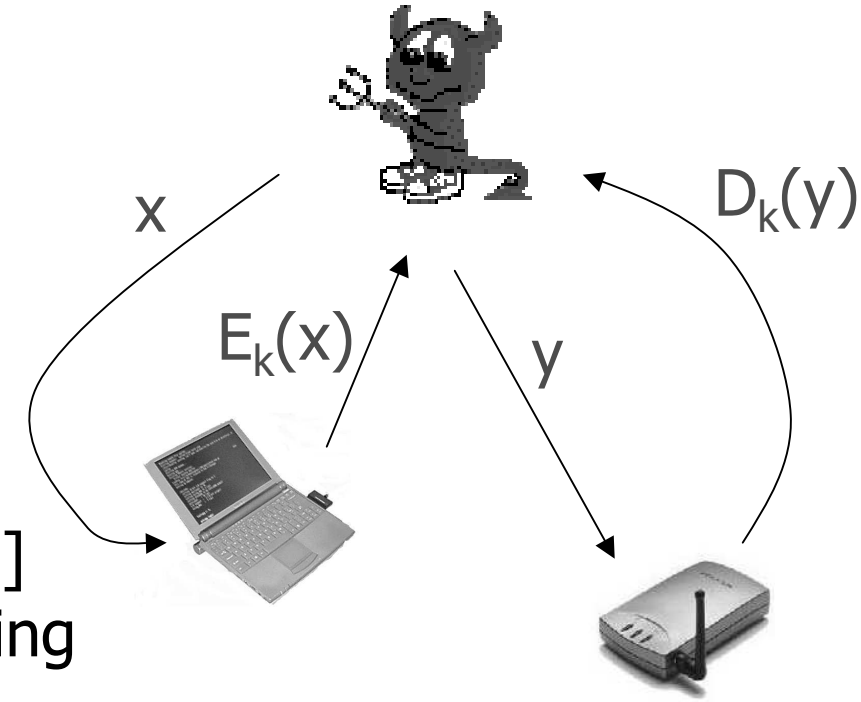
- How could we have prevented these flaws?

Provable security to the rescue!

Modern Crypto Theory (1)

- *Defn.* An encryption algorithm $E : K \times X \rightarrow Y$ is IND-CCA2 secure ("real-or-random") if:

  For all adversaries A,
  $Pr[A^{Ek,Dk}=1] \approx Pr[A^{R,Dk}=1]$
  where R(x) := random string of same length as $E_k(x)$.

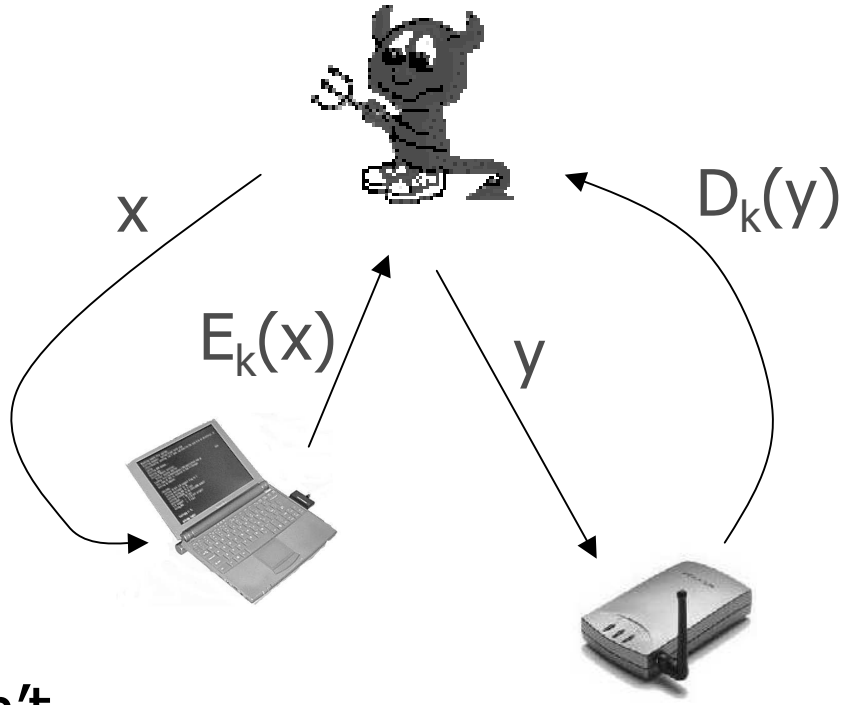


IND-CCA2 = Confidentiality

Modern Crypto Theory (2)

- *Defn.* An encryption algorithm $E : K \times X \rightarrow Y$ is INT-CTXT secure if:

  For all adversaries A,
  $\Pr[A^{Ek,Dk} \text{ forges}] \approx 0$
  where A forges if it makes any query y to D_k that is accepted as valid and wasn't output by some previous query to E_k.



INT-CTXT = Integrity

The Value of Modern Crypto

- Theory of crypto gives us results like this:

  Theorem. If AES is a secure block cipher, then AES-CTR + AES-XCBC-MAC is IND-CCA2 and INT-CTXT secure.

