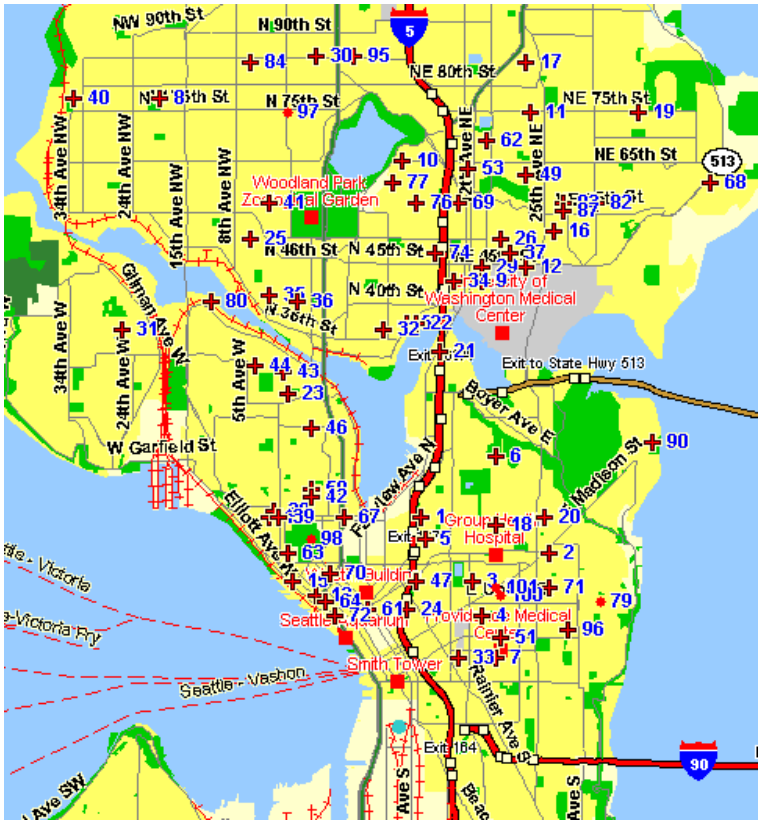
# WLAN Security: Fact, Fiction, and Research

William A. Arbaugh
Department of Computer Science and UMIACS
waa@cs.umd.edu
http://www.cs.umd.edu/~waa
http://www.missl.cs.umd.edu

UNIVERSITY OF MARYLAND

# The Future of WLAN's?

- 4G?
- Hot spot coverage only ala Boingo et. al?
- Or some sort of overlay blend?
- Regardless- the organic growth will continue.



