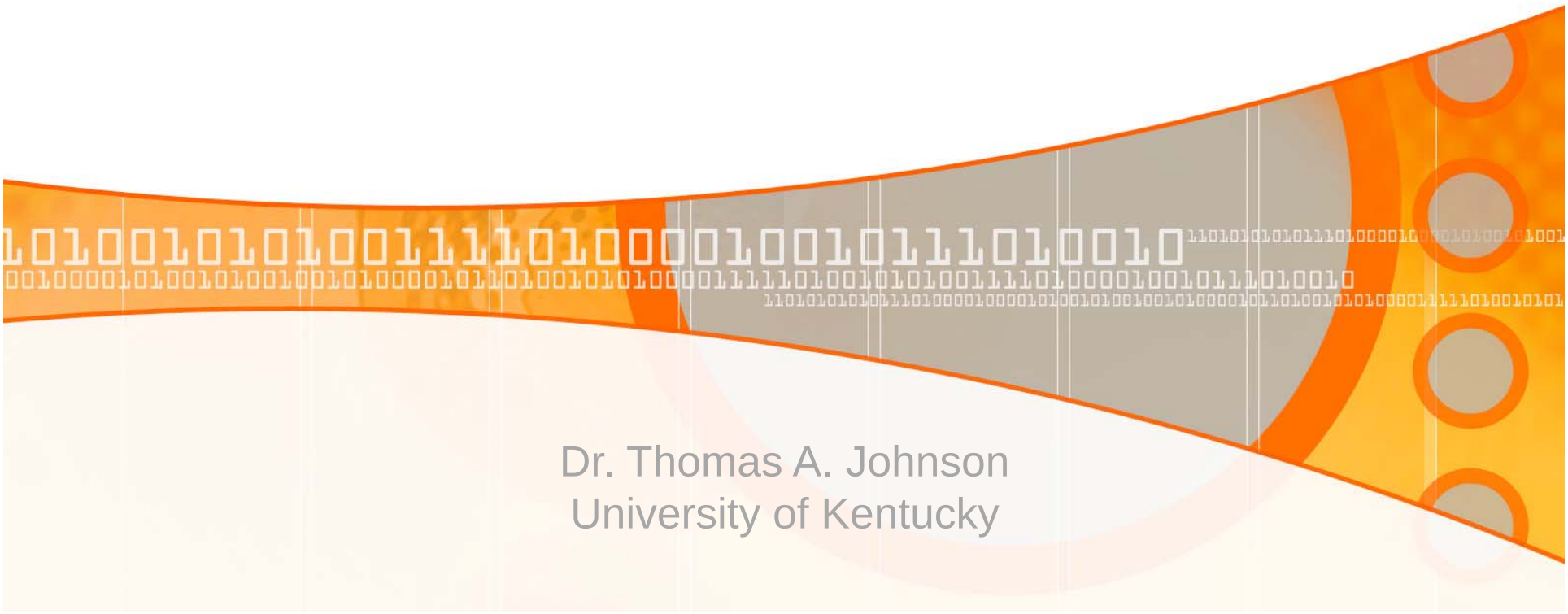
Computer Crimes:
Serial vs. Parallel



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:

Complaint Type	% of Reported Total Dollar Loss	Of those who reported a loss the Average (median) $ Loss per Complaint
Nigerian Letter Fraud	1.7%	$5,100.00
Check Fraud	11.1%	$3,744.00
Investment Fraud	4.0%	$2,694.99
Confidence Fraud	4.5%	$2400.00
Auction Fraud	33.0%	$602.50
Non-delivery (mdse and payment)	28.1%	$585.00
Credit/debit Card Fraud	3.6%	$427.50

2006 Internet Crime Report

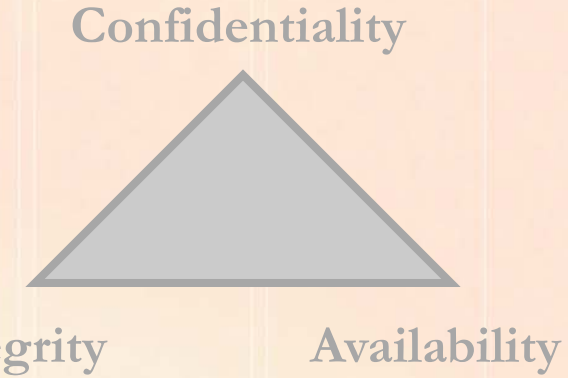
National White Collar Crime Center and the Federal Bureau of Investigation

