WinCE Penetration Project

by Jared Crane (Graduated)
- Sofie Nystrom
- Seny Kamara
- Scott Yost
- Kyle Alexander
- Dan Noland and
- Pascal Meunier

Thanks to Kent Wert and Vince Koser.
We are grateful for Microsoft's support.

- Vulnerabilities in
  - WinCE (TCP/IP)
  - ActiveSync (3 not shown)
  - 802.11 Wireless Standard and implementations

TCP/IP

- Initial Sequence Number Vulnerabilities

- Random packets
  - PocketPC crash
    - from Linux
    - not OpenBSD!

  - Different random number generator means different packet space coverage

- Multiport syn flood
  - Quaking screen DoS

802.11 Networks

- Listen to Beacons
- Associate
- Authenticate
- exchange data

- "Closed" networks
  - No beacon broadcast
  - SSID is "secret"
  - but...
    - can be sniffed from Association request frames

- MAC address list
  - Unique
  - linked to hardware
  - But...
    - can be overwritten
    - Most drivers restrict it to Local ethernet addresses

Authentication

- Trivial to defeat
- A Tells B "I want to associate"
- B tells A: encrypt this
- A chooses pad for encryption
- A sends to B encrypted text
- Eve XORs plain text and encrypted text and gets the pad
- Eve chooses the same pad and gets authenticated

- ISO/IEC8802-11:1999(E) section 8.2.1:
  - *"The IEEE 802.11 standards committee specifically recommends against running an IEEE 802.11 LAN with privacy (WEP) but without authentication. (Doing so...) leaves the system open to significant security threats."*

Security of the Wired Equivalent Privacy (WEP) Algorithm

Kyle Alexander, Seny Kamara,
Pascal Meunier, Dan Noland,
Sofie Nystrom, Scott Yost

April, 2001

winCE@cerias.purdue.edu

Overview

- Motivation
- Introduction to the WEP algorithm
- Analysis of WEP Security Mechanism
- Attacks on WEP
  - Passive
  - Active
- Demo
- Conclusion

Motivations For Research

- 802.11b networks becoming more common
- Broadcasting information makes it more vulnerable to attack.

Introduction to the WEP Algorithm

- WEP – Wired Equivalent Privacy
- An option in IEEE 802.11(b) standard for Wireless LAN communication
- Goal of WEP: To replace the physical security lost in the transition to a wireless network

Components of WEP

- RC4 encryption (stream cipher)
- Integrity Check (IC), CRC-32 checksum (encrypted)
- Initialization Vector (IV), 24-bit (cleartext)

RC4 Overview

- Symmetric key encryption algorithms
- Keystream is generated from the key
- Plaintext is XORed with keystream
- Vulnerable to known plaintext attack

