# CS530
# Wireless Technologies & Implications

Bill Cheng

*http://merlot.usc.edu/cs530-s10*



Copyright © William C. Cheng

# What's Different About Wireless

- Easy (but wrong) answer:
  - wireless communication involves transmission of data by radio or similar means, and this allows an attacker to read the data more readily without requiring physical access to the network
- The problem with this explanation:
  - if you have been paying attention during this course, you will likely note that we have been assuming it is easy for an attacker to intercept data anyway, even on wired networks
  - good security design should assume this
  - yes, it is a little easier for an attacker to eavesdrop with wireless, but there are so many other ways to get the data that wireless doesn't really change this part



Copyright © William C. Cheng

# What's Different About Wireless (Cont...)

- The real answer:
  - wireless communications devices are often disconnected
    - sometimes it is harder to solve security problems if you do not have access to the network (e.g., to reach KDC, DS)
  - such devices may have limited storage or limited computation abilities
  - such systems may be more vulnerable to jamming
    - but on the other hand, it's harder to "cut the line"
  - such systems create a less accountable path into the network
    - can trace back TCP connections
    - but it can be hard to determine last hop for wireless (MAC address can be spoofed in 802.11)



Copyright © William C. Cheng

# A False Sense of Security

- Need to be careful about marketing
- Solutions that provide encryption at the network layer or below provide a false sense of security
  - WEP: Wired Equivalent Privacy is just that
    - link layer, per packet encryption
    - doesn't solve the end to end problems
      - should always use things such as SSH and VPN on top of WEP
    - wires aren't that hard to tap anyway
  - attacks on WEP
    - repeated IV on encryption enables recovery of the key stream
      - 24-bit IV - small space, IV reused in short period
    - authentication reveals secret



Copyright © William C. Cheng

# RC4

```
/* state information */
static uns8 static[256], x, y;

void rc4init(uns8 *key,
        uns16 length)
    /* initialization */
{
    int i;
    uns8 t, j, k=0;

    for (i=256; i--; ) state[i] = i;

    for (i=0, j=0;
            i < 256;
            i++, j=(j+1)%length) {
        t = state[i];
        state[i] =
            state[k+= key[j] + t];
        state[k] = t;
    }
    x = y = 0;
}
```

```
uns8 rc4step()
    /*
     * return next
     * pseudo-random
     * octet
     */
{
    uns8 t;

    t = state[y += state[++x]];
    state[y] = state[x];
    state[x] = t;

    return state[
        state[x]+state[y]
    ];
}
```



Copyright © William C. Cheng

# A False Claim of Security

- Beware of papers like the Bluetooth paper in the assigned readings
  - written by one of the Bluetooth architect
  - these kinds of papers appear all the time, pointing to vulnerabilities in competing products or protocols and showing how their solution does not exhibit these weakness
  - keep in mind that weakness and vulnerabilities are usually approach specific
    - an alternative doesn't exhibit the *same* vulnerabilities is not at all surprising



Copyright © William C. Cheng

# Bluetooth Vulnerabilities

- Bluetooth was designed such that even when a connection is refused, data can be received
  - e.g., when you stand close enough to a store, your device may get an instant message from the store
    - would you like to get a $20 coupon from this store that you are standing next to?
  - bluetooth philosophy is that physical proximity can provide protection - not a good assumption



Copyright © William C. Cheng

# Bluetooth Vulnerabilities (Cont...)

- Bluetooth exhibits serious vulnerabilities in its interface to the user
  - similar to SSL URL authentication problems
    - i.e. that you know the name of the server you were talking to, but not that it was the right server
  - SNARF Attack
    - connect to device without alerting owner
      - attacker can than steal data
  - Backdoor Attack
    - establish trust by pairing, but remove from list of pair devices
  - problem is too few protection domains
    - connection grants access to most data on the device



Copyright © William C. Cheng

# Wireless to Improve Security

- Wireless promotes less constrained reconfiguration
  - topology of network is not constrained by physical wires
  - examples in sensor nets
    - home burglary example - you can cut phone line, but the security system can use a cell phone
- Spread spectrum can be used as a security tool
  - if codes secret, useful to hide communication
  - resistant to jamming



Copyright © William C. Cheng

# Peer to Peer and Ad Hoc Security

- Security protocols may have phases independent of central infrastructure
- Services may be provided by untrusted nodes
- Messages need to be relayed by untrusted nodes
- Devices may be overrun (taken over by enemies)
  - importance of not sharing keys among devices
- Collusion is possible (Byzantine failure)



Copyright © William C. Cheng