CS 525M – Mobile and Ubiquitous Computing Seminar

Mark Figura

About the Paper

"802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions"

Authors: John Bellardo and Stefan Savage

University of California at San Diego

Presented at USENIX Security Symposium, August 2003

Outline

- Purpose
- DoS attacks
- Introduction
- Forged management frame attacks
  - Overview
  - Attack
  - Defense
- MAC attacks
  - Overview
  - Attack
  - Defense
- Conclusions

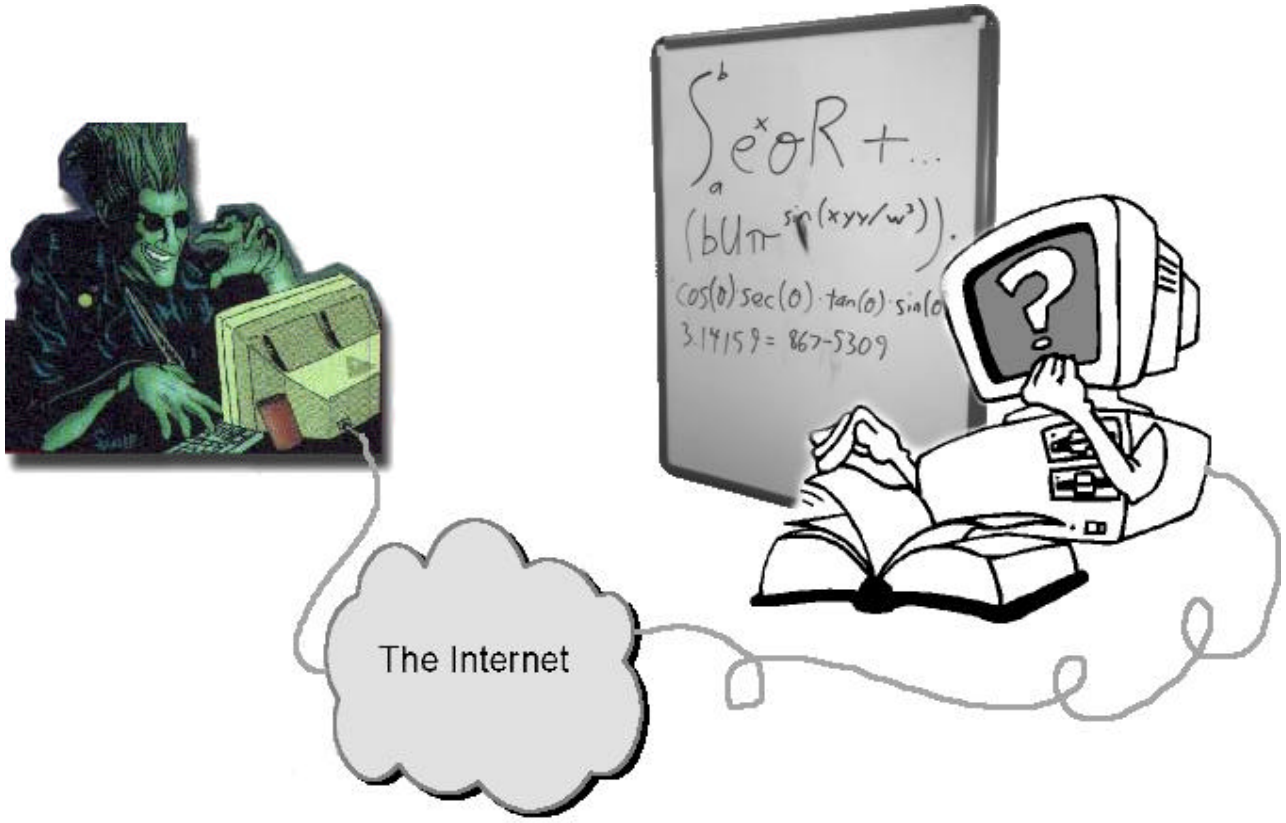
Purpose

- 802.11 networks are everywhere
- Everyone knows that data sent over 802.11 is far from secure, but there are other types of attacks
- What about Denial of Service (DoS) attacks?
  - Different protocols in use than in wired networks
  - Different DoS attacks