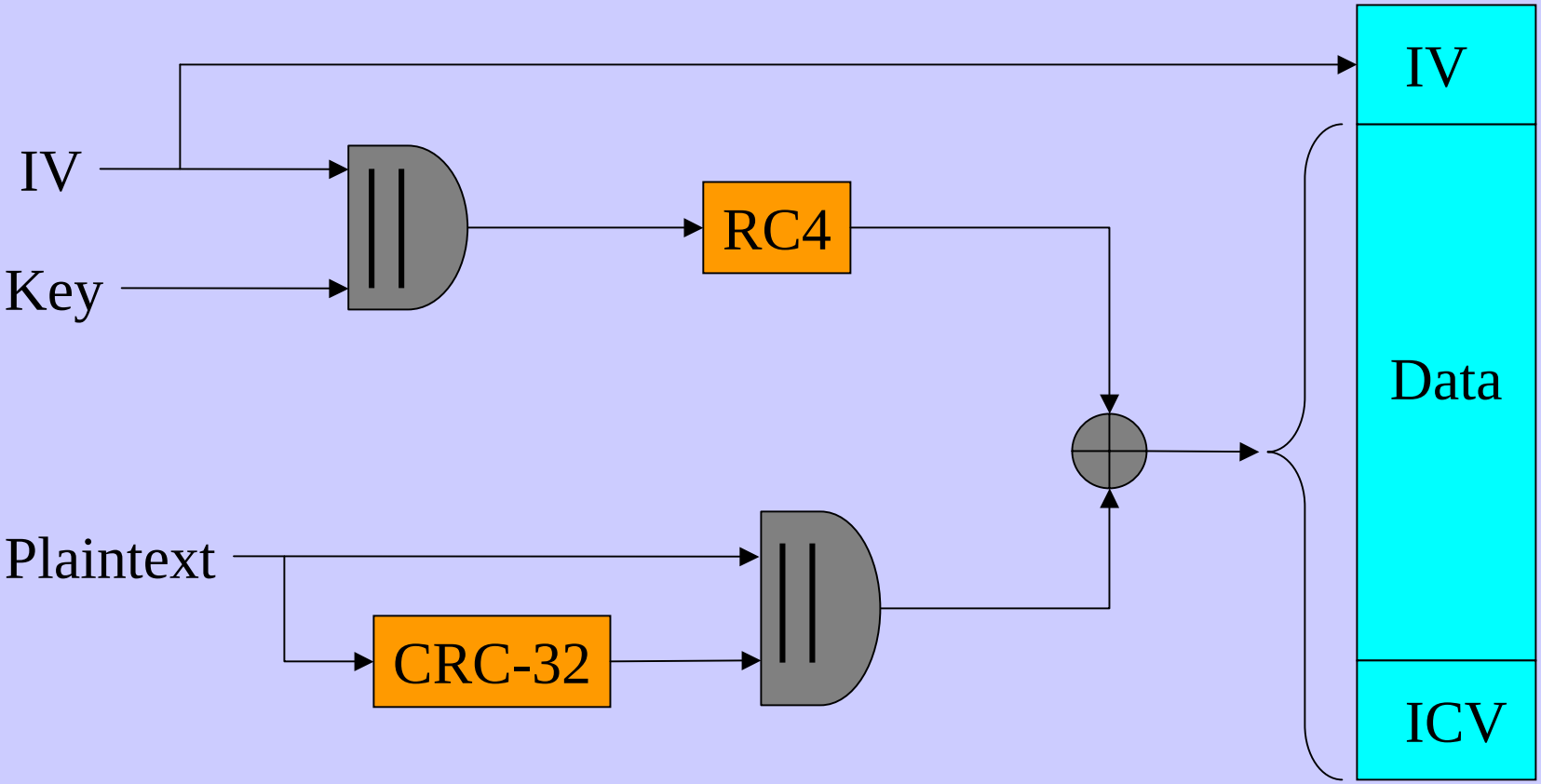
What is an IV?

- IV -- Initialization Vector
- New IV generated for each message
- Concatenated with the key
- Pad (keystream) then generated from IV + Key
- Prevents known plaintext attack
- Transmitted in cleartext

