Morgan Gangwere

Curriculum vitae

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

Goal

To be a part of a crack team of awesome people that deliver solutions. To solve problems when nobody else can in a way that will keep going until UNIX time runs out and beyond. To help make the world a better place.

Education And Certifications

2016 **FCC Amateur Radio license**
Passed element 3 (General)

2015 - ... **Organizational Communications/Professional Writing**
Bachelors of Arts
Expected graduation late 2017, early 2018; University of New Mexico, Albuquerque, New Mexico

2015 **FCC Amateur Radio license**
Passed element 2 (Technician)

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

2008 **LabVIEW CLAD Certification**
National Instruments

Hobbies

- Amateur radio (de KG5IXZ)
- Vulnerability writeups
- Really basic hardware design

Projects

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

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

2016 **ZaibatsuPass**
NFC transit payment reader for Windows Phone

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

2015 **ZaibatsuTel (zaibatsutel.net)**
Personal projects in a memory and processor constrained environment.

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

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

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

DeadUpdate

DeadUpdate (CVE 2016-3966) is a vulnerability in the ASUS LiveUpate software. LiveUpdate performed no authentication in a cleartext channel to deliver updates to ASUS computers and motherboards, allowing arbitrary code execution in environments which are susceptible to HTTP Man In The Middle. Vendor was unresponsive or actively hostile during disclosure to MSRC and CERT. Credited as independent discovery alongside DUOSec, who published at the same time an overview of vulnerable OEM update software, including ASUS LiveUpdate.

ZaibatsuPass

After moving from Android to Windows phone, there was no good alternative to FareBot from Android available on the Microsoft store. The result was ZaibatsuPass, a simple ORCA card reader able to read the last 10 transit actions. The ability to extend to other cards (specifically ones based on the NXP Desfire cards)

ZaibatsuTel

An exercise in systems administration, ZaibatsuTel is hosted through a VPS provider as a means for personal file backup, ZNC bouncer hosting and other projects as the need arises. All resources run in a container with 512MB of RAM and a single core.
As a means to collaborate with other people, ZaibatsuTel is also an organization on GitHub, where projects which are of interest to the general community (security and otherwise) or which are better maintained as a group effort and do not have another place to be.

Jour Et Nuit

Began to scratch an itch, Jour Et Nuit was a testbed for reverse-engineering the protocol of the Xiaomi Mi Band generation 1. Implemented was the ability to pair with the device, read step count and set the daily step goal. Reverse engineering was done through de-obfuscation of Dalvik bytecode from the official Xiaomi application.

Atomic

Atomic is an IRC client forked from yaaic in early 2014 as yaaic was in maintenance mode at the time. The projects have split into different directions due to structural changes. Atomic focuses primarily on the cleansing of technical debt from support of older Android platforms, however new features have been added during development (color schemes and network loss handling.)

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

Presentations

Aug. 2016	**Fiddler On The Roof: A look at Fiddler** *Presented 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** *An 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*

References upon request