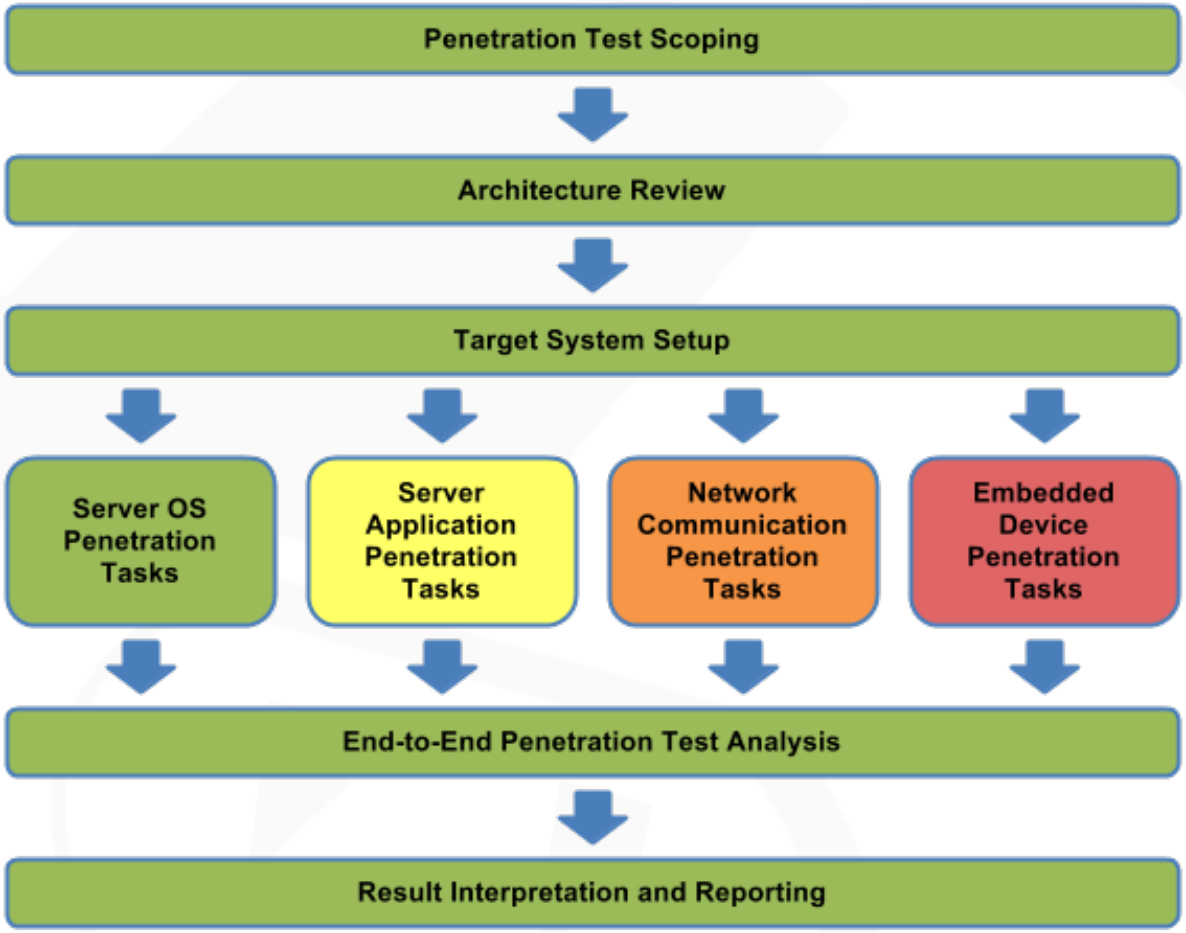
PENTESTING PROPRIETARY RF COMMUNICATIONS

Justin Searle
Managing Partner - UtiliSec

Control Systems and You

- Most companies don't have ICS systems, however they do have related cousins to those control systems
- More important, many of these systems use proprietary RF communications
  - fire alarms
  - proximity cards
  - automotive gates
  - inventory control
  - car alarms
  - conference rooms
  - hospital beds
  - building automation systems
- These systems are all around us, we need only look
- They can also be attacked, so we should assess...