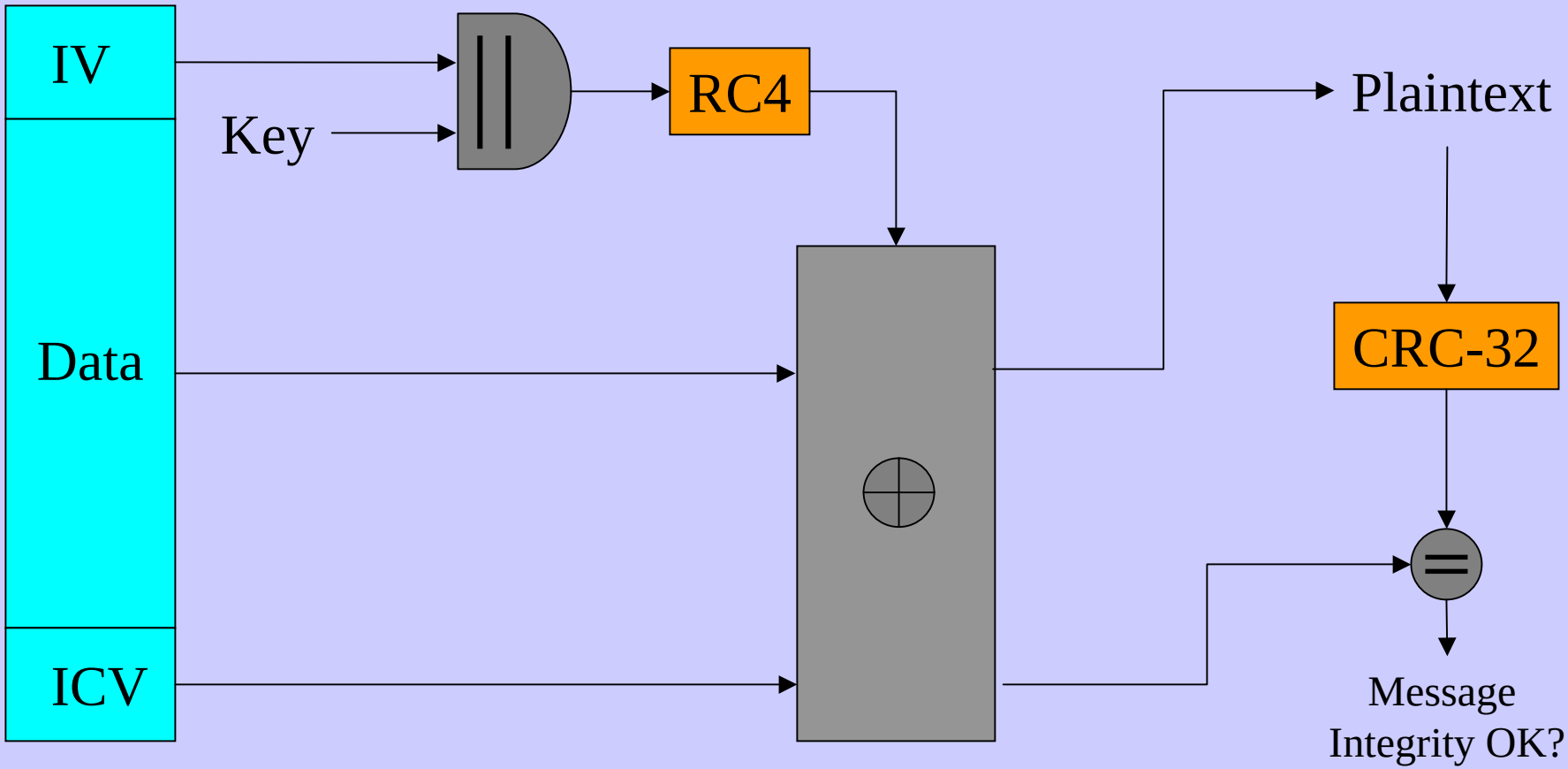
Stream Cipher Mechanism

Alice's message:		`H e l l o  B o b !`
RC4(IV + key):	⊕	`48656c6c6f20426f6221`
Ciphertext:		`2c145d0c27403e63ddf6`
RC4(IV + key):	⊕	`48656c6c6f20426f6221`
Decoded message:		`H e l l o  B o b !`

