BTI Institute

Borders • Trade • Immigration

A Department of Homeland Security Center of Excellence

2019 BTI Institute Summer Internship

Cadet Sarah Donaldson, USMA 2021

UNIVERSITY of HOUSTON

Overview

- Introduction
- Goals and Objectives
- Literature Review
  - Part 1: Dr. Weidong (Larry) Shi's Material
  - Part 2: Dr. Christopher Bronk's Materials
- Additional Activities
- Lessons Learned
- My Experience

Introduction

Intern: Cadet Sarah Donaldson, USMA Class of 2021
Dates: 24 June – 12 July 2019
Major: Applied General Psychology
Minor: Cyber Security & Cyber Engineering
Experience at USMA: Army Track & Field, Class Representative, Company Historian
Hometown: League City, Texas
Why I applied for this Internship: As a potential future Cyber or Military Intelligence Officer in the Army, I was interested to look at how cybersecurity and research is applied in a setting outside of IT and CS courses at the Academy. Because USMA only offers undergraduate coursework, the opportunities to conduct or assist on research, especially as an underclassman, is limited so I was excited to be able to participate in that. I was also interested in seeing how civilian entities work alongside 'big named' entities such as Homeland Security.

Goals and Objectives

Objectives:

- At the end of the internship, the intern will be able to deliver a presentation to discuss usefulness of intelligence collection tools, approaches related to cryptocurrencies, and usage of cryptocurrencies in illicit activities.

Goals: the goal of the internship is to provide training and study of the following:

- Investigation skills
- Intelligence collection tools
- Analysis of approaches related to cryptocurrencies
- Usage of cryptocurrencies in illicit activities including areas such as Darknet marketplaces, terrorism financing, and illicit trade.

These were accomplished via an extensive literature review using materials provided by Dr. Weidong (Larry) Shi and Dr. Christopher Bronk

Literature Review Part 1

What are cryptocurrencies and why are they important?

- Also known as Virtual Currency
- Definition: a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
- CCs are designed as a substitute for government-backed currency and therefore are not nearly as regulated
- The most common (and most exchanged) CC is bitcoin
- The majority of research relating to illicit activity, exchange, and regulation of CCs has been performed in terms of bitcoin

