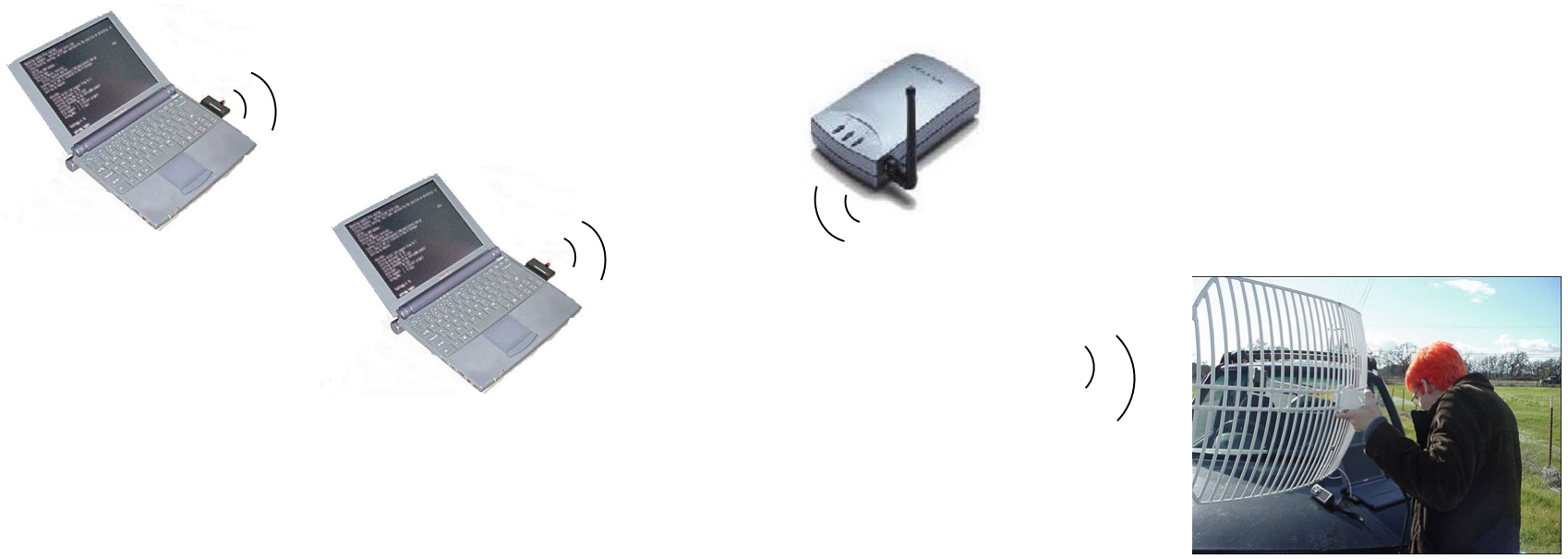
Leveraging RF Leakage for Eavesdropping Detection by AI