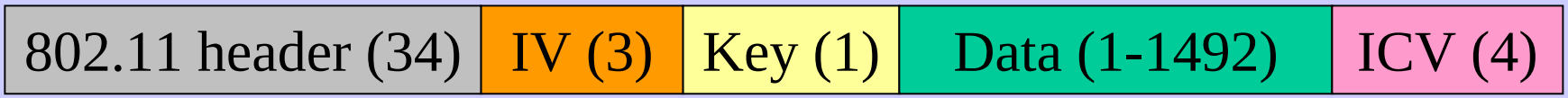
Enciphering with WEP



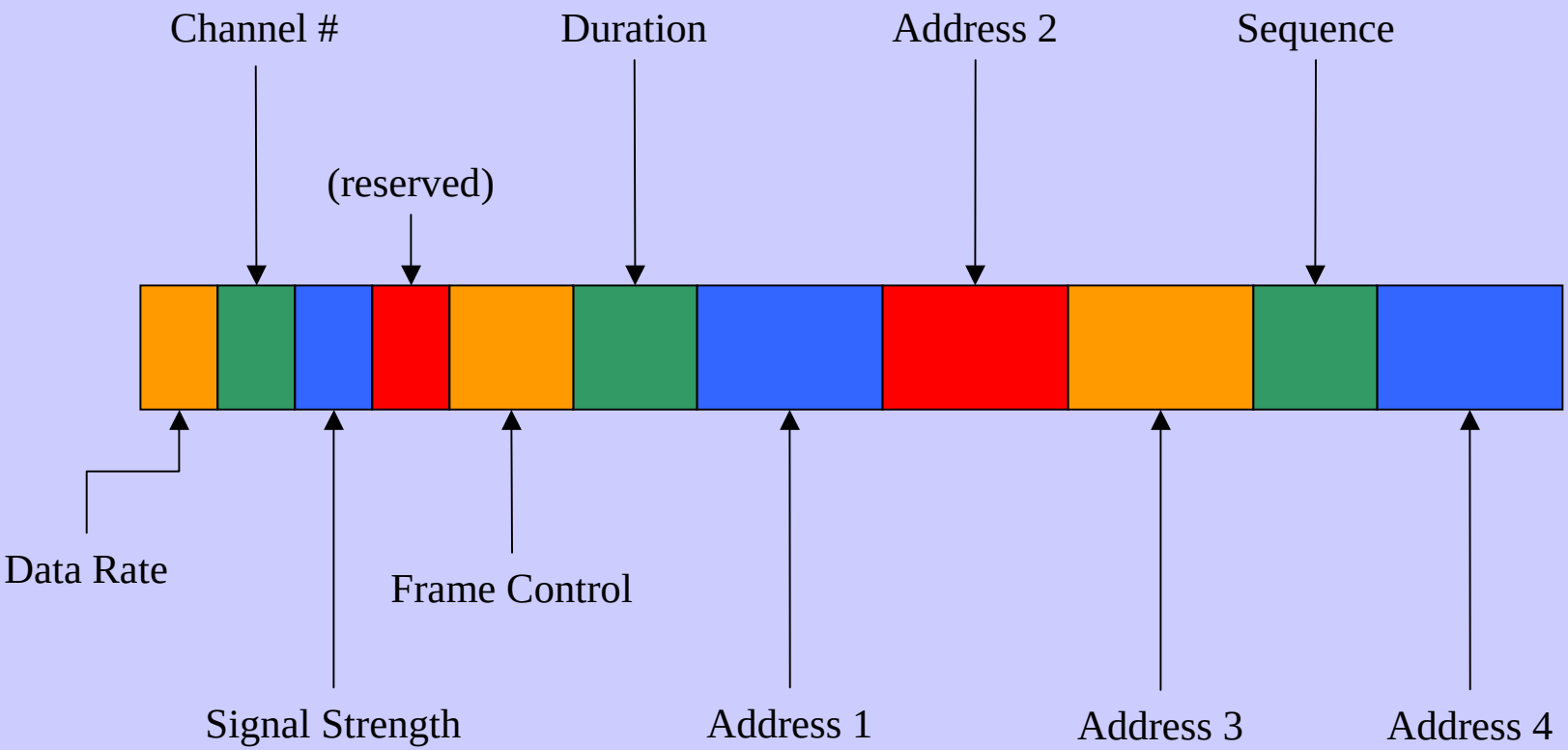
Deciphering with WEP



WEP Encrypted Frame Body



802.11 Header Breakdown



Overview of WEP Attacks

- Passive attack
  - Compromises confidentiality of network
  - Semi-passive approach makes this more practical
  - Takes some time and space to implement
- Active attack
  - Compromises integrity and/or availability of network
  - Requires little time or space

Overview of WEP Attacks

- IV flaws make these easier to implement
- All attack software is user-level code written by undergraduates in spare time

Choice of IV

- Random IV
  - 0xAB45F3
  - 0x58C24B
  - 0x9A02E1
  - 0xDEA824
  - Etc..

- Best choice
- 16777216 possible IVs
- At experimental speeds, it takes about ten days to achieve 87% decryption rate
- Up to 24GB of space needed to store full set

IV Implementation Flaw #1

- 0xAB00F3
- 0x58024B
- 0x9A02E1
- 0xDE0124
- Etc..