# The Threat

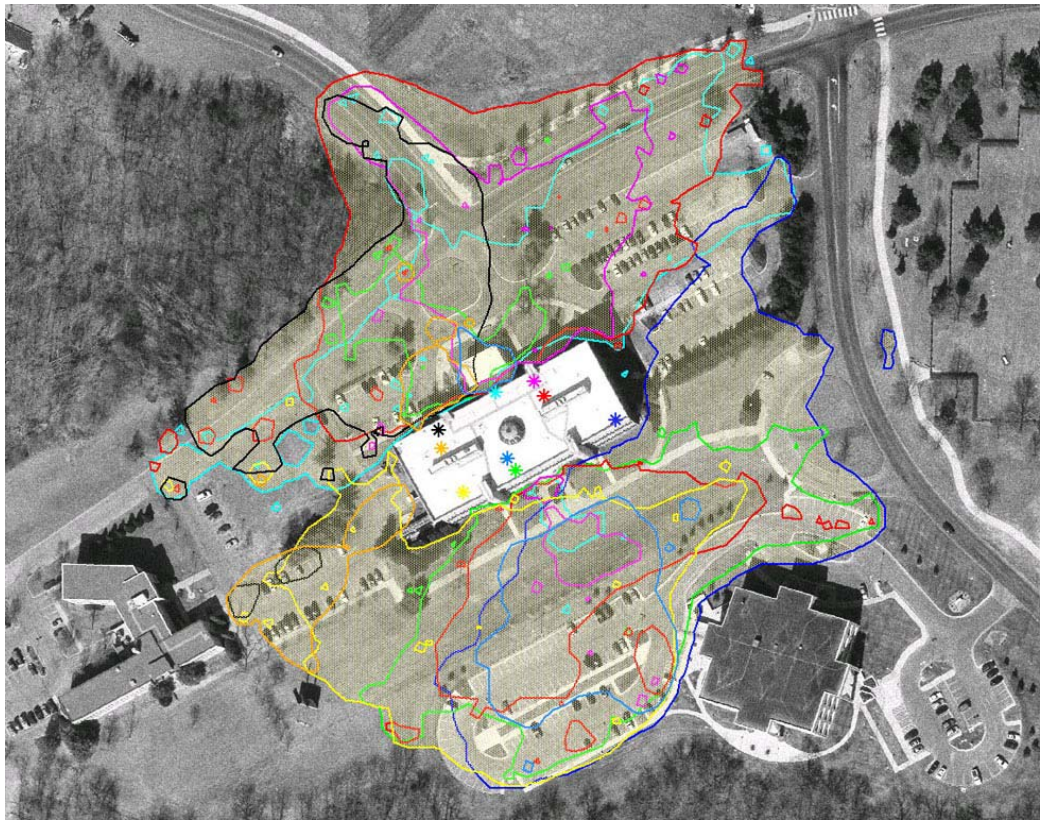
- In general, there are four threat classes[1]:
  - Journeymen (Class 0)
  - Experts (Class 1)
  - Insiders (Class 2)
  - Well funded professionals (Class 3)

1. Modifications to the model originally proposed by [Abraham et. al.].

# Why Wireless Security is Different

- An attacker has access to the transport medium of your network!
  - Essentially elevates the experts to an insider (higher threat)

# The Wireless Threat



Used with permission from KARS: http://www.ittc.ku.edu/wlan/

# Wired Equivalent Privacy

- What exactly does that mean?
- My guess:
  - Prevent unauthorized use (access control, authentication, and integrity)
  - Prevent unauthorized disclosure (confidentiality)
  - ~~Prevent unauthorized eavesdropping~~ (Not likely to happen in consumer wireless)

# Identity

- The current standard only uses the MAC address as a form of identity.
  - Unfortunately, the MAC address is malleable and further compounded by inadequate cryptographic binding [Walker, Borisov et. al., Arbaugh et. al.].
- The future standard uses two forms of identity: MAC address at the link layer, and a user ID at the network layer.
  - Requires cryptographic binding between the two ID's [Mishra et. al.].

*nb*. History buffs will remember that the AMPS (Cellular) system made the same mistake with the equipment serial number (ESN).

