Computer Crimes: Serial vs. Parallel

Dr. Thomas A. Johnson
University of Kentucky
Cyber Crime - Types

• **Serial Computer Crime**
  • Attacks tend to have individual targets
  • Repeat offenders

• **Parallel Computer Crime**
  • Launches single attack against multiple targets
Cyber Crime - Examples

• **Parallel**
  - Nigerian Scam
  - Nation-state Attacks
  - Distributed Denial of Service Attacks (DDoS)
  - Identity Theft
  - Phishing
  - Virus Trojan Horse
  - Financial Fraud
    - Investment
    - Credit
    - Institution
  - Auction Fraud

• **Serial**
  - Mitnick (social engineering)
  - Child Exploitation
  - Identity Theft
  - Cyber Stalking
  - Disgruntled Employee
## Cyber Crime - Examples

The following graph depicts reported monetary losses:

<table>
<thead>
<tr>
<th>Complaint Type</th>
<th>% of Reported Total Dollar Loss</th>
<th>Of those who reported a loss the Average (median) $ Loss per Complaint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nigerian Letter Fraud</td>
<td>1.7%</td>
<td>$5,100.00</td>
</tr>
<tr>
<td>Check Fraud</td>
<td>11.1%</td>
<td>$3,744.00</td>
</tr>
<tr>
<td>Investment Fraud</td>
<td>4.0%</td>
<td>$2,694.99</td>
</tr>
<tr>
<td>Confidence Fraud</td>
<td>4.5%</td>
<td>$2,400.00</td>
</tr>
<tr>
<td>Auction Fraud</td>
<td>33.0%</td>
<td>$602.50</td>
</tr>
<tr>
<td>Non-delivery (mdse and payment)</td>
<td>28.1%</td>
<td>$585.00</td>
</tr>
<tr>
<td>Credit/debit Card Fraud</td>
<td>3.6%</td>
<td>$427.50</td>
</tr>
</tbody>
</table>
Creating a Typology

- Psychological/Psychiatric factors of each
- FBI Crime classification model
- Organized vs. disorganized crime scenes (i.e. hacker signatures)
- Etiology
- What’s causing the person to commit this sort of crime?
- Motive
  - Inferred, attributed or declarative
- Offender profile
  - age, sex, family status, prior offense, job, victim of sexual abuse
- Criminological theory - Application
  - treatment, deterrence-punishment, incapacitation, recidivism
- Treatment modalities cost and effectiveness
- Deterrence/punishment cost and effectiveness
- Prosecution goals (probation, conviction, sentencing)
  - Civil commitment
  - Sexual offender status
- Seeking to place individual in probation, put in jail or change their behavior
Typology – Targets for Attack

- Cyber criminals target CIA components
- Confidentiality
  - Network Security Protocols
  - Network Authentication Services
  - Data Encryption Services
- Integrity
  - Firewall Services
  - Communications Security Management
  - Intrusion Detection Services
- Availability
  - Fault Tolerance for Data Availability
  - Acceptable Logins and Operating Process Performances
  - Reliable/Interoperable Security Processes and Network Security Mechanisms
Typology – Motives

- **Financial/Economic**
  - Sophisticated
  - Subterfuge
- **Social Motivators**
  - Ego/Self-recognition
  - Rebellion against authority
  - Mental illness/Instability
  - Revenge
- **Political Agenda**
- **Sexual Impulses**
- **Obsession/Addiction**
- **Ideological Beliefs**
  - Individual
  - State sponsored
- **Technical Challenge**
  - Desire for entertainment
Typology – Offender Profile

The following graph depicts age comparisons in 1998.

Age of Internet Fraud Criminals

National Consumers League
Internet Fraud Watch Age Ranking 1998

- Thirties: 42%
- Forties: 24%
- Fifties: 12%
- Sixties: 3%
- Seventies: 1%
- Under 20: 2%
- Over 80: 0%

Twenties: 16%
Self-reported computer criminal behavior: A psychological analysis

Marcus K. Rogersa (a), Kathryn Seigfried (b), Kirti Tidke (a)

a - Department of Computer and Information Technology, Purdue University, 401 N Grant Street, West Lafayette, IN 47907, United States
b - Department of Psychology, John Jay College, 445 West 59th Street, New York, NY 10019, United States

(www.elsevier.com/locate/diin)
Typology – Offender Profile

Geographical Distribution of Offenders

Map 1 - Top Ten States by Count: Individual Perpetrators (Number is Rank)

Top Ten States - Perpetrator
1. California – 15.2%
2. New York – 9.5%
3. Florida – 9.3%
4. Texas – 6.5%
5. Illinois – 4.5%
6. Pennsylvania – 3.3%
7. Tennessee – 3.2%
8. North Carolina – 3.1%
9. Ohio – 3.1%
10. New Jersey – 3.0%
Typology – Offender Profile

Chart 7 -- Gender of Perpetrators

- Male: 75.2%
- Female: 24.8%

2006 Internet Crime Report
National White Collar Crime Center and the Federal Bureau of Investigation
Predictors

• Some studies indicate that a strong predictor of computer crimes is previous engagement in other criminal activity.