- Middle byte can only be 00,01,02,03
- Six bits wasted
- 262144 possible IVs
- Takes about four hours to achieve 87% decryption
- Below 400MB to store full set

IV Implementation Flaw #2

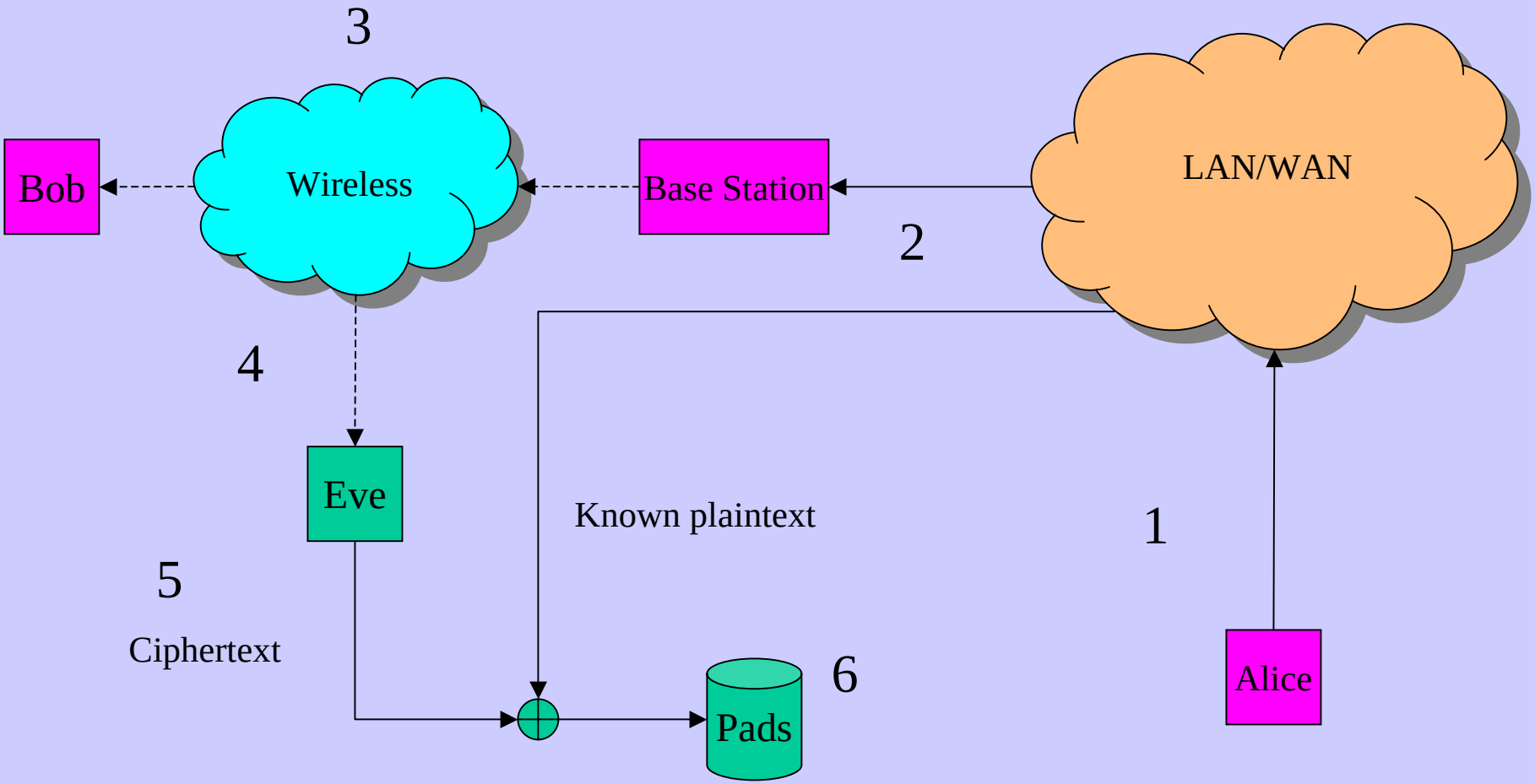
- `0xAB4EF3`
- `0xAB4EF4`
- `0xAB4EF5`
- `0xAB4EF6`
- Etc..

- Chosen sequentially
- Guarantees that we will get full set of pads
- Takes about five days to achieve 100% decryption