- This stops all the attacks shown earlier

  (if the block cipher is secure)

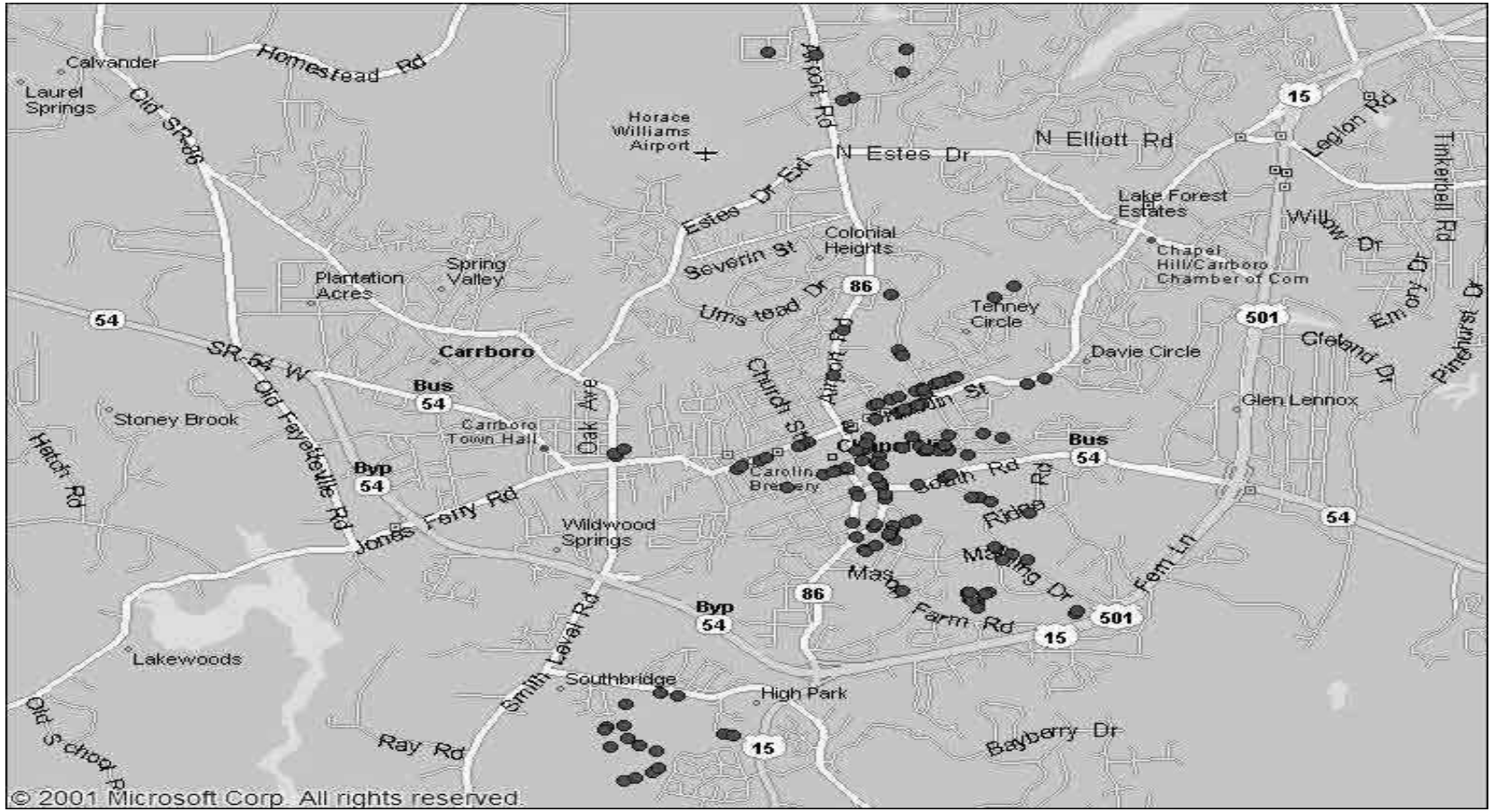
  - And identifies exactly which assumptions we're relying on

➤ Provable security would have prevented WEP's flaws.

