TEAM 20

SOFTWARE DEFINED RADIO LEAKS

Abstract

Following the new wave of wireless technology, wireless keyboards have become increasingly popular. Users pair their keyboards to their computers, and transmit their personal information, passwords and credit card numbers over the air via radio signals. Can this transmission be compromised? What kind of information can we retrieve?

Through this project, we will explore the security of the data sent over wireless transmission between a keyboard and a computer. Our goal is to sniff these transmissions using the appropriate Software Defined Radio (SDR) tools, to obtain valuable information.

Background

Basic overview of RF technology

> Transmitter initiates the RF communication
> It takes the initial data and modifies the signal using a modulation technique to encode the data into the signal
> Signal is transmitted over the air
> Receiver receives and translates the modulated signals into the initial data

Tools

HackRF One (Great Scotts Gadgets)

> SDR that transmits and receives radio signals from 1MHz to 6GHz

Logitech K270 Wireless Keyboard

> Uses Logitech's proprietary Advanced 2.4GHz Technology
> 24 Channels (2.405 ~ 2.474GHz)
> AES 128-bit Symmetric Encryption
> Chip used: nFR24LE1H (Nordic Semiconductor)

GNU Radio & GNU Radio Companion

> Software development toolkit for signal processing and analysis of the digital input
> Create signal flow graphs to capture, transmit, receive, replay, and demodulate signals for analysis in plot graphs

Gqrx

> SDR powered by GNU Radio and Qt graphical toolkit
> Used to identify the current channel used for wireless transmission

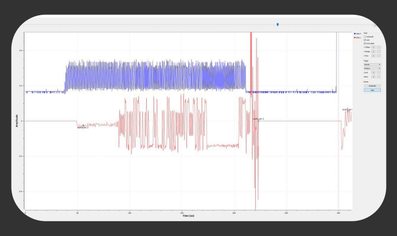
Implementation

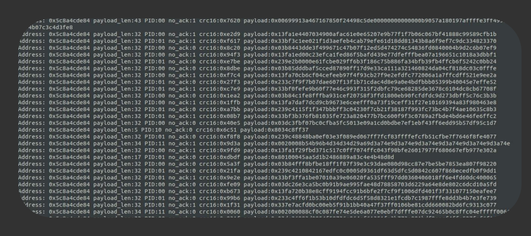
1. Set up
   > Install tools and dependencies
2. Research
   > Dismantle the keyboard
   > Read documentations, datasheets and test reports
   > Determine channel frequencies, modulation scheme and baud rate
3. Construct a flowgraph in GNU Radio Companion
   > Capture analog signals and convert them to digital signals
   > Identify > Filter > Demodulate > Synchronize > Byte stream
4. Script
   > Recover packets from the byte stream
   > Filter false-positive packets
   > Decrypt the packets

Findings

Partial Break

> Detect activities on the keyboard
> Process the captured signals to identify the preamble, payload and ACKs





Challenges

> Niche field requiring in-depth knowledge on signal processing ***
> Following transmission channel hops **
> Signal demodulation **
> Packet filtration ***

Done by:

Kerryn Eer - E0014864
kerryn_eer@u.nus.edu

Tan Wenjian - E0191462
e0191462@u.nus.edu

Ong Ai Hui - E0202723
aihui@u.nus.edu

Ng Wei Xin - E0177126
e0177126@u.nus.edu

References:

http://gqrx.dk/
https://www.gnuradio.org/about/
https://greatscottgadgets.com/hackrf/one/
https://computer.howstuffworks.com/keyboard5.htm
http://www.keil.com/dd/docs/datashts/nordic/nrf24le1_ds_v1_1.pdf
https://blog.aerohive.com/how-are-rf-signals-transmitted-lets-talk-equipment/
https://www.logitech.com/images/pdf/roem/Logitech_Adv_24_Ghz_Whitepaper_BPG2009.pdf

Sponsors:

Acknowledgement:

This project is part of the curriculum of National University of Singapore's CS3235 Computer Security, and has the support of the module coordinator. Tools involved are provided by the module coordinator.