A Practical, Targeted, and Stealthy attack against WPA-Enterprise WiFi

A. Cassola W. Robertson E. Kirda G. Noubir

College of Computer and Information Science, Northeastern University

NDSS 2013

Table of Contents

Northeastern University

WiFi is important:

- Main access method to the Internet
- Millions of people use it at home
- Organizations provide it for employee network access

Threats:

- Eavesdropping, tampering
- Rogue Access Points (Evil Twins)
- Jamming

- WEP (RC4 static key 1999) first broken 2001 allowing key recovery
- WPA TKIP (RC4 dynamic keying, 2002) temporary keystream recovery in 2008
- WPA CCMP (AES dynamic key, 2002) as secure as AES
- PSK: HMAC-SHA1 based functions

$$K = \text{PBKDF2}(SSID||PSK, 4096, 256)$$

$$K_t = \text{PRF-512}(K, MAC_{AP}, MAC_C, N_{AP}, N_C)$$

- Enterprise: Master key derived from protocol interaction: typically client TLS or MSCHAPv2 over TLS (PEAPv0)

Rogue APs trick users into connecting, but

- Competition for client attention, limiting range
- Techniques like WiFi Protected Setup: physical interaction
- RADIUS servers use signed certificates

Jamming can disrupt communication

- 802.11 NIC firmware protected by vendors
- Improvements in Physical Layer limit range

Is WiFi Ok?

Northeastern University

No, it is not

- We can get your password in hours to days
- It will look like an everyday glitch
- Only you will be the target
- Inexpensive ($4,500 or less)

We will show:

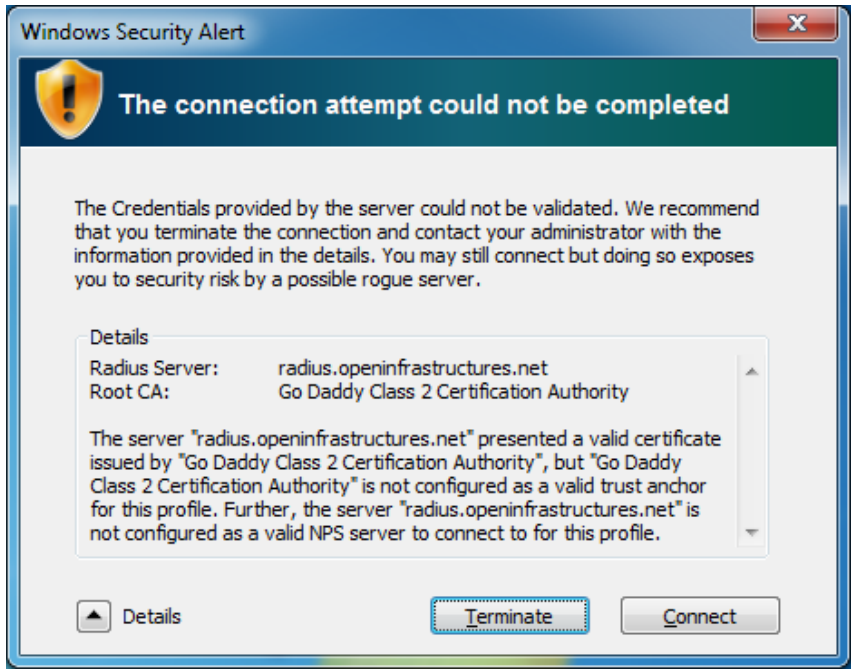
- Current isolated protections are not enough
- Flaws across the stack can be exploited together for maximum effect
- WiFi security needs a more solid foundation to build upon

Rogue AP

- Pose as legitimate member AP of network
- Client connects
- Client accepts certificate
- Listen to and breaks MSCHAPv2

However:

- Client selects "best" AP according to some measure, e.g. received power
- RADIUS servers identify themselves with TLS certificates
- Clients record FQDN of RADIUS server first time
- RADIUS certificate by other names will be refused



Forcing a new profile

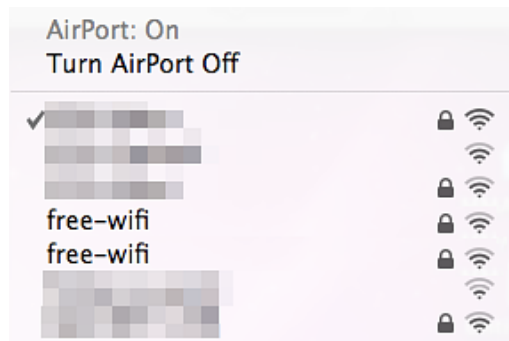
Northeastern University

System is open during new network setup:

- SSID is linked to RADIUS
- Using a different SSID forces a new network entry in client
- OS GUIs do not display SSID non-printable characters
- Use SSID + *control-char*

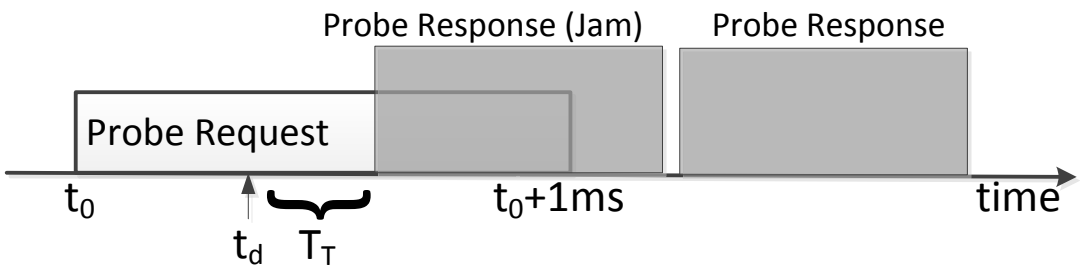
However:

- Repeated entries in table
- What to do? Jam legitimate network



What the jammer must do:

- Decode 802.11 frames from clients
- When client scans for networks, jam probes *before they reach other devices*



t_d = detection

T_T = Turnaround

How fast?

- WPA-Enterprise Probe Requests typically $\sim$ 1Kbit long
- Clients probe at lowest rate for discovery: 1Mbps
- Up to 1ms trasmission time

Jamming benefits (cont.)

Power benefits:

- A naïve Rogue AP must outpower legitimate ones
- We only need to or mangle packets or trigger the NIC's Energy Detector (-80 to -70 dBm from standard doc vs outpowering -30 dBm from afar)
- High gain antennae can increase range even more

Stealth benfits:

- A 802.11-aware jammer can act on specific frame fields
- Can target individual MAC addresses, invisible to others
- Source MAC address at byte 10 means 80μs delay to jam at 1Mbps

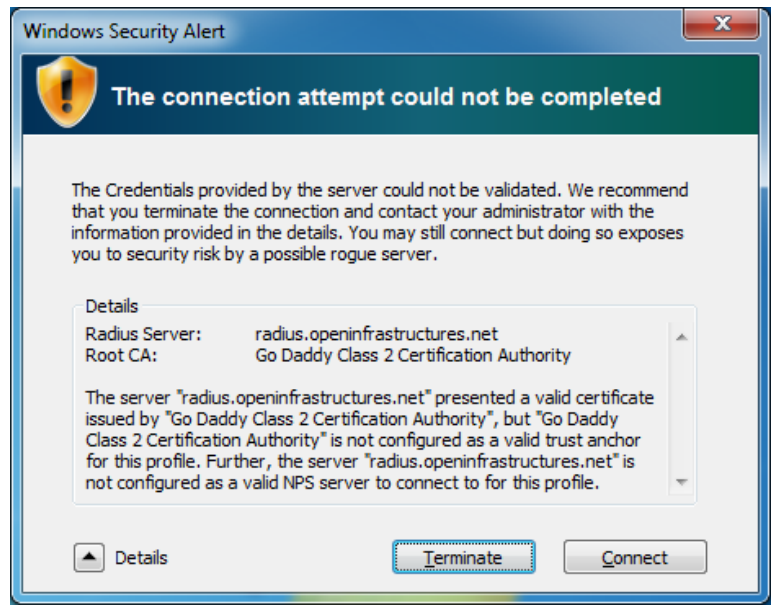
Jamming (cont.)

Jammer pseudocode:

```
function jammer(VMAC, SSID):
  //precompute response train
  packet = build_frame(PROBE_RESP, SSID, VMAC, local_MAC)
  response_sig = 80211_modulate([packet, packet, ...])

  loop:
   if frame_match(VMAC) == MATCH:
     switchTx(on)
     Tx(response_sig)
     switchTx(off)

function frame_match(MAC):
  loop: //move to src address field in responses
   if frame_type(80211_demodulate(radio_in)) == PROBE_RESP:
    plcp_toByte(SRC_ADDR)
    break

  for i = 1...addrlen: //record address
    addr[i] = plcp_nextByte()

  if addr == MAC:
    return MATCH
  else:
    return NO_MATCH
```

