Isaac Musick
December 6, 2015
Software Defined Radio Presentation Notes

Software Defined Radios (SDRs):

- rtl-sdr
  - sub $10
  - Can only listen
  - Frequencies: 25 MHz to 1700 MHz
- Yard Stick One
  - ~$100
  - Can listen or broadcast
  - Frequencies: 281-361 MHz, 378-481 MHz, 749-962 MHz
- HackRF One
  - ~$300
  - Can listen or broadcast
  - Frequencies: 1 MHz to 6 GHz
- BladeRF
  - ~$450
  - Can listen and broadcast at the same time
  - Frequencies: 300MHz to 3.8GHz

Types of attacks with SRDs:

- Passive
  - Can be done by any of the above radios
  - Listen to what is going over the air
  - Use that information maliciously
  - Undetectable
    - Not broadcast anything, so no one can find out
- Active
  - Listen and broadcast information
  - Send malicious information to others
    - Can be done by any radio above except the rtl-sdr
  - Modify or MITM communications
    - Can only be done by the BladeRF
  - Can be found more easily because a signal is being broadcast

Pagers:

- Still used by EMS, Hospitals, Doctors, and emergency response teams
- Completely unencrypted
- Frequencies around 930 MHz
- One way (in general)
  - This means that in order for a message to be sent to a pager, the message must be broadcast to every pager tower in the coverage area.
  - For nation wide coverage, all pager messages are broadcast to the entire nation

How to attack pagers:

1. Find a signal (should be 5 or 9 kHz wide with two peaks)
2. Record some data
3. Feed the data into a pager decoder

Possible passive attacks (works against the entire pager coverage area)

- Targeted attacks
  - Messages have a number to identify the intended recipient
  - By filtering all captured messages for only those containing that number, it is possible to see all messages to a single person
- Blackmail
  - Doctors will send diagnosis with names over the pager system occasionally
  - Other private information is sent by people who think pagers are protected
- Theft
  - Doctors will order drugs to be sent to addresses specified in pages
    - this is somewhat rare
  - People are referred to by name, so it is possible to see who is at work and/or at home
  - Locations of emergencies are broadcast over the pager network
- Setting up for social engineering
  - There is a lot of information that is broadcast that could an attacker construct social engineering attacks
    - Names
    - Addresses
    - Phone numbers
    - Diagnosis
    - Bed numbers in hospitals
    - etc

Possible active attacks (works against everyone in range of your radio)

1. Impersonation
   a) Since there is no sender identification, impersonating a sender is easy
2. Denial of Service
   a) Send out massive numbers of pages to every possible pager number
   b) Make all pagers in range of the SDR useless

GSM:

- Global System for Mobile Communications
  - Used by most of the world for text messages and calls
  - Being phased out of the US in favor of 3G standards
- Encrypted with A5/1
- Frequencies: ~850 MHz, ~1900 MHz
  - in the US, other countries use other frequencies in similar ranges
- Two way
  - The cell tower must maintain connections with ever phone in range

A5/1

- Used to encrypt most GSM communications
- Stream Cipher
  - takes a key and some other information
  - puts it into a pseudo-random number generator (PRNG)
  - outputs a one time pad the same length as the message
- Vulnerable to known plaintext attacks
  - GSM uses known padding for short communications
  - The attack only needs a little bit of known plaintext to work
  - Can find the internal state of the PRNG
    - after doing so it is possible to decrypt all further GSM communications
    - can also run the PRNG backwards and obtain the secret key
  - Requires 2 TB of rainbow tables to work

How to attack GSM:

1. Obtain the rainbow tables for A5/1
2. Capture some traffic
3. Identify a target
4. Feed the target's encrypted communications and the rainbow table into a cracking tool
    1. Most tools only work for communications from the cell tower to the phone, but there is no theroretical reason why communications from the phone to the tower could not be attacked

Possible Passive Attacks

- Read a target's incoming text messages
- Listen to a target's conversation

Possible Active Attacks

- Create a “stingray”
  - use an SDR to create a fake cell tower and MITM all calls and text messages
- Denial of Service
  - Broadcast at the same frequency as the tower to drown out the signal in an area