• Other experts contend that it is difficult to predict/profile certain types of cyber crime such as cyber stalking given the diversity of offenders (i.e, University Professors, Corporate CEOs, etc.)
Predictors

- Anti-social behavior
- Deviant psychological behavior (pornography)
- Disgruntled
- Low self-control
- Addictive personality
- Economic factors
  - Low socio economic status (SES)
  - Unstable family structure
- Age (more common in juveniles)
  - Adolescent history (criminal, anti-social)
- Opportunity
  - Technical expertise
  - Frequency of internet use
- Drug/alcohol use
Who Is Attacking?

- Male
- Aged 18-23
- Not married
- White
- Technical background
- Criminal history

Note: The type of crime may affect the profile of the attacker. For example, career, serial, cyber criminals might not fit this profile.
Who Is Attacking?

• **Classes of computer criminals**
  • Tool makers
  • Tool users
  • Script followers

• **Further, these criminals can be differentiated as:**
  • Hackers
  • Pranksters
  • Career criminals
Network Protection - Methods

Protection methods can be Technical, Operational, Physical, or a combination.

Good preventative goals include:

- **Deterring Malware**
- **Thwarting Fraud**
- **Avoiding Stalkers**
- **Reducing Spam**
- **Deterring Hackers**
- **Safeguarding Data**
- **Effective Monitoring**

*Cybercrime – Piercing the Darkness*
http://library.thinkquest.org/04oct/00460/prevention.html
## Network Protection

<table>
<thead>
<tr>
<th>Protection Method</th>
<th>Proactive</th>
<th>Reactive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Address Translation (NAT)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remote Access Security</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Virtual Private Networking (VPN)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection Systems (IDS) - Host, Network-based</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Computer Incident Response Teams (CIRT)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Layered Security Approach</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Protect Known Vulnerable Ports</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Wireless Security</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies, Procedures, Guidelines</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Best Practices</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>User Education/Training</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery Planning</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Logs (Audit, Network Access, System)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Physical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perimeter Fencing</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Personnel, Building, Locks</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection Systems (IDS) - Alarms, Sensors, CCTV</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Biometrics</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Network Protection – Mechanisms

- **Protection Domain** - enables protection of programs from unauthorized modification or execution interference
- **Trusted Computing Base (TCB)**
- **Security Perimeter** (between TCB and rest of system)
- **Trusted Path** (from user to TCB)
- **Trusted Computer System** (H/W and S/W assurance measures)
- **RINGs (Multiple Protection Domains)**
- **Security Kernel** (Reference Monitor)
- **Logical Security Guard**
- **Security Modes**
  - System High, Multi-Level, Dedicated, Compartmented, Controlled, Limited Access
- **Architecture Related Vulnerabilities**
- **Recovery**
  - Maintenance, Fault-Tolerant, Fail-Safe, Fail-Soft/Resilient, Failover, Cold Start
- **Formal Models**
  - Security, Confidentiality, Integrity
Top Threats

- Internet crime allows anonymity through contact methods other than face-to-face.
- Top ways the threats occur:

2006 Internet Crime Report
National White Collar Crime Center and the Federal Bureau of Investigation
## Top Threats

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Serial</th>
<th>Parallel</th>
<th>Damage Potential</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Eavesdropping (passive, active)</td>
<td>X</td>
<td>X</td>
<td>Variable</td>
</tr>
<tr>
<td>Network Intrusion (external source, back doors, piggybacking)</td>
<td>X</td>
<td>X</td>
<td>High</td>
</tr>
<tr>
<td>Penetration of known vulnerabilities in security perimeter</td>
<td>X</td>
<td>X</td>
<td>Variable</td>
</tr>
<tr>
<td>Denial of Service (DoS)</td>
<td>X</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Distributed Denial of Service (DDoS)</td>
<td></td>
<td>X</td>
<td>High</td>
</tr>
<tr>
<td>Session Hijacking (IP Spoofing, TCP sequence number, DNS poisoning)</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td>TCP Fragmentation</td>
<td>X</td>
<td>X</td>
<td>Variable</td>
</tr>
<tr>
<td>Dial-Up (war dialing, demon dialing)</td>
<td></td>
<td>X</td>
<td>Variable</td>
</tr>
<tr>
<td>Network / Port Scanning</td>
<td></td>
<td>X</td>
<td>High</td>
</tr>
<tr>
<td>Wireless Vulnerabilities (WEP, war driving, eavesdropping)</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon Abuse / Stolen Passwords (legitimate user, masquerade)</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td>Inappropriate System Use by Authorized Users (personal, non-business)</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>X</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>X</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td><strong>Physical</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technological (Keystroke, shoulder surfing)</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td>Physical Damage to Structure (explosives, breach, environment)</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
<tr>
<td>Equipment Theft</td>
<td>X</td>
<td></td>
<td>Variable</td>
</tr>
</tbody>
</table>
Serial and parallel attacks may cross over into one another. For example, a serial attack can be against one entity with multiple exploitation.

Technical attacks are more conducive to parallel computer crimes, while operational and physical tend to be more serial in nature.
Sources


3. Self-reported computer criminal behavior: A psychological analysis, Marcus K. Rogersa (a), Kathryn Seigfried (b), Kirti Tidkea, a - Department of Computer and Information Technology, Purdue University, 401 N Grant Street, West Lafayette, IN 47907, United States, b -Department of Psychology, John Jay College, 445 West 59th Street, New York, NY 10019, United States, www.elsevier.com/locate/diin