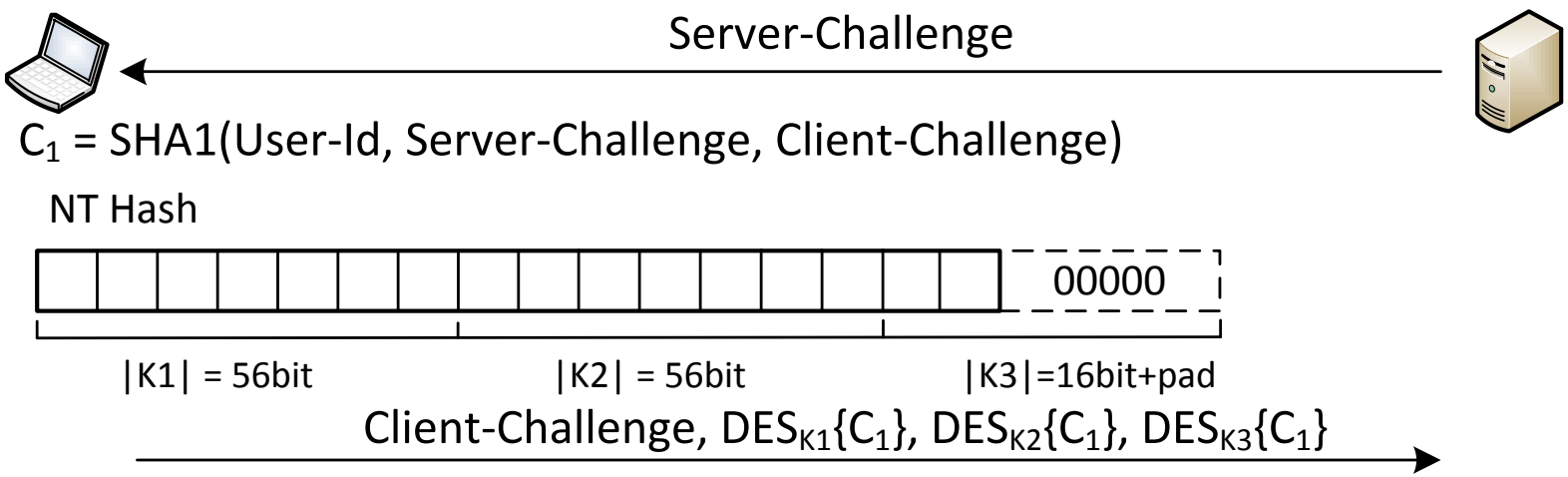
Setup requires human intervention to accept certificate:

1. Build an inconspicuous self-signed cert., emulating behavior of vendors
2. Show legitimate RADIUS cert. $n-1$ times, then our own
   - First attempts will be inspected and accepted, but TLS fails
   - With n such that a user will accept last certificate at a sufficiently high probability