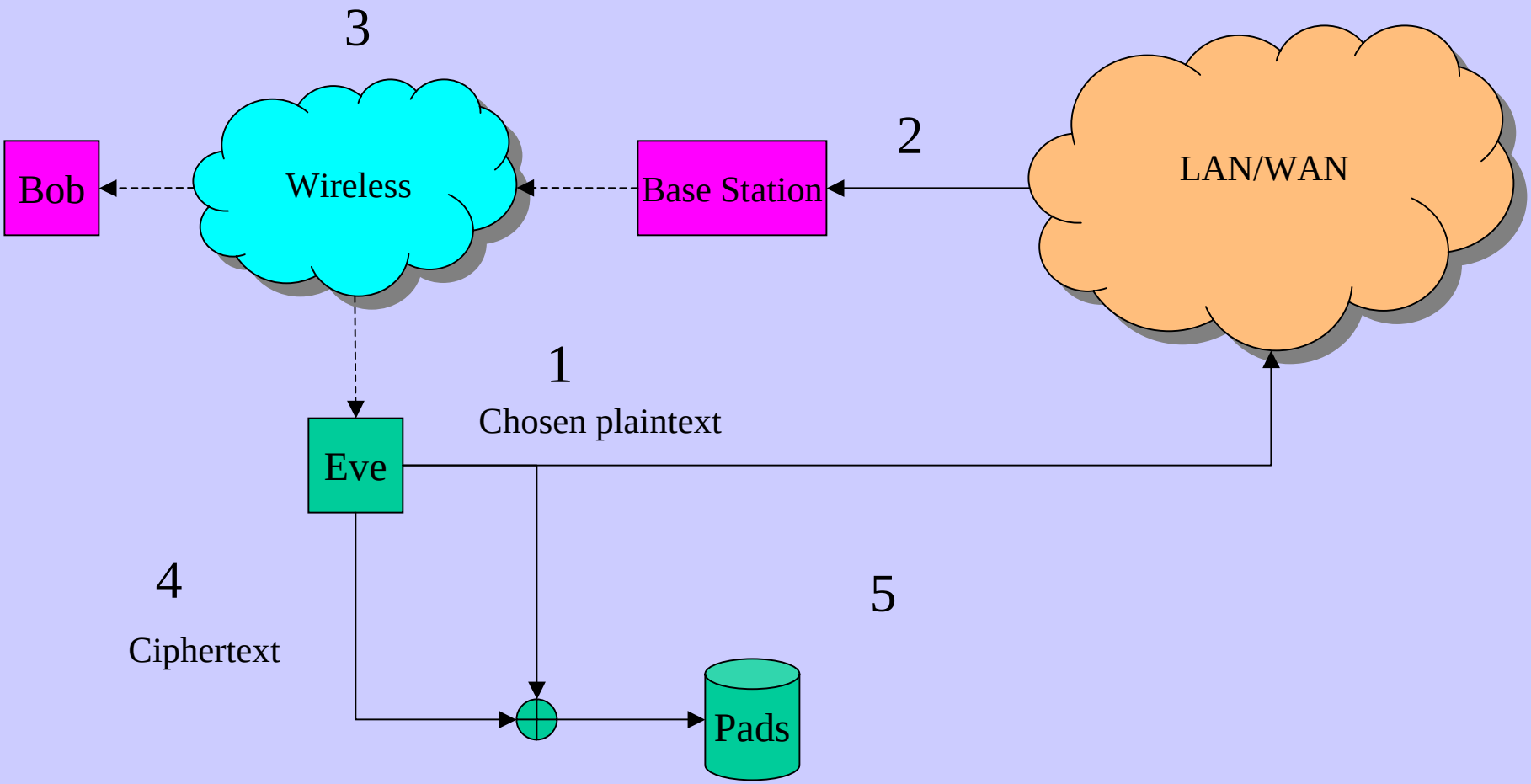
Attacks: Passive

- Collect a set of pads
- Can then decrypt any packet for which we have the pad
- Works equally well for 64-bit or 128-bit encryption
- “Semi-passive” attack – the attacker sends chosen plaintext messages

