Hop Hacking Hedy

atlas, Q, cutaway and SoT

November 16, 2010

Abstract: Frequency Hopping Spread Spectrum makes the interception of transmitted information difficult. So difficult, in fact, that it has been mistaken as an encryption scheme by those who feel that FHSS cannot be easily defeated. Some commercial vendors that utilize FHSS claim it is superior to encryption technologies because "[i]t is common for new encryption schemes to be hacked within months of implementation." [1] They make these claims even after the fact that attacks against Bluetooth and 802.11-based FHSS have already fell victim to public proof-of-concept-based exploitation. Our team will demonstrate the use of low-cost (and in some cases pretty, pink), easily obtained hardware/software to conduct predictive channel hopping analysis coupled with crude spectrum analysis and ultimately identify any given hopping pattern in the 902-928MHz spectrum. Our tools will attempt to identify the hopping pattern of a given FHSS cell within 24-48 hours given sufficient traffic. Upon conclusion this project will demonstrate that 900MHz-based FHSS attacks exist and will eventually affect the confidentiality and integrity of data transferred in the clear across what many organizations consider a "secure-as-is" solution.

Bio: Three guys and a baby. Working hardware to their advantage when others are just trying to make a cheap buck. atlas does the hardware, Q checks that he is correct, SoT keeps us on track, and cutaway helps pull it all together.

Conferences: This talk has not been submitted to any other conference at this time.

Facilities: N/A

Frequency Hopping Spread Spectrum (FHSS) is a Radio Frequency (RF) spectrum sharing scheme intended to allow many unlicensed, unrelated devices to make use of the same radio band. For instance, schemes such as FHSS allow many devices to share the 900MHz spectrum, such as cordless phones and Smart Grid communications. Devices spend a limited amount of time on any given channel before moving to another. In the event interference inhibits communications on any channel, other channels may be used to get around the issue. Historically FHSS has been difficult to track and capture. Devices required to analyze an entire spectrum, such as the 27MHz in the 902-928MHz industrial, scientific, and medical (ISM) band, are very costly. For instance, the USRPv2 with the appropriate daughter board costs approximately $2000, and that's the hacker's toys! Commercial products that make this process simple cost around $10,000. During InGuardians' early Smart Grid research phases, many significant vendors told us "Our FHSS system is too fast to hack." That was it. One vendor, who patented their communications technologies, actually indicated "The present protocol subject matter preferably does not provide any encryption service... without encryption. However, that is not to say that the present protocol subject matter is not a secure protocol. It is in fact a designed protocol, the physical layer for which uses a FHSS technique with a very long frequency-hopping pattern. Eavesdropping on such a system would require a significant engineering effort. This intrinsic security is further enhanced..." [0] Some commercial Smart Grid vendors that utilize FHSS for Neighborhood Area Networks (NAN) claim it is superior to encryption technologies because "[i]t is common for new encryption schemes to be hacked within months of implementation." [1] Even after Bluetooth based FHSS[4] and FHSS 802.11 wireless networks[2] fell victim to attack. It is clear that 900MHz FHSS technologies found in modern Advanced Metering Infrastructure (AMI) devices should not hide behind the pseudo-random patterns of FHSS for security. Considering (AMI) systems are deployed for upwards of 20 years, a day or two of analysis to break a hopping pattern is little time. Most FHSS systems are likely to use each channel 1 to 5 times before repeating. The pattern cannot be inordinately long or devices will take too long to sync up with the rest of the system.

Our team will demonstrate the use of low-cost (and in some cases pretty, pink) hardware/software to conduct predictive channel hopping analysis coupled with crude spectrum analysis and ultimately identify any given hopping pattern in the 902-928MHz spectrum. Tools such as the Texas Instrument CC1111 USB transceiver and the GirlTech IM-ME provide a sufficient 8051 microcontroller and sub-GHz radio (the same radio used in many Smart Meters.) Our tools should identify the hopping pattern of a given FHSS cell (devices which share the same, often MAC address-based hopping pattern) within 24-48 hours given sufficient traffic, as is expected from most Smart Meter networks. To aid in our research, ANSI C12.22 allows completely unencrypted/unauthenticated PING behavior, so we can fully test the entire hopping pattern when attacking Smart Metering networks compliant to this standard.