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*

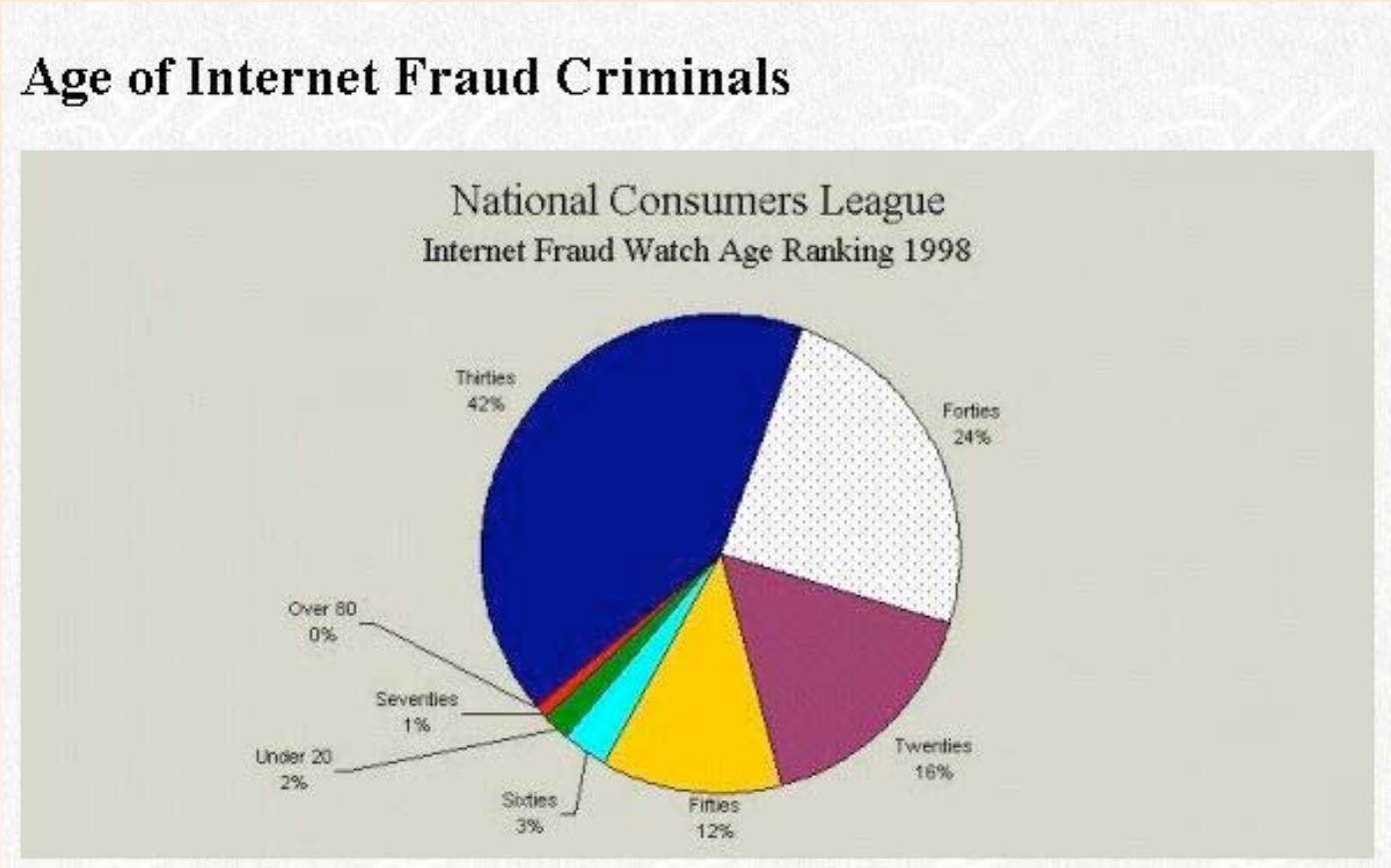


Typology – Motives

- *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



Typology – Offender Profile

The following table depicts demographic data in 2006

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)*

Table 1 – Respondent demographics

Participants	Percentage (frequency)	
	Computer criminals	Non-computer criminals
Gender		
Male	86.8 (59)	88.9 (8)
Female	13.2 (9)	11.1 (1)
Total	100 (68)	100 (9)
Age		
18–20	51.4 (35)	33.3 (3)
21–23	39.7 (27)	44.4 (4)
24–27	7.4 (5)	22.2 (2)
28 or older	1.5 (1)	0
Total	100 (68)	100 (9)
Year in college		
Freshman	7.4 (5)	0
Sophomore	45.6 (31)	33.3 (3)
Junior	10.3 (7)	11.1 (1)
Senior	36.8 (25)	55.6 (5)
Total	100 (68)	100 (9)
Ethnicity		
White	85.3 (58)	77.8 (7)
Asian American	8.8 (6)	11.1 (1)
African American	1.5 (1)	0
Indian	1.5 (1)	0
Asian	1.5 (1)	11.1 (1)
Asian (India)	1.5 (1)	0
Total	100 (68)	100 (9)
Major		
Comp. tech	91.2 (62)	100 (9)
Comp. graphics	1.5 (1)	0
Comp. science	1.5 (1)	0
Other	5.9 (4)	0
Total	100 (68)	100 (9)