DoS attacks

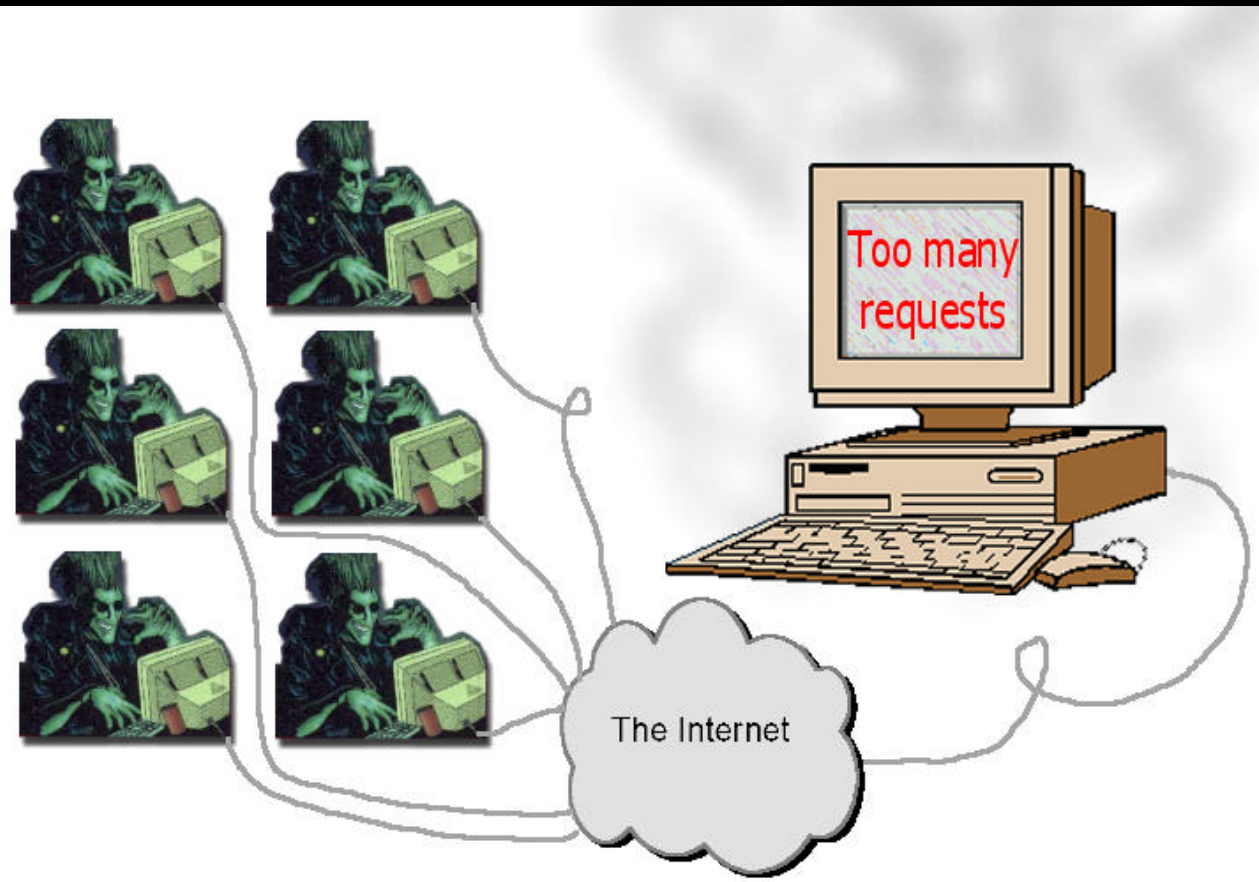
- Deny usage of a service
  - Website
  - Normal usage of a desktop computer
  - Wireless access
- 2 types of DoS attacks…

Computationally Expensive



The hacker asks the attacked computer to do processing. For example, “Generate an asymmetric key pair. Then throw them away.” Repeat

Flooding



Very many simple requests sent to the attacked computer. Makes it hard to connect to the computer for legitimate purposes.

Introduction to the paper

- 802.11 is BIG
  - Hackers like to attack big things
- New security extensions
  - WPA, 802.11i, 802.1X
  - Computer security
    1. Confidentiality ✓
    2. Integrity ✓
    3. Availability **NO!!**

Introduction to the paper(2)