ICS Pentesting Methodology

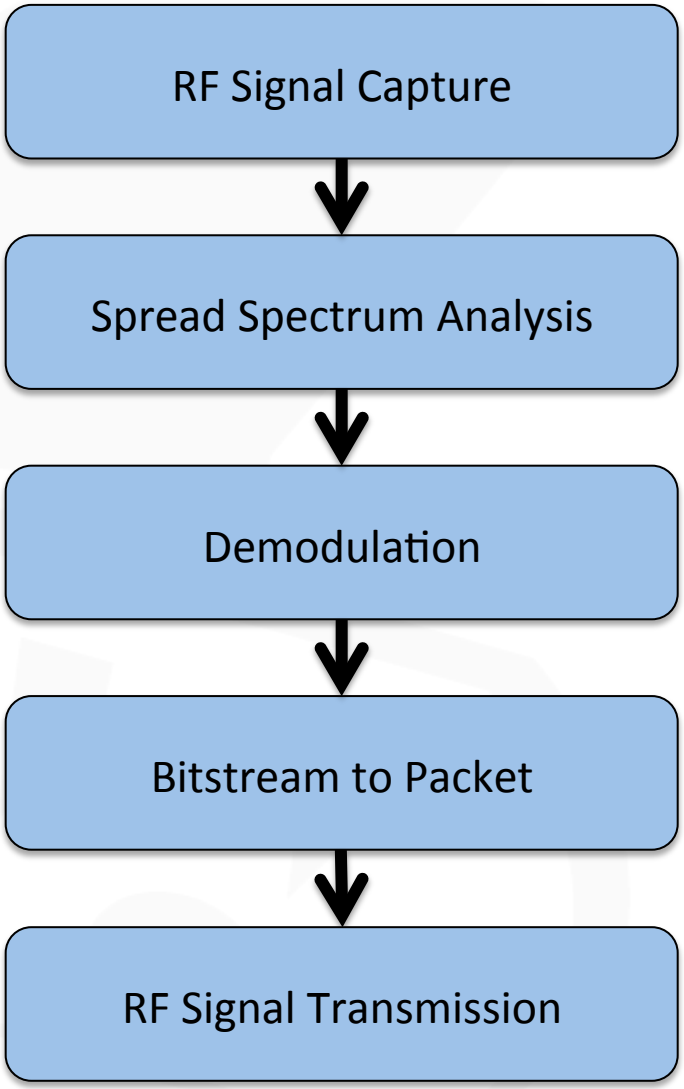


- Green: Tasks most frequently and require the most basic of penetration testing skill
- Yellow: Tasks commonly performed and require moderate penetration testing skill
- Orange: Tasks that are occasionally performed but require higher levels of expertise
- Red: Tasks performed infrequently and require highly specialized skills

SamuraiSTFU Distro

- Leverage last 5 years of experience developing and managing the SamuraiWTF (Web Testing Framework) project
- Live DVD / VM for ICS penetration testing
  - Primary audience is electric asset owner and vendor security teams
  - Secondary audience is security contractors
  - Academia and independent researchers
- Include "cream of the crop" free and open source tools for all aspects of SG Pentesting
  - Best web pentesting tools (small subset of SamuraiWTF)
  - Best network pentesting tools (small subset of Backtrack)
  - Best hardware pentesting tools (not currently included on any distribution)
- Include documentation on tools, architecture, methodology, and protocols
- Include simulated ICS systems for educational purposes
- Include sample packet captures and data dumps for exercises

RF Pentesting Methodology



Task 1: RF Signal Capture

- ***Level of Effort***: Medium to High
- ***Task Description***: Use a tool, such as a software defined radio (SDR) to find and capture the RF communications of the target field device.
- ***Task Goal***: Obtain data for following tasks.

Tools to Capture Signals

Software Defined Radio (SDR)

- Hardware Options
  - TV Tuner: $20 (capture only)
  - HackRF: $300
  - USRP2: $2000
- Pros
  - Flexible because it acquires the signal via hardware and does all processing in software
  - GNURadio and GNURadio Companion are the tools of choice
- Cons
  - Easy to get lost in the complexity
  - Can be very computer resource intensive, sometimes making virtual machines difficult

RFCat + Hardware Radio

- Hardware Options
  - IM-Me dongle: $35
  - CC1111EMK dongle: $49
  - TI EZ430 Chronos CC1111 Access Point: $58
- Pros
  - RFCat configures hardware on the fly so it is fast
  - Simpler to use than GNURadio
  - Frequency hopping recovery
- Cons
  - Must re-flash the hardware before first use
  - Far fewer options for signal processing, but sufficient for most pentest uses