The tool must identify several key components of the FHSS traffic: modulation scheme, channel duration, sync-bit duration (time identifying 0b10101010), sync-word, (two bytes which identify the start of frame, hopping type and pattern), frame-size (auto or fixed), and whether any whiz-bang special XOR is applied to data before interpretation. For our purposes, we cheat and research what kind of modulation scheme is in use, or manually change the radio to identify frames in use on each of the schemes provided by the ChipCon radio. More analysis can be done to automate this in the future, though it is not our goal of this paper. Channel duration is simply identified by monitoring one channel over a few cycles through the hopping pattern. Sync-word is fairly easily identified by setting down the sync-bit duration and setting the sync-word to 0xAAAA (0b1010101010101010). While this pattern is intended to remove false-positives and identify frames for a given system, setting the sync-word thus matches the sync-bit process to the sync-words and provides raw frames (albeit, potentially bit-shifted). This modification can be manually or automatically applied by identifying other key bytes in the frame. For identifying the hopping pattern, our tools use a fixed length frame in order to get the most access to data going over the airwaves. Analysis of frames can determine if a system is using fixed-framing, or one of the auto-framing options commonly used in FHSS by looking for a frame-size byte in the front of the frame. FHSS has developed four primary methods of "syncing" new radios into a given cell. In one method, called "static acquisition channel", all radios wait on a particular channel to start communication. If this channel is identifiable, the pattern is easily collected as all communication starts at the beginning of the pattern, every time. In another sync method, let's call it "receiver acquisition channel", the receiver waits on a random channel for the transmitter to "catch up," and in a related method "transmitter acquisition channel" the transmitter sends a time-sync frame on the same channel until the receiver catches up. While receiver-acquisition channel has some deterministic behaviors, the transmitter acquisition channel method requires the transmitter wait a long time for others to sync up. This weakness causes "transmitter acquisition channel" to be ill-designed for mesh networks or networks with star-like topology. In our research, we have selected to focus on the "static acquisition channel" sync method because it is most likely the candidate for mesh and star-like networks that interest us. Future research may include automatically identifying other sync mechanisms. As stolen from Wikipedia [7]:

- The initiating party sends a request via a predefined frequency or control channel.
- The receiving party sends a number, known as a seed.
- The initiating party uses the number as a variable in a predefined algorithm, which calculates the sequence of frequencies that must be used. Most often the period of the frequency change is predefined, as to allow a single base station to serve multiple connections.
- The initiating party sends a synchronization signal via the first frequency in the calculated sequence, thus acknowledging to the receiving party it has correctly calculated the sequence.
- The communication begins, and both the receiving and the sending party change their frequencies along the calculated order, starting at the same point in time.

Identifying the hopping pattern consists of a combination of predictive channel hopping analysis coupled with crude spectrum analysis. These fancy terms basically mean that our tools sit and listen on a channel of interest until a frame is received. Once a frame is received, either the tool predictively jumps to another channel and waits a given amount of time before giving up, or the tool enters spectrum-analysis mode, scanning through all channels watching for alterations in the RSSI level. By keeping track of what channel hop combinations work, plotted to a time domain our tools piece together the hopping relationship which exists between two channels. Once the hopping pattern and other communication details are known, traffic analysis is employed to identify the bytes of your target protocol. Given an understanding of this, you may now build your network adapter. Let the games begin!

FHSS technologies (especially those considered proprietary) will fall to data monitoring and injection. These attacks will directly affect the confidentiality and more importantly, the integrity of the data transferred in the clear across this "secure-as-is" solution. Strong cryptography with limited-access random key material, coupled with excellent system design and hacking analysis is required to provide the best level of security. Vendors must assume FHSS is a network enabler, not a security feature.

[0] http://www.europatentbox.com/patent/EP2059911A2/description/109529.html – SubSection 00563
[1] http://www.bannerengineering.com/en-US/wireless/surecross_web_faqs
[2] http://www.mt-online.com/component/content/article/76-january2007/173-going-wireless.html?directory=90
[3] http://www.blackhat.com/presentations/bh-europe-09/Havelt/Black-Hat-Europe-2009-Havelt-FHSS-Network-Security-whitepaper.pdf
[4] www.ossmann.com/shmoo-09/ossmann-spill-shmoo-2009.pdf
[5] http://www.gc.energy.gov/documents/FloridaPowerLight_Comments_CommsReqs.pdf
[6] http://www.opencircuits.com/FHSS
[7] http://en.wikipedia.org/wiki/FHSS