Wireless eavesdropping

802.11 wireless networking is on the rise

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

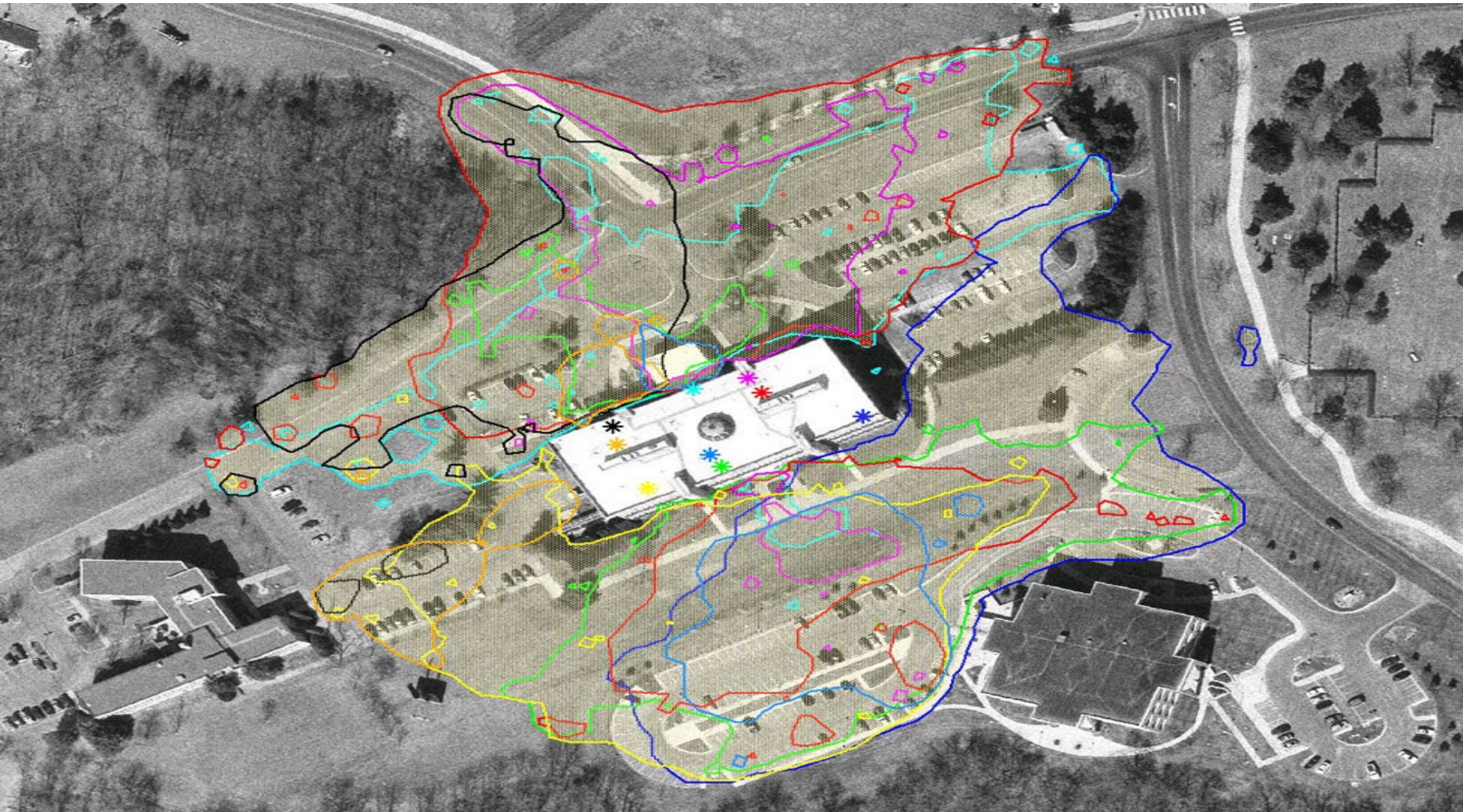
Wireless eavesdropping



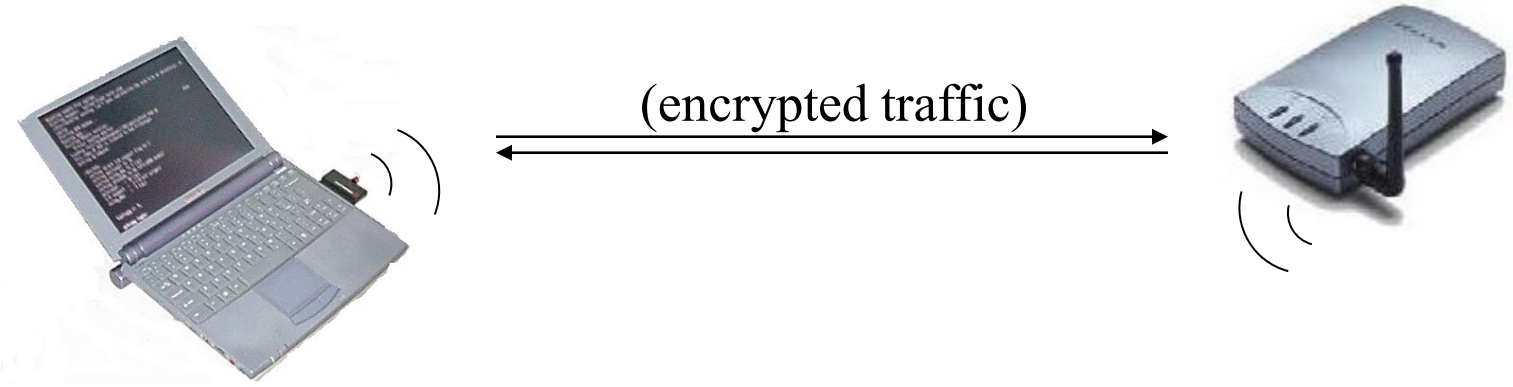
Wireless networking is just radio communications

