

# 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 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**  
*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*

### 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**  
*Initial framework to use the Kaitai.io binary unpacker with .NET*
- 2016 **PhreakOut**  
*MF/DTMF tone generator for Windows 10*
- 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*

### 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 Phone. Largely a port of FareBot from Android, able to get balance and historical records for ORCA cards. Open source on GitHub.

## ZaibatsuTel

An exercise in systems administration, Zaibatsu-Tel 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.

## 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**  
*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*

## 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, ~~TeX~~
- 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 October 17, 2016.

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