Network Forensics

Yong Guan

Department of Electrical and Computer Engineering
Associate Director for Research, Information Assurance Center
Iowa State University

August 5, 2016

Our Research Foci

- Cyber Attacks and Crimes: A painful side-effect of the innovations of Computer and Internet technologies
  - Almost all physical crimes involve digital evidence
  - Low percentage of cases reported to law enforcement
- Our Research Foci in DF and Security:
  - Build Accountability & Incident Response
  - Security Monitoring & Impact Analysis
  - Human-centered Security
- **Recently awarded the first and only NIST CoE in Forensics, 2015-2020.**

NIST Center of Excellence in Forensics- CSAFE

- Motivated by the Innocence Project - http://www.innocenceproject.org/
- 5 year project, led by Prof. Alicia Carriquiry (ISU), with partners: MFRC (Ames Lab), CMU, Virginia, and UC Irvine.
- Core Theme:

> CSAFE aims at advancing the statistical and probabilistic bases of analyses for common forms of pattern and digital evidence, thereby fulfilling the goal of placing forensic science on a firm scientific foundation.

Two focused areas:

- Pattern Evidence
- Digital Evidence

csafe
Center for Statistics and Applications in Forensic Evidence

CSAFE - Broad Center Objectives

- Develop, in collaboration with NIST scientists, new methods for forensic evidence, including objective measures of quality and assessment of sources of variation.
- Develop new inference techniques that account for various sources of uncertainty.
- Establish a sound bases of interpretation for forensic evidence in judicial settings, including test standards and standardized terminology.

csafe
Center for Statistics and Applications in Forensic Evidence

IOWA STATE UNIVERSITY

CSAFE – Digital Forensics Objectives

Digital Forensics plays an increasingly significant role in forensic analysis

- Digital world has been the locus of various forms of cybercrime (desktop & laptop computers, cell phones, servers, etc.)
- Almost all physical crimes involve digital evidence (email, logs, etc.)

Key issues:

- Identify the devices used in a crime
- Identify the individual that actually used the device
- Prove a relationship between the individual and evidential data about a criminal activity
- Work with incomplete digital evidence, errors or uncertainty

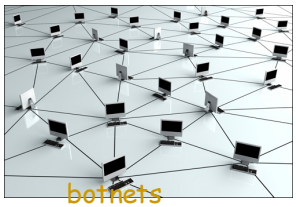
csafe
Center for Statistics and Applications in Forensic Evidence

IOWA STATE UNIVERSITY

> *"Liberty means responsibility. That is why most men dread it."*
>
> — George Bernard Shaw

http://www.fbi.gov/news/stories/story-index/cyber-crimes

Scareware/malvertising



botnets

Cyber Banking Fraud

Online Child Predators

IOWA STATE UNIVERSITY

A few interesting things

- SODDI

IOWA STATE UNIVERSITY

Who were they?

- SODDI (Some Other Dude Did It)
  - Trojan Defense

IOWA STATE UNIVERSITY

Cyber Crime **A painful side-effect of the innovations of Computer and Internet technologies**

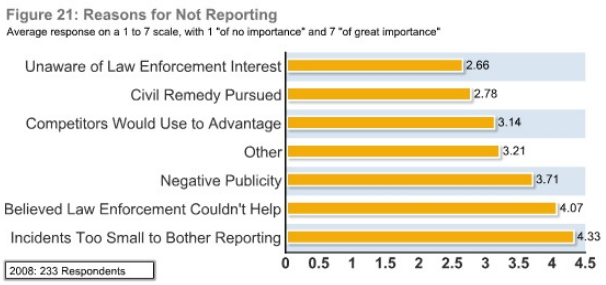
- The possibility of becoming a victim of cyber crime is the number one fear of billions of people
- The findings in annual CSI/FBI Computer Crime and Security Surveys confirm that cyber crime is real and continues to be a significant threat, and cause ruinous financial damage
  - Low percentage of cyber crime cases reported to law enforcement. (In 1996, only 16%; in 2008, 27%)
  - Vast majority of cyber crimes never get caught or prosecuted

Why?

IOWA STATE UNIVERSITY

Cyber Crime **A painful side-effect of the innovations of Computer and Internet technologies**

- **Why?**



- Concern of negative publicity
  - Attracting other cyber-attackers
  - Undermining the confidence of their customers, suppliers, and investors
  - Inviting the ridicule of their competitors

IOWA STATE UNIVERSITY

Cyber Crime A painful side-effect of the innovations of Computer and Internet technologies

Cyber criminal activity is growing – not steadily but exponentially, both in frequency and complexity

- Much harder to detect than crimes in the physical world
- Often insiders
- Indirectly through various hiding techniques
  - Botnets
  - Information hiding: steganography, covert channel, etc
  - Anonymity proxies
  - Stepping Stones
  - ……

IOWA STATE UNIVERSITY

Challenges to Digital Forensics

- Increased data size & urgency
  - Data centers, Storage, Time
- Increased use of encryption
  - Child pornography case
- Increased complexity
  - ISP, device diversity
- Anti-Forensics
  - Anonymity
  - Steganography
- "Co-Space"

IOWA STATE UNIVERSITY

Why forensics so challenging

A complex example "Two Player Game - Chess"

Observable with complete and precise info

In cyberspace, do we have an observable "chessboard"?

Two or more player game with

Incomplete and imprecise info

IOWA STATE UNIVERSITY

Outline of This Tutorial

- Overview
- Forensic Q&A
- Case Study
- Traceback
- A Forensic Look of Bitcoin/Cryptocurrency
- Accountability vs Anonymity
- Summary and Future Directions