Enfield, NH, United States
imstillinurstuff@hotmail.com

Ella Rose

I love algorithm design and information theory. I have interests in cryptography, mathematics, networking, computer science, and digital signal processing.

I am the author an application framework for python that facilitates the development of fully featured applications for a minimum amount of code. My goal is to develop my own desktop environment and eventually an app store built around it.

Technical Skills

Likes: python security networking cryptography verilog c
Dislikes: regex

Experience

Software engineer
python, security, network-programming

- Developing new modules and packages
    - Using notepad++ for development
- Maintaining and fixing modules
- Writing documentation
- Committing code to github

Independent Researcher *Nov 2016 → Current*
cryptography

I develop cryptographic algorithms, including a post-quantum public key cryptosystem.

Projects & Interests

crypto – https://github.com/erose1337/crypto *Jun 2016 → Current*
cryptography, cryptanalysis, block-cipher, hash

This repository contains my research into cryptographic algorithm design and cryptanalysis.

Included are tools for cryptanalysis of symmetric primitives, as well as my own designs for ciphers, PRPs, hashes, and public key cryptosystems.

Most of the files are written in python. Some are written in C, which was done to test how the algorithm performs on the native CPU.

pride – https://github.com/erose1337/pride *Oct 2014 → Current*
python, concurrency, networking, audio, pysdl2, sqlite3, security, cryptography

Pride offers consistent and concise development patterns for rapidly developing fully featured applications in python.

I am the sole developer, and my responsibilities include the maintenance and development of the project.

Readings

Gray Hat Python: Python Programming for Hackers and Reverse Engineers – Justin Seitz – http://www.amazon.com/Gray-Hat-Python-Programming-Engineers/dp/1593271921

This book taught me about the lower levels of the x86 architecture, and gave me some familiarity with the windows api.

Black Hat Python: Python Programming for Hackers and Pentesters – Justin Seitz – http://www.amazon.com/Black-Hat-Python-Programming-Pentesters/dp/1593275900

Black Hat python gave me some background on network security. I am not a red team member, and I have never executed any kind of attack - I use this information to learn how to defend and secure my applications.

High Performance Python: Practical Performant Programming for Humans – Micha Gorelick, Ian Ozsvald – http://www.amazon.com/High-Performance-Python-Performant-Programming/dp/1449361595

High performance python helped me to understand why python is generally slower then natively compiled languages like C. It also helped me to understand what can be done about it.

Cython would probably be my go-to for anything that's 1: not crypto 2: written in python 3: needs to be fast, especially if the goal is redistribution. Pypy would probably result in more or less equivalent speeds, but requires installation and has jit overheard, leaving me to favor Cython.

I wouldn't use cython with crypto algorithms because I feel the source for a cryptographic algorithms should compile as exactly as it is written, and cython has a lot of translation to do. I love python, but I'd still code crypto directly in C and not cythonize it.

Pro Python – Marty Alchin, J. Burton Browning – http://www.amazon.com/Pro-Python-Marty-Alchin/dp/1484203356

I read this a while ago, when I first learning. It helped get the general "feel" of python, and how things are usually done in the language. It includes an overview of the "zen of python", which explains why things are done the way they are. I find explaining the reasons for "why" something should be done to be at least as important as "what" needs to be done.

Beginning Game Development with Python and Pygame: From Novice to Professional (Expert's Voice) – Will McGugan – http://www.amazon.com/Beginning-Game-Development-Python-Pygame/dp/1590598725

This was the first book about python I read, and it got me into programming in general.

In fact, it's arguable that this book is what encouraged the development of my own project. Pride started out as a simple experiment with pygame and drawing things to the screen. Eventually I started working on other things like networking, and always maintained that everything developed previously should function concurrently with new additions.

Secrets and Lies: Digital Security in a Networked World – Bruce Schneier – http://www.amazon.com/Secrets-Lies-Digital-Security-Networked/dp/0471453803

A good initial exposure to cryptography and information security. It manages to avoid basically any math or code, and to be entertaining at the same time.

The Design of RijndaeL: AES - The Advanced Encryption Standard (Information Security and Cryptography) – Joan Daemen, Vincent Rijmen – http://www.amazon.com/The-Design-RijndaeL-Information-Cryptography/dp/3540425802

The Design of Rijndael explains the reasoning for why the AES was designed the way that it is. It presents an incredible amount of detail, and it justifies every last step of the design. Daemen and Rijmen are seasoned experts in the field of cipher design, and it is evident in their work.

Tools

First Computer:	Custom build
Favorite Editor:	Notepad++