# Access Control

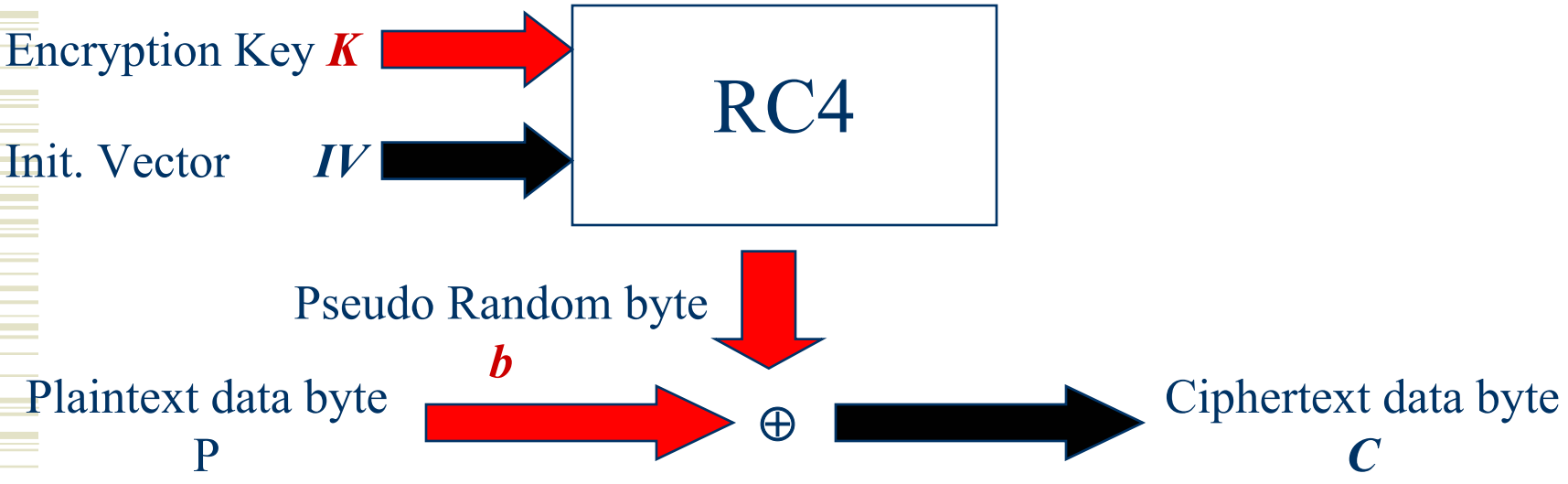
- MAC access control lists
  - MAC address is forgeable [Arbaugh et. al.]
- Proprietary "closed network" used a shared secret as access token.
  - Access tokens broadcast in the clear in management frames [Arbaugh et. al.]

*nb*. Here the reliance on the expense/difficulty in eavesdropping as a security mechanism is again a mistake the cellular community made.

# Integrity

- The lack of any message authenticity mechanism, or the reliance on error detection (CRC) for integrity protection.
  - A linear CRC combined with a linear combiner, XOR, allows “bit flipping” [Borisov et. al.].

# Confidentiality via WEP




Decryption works the same way: $P = C \oplus b$

# Confidentiality

- IV space is only $2^{24}$
  - Creates Depth [Walker, Borisov et. al.]

    $c_1 \oplus c_2 = (p_1 \oplus r) \oplus (p_2 \oplus r) = p_1 \oplus p_2$
- Lack of Replay protection combined with stream cipher
  - Asynchronous known plaintext attack [Walker, Borisov et. al.]
  - Synchronous known plaintext attack [Arbaugh]
- IV as first part of key
  - Induces several classes of weak IV's. The most damaging being when the IV is of the form <n,FF,x> [Fluhrer et. al.]

