Leftovers:
Public-Key Infrastructure

3/10/2010

Certificate Chains

Certificate:

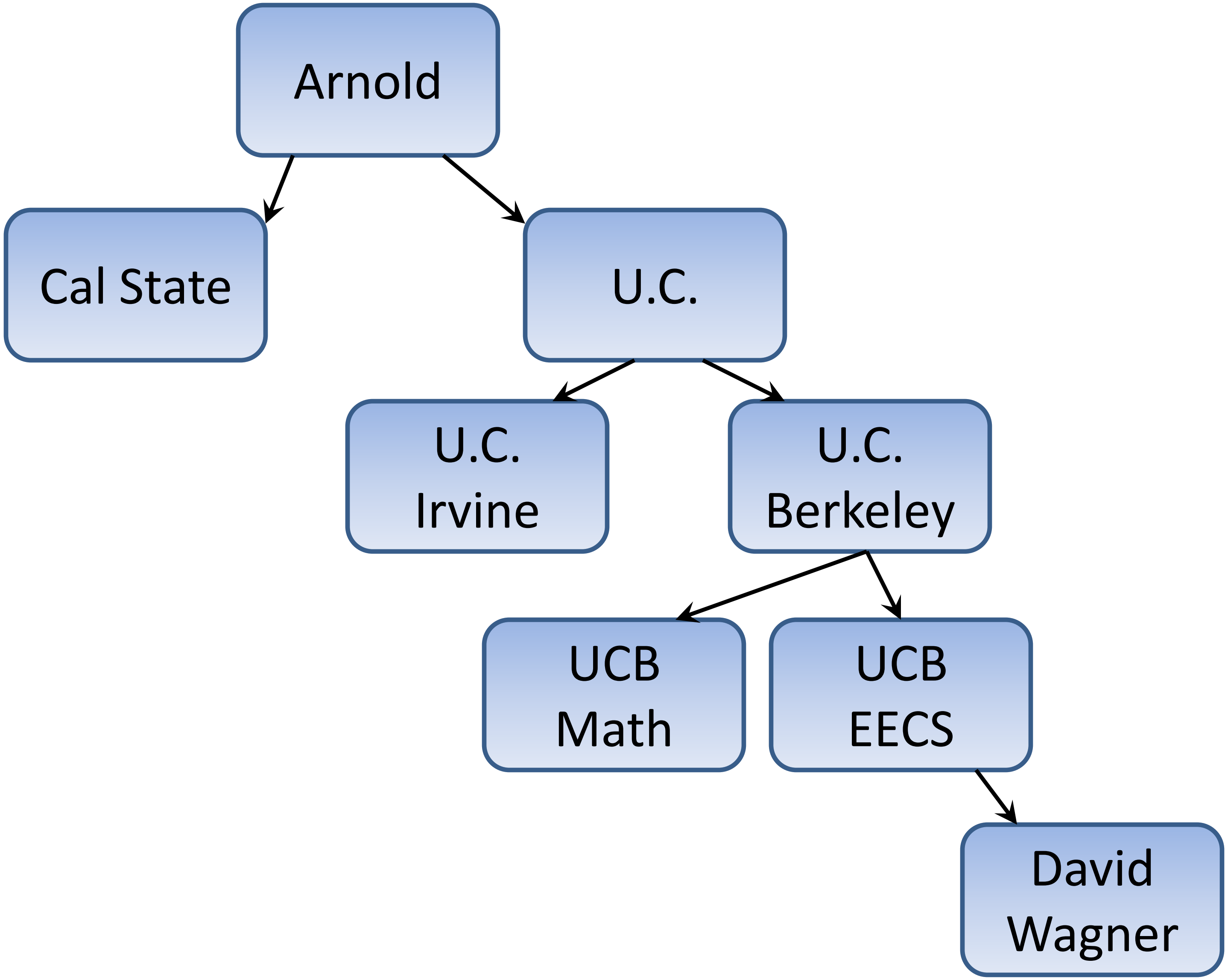
{David Wagner's public key is K_{Dave}}$_{K^{-1}{}_{Arnold}}$

Certificate chain:

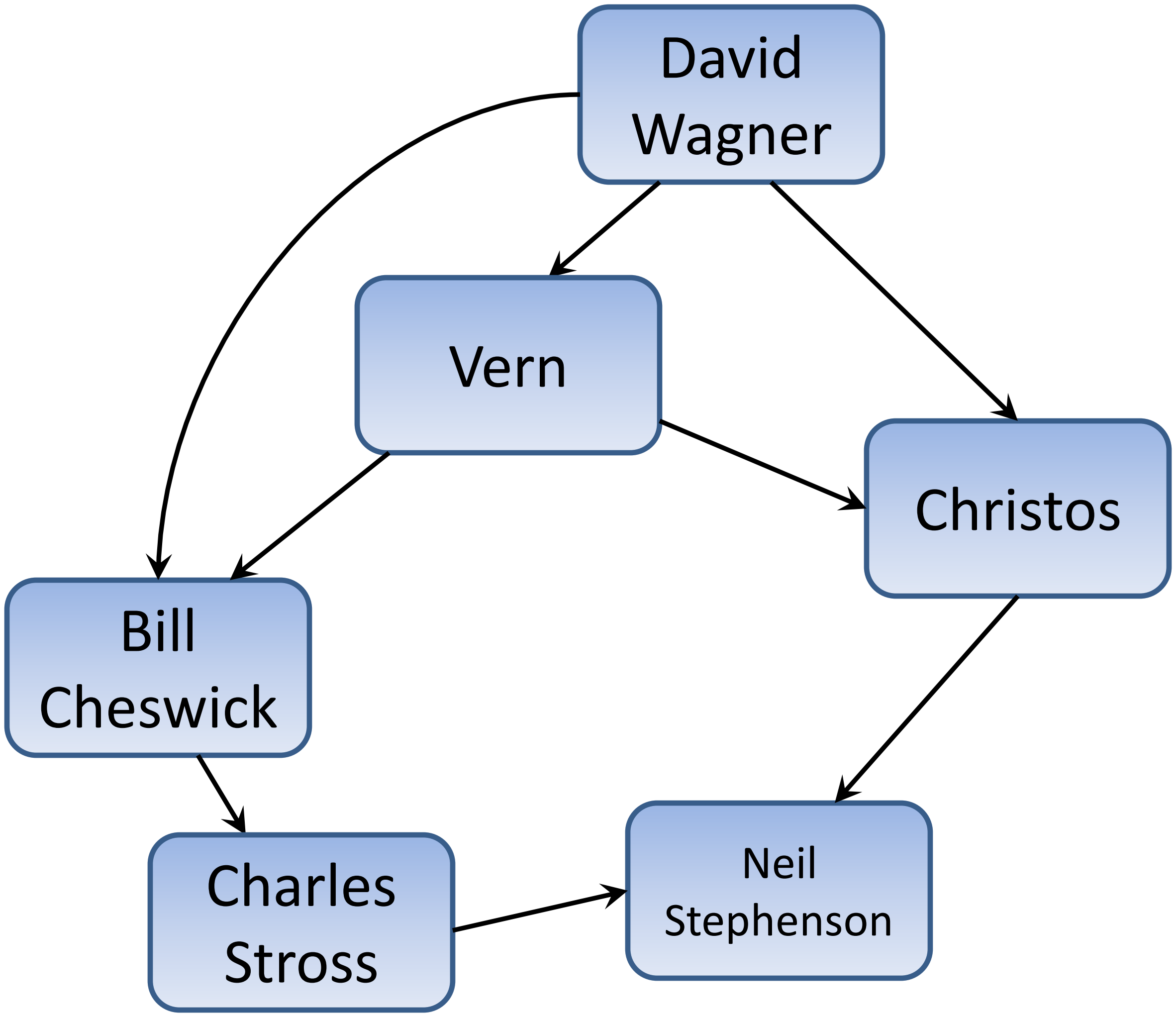
{UC Berkeley's public key is K_{UCB}}$_{K^{-1}{}_{Arnold}}$