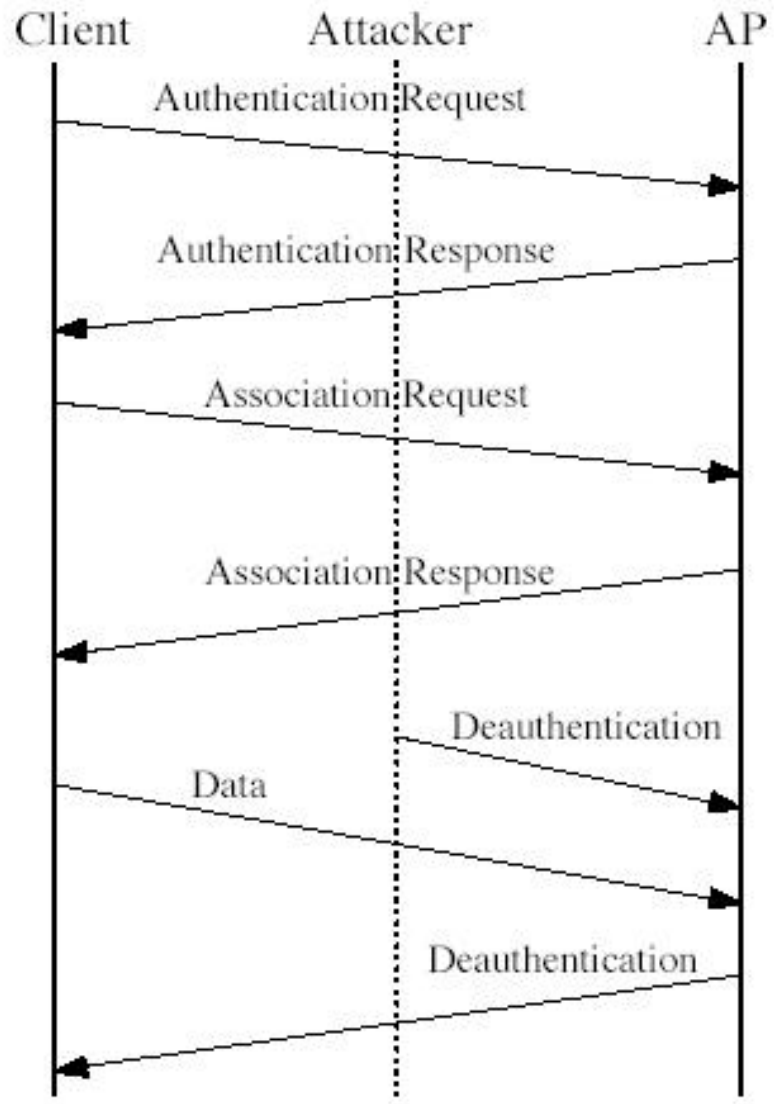
Four contributions from the paper…

1. Describe vulnerabilities
2. Demonstrate that attacks are possible with off-the-shelf hardware
3. Demonstrate attacks in action
4. Countermeasures

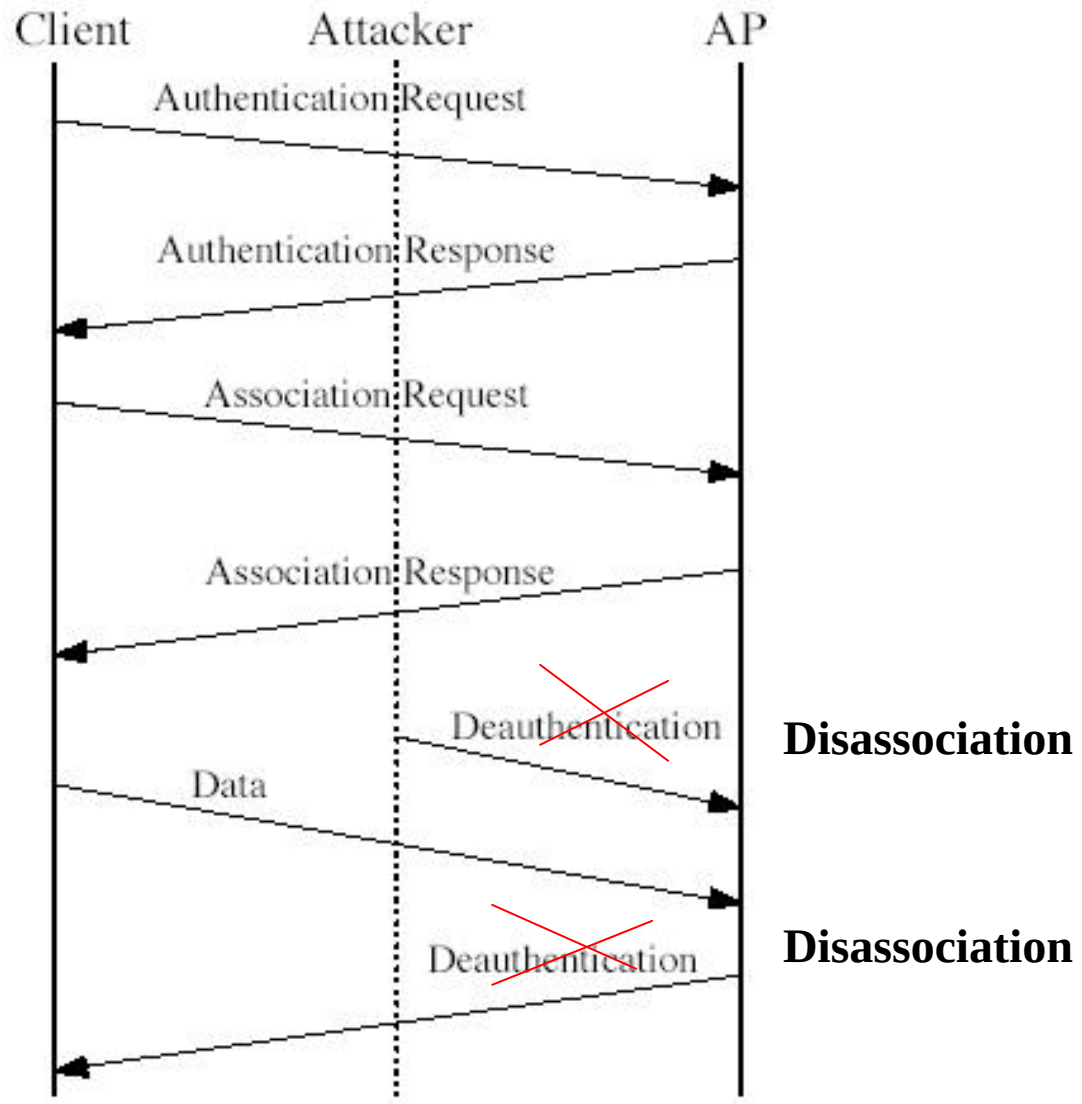
Management Frame Attacks

- 3 types of frames in 802.11
  - Data frames
    - Contain application data
  - Control frames
    - Used for MAC
    - Talk about these later…
  - Management frames
    - Communication with AP(s)
    - 3 attacks coming up…

Deauthentication



Disassociation



Deauthentication vs Disassociation

- Once deauthenticated…
  - Reauthenticate
  - Reassociate

2 ✓

- Once disassociated…
  - Reassociate

1

Power Saving (active client)

- Normally…
  - Ask the AP to buffer inbound packets
  - Go to sleep
  - Wake up, ask AP if anything came in
- Attack
  - Ask the AP to buffer inbound packets
  - Go to sleep
  - Attacker asks AP if anything came in
  - Wake up – no messages

Power Saving (passive client)

- AP periodically broadcasts traffic indication map (TIM)
  - Contains information about buffered packets
  - Attacker can transmit spoofed TIM
  - Client goes back to sleep because the TIM received said there were no packets waiting

Attacking – Can we?