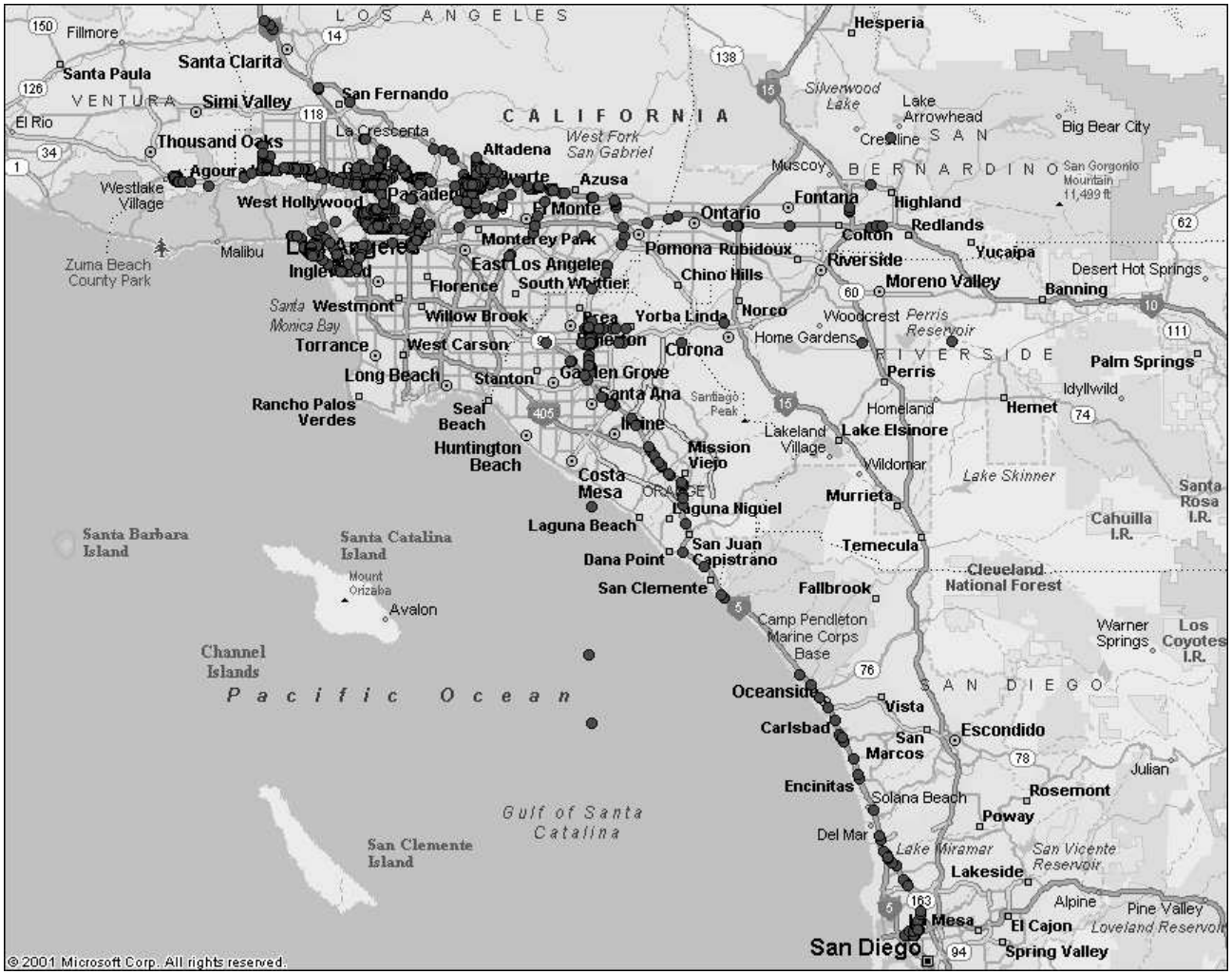
War Driving

- 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

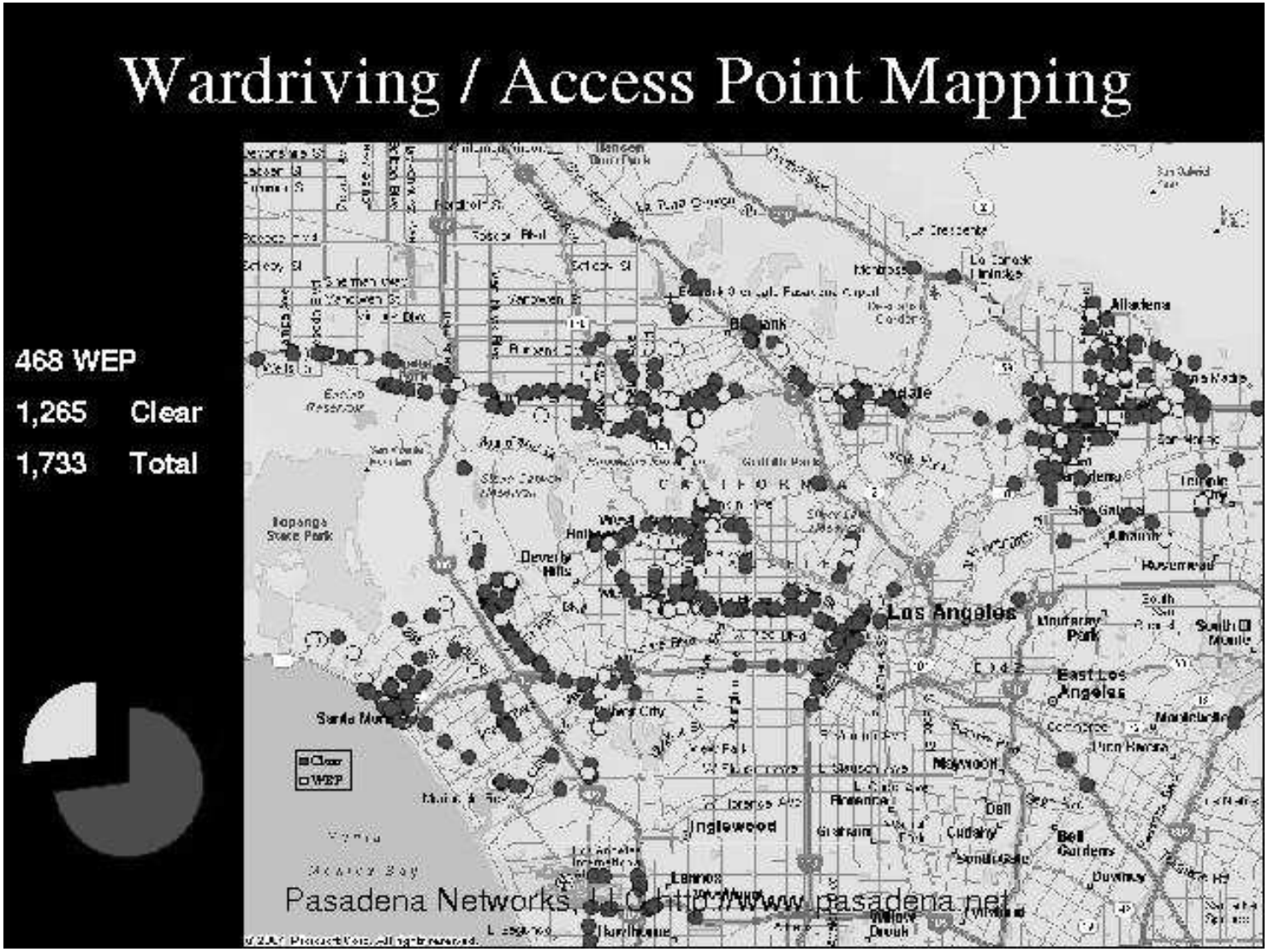
War Driving: Chapel Hill



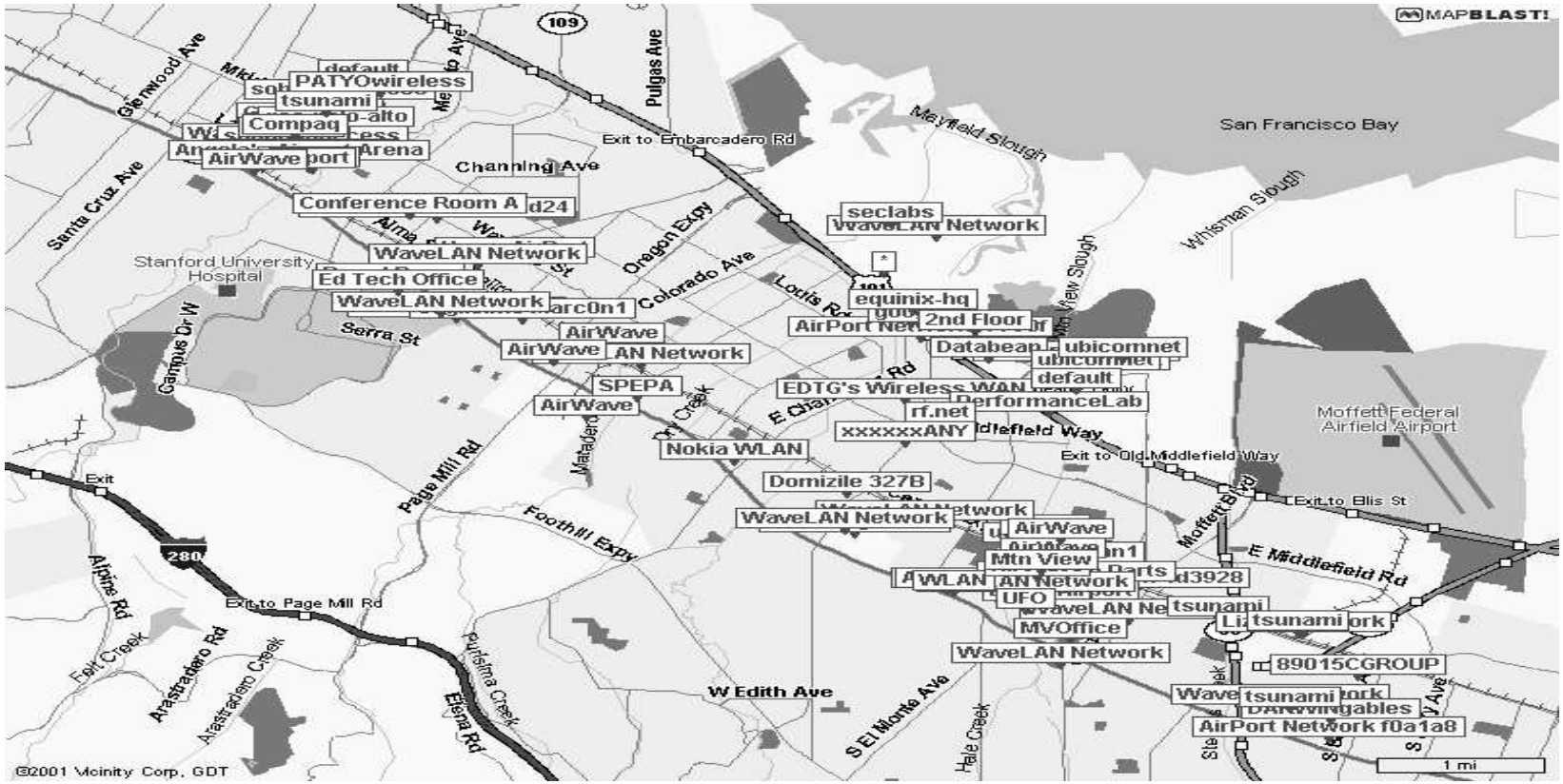
Driving from LA to San Diego



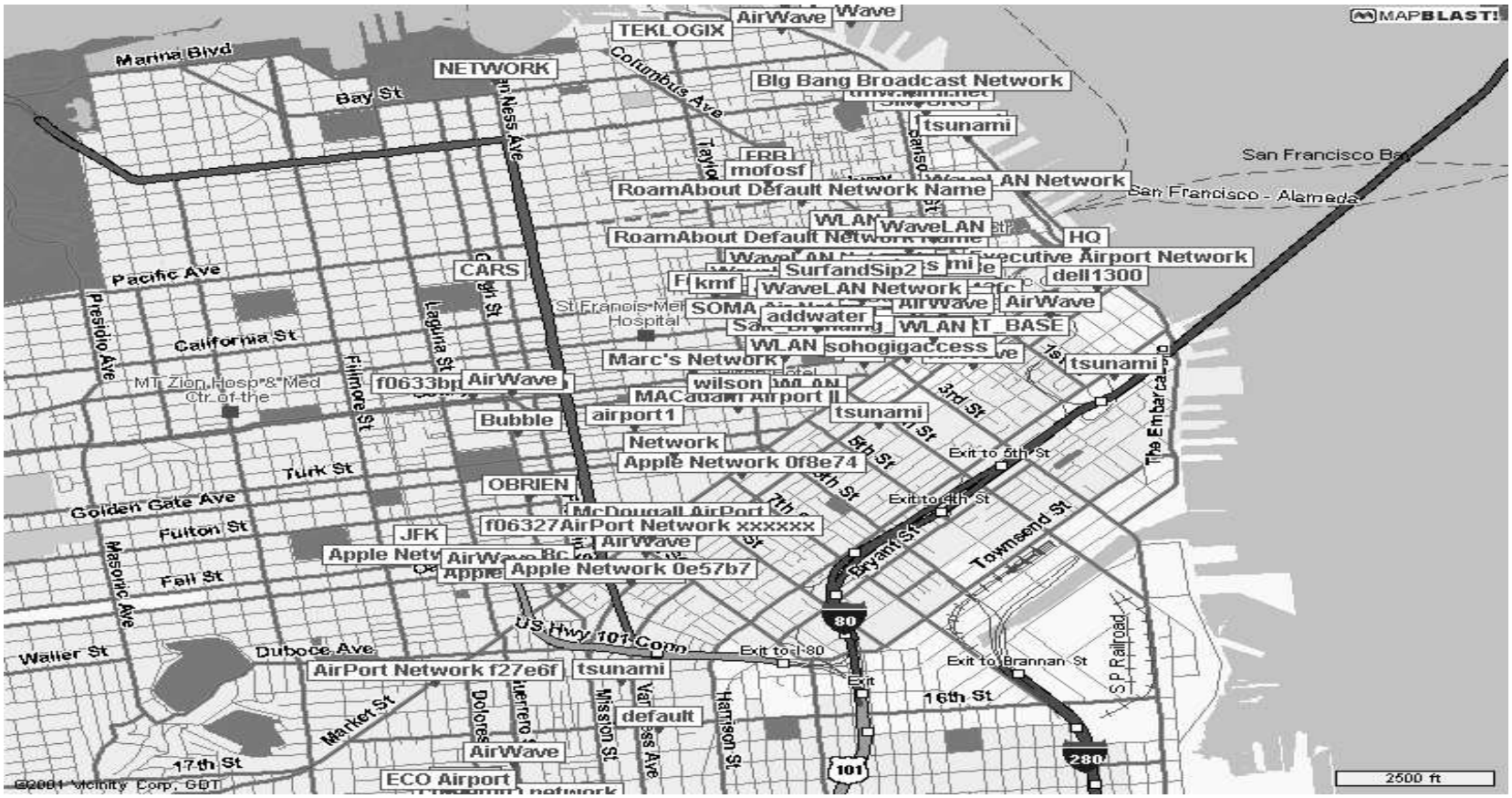
Wireless Networks in LA



Silicon Valley



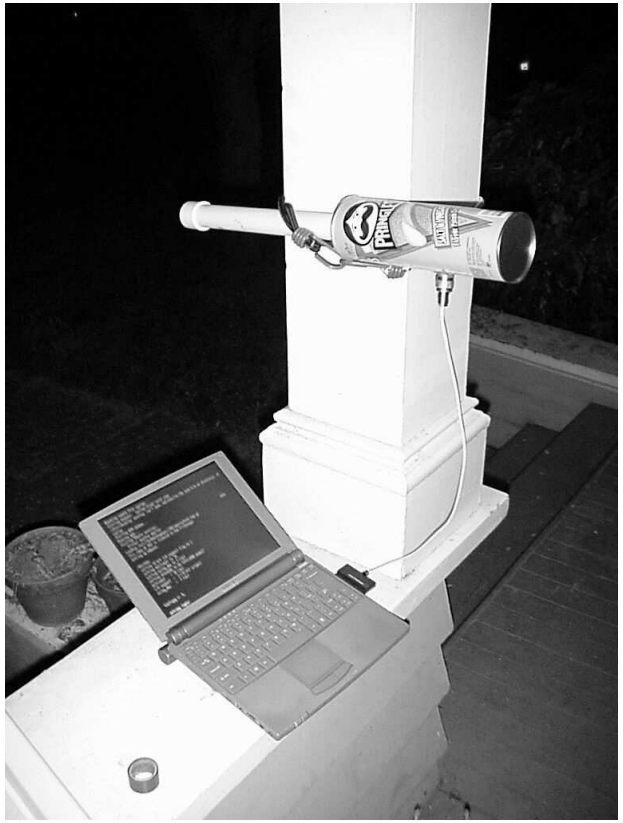
San Francisco

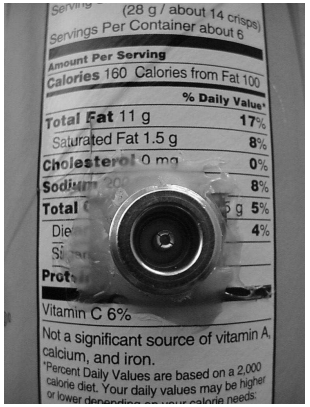


Toys for Hackers