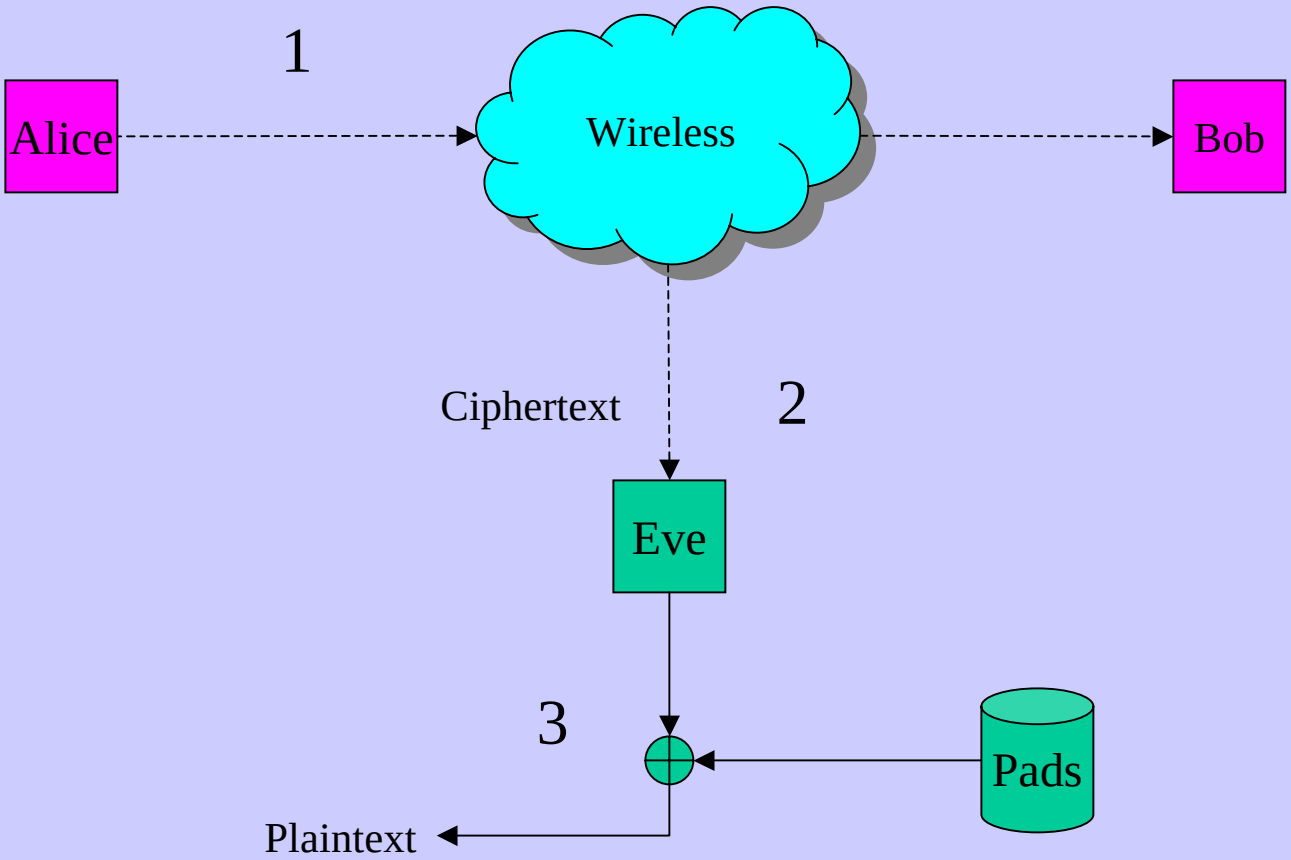
Passive Pad Collection



“Semi-passive” Pad Collection



Packet Decoding



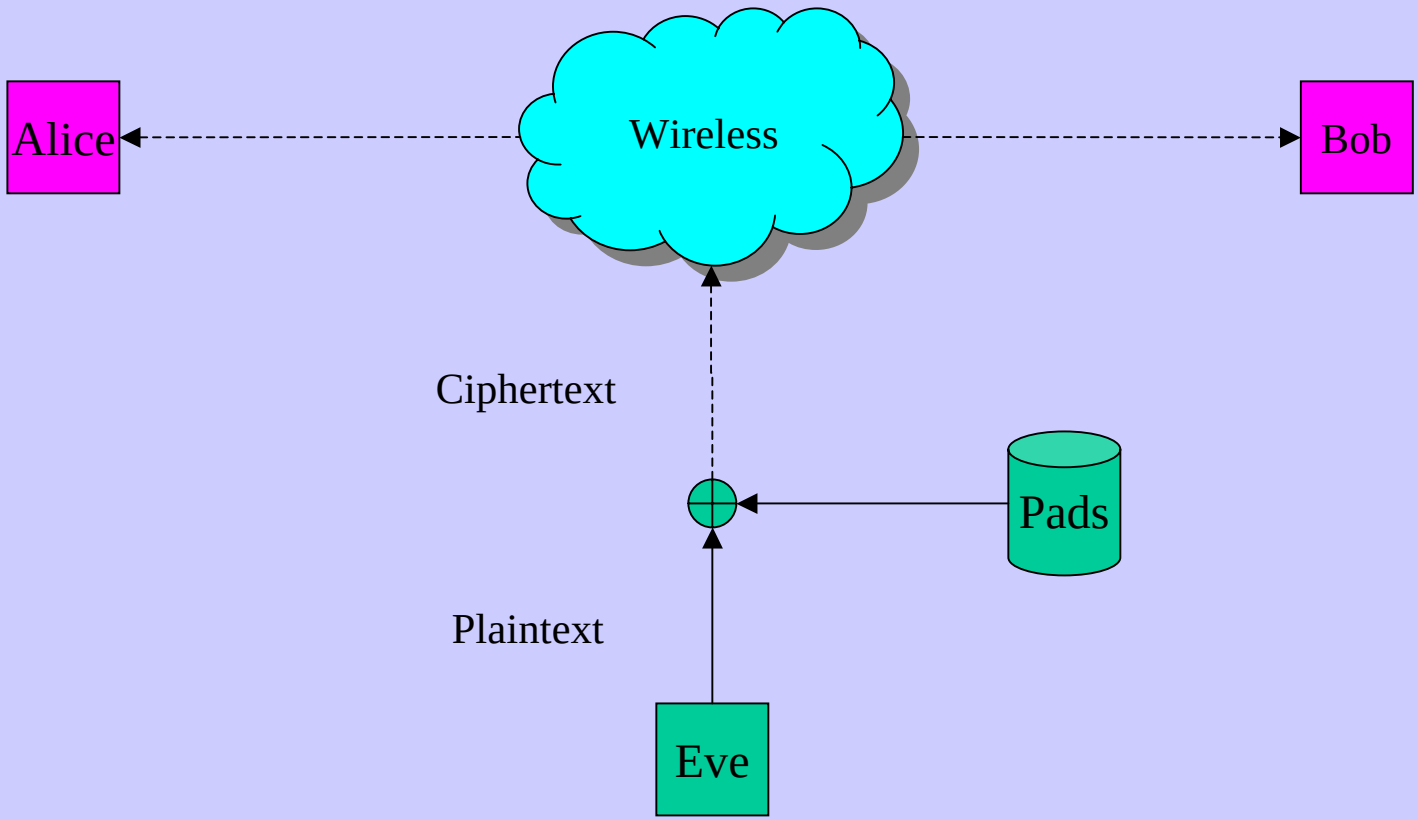
Attacks: Passive

- Pad collection requires traffic across the network.
- Need to intercept over 24GB of data for full attack
- If IV generation is flawed, this becomes even easier
- Can mount a less complete attack
  - 20 bytes are sufficient to attack telnet, rlogin, FTP authentication
  - < 400 MB to store full set of 20-byte pads
  - With Cisco IV flaw, this attack requires only 15MB
- Can spread the attack over time to inhibit detection

Attacks: Active

- First collect one or more pads.
- 802.11(b) spec does not prevent reuse of IV
- Can then send encrypted packets onto the network using only one IV/pad combination.
- Does not require sending large amounts of traffic or storage space
- Requires driver-level code changes to implement

Send Pads Onto Closed Network



Testbed Details

- Cisco base station
- Ipaq with Lucent WaveLAN Gold card (Bob)
- OpenBSD system with Aironet card (Alice/Eve)
- Libpcap, Libnet

Demo of Semi-Passive Attack on WEP

Conclusion

- Size of IV space too small
  - Current IV space is vulnerable to casual attack
  - Time to attack and space to store pads are within the range of casual attacker
  - If IV were four bytes, would require 6TB to store a full set of pads
  - Would require over seven years to collect 87% of pads
  - Time and space would be too large for casual attack with current hardware

Conclusion

- No key management protocol
  - Keys must be changed manually at access point and each client
  - Key interface is non-standard
  - If keys are not changed regularly, an attacker only needs to collect pads once
  - This also allows the attacker to spread out the collection attack to make it less noticeable

Conclusion

- None of these methods would defeat the active attack because it only requires one pad.
- A casual attacker can currently compromise a WEP-protected 802.11(b) network with a minimal amount of resources.