Typology – Offender Profile

Geographical Distribution of Offenders

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

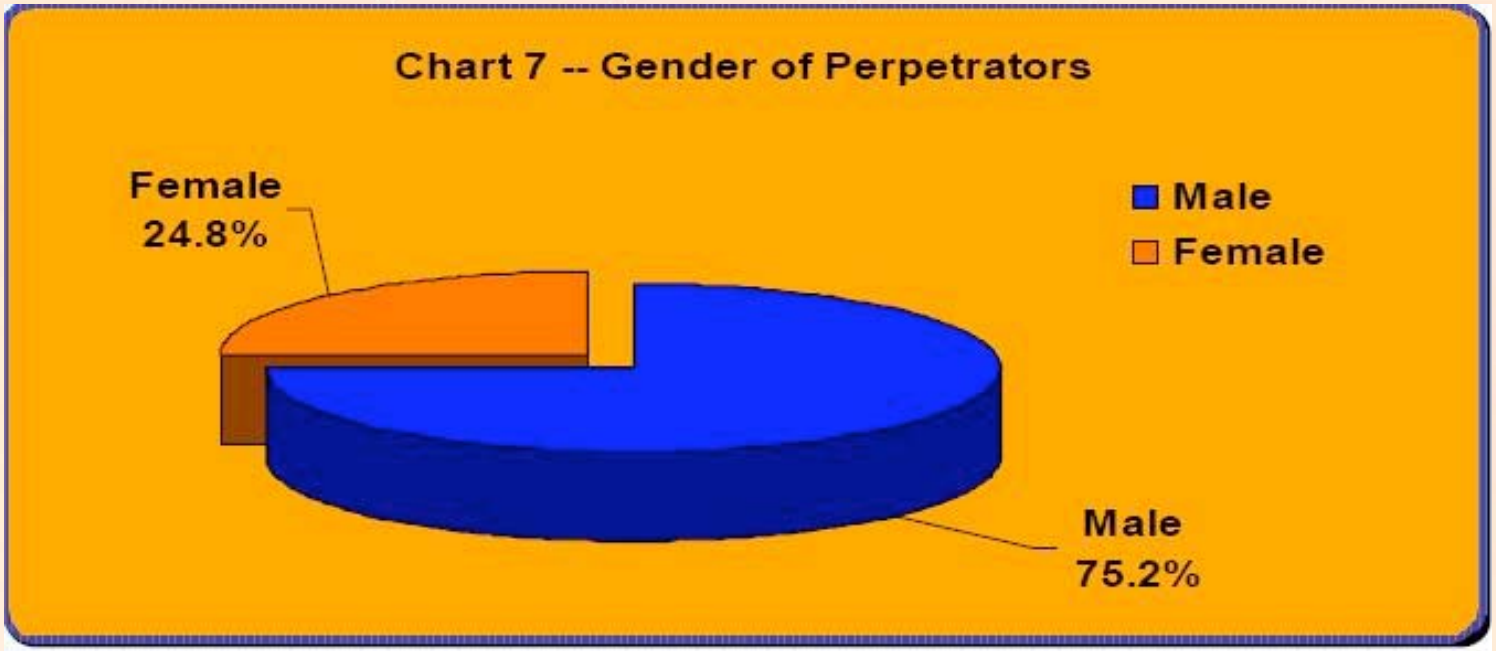
Top Ten States - Perpetrator

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%

2006 Internet Crime Report

National White Collar Crime Center and the Federal Bureau of Investigation

Typology – Offender Profile



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.*
  - *The General Theory of Crime as a Predictor of Computer Crime in a College Aged Sample (D.R. Foster, 2006)*
- *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