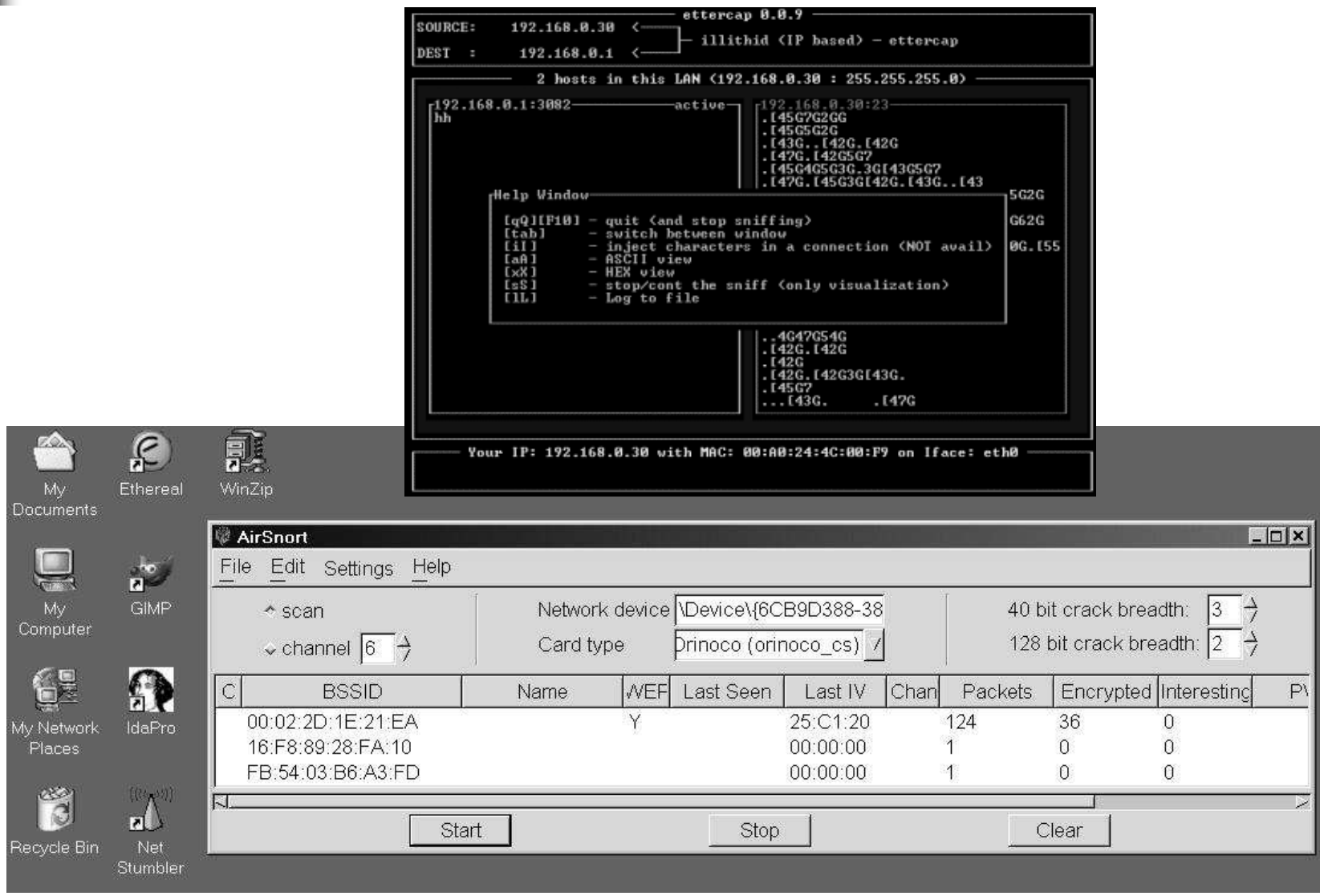
Toys for Hackers

A Dual-Use Product



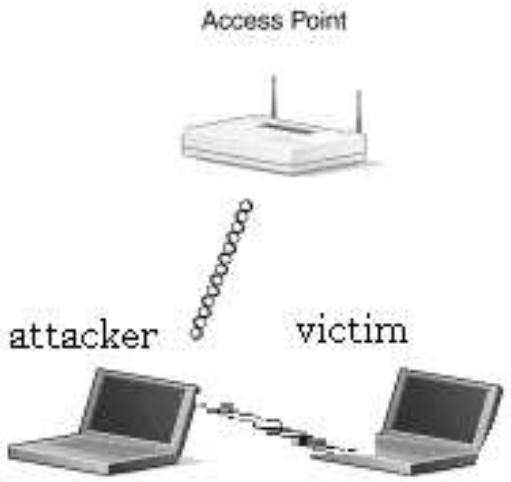


Attack Tools



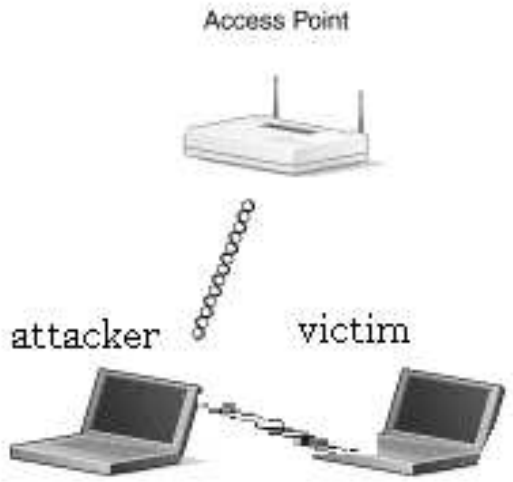
More Attack Tools

```
#./kracker_jack -b 00:40:96:5b:37:af -v 00:07:85:92:db:a9 -c 1 -C 8 -i aj0
.168.20.254 -V 192.168.20.119 -B 192.168.20.255 -n 255.255.255.0
Starting Monkey in the Middle Attack:

victim: 00:07:85:92:db:a9
bssid:  00:40:96:5b:37:af

seeding random number generator for ipsec...done.
setting up rsa keys...done.
configuring airjack device...done.
forcing ourselves in the middle...done.
configuring lucent card...done.
coercing our card to associate as the victim...done.

layer 1 insertion complete.

forcing our public key into the victim's dns KEY record...done.
(server) starting isakmp main mode round trip 1...done.
(client) starting isakmp main mode round trip 1...done.
(server) starting isakmp main mode round trip 2...done.
(client) starting isakmp main mode round trip 2...done.
(server) starting isakmp main mode round trip 3...done.
(client) starting isakmp main mode round trip 3...done.
intersepting dns KEY lookup for server address...done.
(server) starting isakmp quick mode round trip 1...done.
(client) starting isakmp quick mode round trip 1...done.
(server) starting isakmp quick mode round trip 2...done.
(client) starting isakmp quick mode round trip 2...done.

IPSEC Tunnel insertion complete...
```