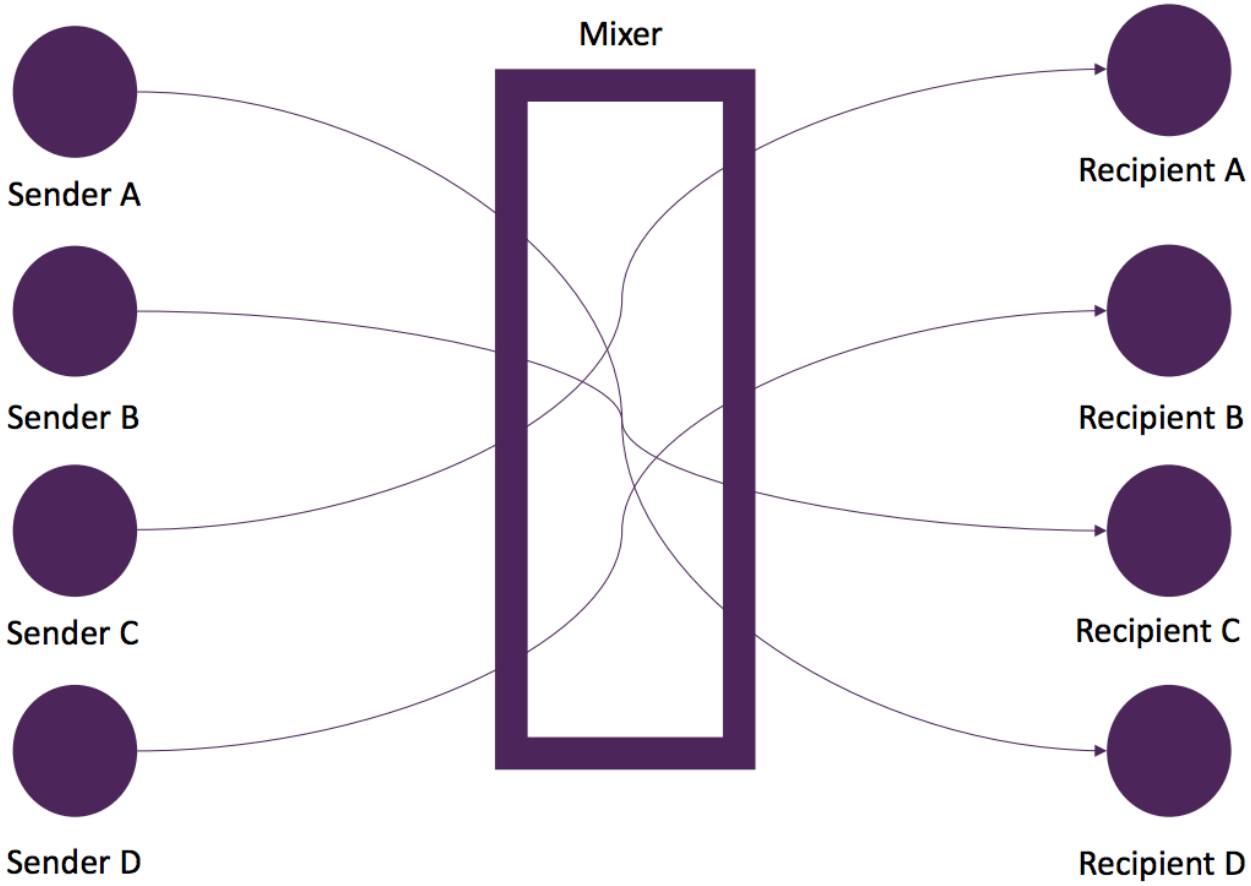
Literature Review Part 1

What are potential financial crime risks associated with cryptocurrencies?

- Anonymity/Pseudonymity
  - There is no face-to-face bank transactions, only public identifier keys (individual alphanumeric keys) and many illegal users have multiple to hide number and type of transactions
- Rapid International Transaction Settlement
  - Much faster and does not have the oversight of a regular bank
- Decentralization and Lack of Contained Environments
  - Anyone can be participating anywhere they have internet access
- Money Laundering
  - Use of mixers/tumblers to mask money gained illegally
- Terrorist Financing
- Fraud
  - Transactions are irreversible
- Cybercrime
  - Use of ransom/malware and hacking sites and bitcoin wallets
- The Dark Web and its marketplaces

Literature Review Part 1

Use of mixers/tumblers in cryptocurrency



Literature Review Part 1

How much crime is occurring via cryptocurrency transactions?

- An estimated 25% of Bitcoin users participate in illegal activity
- About 44% of Bitcoin transactions are illegal

What methods exist to find and track illegal users?

- Bitcoin seizures by law enforcement
- Undercover law enforcement as dealers and buyers
- Users identified on forums such as Reddit
- Use of identifiers
  - Network Cluster analysis: Did someone purchase on known illegal markets?
  - The amount of money per transaction

Are there alternative methods?

- A team of investigators worked and were successful in identifying suspected illegal marketplace users with only average office laptops using the methodology below

Literature Review Part 1

Why is regulation so complicated?

- Some countries have attempted to ban the use of CCs but as proven by active sex and drug marketplaces on the Dark Web, those looking to perform illegal activities will find a way
- The AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) is a division of the International Monetary Fund that controls many of the regulations on the exchange and use of currency
- In the US, states have individual AML/CFT regulations so companies looking to capitalize on the CC industry may avoid certain states (NY)
- Different nations also have wildly differing levels of regulation
- The very design of Bitcoin is meant to preserve privacy/anonymity therefore a system for tracking names and transactions would concern users

Why is this important?