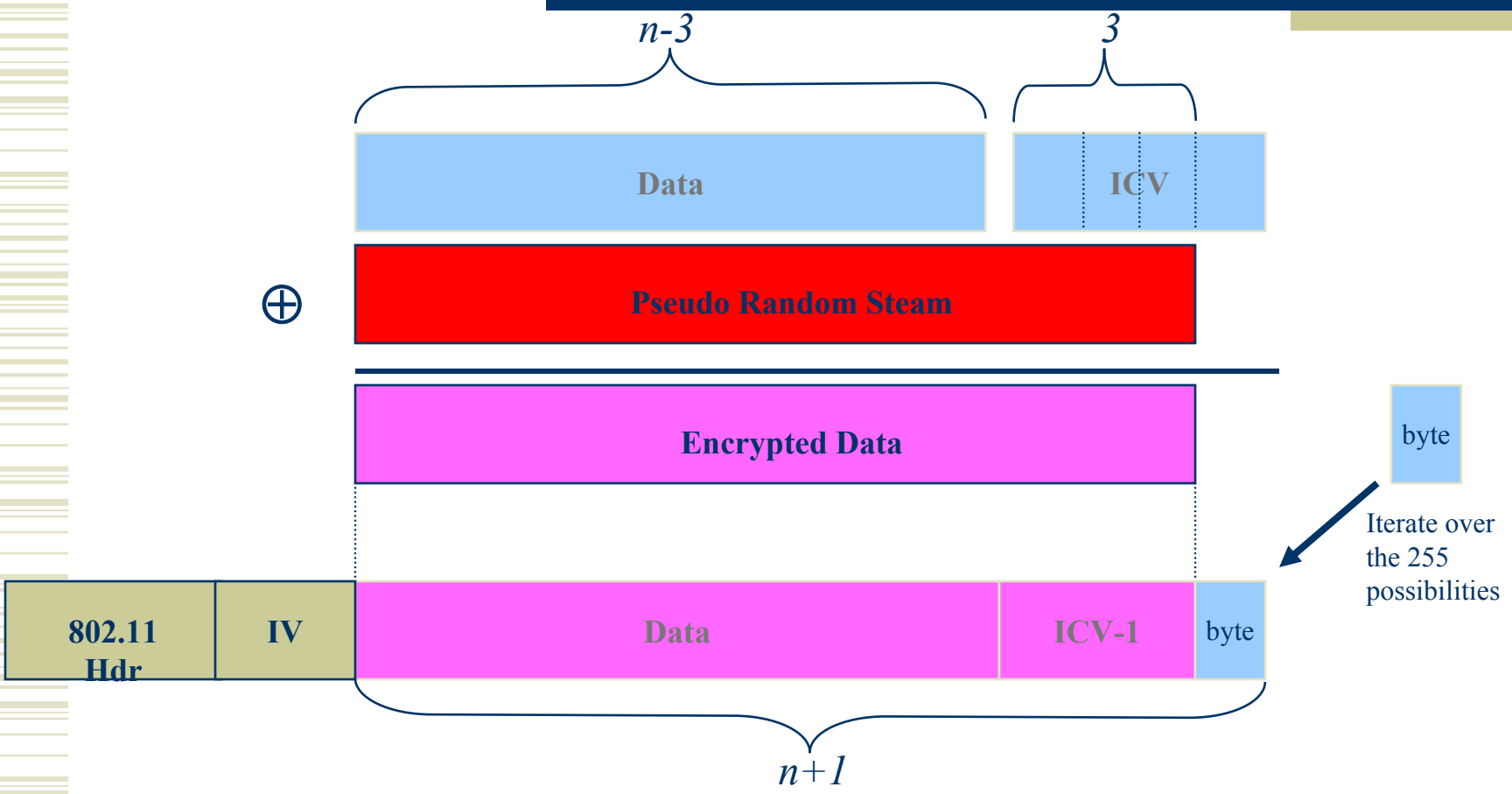
# Inductive Chosen Plain Text Attack

- *Base Case*: Recover an initial pseudo random stream of length $n$ from known plain text.
- *Inductive step*: Extend size of known pseudo random to $n+1$ by leveraging the redundant information in the CRC.