More Attack Tools

```
#./kracker_jack -b 00:40:96:5b:37:af -v 00:07:85:92:db:a9 -c 1 -C 8 -i aj0
.168.20.254 -V 192.168.20.119 -B 192.168.20.255 -n 255.255.255.0
Starting Monkey in the Middle Attack:

victim: 00:07:85:92:db:a9
bssid:  00:40:96:5b:37:af

seeding random number generator for ipsec...done.
setting up rsa keys...done.
configuring airjack device...done.
forcing ourselves in the middle...done.
configuring lucent card...done.
coercing our card to associate as the victim...done.

layer 1 insertion complete.

forcing our public key into the victim's dns KEY record...done.
(server) starting isakmp main mode round trip 1...done.
(client) starting isakmp main mode round trip 1...done.
(server) starting isakmp main mode round trip 2...done.
(client) starting isakmp main mode round trip 2...done.
(server) starting isakmp main mode round trip 3...done.
(client) starting isakmp main mode round trip 3...done.
intersepting dns KEY lookup for server address...done.
(server) starting isakmp quick mode round trip 1...done.
(client) starting isakmp quick mode round trip 1...done.
(server) starting isakmp quick mode round trip 2...done.
(client) starting isakmp quick mode round trip 2...done.

IPSEC Tunnel insertion complete...
```



- Sophisticated attack tools are readily available

Problems With 802.11 WEP

- WEP cannot be trusted for security
  - Attackers can eavesdrop, spoof wireless traffic
  - Also can break the key with a few minutes of traffic
- Attacks are serious in practice
  - Attack tools are available for download on the Net
- And: WEP is often not used anyway
  - High administrative costs (WEP punts on key mgmt)
  - WEP is turned off by default

History Repeats Itself…

wireless security: not just 802.11

History Repeats Itself…

cellphones

1980 analog cellphones: AMPS

analog cloning, scanners
- fraud pervasive & costly

digital: TDMA, GSM

1990

TDMA eavesdropping [Bar]

more TDMA flaws [WSK]
GSM cloneable [BGW]
GSM eavesdropping [BSW,BGW]