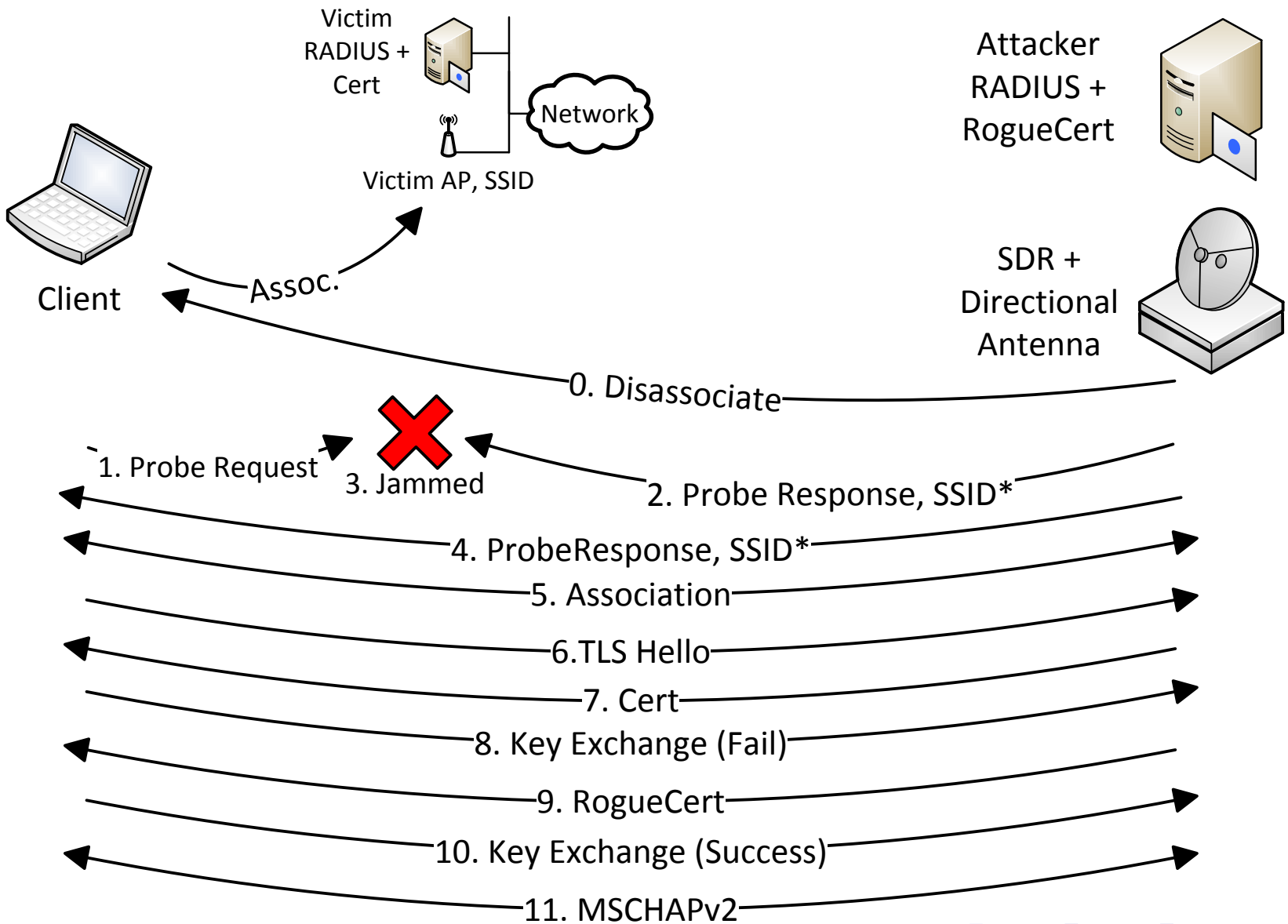


WPA-Enterprise networks use MSCHAPv2 for user authentication

- Widely deployed
- Integrates well with existing infrastructure
- Believed to be sufficiently safe when performed over a secure channel (TLS)



Putting it together



Implementation

Northeastern University

Software-defined Radio:

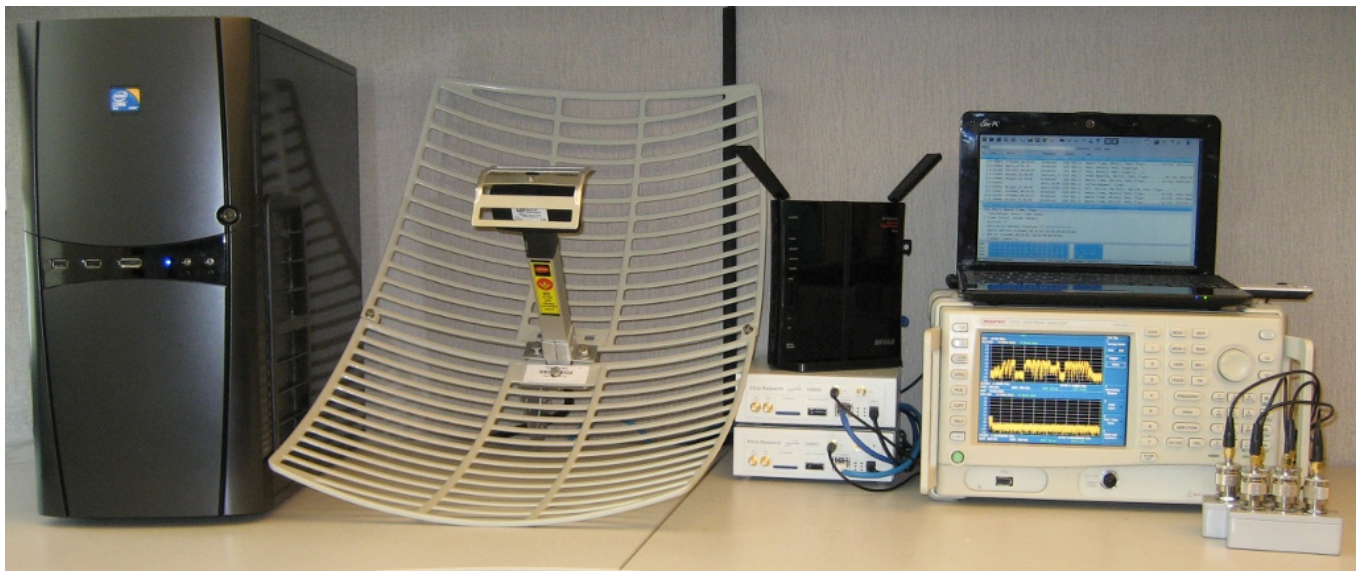
- Software implementation of radio signal processing
- Includes software API and libraries to develop own processing blocks
- Third party code
- Relatively inexpensive hardware (e.g. Ettus' USRP family) available
- GNURadio SDR uses python, C++ for development: speed, ease
- Easier than building chips, RF and firmware