{David Wagner's public key is K_{Dave}}$_{K^{-1}{}_{UCB}}$

Hierarchical CAs

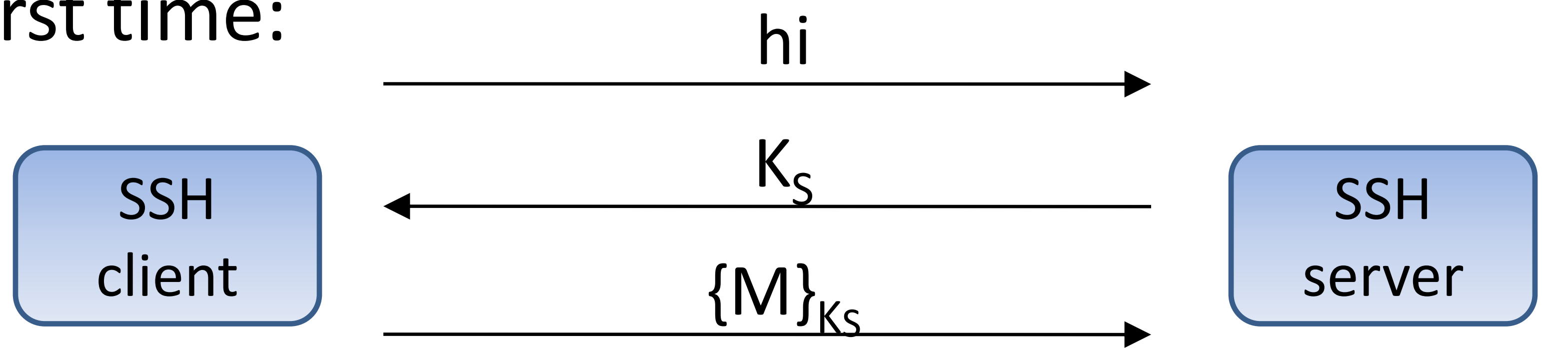


Web of Trust

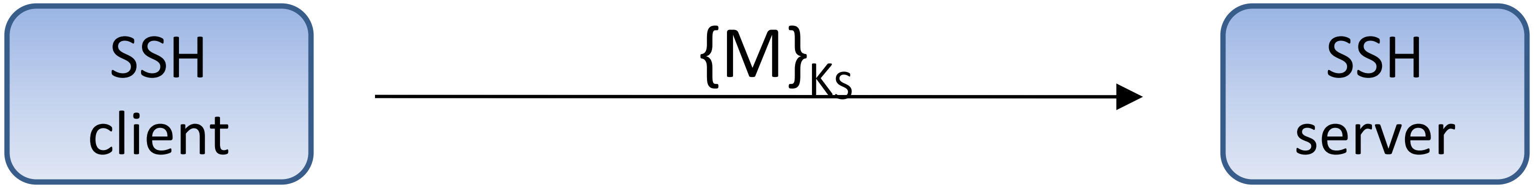

David Wagner
Vern
Christos
Bill Cheswick
Charles Stross
Neil Stephenson

SSH

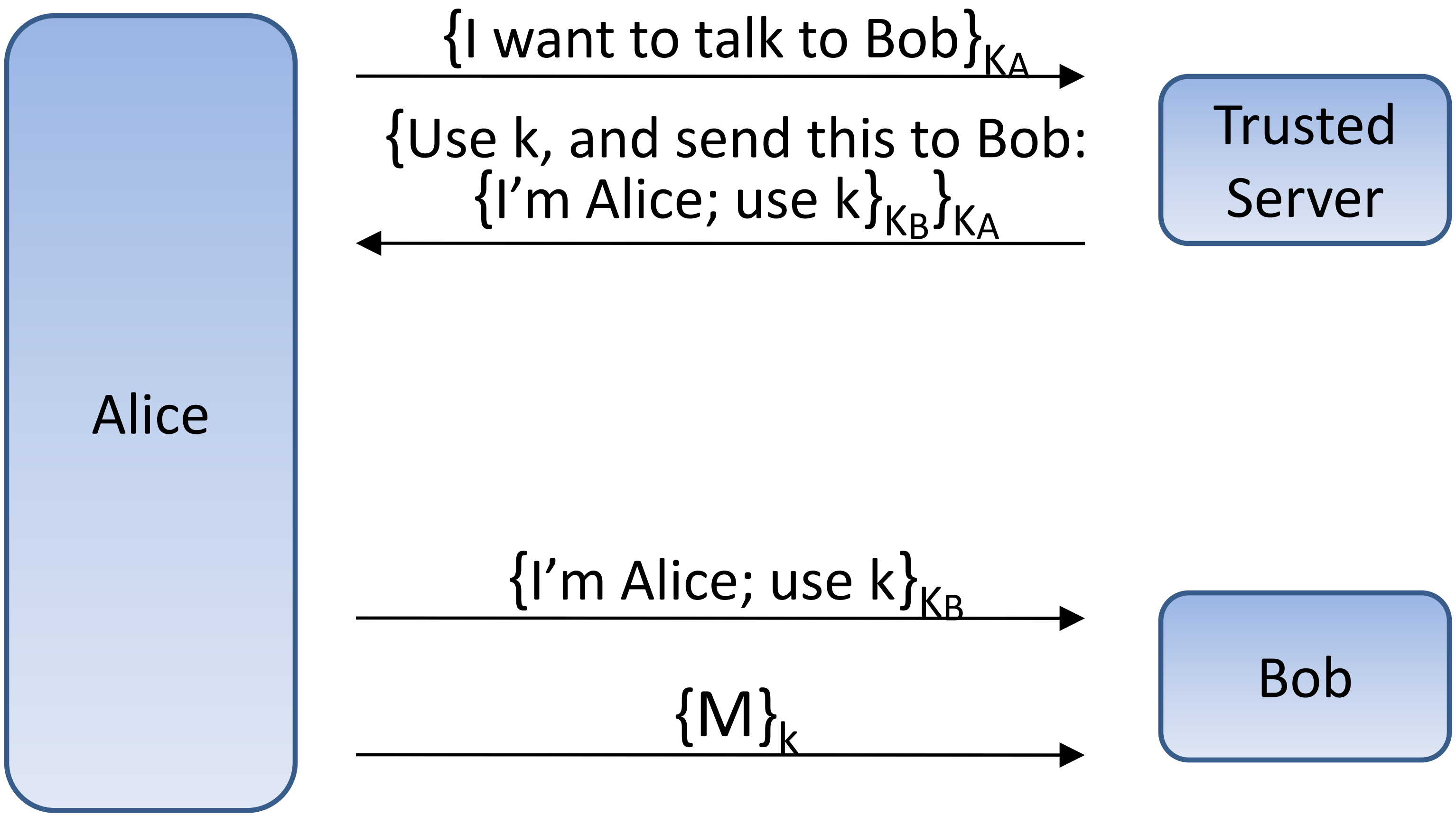
First time:

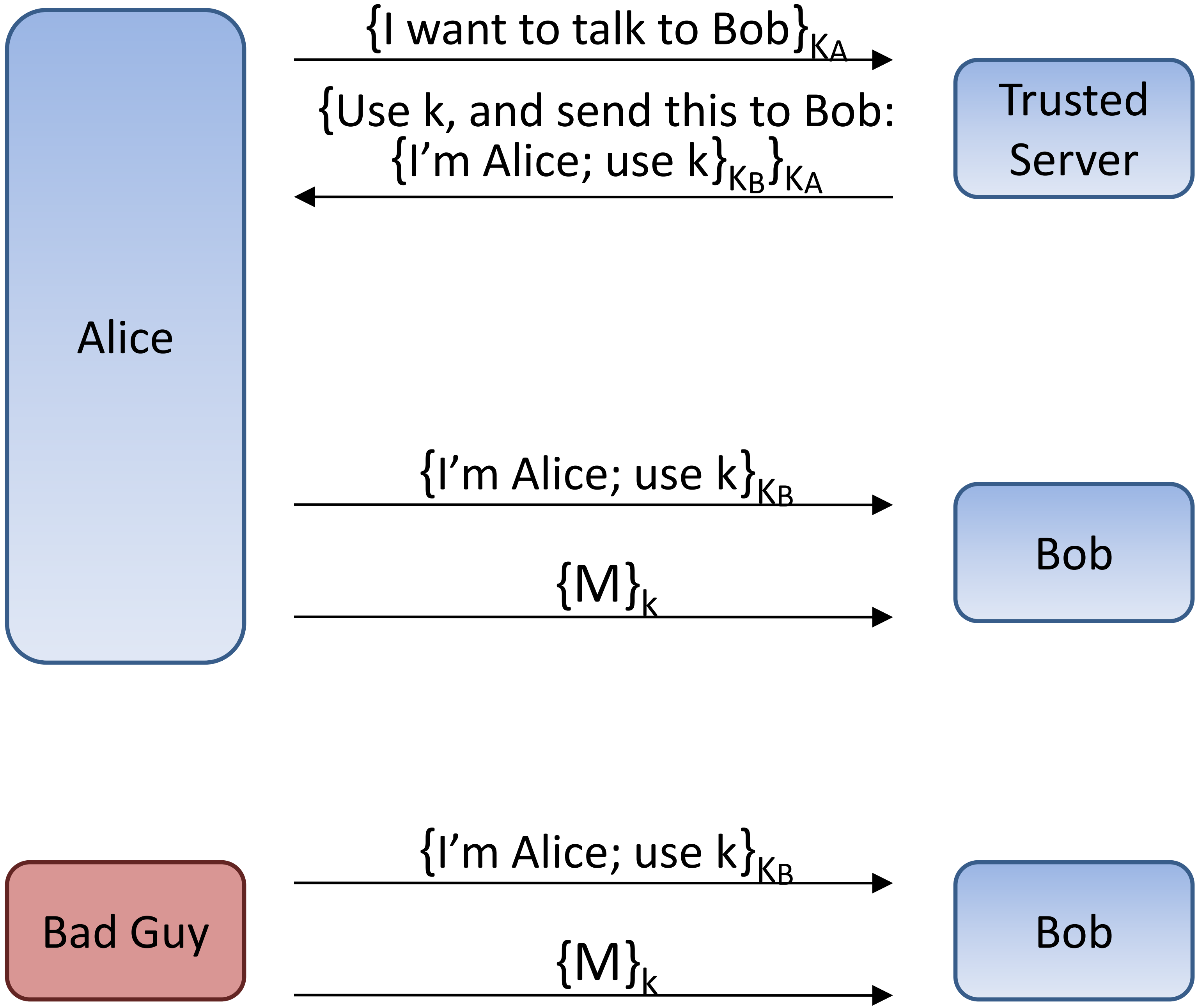


All subsequent logins:



Needham-Schroeder

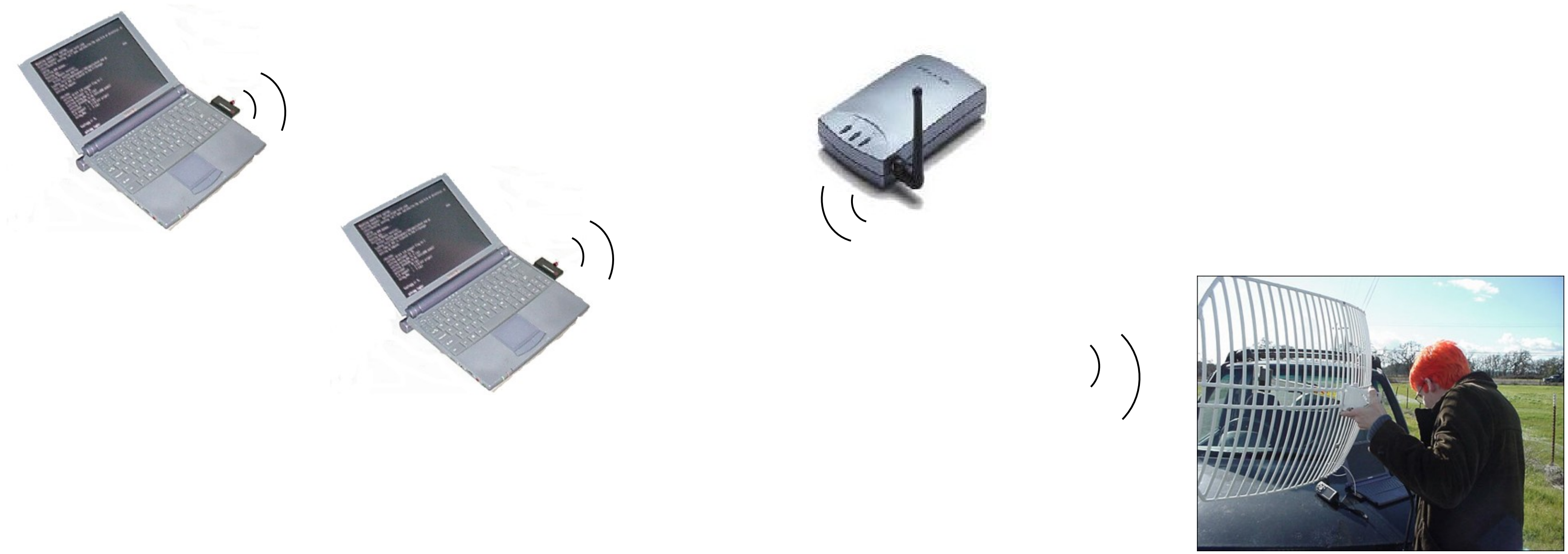



Alice
{I want to talk to Bob}$_{KA}$
Trusted Server
{Use k, and send this to Bob: {I'm Alice; use k}$_{KB}$}$_{KA}$
{I'm Alice; use k}$_{KB}$
{M}$_k$
Bob
Bad Guy
{I'm Alice; use k}$_{KB}$
{M}$_k$
Bob

Attacks on Cryptography

3/10/2010

The Security Problem



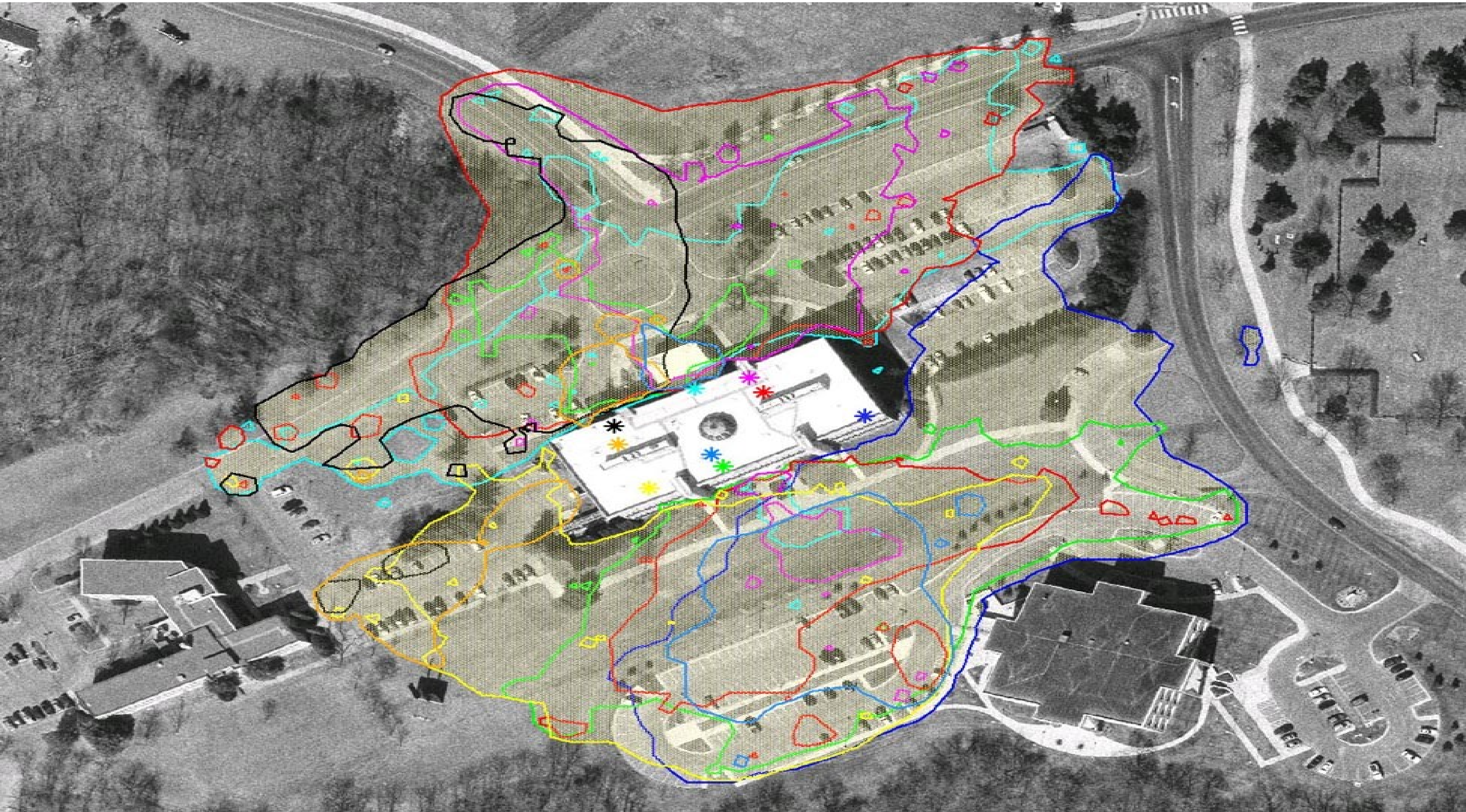
Wireless networking is just radio communications