- To conduct these attacks, we need to send management frames
- All we (as users of the wireless NIC) need to do is send data frames
- The wireless NIC should take care of management frames on its own and not allow a programmer to access this functionality
- Unfortunately, most wireless NICs based on the same design
  - Studied by hackers
  - Can send management frames using undocumented “features” when NIC is in HostAP or HostBSS mode

Attacking – Yes, we can

- Good news for hackers!
- Software-only solution
  - No custom hardware necessary
  - Can conduct DDoS attacks

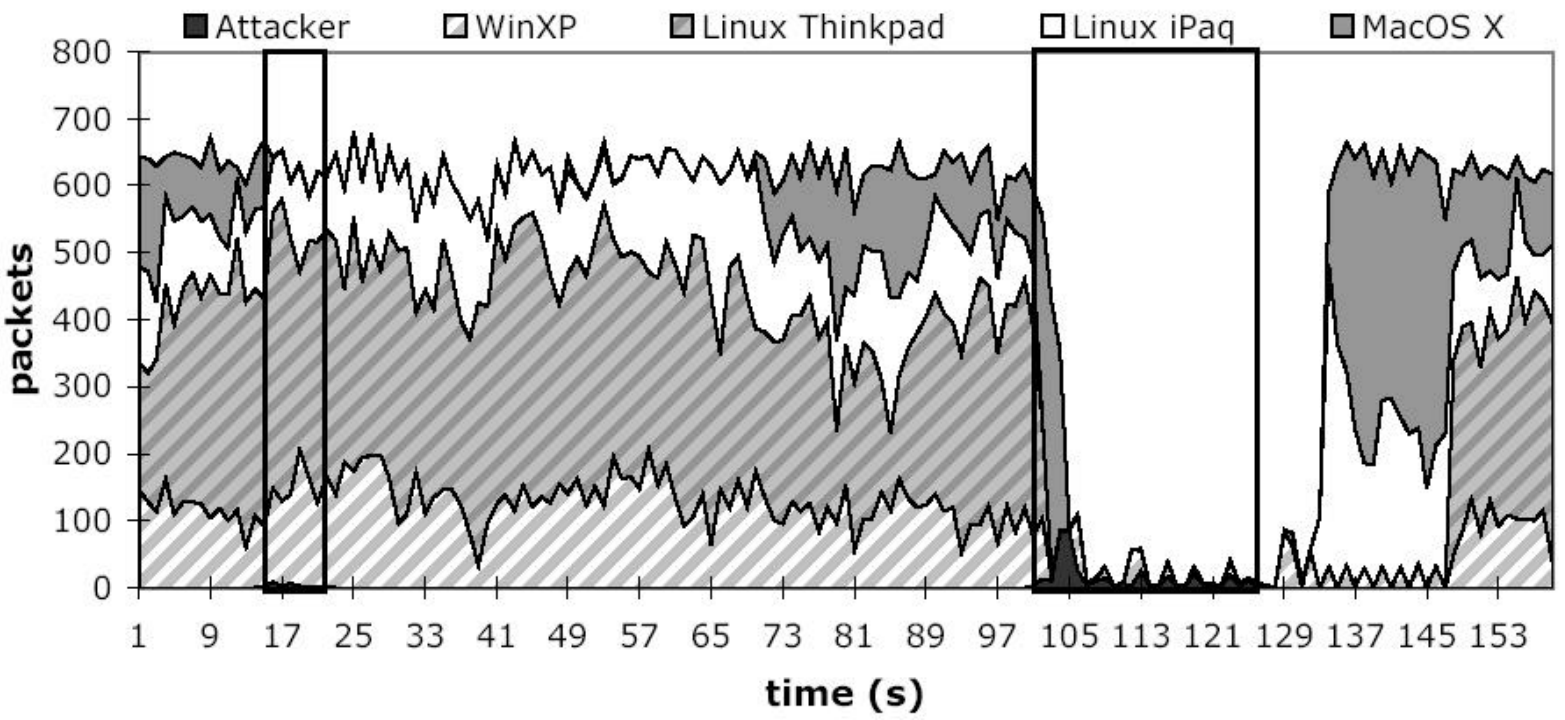
Attacking – Tools

- **Off the shelf iPAQ H3600 running Linux**
- **Dlink DWL-650**
- **Does NOT take much!**
  - **Fits in your pocket**

Deauthentication - Attack

- Custom ‘Swat’ program sniffs network
- If a ‘target’ sends a data or an association response frame, send a spoofed deauthentication frame to the AP ‘from’ the target
- Test conducted with 4 client machines, 1 AP, and 1 attacking machine