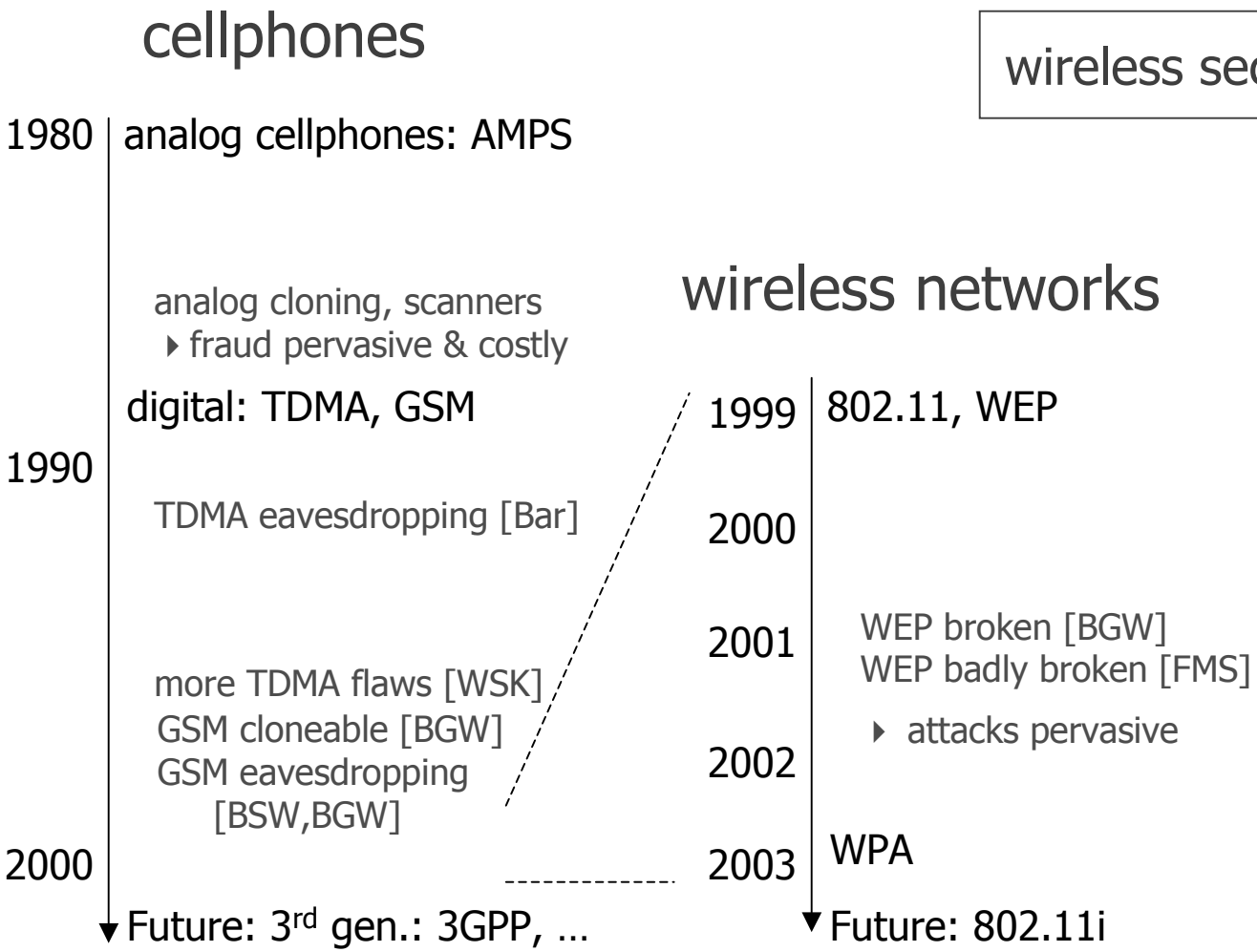
2000

Future: 3rd gen.: 3GPP, …

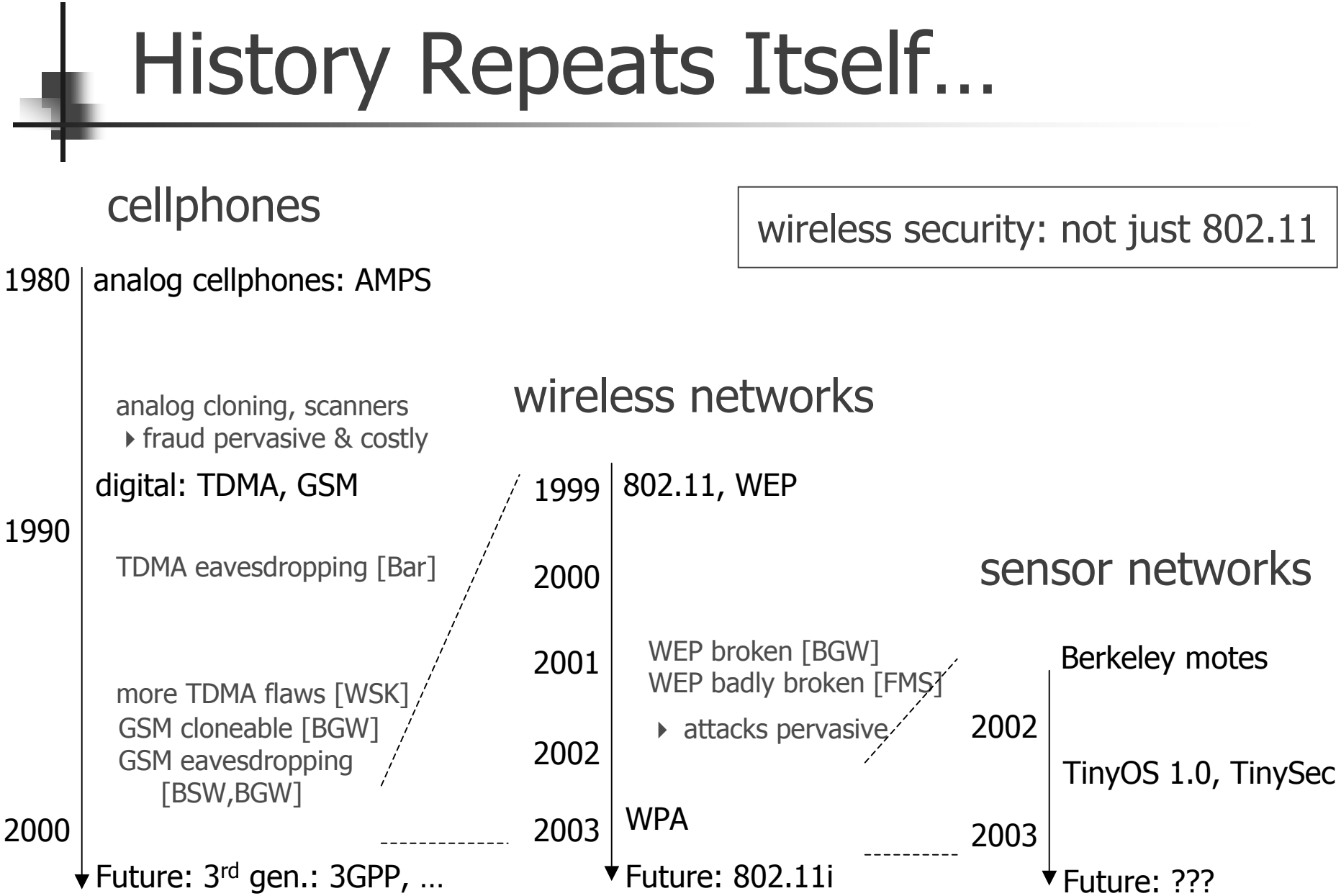
wireless security: not just 802.11

History Repeats Itself…

wireless security: not just 802.11



History Repeats Itself…



What: Research Challenges

- Securing the communication channel
  - Low-power cryptography, spread spectrum
  - Key management
  - 802.11i CCMP, TinySec, etc.
- Security against node compromise/capture
  - Key management, revocation, and re-keying
  - Tamper resistance
  - Resilient distributed algorithms, resilient aggregation
  - Intrusion detection and response
  - Secure routing, location authentication, broadcast authentication
- Privacy, and sensor networks
  - Selective data revelation, audit, exploiting DRM
  - Legal foundations

Conclusions

- *The bad news:*
  802.11 cannot be trusted for security
  - 802.11 encryption is readily breakable, and 50-70% of networks never even turn on encryption
  - Hackers are exploiting these weaknesses in the field

- *The good news:*
  Fixes (WPA, 802.11i) are on the way!

Who: Participants

Crossbow

CITRIS
Center for Information Technology
Research in the Interest of Society

ISAT

BOSCH

TinyOS

DARPA

Intel Research
network of laboratories

Berkeley
University of California

UCDAVIS
University of California, Davis

wireless security @ Berkeley: a growing collaboration