Disadvantages:

- Passing signals to host CPU for processing introduces delay
- 802.11 22MHz channel requires higher sampling rate of USRP2 ($1,500) and later

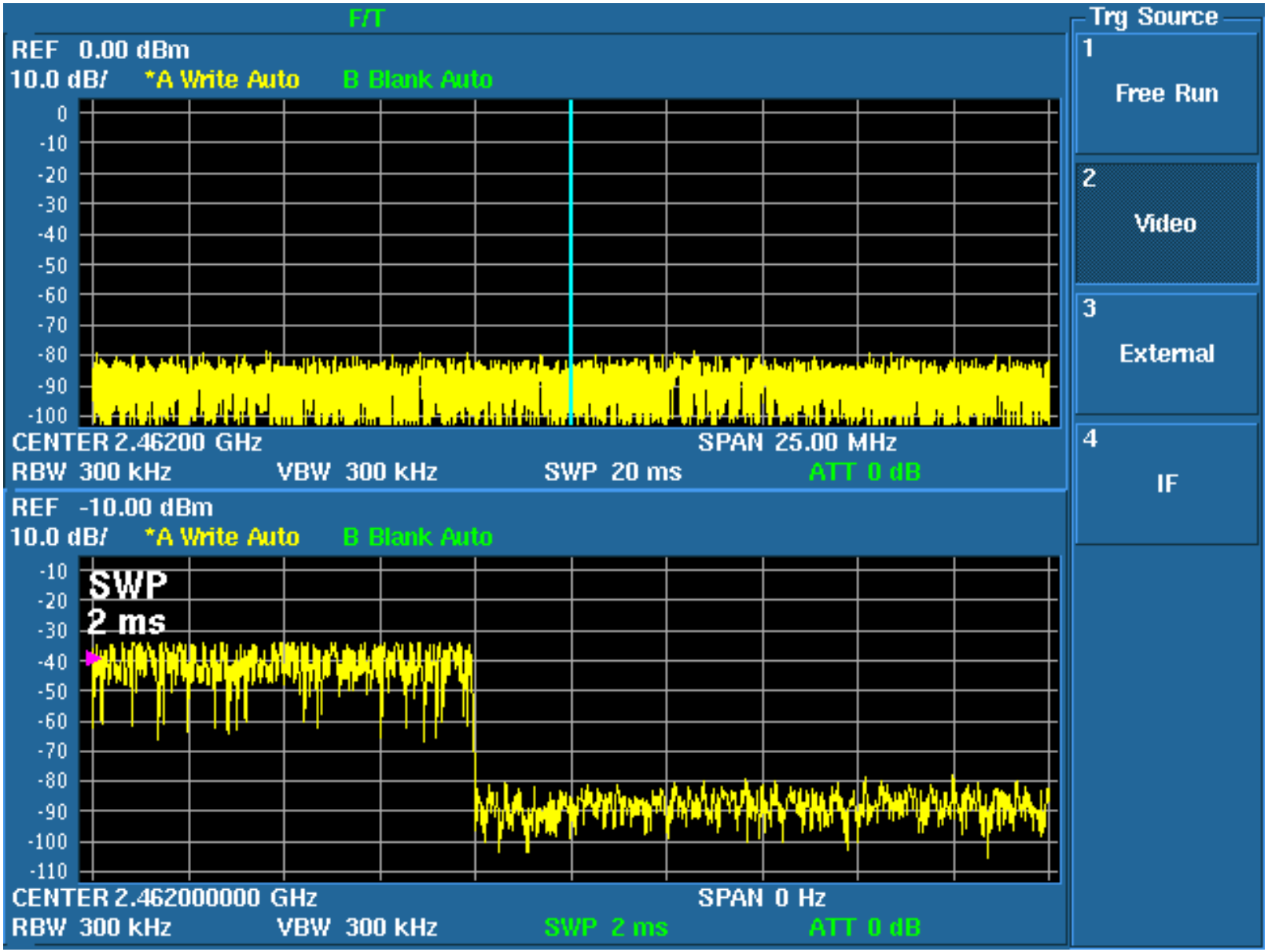
Prototype

Component	Cost (USD)
1 Desktop Core 2 Quad 4GB RAM	580.00
2 USRP2 boards	3,000.00
2 RFX2400 boards	550.00
1 802.11b/g/n router	66.00
1 Parabolic grid ant.	47.99
1 Standard TLS certificate+domain	178.47
Total	**$4,422.46**