Finding the Right Frequencies

- Initial Architecture Review and Interviews
- Product Documentation
- RF Regulatory Registration Databases
  - FCC ID Search (U.S.)
    http://transition.fcc.gov/oet/ea/fccid/
- Patent Filings
  - Patent Number Search (U.S.)
    http://appft1.uspto.gov/netahtml/PTO/srchnum.html
  - Patent Keyword Search (U.S.)
    http://appft1.uspto.gov/netahtml/PTO/search-bool.html
- Patiently digging through available ISM bands

ITU Defined ISM Bands

Frequency range		Bandwidth	Center Frequency	Notes
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	
433.050 MHz	434.790 MHz	1.84 MHz	433.920 MHz	Region 1: Europe, Africa, Middle East, Russia, Mongolia, but most accepted world wide
868.000 MHz	870.000 MHz	2 MHz	869.000 MHz	Not ISM but SRD band for Europe and India
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2: Americas, Greenland, and Pacific Islands
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	(used by Wi-Fi, Bluetooth, and ZigBee)
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	(used by Wi-Fi)
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

Task 2: Spread Spectrum Analysis

- ***Level of Effort***: Medium to High
- ***Task Description***: Determine if the RF communication uses one of the spread spectrum techniques (FHSS, DSSS, THSS, CSS). Analyze the RF capture to attempt to determine the spread spectrum algorithm used. Alternately, bus sniffing captures near the RF chip may also be used to determine this information.
- ***Task Goal***: Obtain data for following tasks.

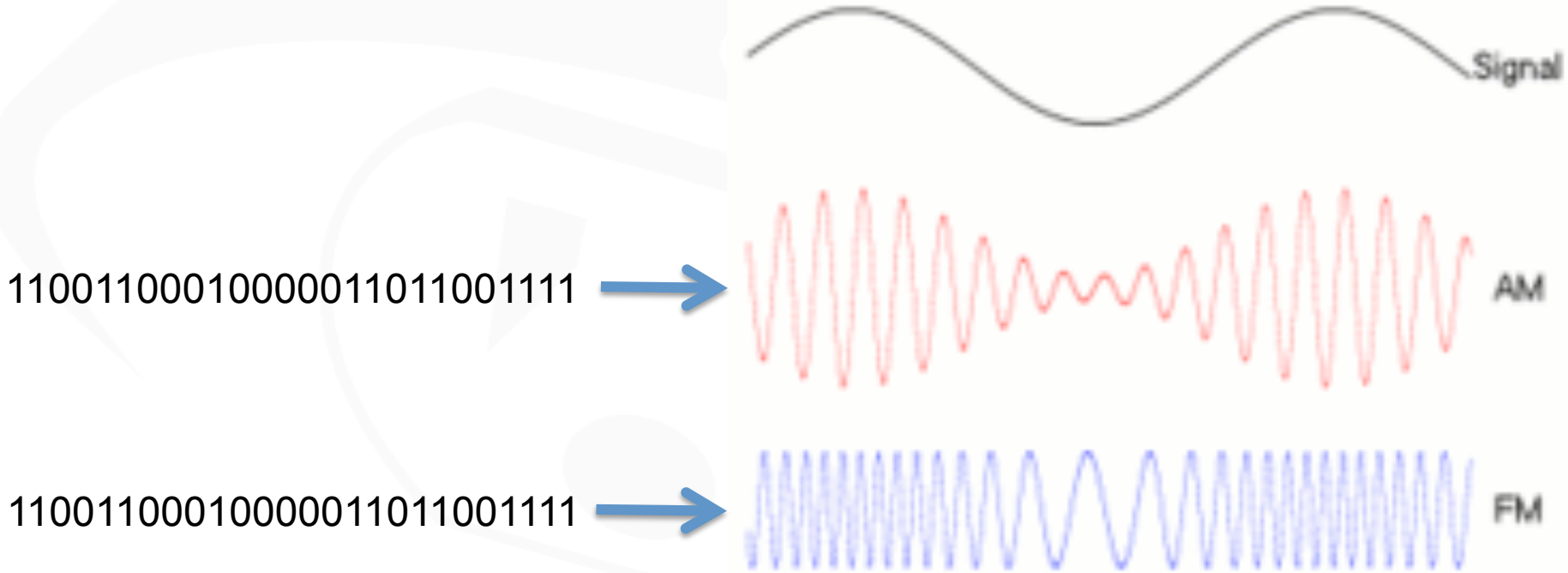
Recovering the SS Algorithm

- Initial Architecture Review and Interviews
- Product Documentation
- RF Regulatory Registration Databases
  - FCC ID Search (U.S.)
    http://transition.fcc.gov/oet/ea/fccid/
- Patent Filings
  - Patent Number Search (U.S.)
    http://appft1.uspto.gov/netahtml/PTO/srchnum.html
  - Patent Keyword Search (U.S.)
    http://appft1.uspto.gov/netahtml/PTO/search-bool.html
- Recovering from the RF chip
- Recovering from the Firmware or Software
- Capturing using Bus Sniffing

http://www.digitalbond.com/blog/2013/02/11/s4x13-video-atlas-on-rf-comms-security-and-insecurity/