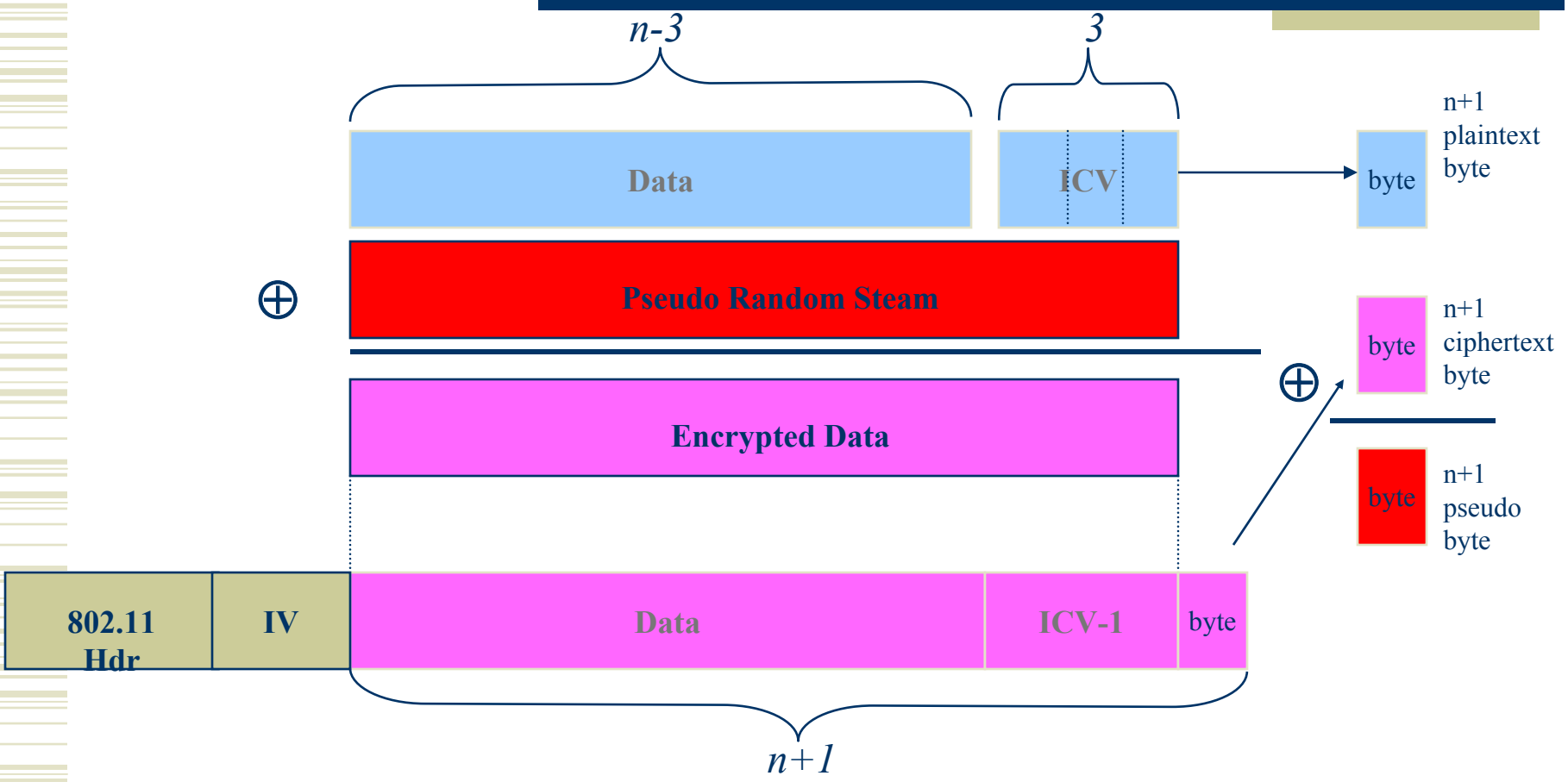
# Base Case

- Find initial pseudo random stream of size *n*.
  - Identify DHCP Discover messages from externals, e.g. size, and broadcast MAC address.
    - Known source (0.0.0.0), destination (255.255.255.255), header info
    - Allows the recovery of 24 bytes of pseudo random stream: Let $n = 24$

# Inductive Step



# After Response



# Attack Cost

- Assume moderately aggressive attacker:
  - ~100 attacker transmissions per second
  - NOTE: ICV failures will not be passed to OS and thus the attack is difficult to observe (failed ICV counter not withstanding)
- 1.6 hours to recover 2300 byte MTU regardless of IV and key size worst case
- ~40 minutes in average case