- Hence anyone with a radio can eavesdrop, inject traffic

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

- 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 ⊕ RC4(K, IV)

IV, P' ⊕ 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 ⊕ P' = C ⊕ C'), which might reveal both plaintexts

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

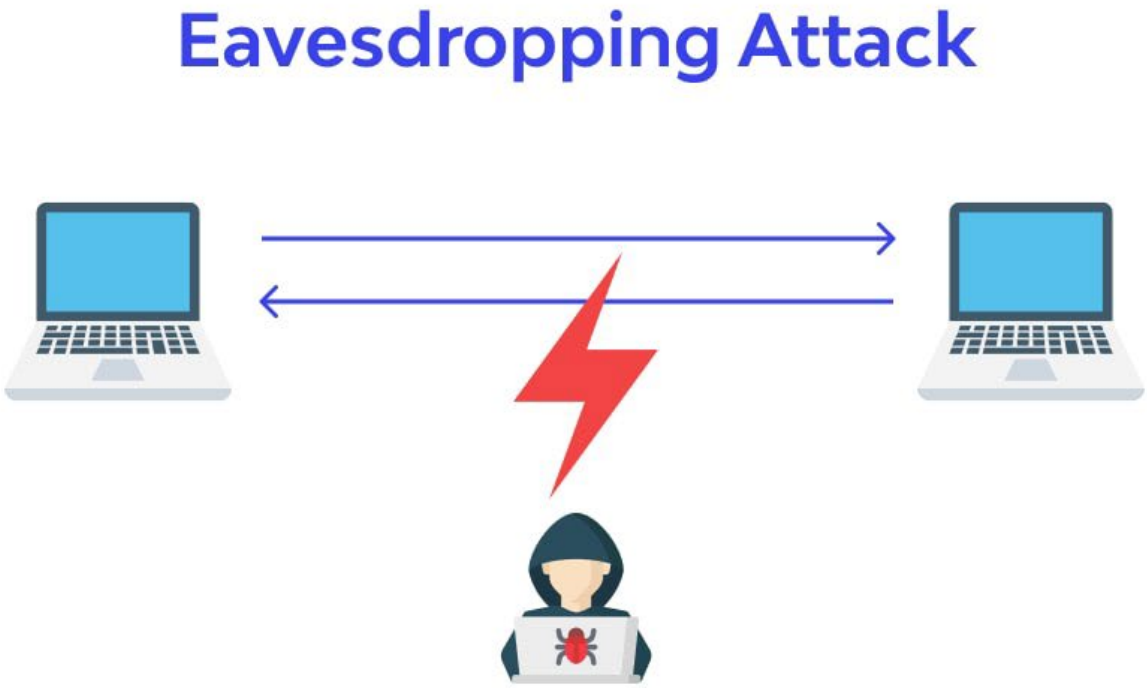
Attack: Keystream Reuse

- 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

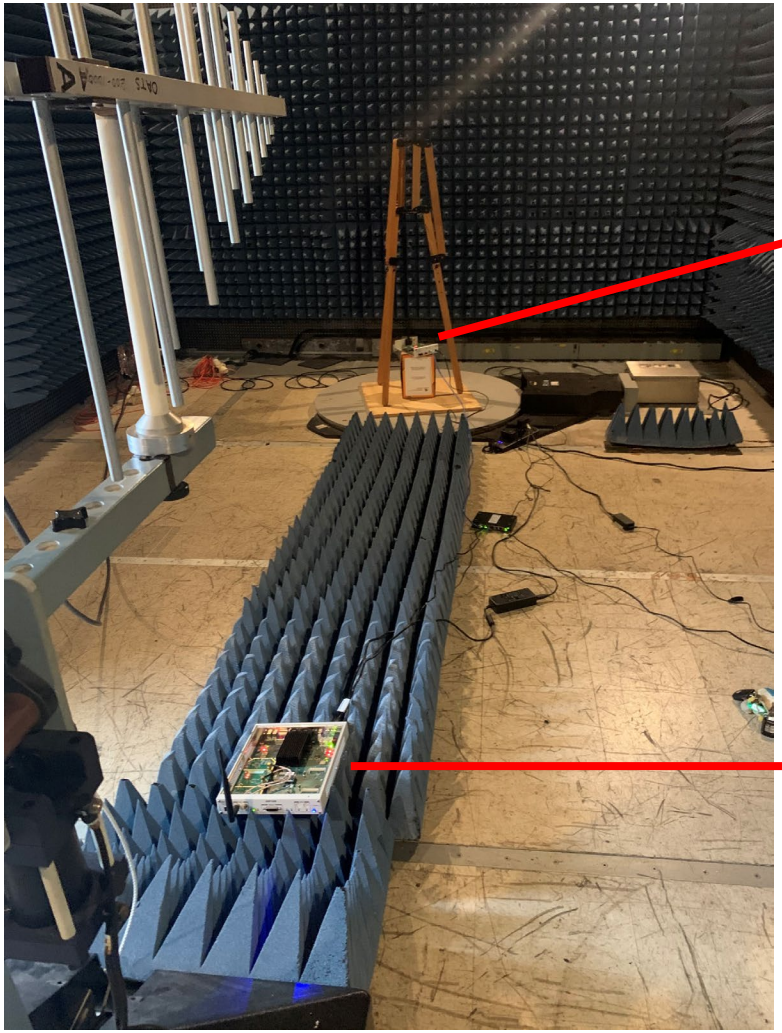
Toys for Hackers

How to detect eavesdrop

wallarm

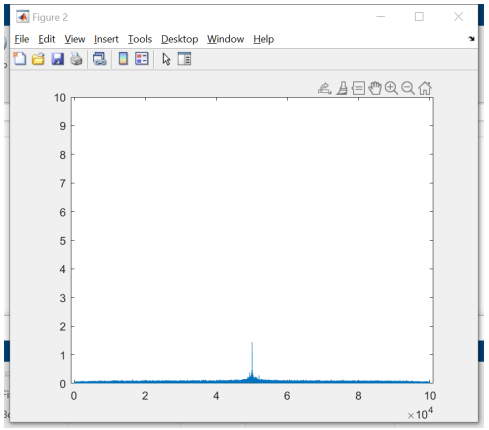


EM leakage on all wireless devices

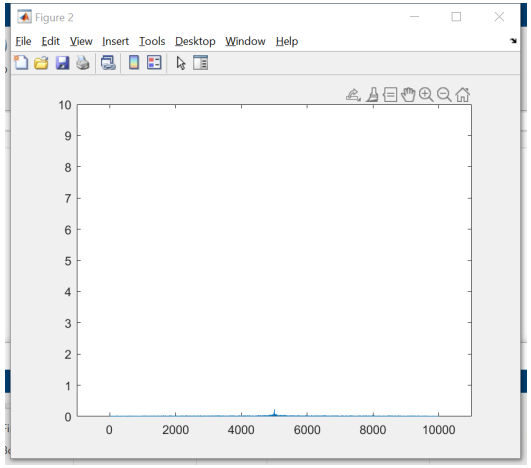


eavesdropper

