

# Overview of Cybercrime



## CJ341 – Cyberlaw & Cybercrime Lecture #2

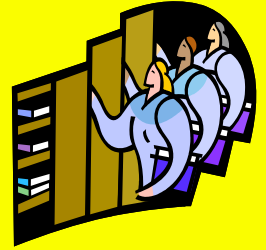
M. E. Kabay, PhD, CISSP-ISSMP  
D. J. Blythe, JD  
School of Business & Management

1

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Topics

- Computers and Crime
- Fundamentals of IA
- Computers and Crime
- Terminology
- Criminal Hacker Propaganda



2

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Computers and Crime (1)



- Computers can play three roles in crime
  - ❑ Target
  - ❑ Tool
  - ❑ Repository of evidence
- Information assurance attempts to reduce vulnerabilities of systems to attacks
- Secure design and programming try to reduce vulnerabilities of code to misuse
- Cyberforensics provide methods for securing evidence from computers and networks

3

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Computers and Crime (2)



- Computer crime always is directed against a computer – everything else is computer-related crime
- Computers as the victim or target
  - ❑ Theft (as a byproduct of an attack against a computer)
  - ❑ Vandalism
  - ❑ Denial of service
  - ❑ Malware targets: viruses, worms, Trojans
- Computers as tools
  - ❑ Fraud
  - ❑ Identity theft
  - ❑ Industrial espionage
  - ❑ Information warfare
- Computers as repositories of evidence
  - ❑ Logs
  - ❑ Journals
  - ❑ Documents
  - ✓ Michigan v Miller (see later in notes)

4

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Fundamentals of IA: What are We Protecting?



- The Classic Triad
- The Parkerian Hexad
  - ❑ Confidentiality
    - ✓ Confidentiality & Possession Losses
  - ❑ Possession
  - ❑ Integrity
    - ✓ Integrity & Authenticity Losses
  - ❑ Authenticity
  - ❑ Availability
    - ✓ Availability & Utility Losses
  - ❑ Utility

5

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## The Classic Triad



C – I – A

6

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## The Parkerian Hexad



Protect the 6 *atomic elements* of INFOSEC:

- Confidentiality
- Possession or control
- Integrity
- Authenticity
- Availability
- Utility

7

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Why “Parkerian?”



8

son. All rights reserved.

## Confidentiality



Restricting access to data

- Protecting against unauthorized disclosure of *existence* of data
  - ❑ E.g., allowing industrial spy to deduce nature of clientele by looking at directory names
- Protecting against unauthorized disclosure of *details* of data
  - ❑ E.g., allowing 13-yr old girl to examine HIV+ records in Florida clinic



9

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Possession



Control over information

- Preventing physical contact with data
  - ❑ E.g., case of thief who recorded ATM PINs by radio (but never looked at them)
- Preventing copying or unauthorized use of intellectual property
  - ❑ E.g., violations by software pirates



10

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Confidentiality & Possession Losses



- Locating
- Disclosing
- Observing, monitoring, and acquiring
- Copying
- Taking or controlling
- Claiming ownership or custodianship
- Inferring
- Exposing to all of the other losses
- Endangering by exposing to any of the other losses
- Failure to engage in or to allow any of the other losses to occur when instructed to do so

11

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Integrity



Internal consistency, validity, fitness for use

- Avoiding physical corruption
  - ❑ E.g., database pointers trashed or data garbled
- Avoiding logical corruption
  - ❑ E.g., inconsistencies between order header total sale & sum of costs of details



12

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Authenticity

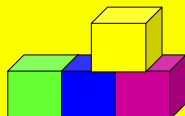
Correspondence to intended meaning

### ➤ Avoiding nonsense

- ❑ E.g., part number field actually contains cost

### ➤ Avoiding fraud

- ❑ E.g., sender's name on e-mail is changed to someone else's



13

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Integrity & Authenticity Losses

- Insertion, use, or production of false or unacceptable data
- Modification, replacement, removal, appending, aggregating, separating, or reordering
- Misrepresentation
- Repudiation (rejecting as untrue)
- Misuse or failure to use as required

14

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Availability

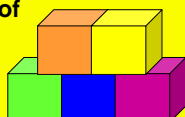
Timely access to data

### ➤ Avoid delays

- ❑ E.g., prevent system crashes & arrange for recovery plans
- ❑ Denial-of-service (DoS) attacks can be ruinous
- ❑ High-volume commercial sites can lose \$M

### ➤ Avoid inconvenience

- ❑ E.g., prevent mislabeling of files



15

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Utility

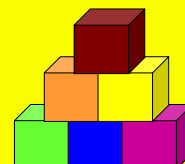
Usefulness for specific purposes

### ➤ Avoid conversion to less useful form

- ❑ E.g., replacing dollar amounts by foreign currency equivalent

### ➤ Prevent impenetrable coding

- ❑ E.g., employee encrypts source code and "forgets" decryption key



16

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Availability & Utility Losses