Task 3: Demodulation

- ***Level of Effort***: Medium to High
- ***Task Description***: Analyze the RF capture to determine modulation technique used.
- ***Task Goal***: Obtain data for following tasks.



Analog Modulation Types

- Amplitude modulation (AM)
  - Double-sideband modulation (DSB)
    - Double-sideband modulation with carrier (DSB-WC)
    - Double-sideband suppressed-carrier transmission (DSB-SC)
    - Double-sideband reduced carrier transmission (DSB-RC)
  - Single-sideband modulation (SSB, or SSB-AM)
    - SSB with carrier (SSB-WC)
    - SSB suppressed carrier modulation (SSB-SC)
  - Vestigial sideband modulation (VSB, or VSB-AM)
  - Quadrature amplitude modulation (QAM)
- Angle modulation
  - Frequency modulation (FM)
  - Phase modulation (PM)

Digital Modulation Types

- Phase-shift keying (PSK):
  - Binary PSK (BPSK); Quadrature PSK (QPSK); 8PSK; 16PSK; Differential PSK (DPSK); Differential QPSK (DQPSK); Offset QPSK (OQPSK); π/4–QPSK
- Frequency-shift keying (FSK):
  - Audio frequency-shift keying (AFSK); Multi-frequency shift keying (M-ary FSK or MFSK); Dual-tone multi-frequency (DTMF)
- Amplitude-shift keying (ASK)
  - On-off keying (OOK); M-ary vestigial sideband modulation, for example 8VSB
- Quadrature amplitude modulation (QAM) - a combination of PSK and ASK:
  - Polar modulation like QAM a combination of PSK and ASK.
- Continuous phase modulation (CPM) methods:
  - Minimum-shift keying (MSK); Gaussian minimum-shift keying (GMSK); Continuous-phase frequency-shift keying (CPFSK)
- Orthogonal frequency-division multiplexing (OFDM) modulation:
  - discrete multitone (DMT) - including adaptive modulation and bit-loading.
- Wavelet modulation
- Trellis coded modulation (TCM), also known as trellis modulation

Recovering the Modulation

- Initial Architecture Review and Interviews
- Product Documentation
- RF Regulatory Registration Databases
  - FCC ID Search (U.S.)
    http://transition.fcc.gov/oet/ea/fccid/
- Patent Filings
  - Patent Number Search (U.S.)
    http://appft1.uspto.gov/netahtml/PTO/srchnum.html
  - Patent Keyword Search (U.S.)
    http://appft1.uspto.gov/netahtml/PTO/search-bool.html
- Recovering from the RF chip
- Recovering from the Firmware or Source Code

From the Chronos Source Code

- *// Product = CC1101*
- *// Chip version = A (VERSION = 0x04)*
- *// Crystal accuracy = 10 ppm*
- *// X-tal frequency = 26 MHz*
- *// RF output power = 0 dBm*
- *// RX filterbandwidth = 232.142857 kHz*
- *// Deviation = 32 kHz*
- *// Datarate = 76.766968 kBaud*
- *// Modulation = (1) GFSK*
- *// Manchester enable = (0) Manchester disabled*
- *// RF Frequency = 905.998993 MHz*
- *// Channel spacing = 199.951172 kHz*
- *// Channel number = 0*

Task 4: Bitstream to Packet

- ***Level of Effort***: Medium to High
- ***Task Description***: Use a tool to decode and extract communications payload from RF capture.
- ***Task Goal***: Obtain data for following tasks.

Task 5: RF Signal Transmission

- ***Level of Effort***: Medium to High
- ***Task Description***: Use a tool to transmit RF signals at the appropriate frequencies and hopping patterns to either replay captured data, impersonate the target field device, or attempting to cause denial of service scenarios.
- ***Task Goal***: Identify vulnerabilities in the RF signaling.

Contact Information

www.utilisec.com
sales@utilisec.com

Justin Searle
personal: justin@meeas.com
work: justin@utilisec.com
cell: 801-784-2052
twitter: @meeas