Deauthentication - Results



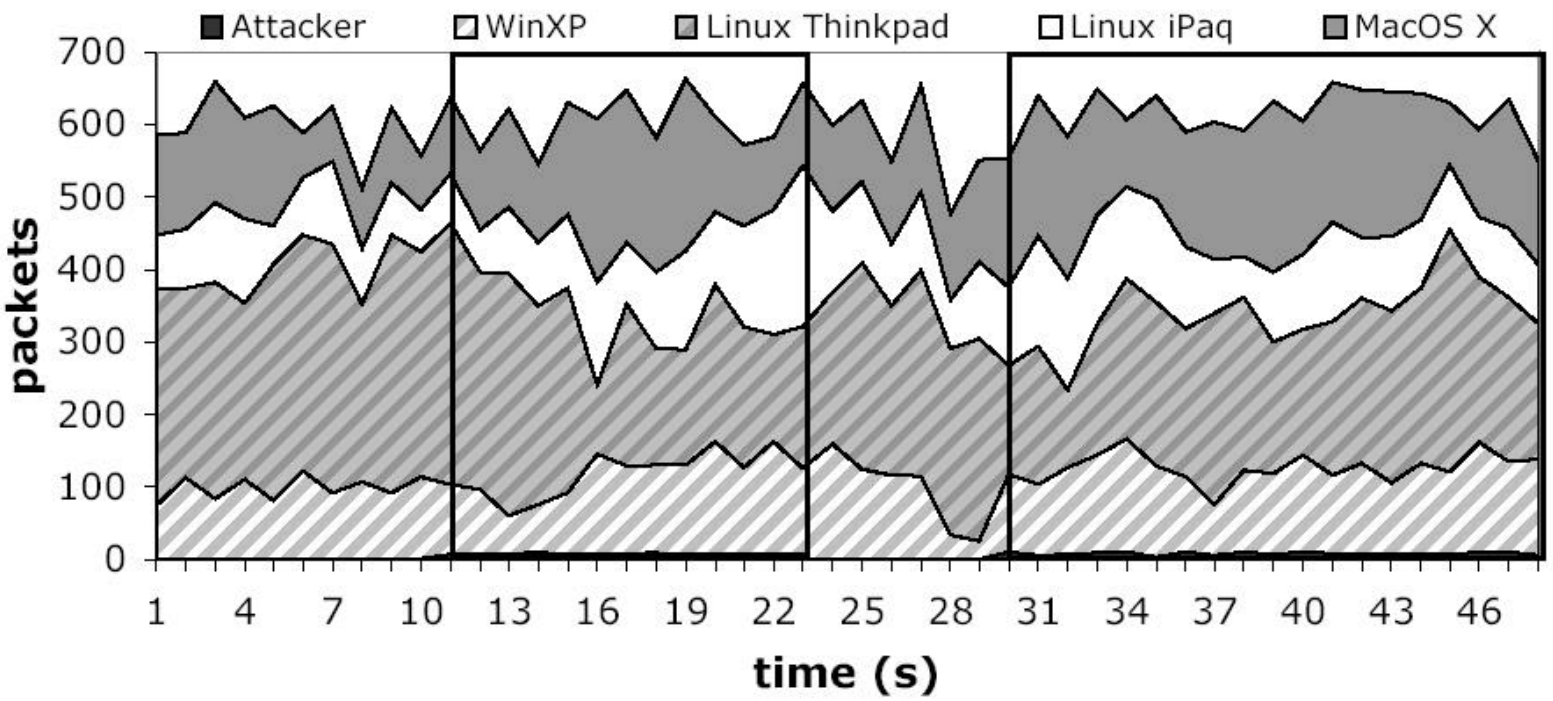
Why does this work so well?

- After reauthentication, TCP's sending rate is in slow-start
- Only a few (if any) packets will get through before the connection is shut down by the attacker
- Notice that a bit of XP's traffic gets through – this is UDP used by various Windows networking services

Deauthentication - Defense

- Buffer deauthentication requests at the AP for 5-10 seconds
- If more data packets come in, this is a bogus deauthentication request and can be thrown out
  - If the client actually requested deauthentication, it would close the connection and not send any more data
- Same technique can be applied to the disassociation attack

