Morgan Gangwere

Curriculum vitae

135 Hortencia
Sandia Park, New Mexico
+1 505 859 3377 / +1 505 639 7551
morgan.gangwere@gmail.com
zaibatsutel.net

Goal

To help people, products, teams and ideas go to 11, then right to infinity... *and beyond.*

Presentations

Aug. 2016 **Fiddler On The Roof: A look at Fiddler**
*P*resented at **DEF CON 24** at the Wall of Sheep, a look at the Fiddler web proxy from basics to extensions incl. a simple proof of concept credential stealing extension.

Apr. 2013 **Git: Zero to Hero**
A Skin-Deep look at DVCSs and how to think with Git, presented to NMUG (New Mexico .NET Users Group.)

Feb. 2012 **Typesetting Beautiful Presentations**
A 5 minute Flash Talk on presentations, typefaces and driving home points, presented at Ignite NM 2012

Oct. 2011 **Cross-Platform Development with Mono**
*A*n informal discussion of the differences between the Microsoft and Mono .NET toolchains; presented for NMUG

Jul. 2010 **Effective User Interfaces**
A crash course in good interfaces for developers, presented to NMUG

Projects

Many of these projects can be found on my GitHub profile.

These are only a selection of the projects I have worked on; many proof-of-concept projects never see a public git repository; Many more projects can be found on my GitHub profile: `https://github.com/indrora`

2016 **Kaitai.io .NET runtime**
*I*nitial framework to use the Kaitai.io binary unpacker with .NET

2016 **PhreakOut**
MF/DTMF tone generator for Windows 10; published on Microsoft Store

2016 **ZaibatsuPass**
*NF*C transit payment reader for Windows 10; published on Microsoft Store

2016 **DeadUpdate (CVE 2016-3966)**
*V*ulnerability in ASUS's LiveUpdate software

2015 **ZaibatsuTel (zaibatsutel.net)**
A personal "brand" used for software projects and services useful in a day to day environment as a student.

2016 **Jour Et Nuit**
*P*roof of concept reverse engineering a Bluetooth Low-Energy protocol.

2015 **OpenKeychain (openkeychain.org)**
*C*ontributed bugfix for GSoC 2015 qualification, fixed bug involving large transactions.

2014 **Atomic**
*F*ork of yaaic focused on stability and technical debt payment

Kaitai .NET runtime

Kaitai is a generic binary unpacking suite intended for reverse-engineering. Extention to other platforms is done through a language-specific code generator and base library. Kaitai lacked a .NET runtime, and as a result the groundwork for a .NET runtime was started in CSharp.

DeadUpdate

Disclosed vulnerability in Asus LiveUpdate software (CVE 2016-2966) which allowed vulnerable devices to execute arbitrary executables in environments vulnerable to HTTP MITM attacks. Followed disclosure through CERT, published to personal blog.

ZaibatsuPass

ORCA card reader for Windows 10. Largely a port of FareBot from Android, able to get balance and historical records for ORCA cards with the framework to easily extend to other cards supported by FareBot. Uses the PCSCSDK from the Microsoft SDK samples, modified to include a more complete Mifare DESfire card protocol. Open source

on GitHub. Published on the Microsoft Store.

PhreakOut

A DTMF/MF Tone generator. Written over the course of a few afternoons to learn how to build Windows 10 media applications. Effectively a "Blue Box in your pocket", PhreakOut is extendable to more than just DTMF and MF tones, but also to any keypad based tone generation system. PhreakOut is also my first application published on the Microsoft store.

ZaibatsuTel

ZaibatsuTel acts as a public identity for my software development projects. In this way it allows for a certain ethos. On the other side, I use it as a way to maintain a personal archive of content (not visible to the public) and keep services for my personal use alive and running.

Jour Et Nuit

A proof of concept reverse-engineering of BTLE protocols used in the Xiaomi Mi Band (1st generation) device. App was able to get step count and set some data about the user, but ultimately was overshadowed by more mature projects.

Atomic

IRC client for Android; forked from yaaic in early 2014. Focuses primarily on the cleansing of technical debt from support of older Android platforms, though new features have been added during development (color schemes and network loss handling.)

Education And Certifications

2016 **FCC Amateur Radio license**
*P*assed element 3 (General)

2015 - ... **Organizational Communications/Professional Writing**
Bachelors of Arts
*E*xpected graduation late 2018, early 2019; University of New Mexico, Albuquerque, New Mexico

2015 **FCC Amateur Radio license**
*P*assed element 2 (Technician)

2008 – 2014 **Network Administration**
Associates in Applied Sciences
*C*entral New Mexico Community College

2008 **LabVIEW CLAD Certification**
*N*ational Instruments

Communication skills

English Native speaker

French Semi-literate - basic functional skills

Software skills

Best level C Sharp, .NET RE, Dalvik RE

Good level C, C++, Java, PHP, LaTeX

Intermediate Bash, git, svn, Linux (Debian, Fedora, Arch)

Basic level LabVIEW, BSD, Windows Administration, kernel hacking, Cisco IOS

Hobbies

- Amateur radio (de K9HAX)
- Vulnerability writeups
- Really basic hardware design

Since you've read this far: This document is a living document! If you're reading this and are a human, consider checking out the latest version:

http://tsunami.zaibatsutel.net/cv.pdf

This document was last compiled on January 29, 2017.

The usual stuff comes at the end: References, samples, etc – Ask for them. They're a thing.