- – Hence anyone with a radio can eavesdrop, inject traffic

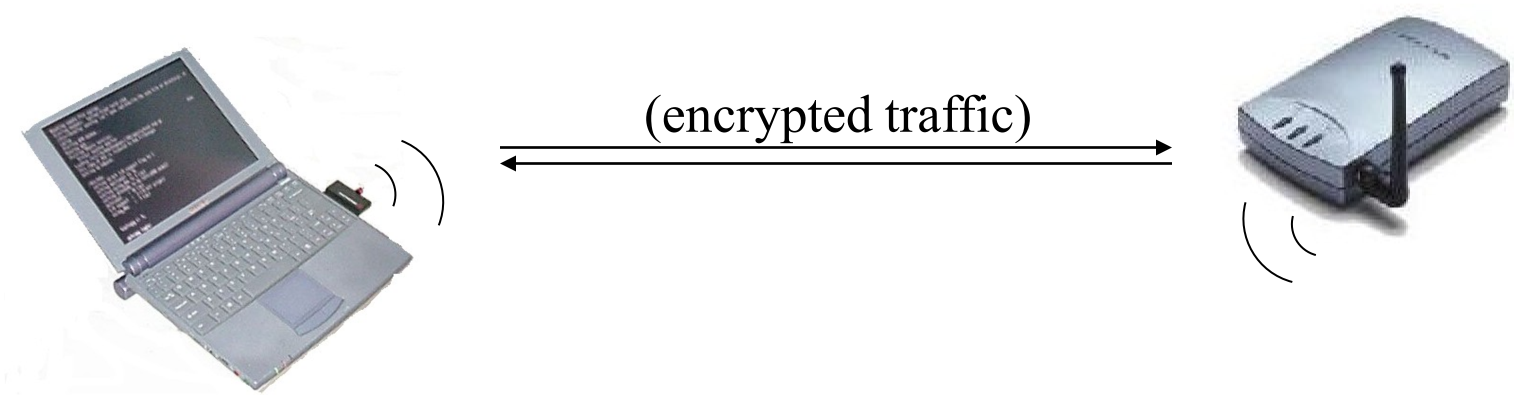
Toys for Hackers

The Security Risk: RF Leakage

The Risk of Attack From Afar



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

WEP - A Little More Detail

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

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

A Risk of Keystream Reuse

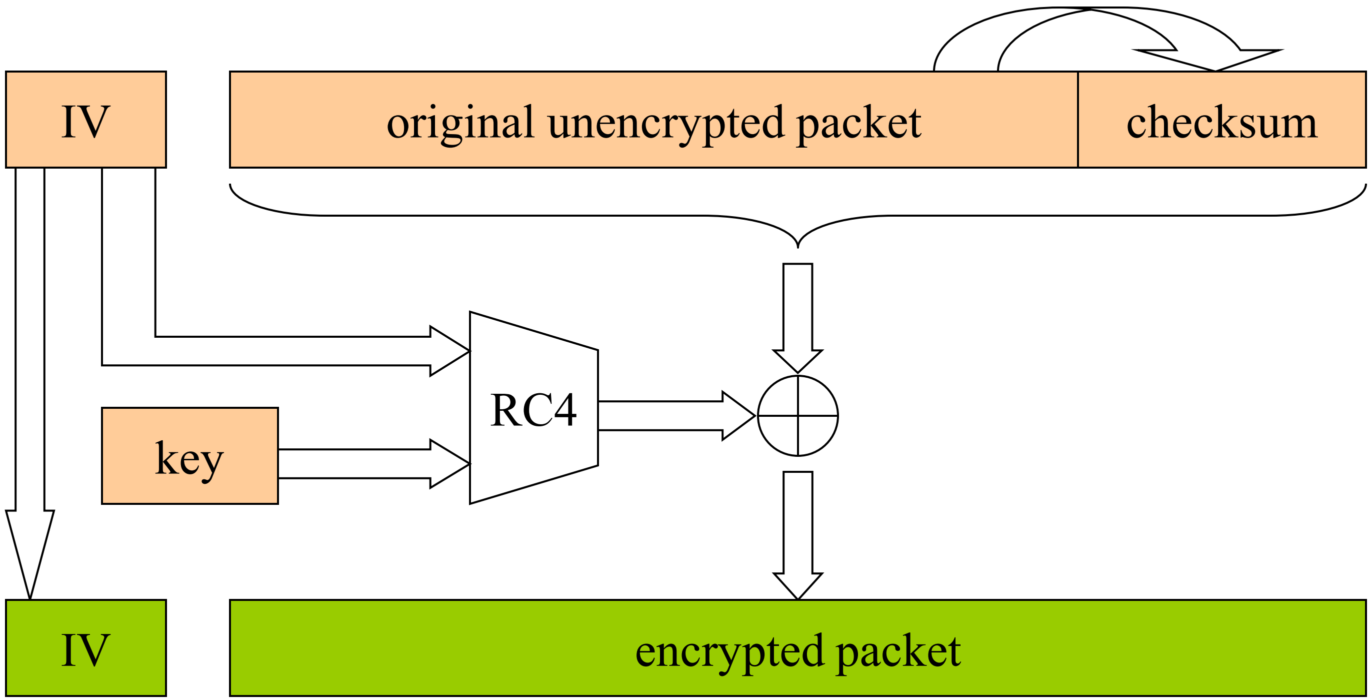
IV, $P \oplus RC4(K, IV)$ →

IV, $P' \oplus RC4(K, IV)$ →

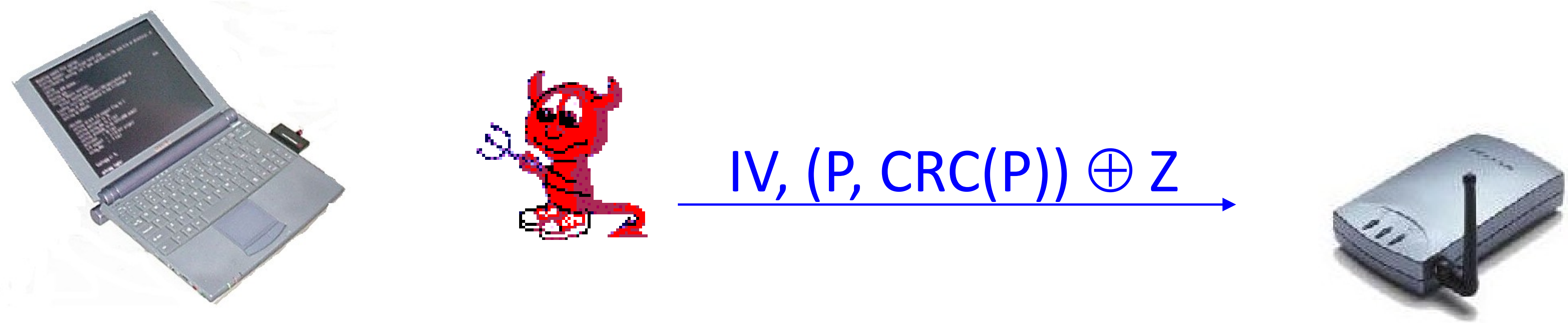