# WEP Costs

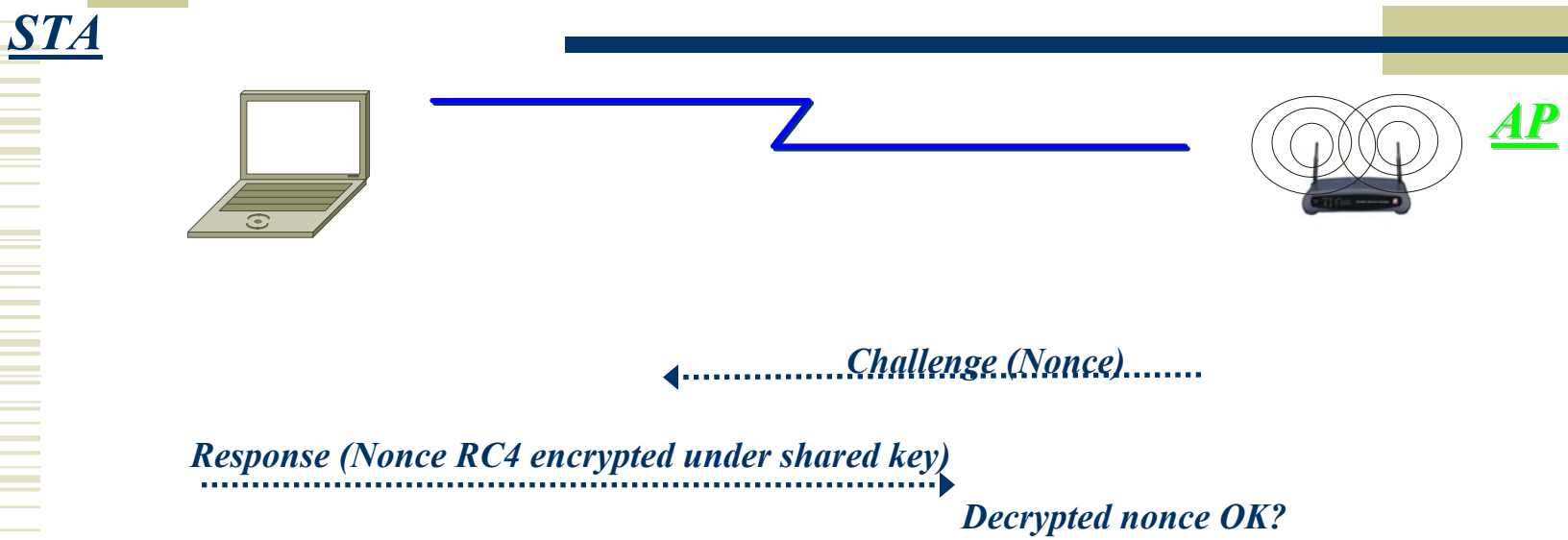
- 46 hours to build full dictionary of <*IV, pseudorandom*> with one attacking host (~35GB)

- But, the attack is embarrassingly parallel.
  - Four attacking hosts: 11.5 hours
  - Eight attacking hosts: 5.75 hours

# Authentication

- The use of a challenge response system covered by a Vernam cipher.
  - Eavesdropping on a single successful authentication provides the attacker the ability to authenticate at will [Arbaugh et. al., Borisov et. al., Walker]

# Authentication Attack




With what we know now, an easy attack is obvious:

- Record one challenge/response with a sniffer
- Use the challenge to recover the random stream: $r = challenge \oplus response$
- Use the recovered random stream to encrypt any subsequent challenge:

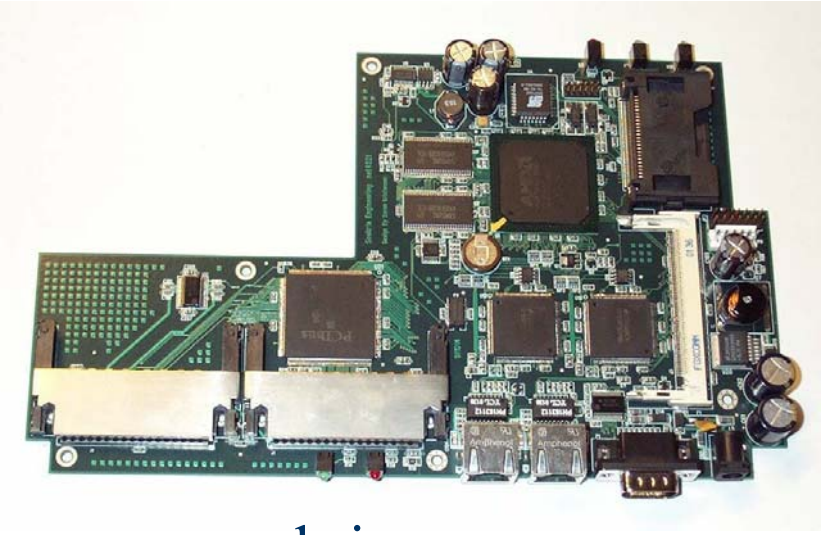
$$response = challenge \oplus r$$

# UMCP WLAN/WMAN Test Bed

- Currently funded by a Critical infrastructure grant from NIST (two of four years funded).
- First phase deployment involves ~40 WLAN access points in a single building (IOC August 16, 2002).
- Second phase extends coverage to a second building and outside areas (IOC TBD).
- Additional (currently unfunded) phases will include merging with University WMAN, and creation of an overlay network (IEEE 802.11a, GPRS/CDPD).

# Test Bed Hardware

- Soekris Net4521
- 100/133 Mhz AMD ElanSC520
- 16-64 Mbyte SDRAM, soldered on board
- 1 Mbit BIOS/BOOT Flash
- CompactFLASH Type I/II socket, 8 Mbyte FLASH to 1Gbyte IBM Microdrive
- 1-2 10/100 Mbit Ethernet ports, RJ-45
- 1 Serial port, DB9.
- Power LED, Activity LED, Error LED
- Mini-PCI type III socket. (for optional hardware encryption.)
- 2 PC-Card/Cardbus slots, for wireless adapters
- 8 bit general purpose I/O, 14 pins header
- Hardware watchdog
- Board size 9.2" x 5.7"
- Power either 5V DC fixed or 12-60V DC, max 12 Watt
- Supports Power over Ethernet using proposed 802.3af standard
- Operating temperature 0-60 °C



www.soekris.com

# Test Bed Software

- OpenBSD or FreeBSD OS base
  - http://www.openbsd.org or http://www.freebsd.org
  - Prism2 host AP driver included in current trees of both OpenBSD and FreeBSD
  - IEEE 802.1X from http://www.open1x.org (UMCP students funded by NIST CIP grant)
  - AES mode and TKIP source from NAI Labs, Inc. as part of CIP grant.
  - Remote management software TBD

# Research Questions

- Metric based trust model
  - How to provide an efficient mathematical basis for trust?
- Convergence to overlay networks
  - How to provide unified Authentication, Authorization, and Accounting (AAA)?
  - How to provide secure mobility?

# Research Questions

- Transformation of security “best practice” from a “moat” model to an “island” model where each information device must protect itself (unification of ad-hoc and infrastructure protection).
  - How to provide such protection?
  - How to manage such a decentralized model?

# Your Questions

# References


D. Abraham, G. Dolan, G. Double, and J. Stevens, "Transaction Security System," *IBM Systems Journal*, vol. 39, pp. 206-229, 1991.

William A. Arbaugh, Narendar Shankar, and Y. Justin Wan, "Your 802.11 Wireless Network has No Clothes," presented at First International Conference on Wireless LANs and Home Networks, Singapore, 2001.

Nikita Borisov, Ian Goldberg, and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," presented at The Seventh Annual International Conference on Mobile Computing and Networking, Rome, Italy, pp. 180-188, 2001.

Arunesh Mishra, William A. Arbaugh, “An Initial Security Analysis of the IEEE 802.1X Standard,” Department of Computer Science, University of Maryland at College Park, CS-TR-4328, Feb 2002.

Walker, J., Unsafe at any key size: An Analysis of the WEP Encapsulation. 2000, IEEE 802.11 Task Group E, IEEE 802.11/00-362.

# Links

- You can find the previous references plus additional information (standards etc.) at:
  - http://www.cs.umd.edu/~waa/wireless.html
  - http://www.drizzle.com/~aboba/IEEE