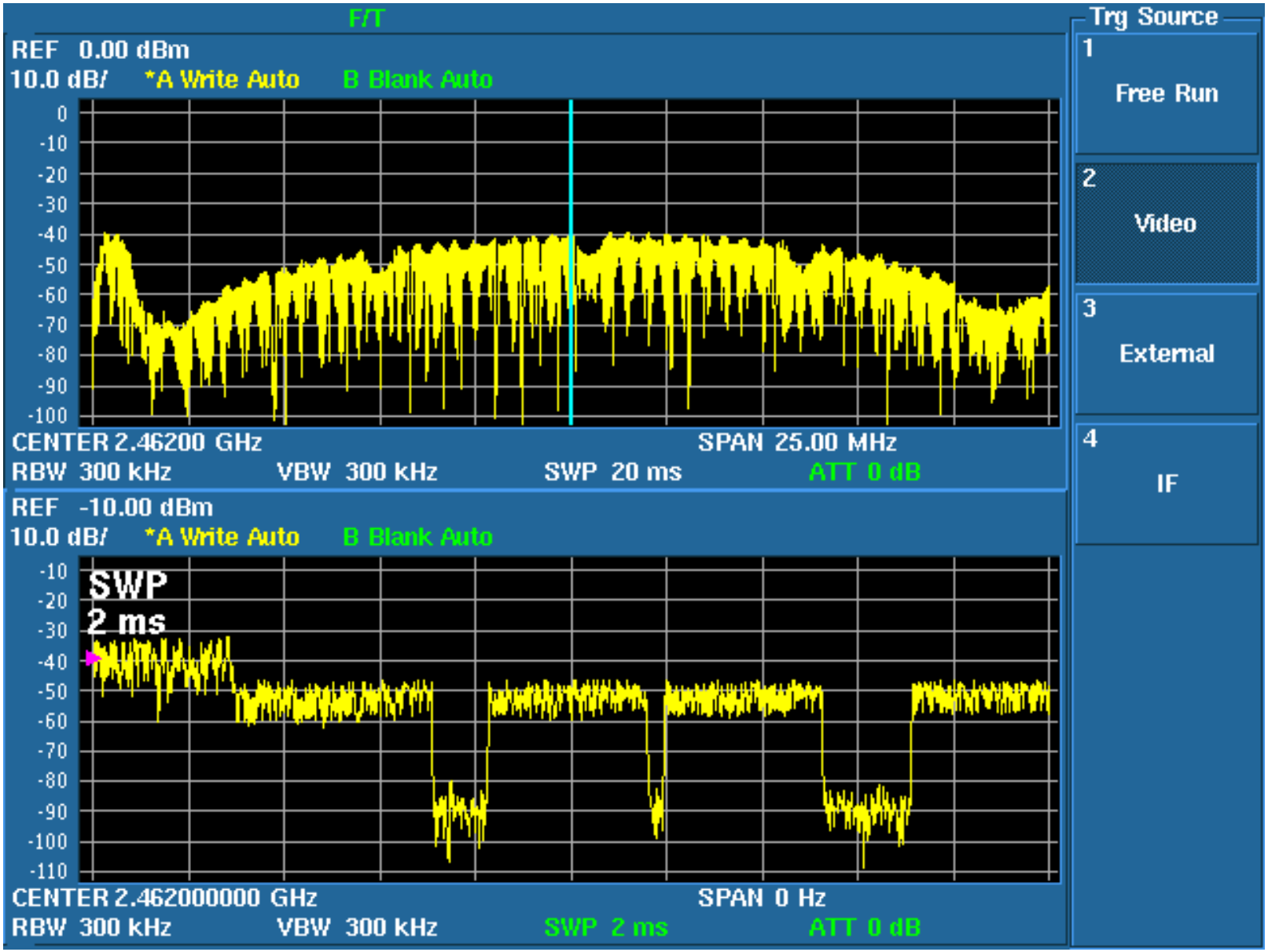
Testing reaction time

Northeastern University



Testing reaction time