- In some implementations, IVs repeat.
  - If we send two ciphertexts (C, C') using the same IV, then the xor of plaintexts leaks ($P \oplus P' = C \oplus C'$), which might reveal both plaintexts

➤ Lesson: If RC4 isn't used carefully, it becomes insecure

WEP -- Even More Detail



Attack #2: Spoofed Packets

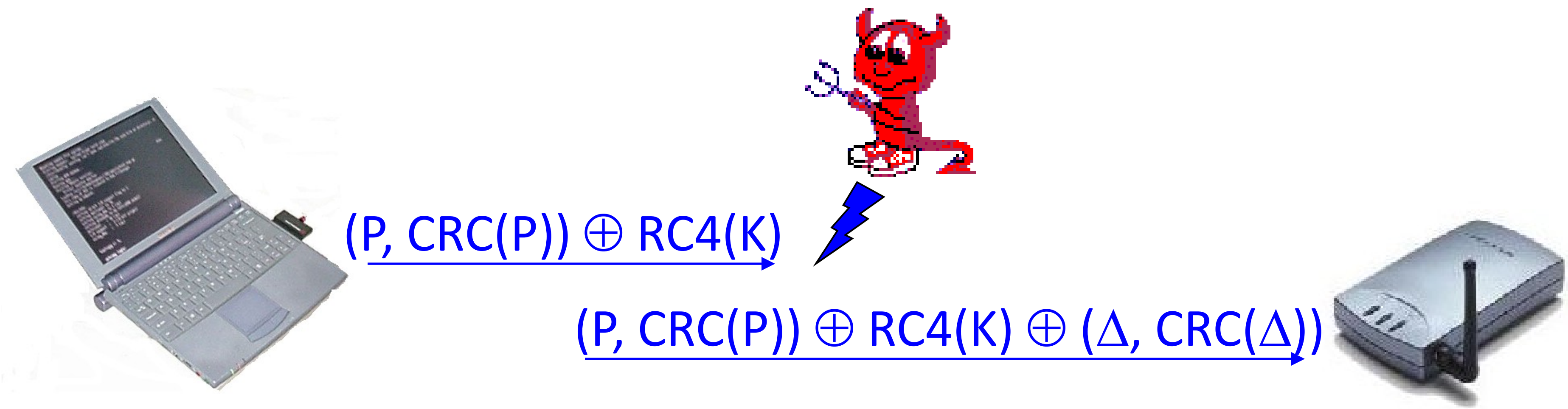


- Attackers can inject forged 802.11 traffic
  - Learn Z = RC4(K, IV) using previous attack
  - Since the CRC checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