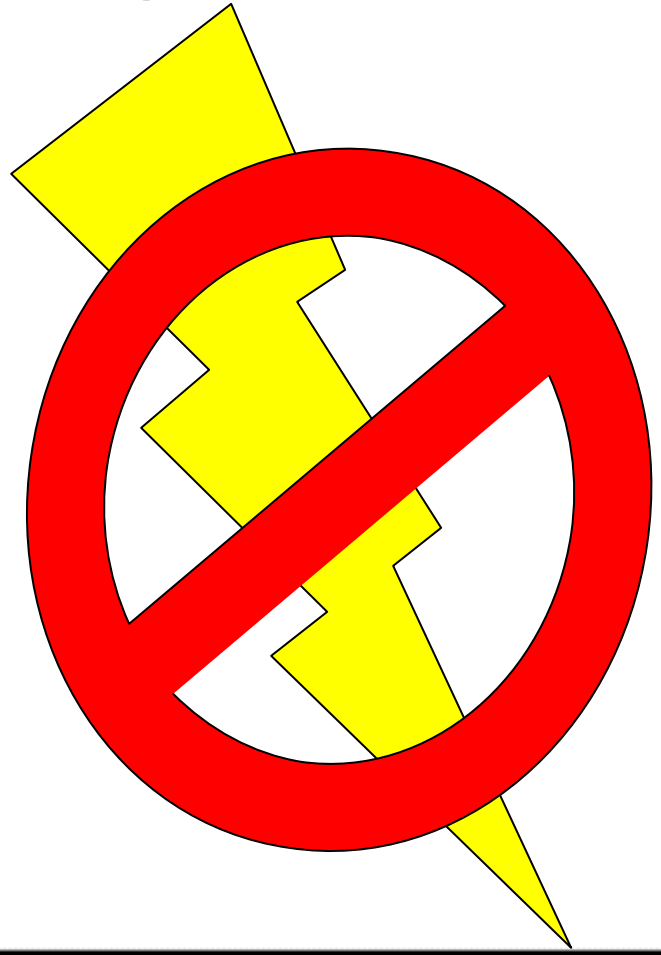
Deauthentication - Defense



- Works very well!
- But what if the client moves and switches APs?
  - Attacker could take over the old connection that remains open for a few seconds.

Powersaving?

- No mention of how to avoid the powersaving attacks discussed before…



Control Frame Attacks

- Control frames used for MAC
- Preventing collisions in transmission range…
  - Before a frame can be sent, the sender must wait…
    - Distributed Coordination Function Interframe Space (DIFS) if starting a new ‘frame exchange’
    - Short Interframe Space (SIFS) if sending another frame as part of a frame exchange

Control Frame Attacks

- Preventing collisions from interference with nodes just outside of transmission range…
  - ‘duration’ field in each frame
    - Reserves channel for x microseconds
  - Can be used to help avoid interference with hidden terminals

SIFS Attack

- Send a frame just before the SIFS period times-out
  - No one else can send their frames
  - A SIFS period is 20microseconds, so the attacker would have to send 50,000 packets/second
    - Batteries will drain quickly
  - Not necessary to completely disable network – just making it slow is also ‘good’

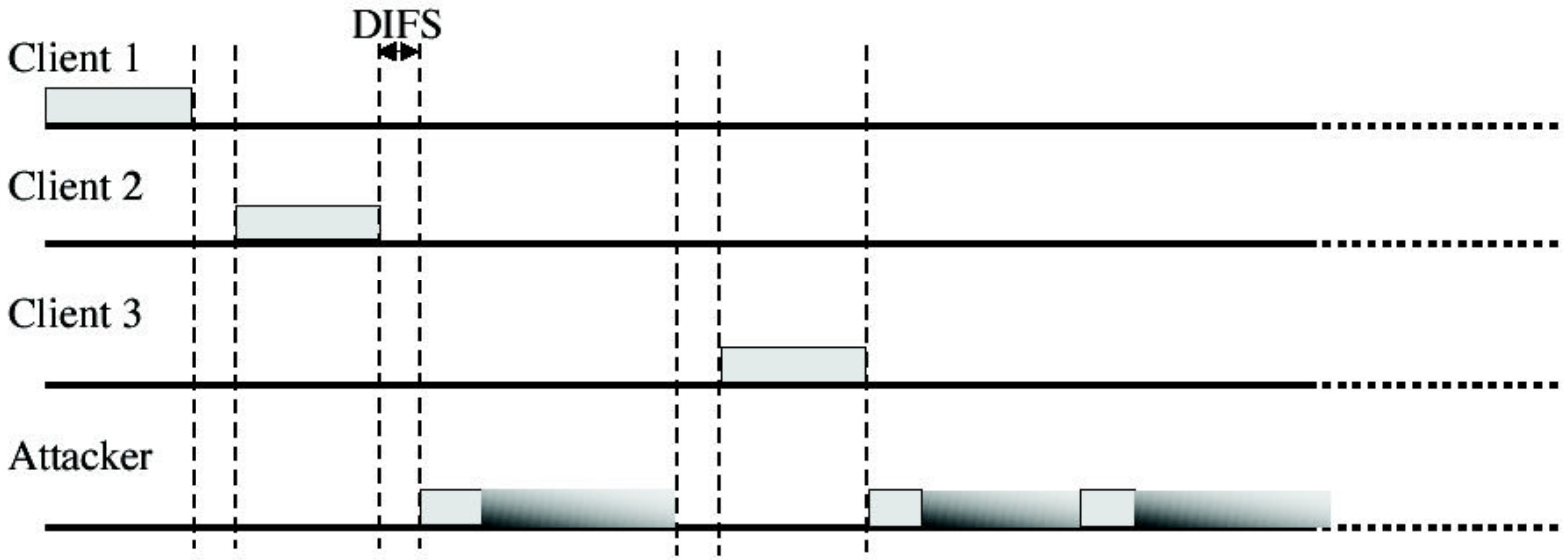
SIFS?