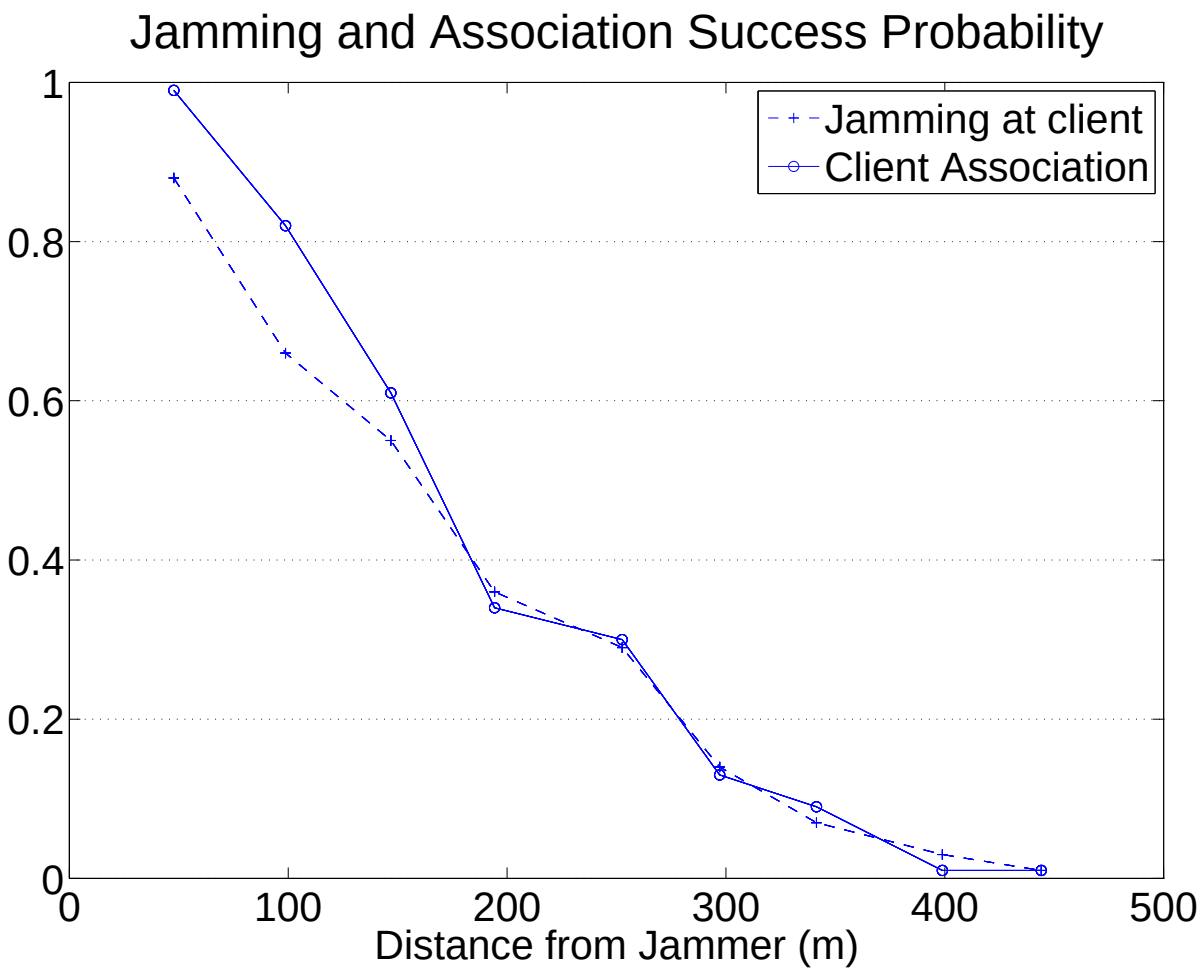
Northeastern University



Range test

Ran 1,000 client trials per site, at 50m intervals, 19dBi gain antenna.