➤ Attackers can bypass 802.11 access control

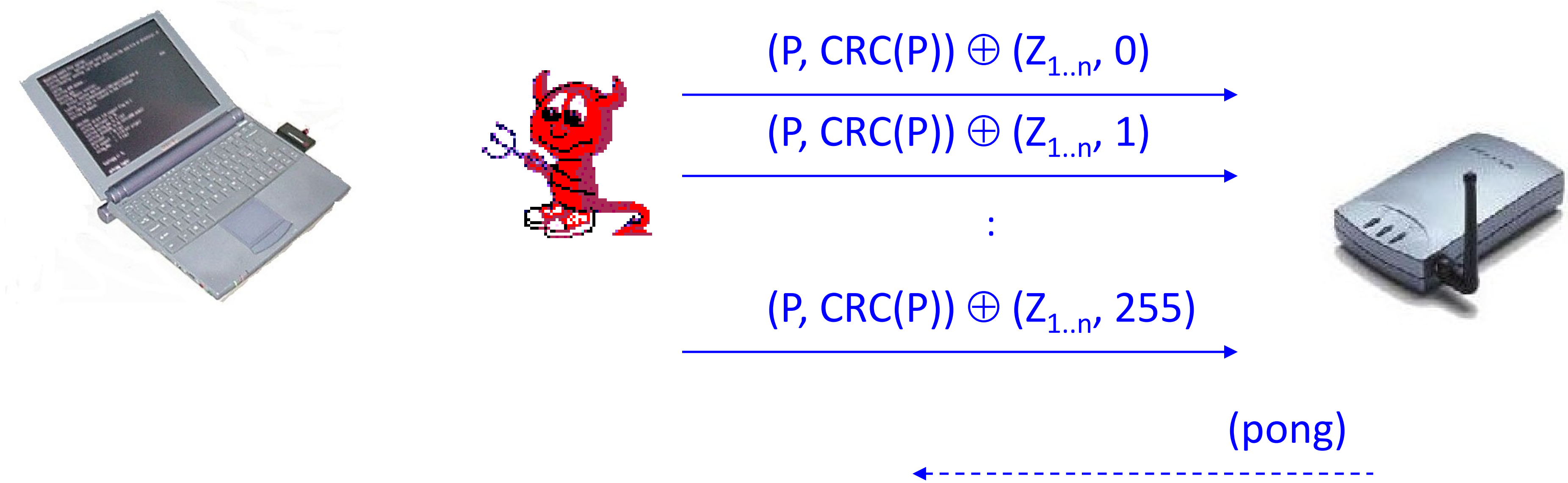
- All computers attached to wireless net are exposed

Attack #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

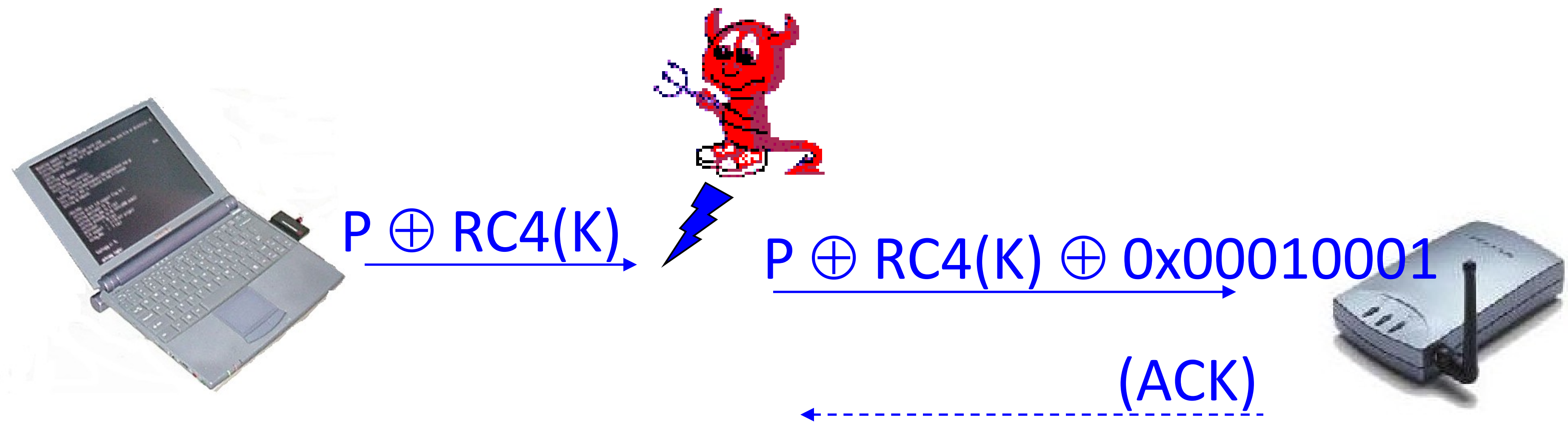
Attack #4: Inductive Learning



- 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 $n=1,2,\ldots$, until all of RC4(K, IV) is known

Credits: Arbaugh, et al.

Attack #5: Reaction Attacks



- TCP ACKnowledgement returned by recipient
  ⇔ TCP checksum on modified packet (P ⊕ 0x00010001) is valid
    ⇔ wt(P & 0x00010001) = 1

➤ Attacker can recover plaintext (P) without breaking RC4

Wardriving / Access Point Mapping

468 WEP

1,265 Clear

1,733 Total

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