- Paper makes no mention of a defense for this attack
- Sort of impractical without AC power
- Sort of silly when there are better control-frame attacks like the NAV attack…

NAV Attack

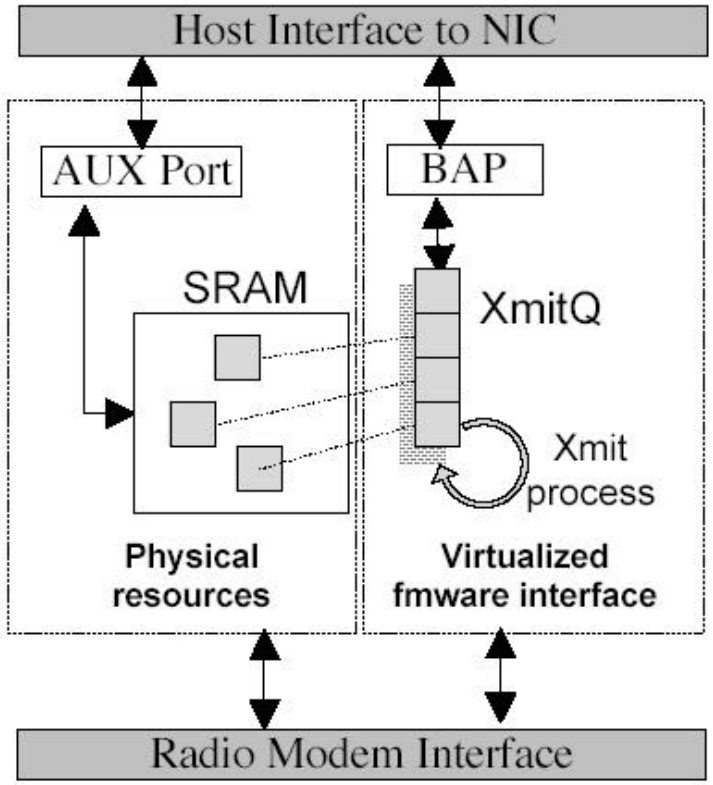
- When a frame is received, its ‘duration’ is noted in each client’s network allocation vector (NAV)
- Until a client’s NAV expires, it will not transmit
- The attacker can continually reserve the channel for lengthy durations
- Maximum NAV length is about 32ms
  - Attacker must transmit about 30 frames/second
  - Much less than 50,000!

NAV Attack



Attacking

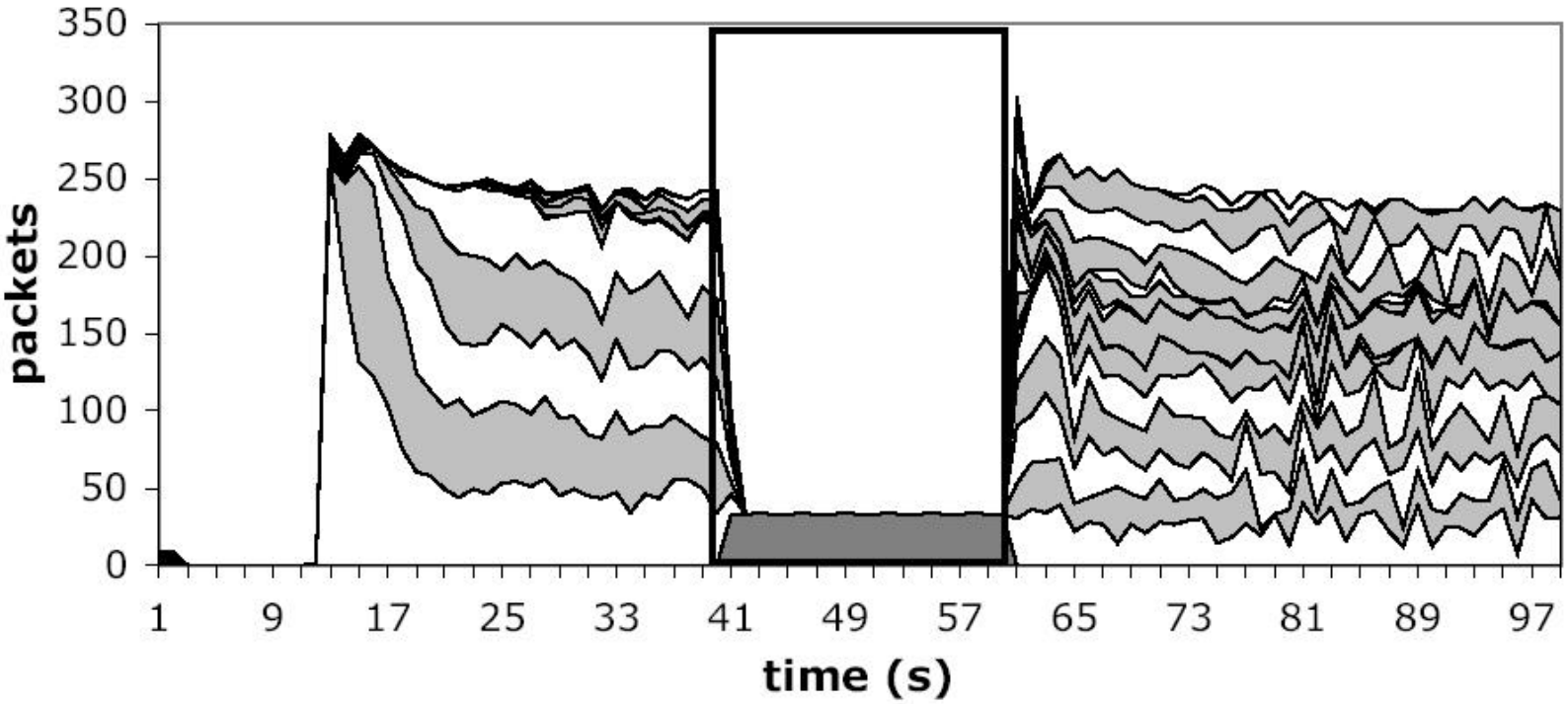
- Can we send control frames in off-the-shelf hardware?
- Using more undocumented “features,” – yes!