- Jam success: Only Rogue SSID appears at client

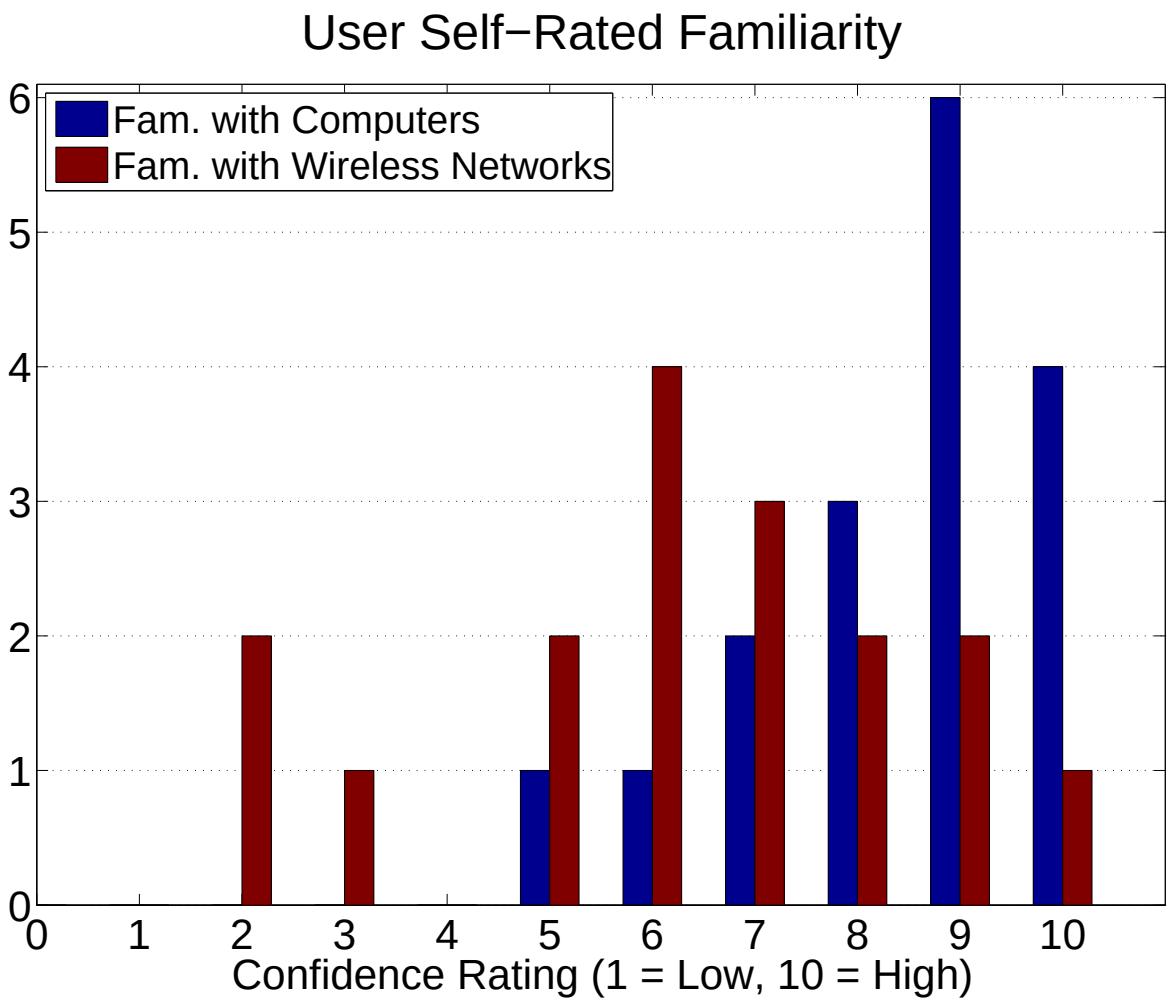


User Study

- Experiment room setup with prototype
- 17 users gave consent to be part of study
  - At least 5 participants had academic networking security background
  - All participants shared CS, Engineering background
- Task: connect to WiFi and browse (i.e. web search, captchas, following links)
- Users self-rated familiarity with computers and WiFi networks
- Debriefing after test
- Capture data anonymized and encrypted with AES-256

User Study Results

All users accepted Rogue Certificate, only one reported seeing a duplicated SSID.



User passwords

- Dictionary search 8-character alphanumeric yielded **two user passwords in three hours**
- NTHASH in MSCHAPv2 can be broken with 1 DES key search
- Cloud computing services (EC2) provide GPUs and OpenCL access for $2.10 per hour
- Est. 10-day DES search with 1 EC2 large instance would cost little over $1,000

Conclusions

Northeastern University

Lessons:

- Isolated defense efforts provide some measure of protection
- Flaws don't stay isolated
- Even if UI design is not usually addressed as part of security, it has an effect
- A solid foundation to build protocols

Countermeasures:

- Trust relationship between SSID and RADIUS certificate crucial
- UI considerations: non-printable characters
- Move away from MSCHAPv2, strong-password protocols offer better guarantees
- Adopt secure-pairing techniques to limit vector of attack

Thank you