- Because CCs have no governmental backing, they have no borders
- In this case, what is to stop criminals from simply moving their activities to somewhere less regulated/monitored?
- In order to truly regulate and monitor activities using CCs, states and nations must cooperate and collaborate to produce similar legislation

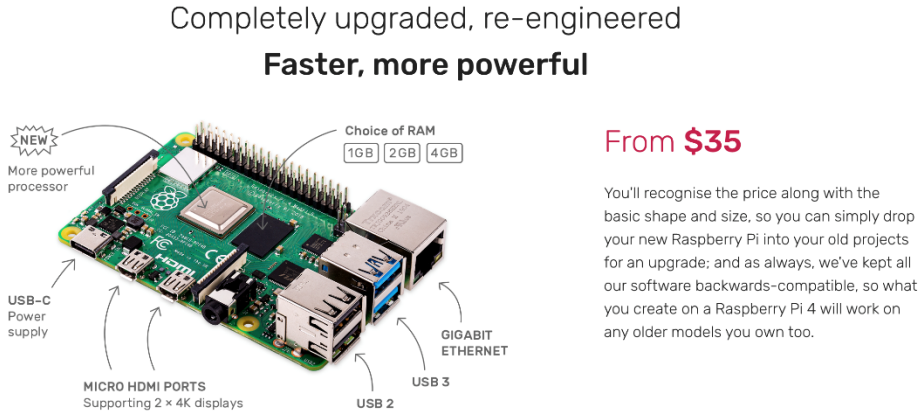
Literature Review Part 2

What are our concerns in modern cybersecurity?

- Leaders are generally uninformed
  - "I have sat in very small group meetings in Washington unable to decide on a course of action because we lacked a clear picture of the long term legal and policy implications of any decision we might make." –GEN Michael Hayden, former CIA Director
- The only difference between a glitch and an attack is malice which can be difficult to differentiate
- Attacks can happen silently, discovered only after damage is done
- We (the US) are generally uninformed about the cyber capabilities of other nations
- The limit does not seem to exist (or at least we've yet to find it)
  - Stuxnet and the Iranian nuclear plant
  - Dr. Bronk's theoretical paper: what could happen, especially to the military if China launched a full-scale cyber attack

Literature Review Part 2

- The military's dependence on technology for communication and intelligence
  - The DOD has defined cyberspace as its "fifth domain" (land, sea, air, and space)
  - Personal experience in a SCIF (Sensitive Compartmented Information Facility: Secure room or data center)
- Individuals and small groups are just as large of a security concern as foreign governments
  - In June, it was discovered that NASA's JPL (Jet Propulsion Laboratory) was hacked using a Raspberry Pi (see right)



Literature Review Part 2

- "Hacktivism": the idea of promoting or resisting some kind of political or societal change through nonviolent but often legally questionable cyber means of protest
  - 1989 hack that infiltrated NASA and the Department of Energy as a protest against nuclear energy research
  - 2001 hack by Chinese hacktivists denied service to many government-sponsored websites such as The White House's
- Terrorist Organizations using the Internet
  - The ability to conduct widespread recruiting and propaganda planting
  - All of the 9/11 attackers had Hotmail account and were believed to have used them to coordinate
- Large-scale use of malware and ransomware
  - Seizing systems in hospitals, banks, network denials-of-service

Conclusion

Thank you for your time these past three weeks and for listening to my presentation!

Go Coogs and Beat Navy!

Literature Review: Sources

- United States of American v. Alexandre Cazes
- Virtual Currencies and Financial Crime: Challenges and Opportunities
- Exploring Spatio-Temporal and Cross-Type Correlations for Crime Prediction
- Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?
- Seize and Desist? The State of Cybercrime in the Post-AlphaBay and Hansa Age
- Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations
- The Dark Side of Cyber Finance
- Blown to Bits: China's War in Cyberspace, August–September 2020
- Cybersecurity and Cyberwar: What Everyone Needs to Know
- Silk Road: The Dark Side of Cryptocurrency