- Destruction, damage, or contamination
- Denial, prolongation, acceleration, or delay in use or acquisition
- Movement or misplacement
- Conversion or obscuration

17

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Michigan v. Miller (2001)\*

- Michigan housewife Sharee Miller
  - ❑ Pathological liar, schemer, sociopath
  - ❑ Met Missouri man Jerry Cassaday in Internet chat room
  - ❑ Miller concocted tales of abuse by her husband
  - ❑ Met and had sex with Cassaday
  - ❑ Told him she was carrying his child
  - ❑ But actually had tubal ligation
  - ❑ Claimed husband Bruce was in organized crime (really ran salvage yard)
- Cassaday killed Bruce Miller with a shotgun.
  - ❑ Miller dropped Cassaday after murder
  - ❑ Cassaday shot himself
  - ❑ Left logs of e-mails and IM



18

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Michigan v. Miller\* (cont'd)



*"Michigan vs Miller is a classic murder triangle that was planned over the Internet. The news media at the time was claiming that this was the first prosecution where the Internet was key in the planning of a murder. . . . The case itself was made from a briefcase left behind by a jilted lover, an ex homicide detective, who committed suicide. Jerry Cassaday had driven to Michigan and killed Bruce Miller, Sharee Miller's husband."*

*Computer Forensics played a major part in building the history of the seduction and validating evidence left by Jerry Cassaday. Prosecutors clearly state that without the computer forensic evidence, no prosecution would have been possible.*

*Sharee Miller [went to] prison for Conspiracy to Commit First Degree Murder – Life Sentence and Second Degree Murder – 54-82 years. . . ."*

\* <http://www.secureworldexpo.com/events/conference-details.php?cid=446>

Also <http://www.examiner.com/list/sharee-miller-where-she-is-now-timeline>

19

## Terminology and References



### ➤ CJ341 materials

□ <http://www.mekabay.com/courses/academic/norwich/cj341/index.htm>

### ➤ Learn basic terms: see *Glossary* and texts

□ Glossary available online

✓ <http://www.mekabay.com/overviews/glossary.htm>

✓ <http://www.mekabay.com/overviews/glossary.pdf>

### ➤ Other reference materials

□ <http://www.mekabay.com/overviews/index.htm>

□ <http://www.mekabay.com/methodology/index.htm>

### ➤ Department of Justice Cybercrime site

□ <http://www.justice.gov/criminal/cybercrime/>

□ Constantly updated list of press releases and documents about computer-related crime

20

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Criminal Hacker Propaganda



1. "I don't know why you system guys are getting your shorts in a knot: we're just looking around – we're not doing any harm." – *Eric Corley ~1996 at a panel discussion organized by the NCSA*
2. "Breaking into your systems is doing you a favor by showing you your vulnerabilities so you can fix them."
3. "Vandalizing Web sites / writing viruses / creating denial-of-service attacks improves security by forcing manufacturers to improve their products."
4. "Information wants to be free."

21

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Propaganda from IP Thieves



1. "Everyone's doing it."
2. "We won't get caught."
3. "It's the music / software industry's fault: if they don't want theft, they should charge less."
4. "It's the producers' fault: if they don't want theft, they should make it technically impossible."
5. "It doesn't hurt anyone."
6. "It only hurts a company — I wouldn't steal it from an individual."
7. "The music industry is violating the rights of the musicians, so breaching copyright is a Good Thing."
8. "Our theft is helping the software / music industry increase their sales."
9. "No software / music / art should ever be copyrighted — it should always be free."
10. "But I need it and I don't want to pay for it."

22

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## IS340 Class Notes about Computer Crime



### IS340 Lectures

[http://www.mekabay.com/courses/academic/norwich/is340/is340\\_lectures/index.htm](http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/index.htm) or <http://tinyurl.com/340-LECTURES>

- CSH5 Ch 2 History of Computer Crime
- CSH5 Ch 14 Information Warfare
- CSH5 Ch 15 Penetrating Computer Systems and Networks
- CSH5 Ch 16 Malicious Code
- CSH5 Ch 17 Mobile Code
- CSH5 Ch 18 Denial-of-service Attacks
- CSH5 Ch 19 Social Engineering and Low-Tech Attacks
- CSH5 Ch 20 Spam, Phishing and Trojans

CSH5 = Bosworth, Kabay & Whyne. *Computer Security Handbook*, 5<sup>th</sup> edition. Wiley, 2009.

23

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

# Now go and study



24

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.