Reducing Crime in Cyberspace: A Privacy Industry View

(Stephanie Perrin)

(Adam Shostack)

Roger Dingledine

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialogue
- Post 9/11 Additions

Who We Are: Tor

- Started in 2002 to build strong privacy systems
- Two main developers plus many volunteers (free software project)
- Funded by US Department of Defense and Electronic Frontier Foundation

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

Our Goal

- Prevent People From Being Victimized
  - Victims of criminal invasions of privacy
  - Victims of non-criminal invasions
    - By Individuals
    - By Organizations
    - By Technical Accident
- Our goal today is to open a dialogue with you
  - We share many goals
  - We look forward to working together

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

A Short History of Privacy

- Provide Context For Discussion
  - Understand Laws, International Activity
  - Privacy Invasive Technologies
- OECD
- EU Data Protection
- Canada’s Bill C-6, Charter of Rights
- US Constitution and case law

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

Crime in Cyberspace

- Cyberspace crimes
- Physical World Crimes
- How they blend
  - Line can be hard to define
- Privacy and Hacking

Cyberspace Crimes

- Cybercrime is Diverse
  - Denial of Service & distributed variants
  - Stealing money
  - Stealing bits
  - Hacking
- Cybercrimes that blend into the real world
  - Stalking
  - identity theft

Cyberspace Crimes (2)

- Some types are aided by privacy (DDOS, Hacking)
- Some types are privacy-neutral
  - Stealing money from a bank
- Some types are hindered by privacy
  - Identity Theft
- Some the only defence is privacy
  - Stalking

Real World Crime and Cyberspace

- Talking about cybercrime often blends into physical world crime
  - Planning terrorist acts with email
  - Drug Trafficking
  - Money Laundering
  - Fencing Stolen Goods
    - Who wants to shut down Ebay?
  - Kiddie Porn

Real World Crime and Investigation

- Who cares if its encrypted?
- Subject under investigation can be targetted even with encryption
  - Traditional Surveillance
  - Computer Security is poor
  - Undercover Activity

Real World Policing and Cybercrime

- Desire for Perfect Information
  - Doesn’t exist offline
  - Won’t exist online
    - Perfect information is a myth
- Why try to create it online?
  - Good reasons not to
    - Fundamental liberties
    - Cost of transactions
- Risk of “perfect” data being abused

Privacy and Criminals

- Criminals have privacy
  - Motivation to learn
  - Motivation to buy
  - Identity theft
- Normal People and Police don’t
- The worst of all possible worlds

Privacy and Hackers

- Hackers have privacy
  - Break into system
  - Destroy the logs
  - Repeat as needed
  - They don’t use or need our software
- Normal People and Police don’t
- The worst of all possible worlds

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

Monitoring of Cyberspace

- Investigation
- Traffic Analysis and Surveillance
- Undercover Operations
- The Threat of Perfect Knowledge

Investigation

- Tor reduces utility of logs
- Tor blocks sniffers
- Tor hides information that an investigator may want
- Tor does not prevent
  - People from revealing information
  - People hacking into computers (DIRT, Back Orifice)
  - One-on-One surveillance (TEMPEST,video)

Traffic Analysis and Surveillance

- Tor reduces ease of traffic analysis
  - We’re not sure how much
- Use of Tor is observable by analyst

Undercover Operations

- Are an effective tool
- Tor makes it easy for a law enforcement officer to infiltrate
- Tor protects privacy of family of LE

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialogue

Technologies of Privacy

- The Tor System
- Critical Infrastructure Protection
- Minimal Disclosure Technologies

The Tor Network

- Designed to maximize privacy
- No back doors
- Known flaws listed in whitepaper

No Back Doors

- Systems with backdoors hard to defend
- Digital Millenium Copyright Act (US)
- Raytheon, Northwest Airlines
- Too many keys must be distributed
- Due Process weakened by back door
- Weakens evidence chain
- Industrial Espionage
- Rogue States

Known Flaws Enumerated

- Security Experts like public analysis
- We encourage analysis and examination
- Some flaws can be exploited
- Listed in a whitepaper

Critical Infrastructure Protection

- Tor can protect
  - Whistleblowers
  - Security Exploit Information
- Privacy is part of the information infrastructure
  - *Requires* Protection
  - Enables growth of the medium

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialogue

Opening a dialogue

- Our goal today is to open a dialogue with you
  - We’ve explained what we do and why
  - We share many goals
- We look forward to working together
  - Education
    - Risks
    - Proper Behavior
  - Sharing information and education

Post 9/11 Additions

- Slides through this point are unchanged
- Delivered to Interpol’s Working Group on Computer Crime
- State of the Freedom Network
- Security Analysis of Network
- Al Qaeda Communication

George Bush on the Attacks

- America was targeted for attack because we're the brightest beacon for freedom and opportunity in the world. And no one will keep that light from shining. Today, our nation saw evil, the very worst of human nature. And we responded with the best of America -- with the daring of our rescue workers, with the caring for strangers and neighbors who came to give blood and help in any way they could.

(Sept 11, 8:30 PM address)

Freedom Network shut down

- Decision made June, 2001
  - Economic factors
  - 15,000 users
  - $150,000 month costs
- Planned announcement Sept 15, 2001
  - Announcement delayed
  - Avoid claims that we were ordered to shut it down
  - Intel agency interactions

Security Analysis

- Group dedicated to analysis
- Analysis of real time networks
  - Not going to withstand a dedicated attack
- Simple statistical analysis will win
  - Fast tap
  - Lots of disk space

Al Qaeda Tradecraft

- DISCLAIMER:
  - I know what I read in the press.
  - (The press stinks)
  - You may know more than me

Tactics

- Couriers
- Save messages as draft at hotmail
  - Share passwords
  - Never send it
  - http://www.jihadwatch.org/archives/002871.php
    - (Google: al qaeda hotmail draft)
- Cyber-cafes
- Codewords (marriage, sale, goods)

Crypto

- Seem to use locally designed weak systems
  - training manuals on internet
  - WSJ reporter laptop
  - Pakistani computer specialist (recent capture)
- Continues pattern of low tech and understood
- Unlikely to use internet privacy technology

Summary

- No evidence of terrorist use of privacy tech (as we’ve defined it)
- National or regional technical means can defeat what we built
  - without backdoors