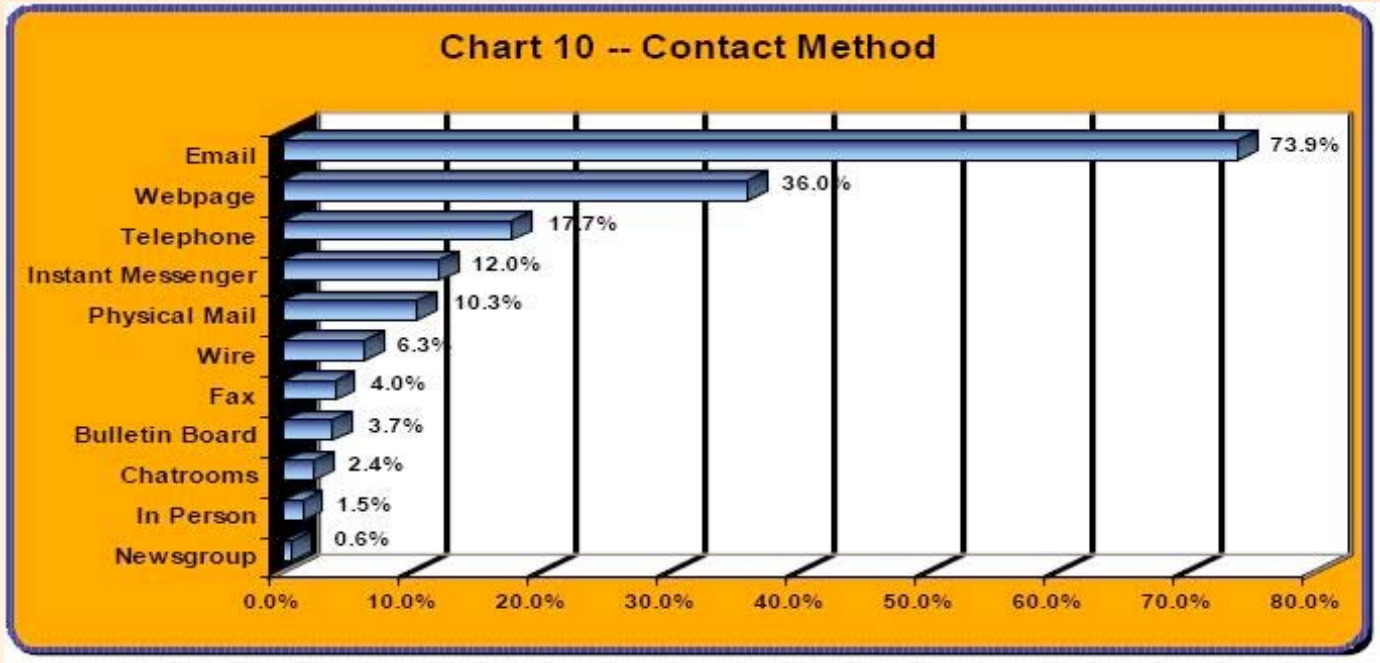
Protection Method	Proactive	Reactive
Technical		
Network Address Translation (NAT)	X	
Remote Access Security	X	
Virtual Private Networking (VPN)	X	
Intrusion Detection Systems (IDS) - Host, Network-based	X	X
Computer Incident Response Teams (CIRT)		X
Layered Security Approach	X	
Vulnerability Scanning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

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

Attack Type	Serial	Parallel	Damage Potential
Technical			
Electronic Eavesdropping (passive, active)	X	X	Variable
Network Intrusion (external source, back doors, piggybacking)	X	X	High
Penetration of known vulnerabilities in security perimeter	X	X	Variable
Denial of Service (DoS)	X		High
Distributed Denial of Service (DDoS)		X	High
Session Hijacking (IP Spoofing, TCP sequence number, DNS poisoning)	X		Variable
TCP Fragmentation	X	X	Variable
Dial-Up (war dialing, demon dialing)		X	Variable
Network / Port Scanning		X	High
Wireless Vulnerabilities (WEP, war driving, eavesdropping)	X		Variable
Operational			
Logon Abuse / Stolen Passwords (legitimate user, masquerade)	X		Variable
Inappropriate System Use by Authorized Users (personal, non-business)	X		Variable
Social Engineering	X		High
Insider Threat	X		High
Physical			
Techological (Keystroke, shoulder surfing)	X		Variable
Physical Damage to Structure (explosives, breach, environment)	X		Variable
Equipment Theft	X		Variable

Notes and Observations

- *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

1. The CISSP and CAP Prep Guide – Platinum Edition, Wiley Publishing Inc., 2007, Ronald L. Krutz and Russell Dean Vines
2. 2006 Internet Crime Report, National White Collar Crime Center and the Federal Bureau of Investigation, www.fbi.gov/page2/march07/ic3031607.htm
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
4. Cybercrime – Piercing the Darkness, http://library.thinkquest.org/04oct/00460/prevention.html
5. Studies and Surveys of Computer Crime, M.E. Kabay, Ph.D, CISSP, http://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf
6. http://www.crime-research.org/news/2002/11/Mess0903.htm