NAV - Attack

- Attack conducted using high duration values in ACK frames
- 18 clients, 1 AP, 1 attacker
- Simulated with NS
  - All 802.11 products tested did not wait for the duration to expire
  - Against the specification, so assume it's a bug and will be fixed

NAV - Results

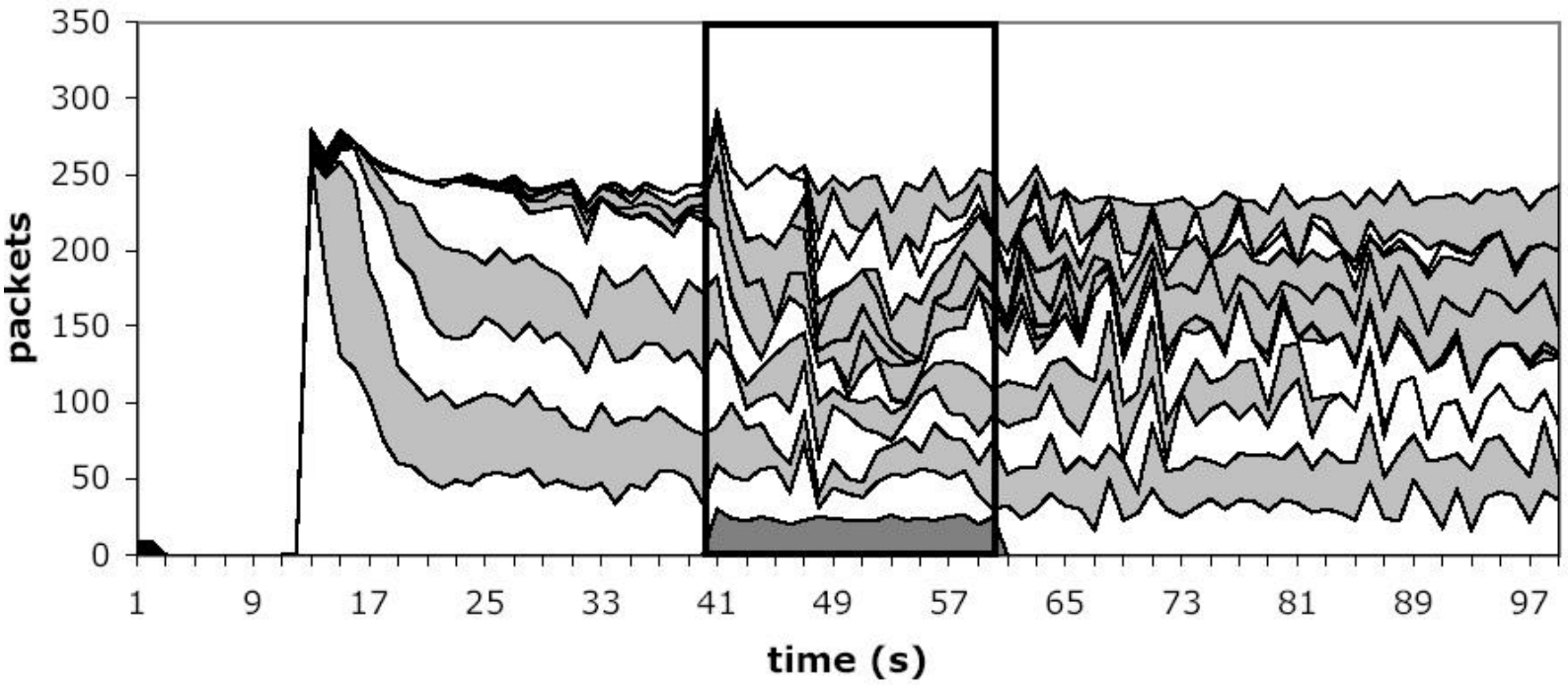


Uh-oh – the attacker has totally taken over the channel!

NAV – Defense – Cap

- Limit maximum duration
  - ‘Low cap’ – short
    - Used when only an ACK or CTS are valid
  - ‘High cap’ – longer
    - Used when data is expected
    - Data length is not known in advance, so the maximum is the time to transmit the maximum-length data packet

NAV – Defense – Cap



- Works to a point, but if attacker sends fast enough, the network can still be shutdown

NAV – Defense - Intelligence

- There are certain restrictions on most types of frames…
- ACK frames should only be long if packets are fragmented. Usually fragmentation is not used, so ACKs should never be long.
- Data frames should not be longer than it takes to transmit a full-length frame unless fragmentation is used.
- RTS should be followed closely by CTS and data. If not, don’t continue to wait.
- CTS frames should be thrown away if not received directly after an RTS.

Conclusions

- These techniques can be used as a stop-gap solution
- We really need authentication of 802.11 management and control frames
  - This would solve all of the problems described in the paper

What's the Point?

- If authentication of management and control frames would fix this, why did the authors of this paper do all this work?
- Implementing authentication in 802.11 is similar to switching the Internet over to IPv6.
  - Solves a lot of problems
  - Everyone has to buy new stuff
    - Many wireless products cannot be software-upgraded because of the increased processing required
    - No one wants to replace all of their existing wireless equipment - $$$$

Questions?