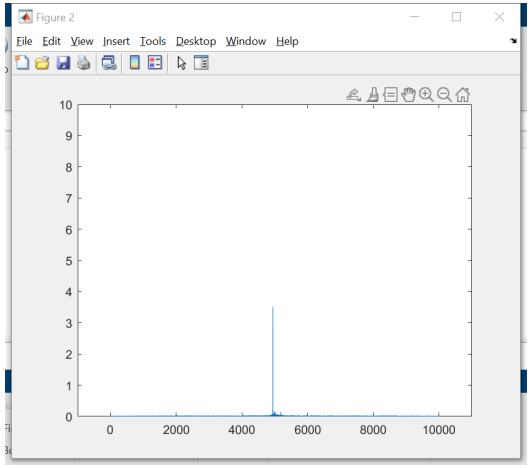
sensor



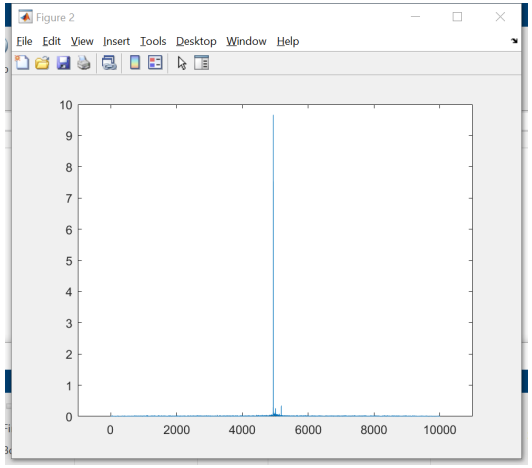
EM leakage on all wireless devices



4m



2m



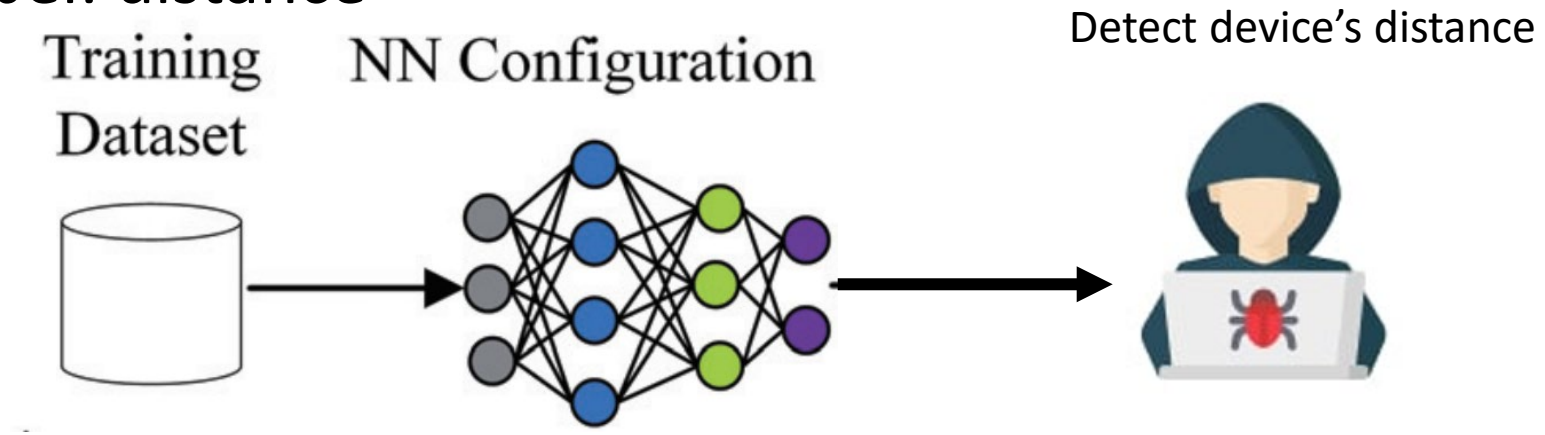
0m

Observations at different distances

EM leakage on all wireless devices

Data: Spectrum

Label: distance



Distance	Accuracy
Short (0m~2m)	96.3%
Long (>2m)	93.1%