A Framework of Distributed Agent-based Network Forensics System

Dr. Ren Wei

School of Information
Zhongnan University of Economics and Law
Wuhan, P.R.China 430064

Agenda

- Concepts
- Classification
- Approaches
- Goals
- Architecture
- Functions
- Tools
- Characters
- Challenges

Network Forensics

On the First DFRWS:

The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources …

What is it?

My Opinion:

- Digital Forensics in Network Environment
- E-evidence IN network obtained
- Obtain e-evidence VIA network

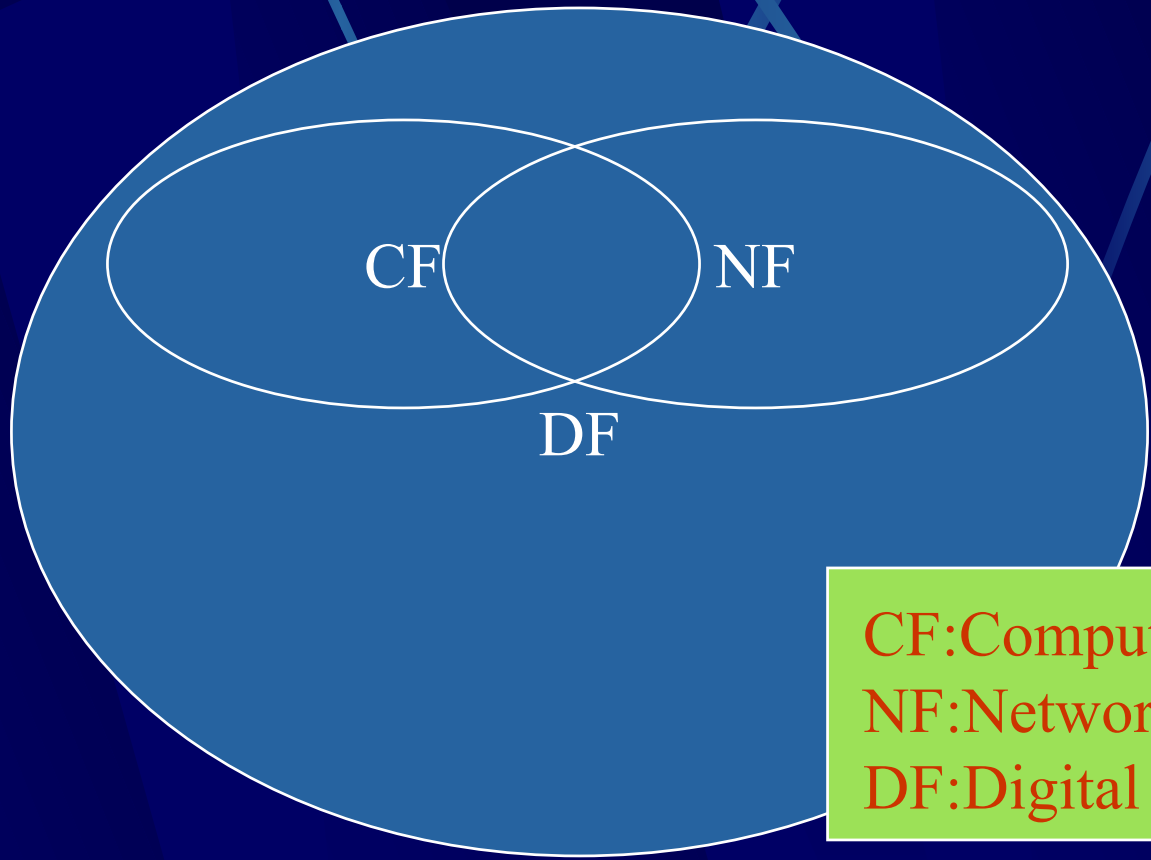
IN network

- Firewall log
- HIDS log
- NIDS alert
- Host System Event
- Network Packets

VIA network

- Log Analysis
- Log Integration
- Packet Capture
- Protocol Analysis
  - POP3,SMTP
  - FTP,TELNET,HTTP

Where is it?



CF:Computer Forensics
NF:Network Forensics
DF:Digital Forensics

Brother Or Child?

Internet Forensics

Wireless Forensics

Online Forensics

Approaches

- Packet Capture
- Packet Filter
- Protocol Analysis
- Data Fusion
- Distributed Agent
- Data Mining
- IP Traceback
- Mapping IP to Geographic Location

Goals

- Adaptive Capture of Network Traffic
- Integration of Forensics Data
- Active Response for Investigational Forensics
- Guide the Enhancement of Firewall and IDS system

System Architecture

- Network Forensics Database
- Network Forensics Server
- Network Forensics Distributed Agents

Server Function

- Build the Database of Mapping Topology
- Capture the Network Traffic
- Filter and Dump the Traffic Steam
- Transform Traffic Steam into Database
- Forensics Database Mining
- Network Protocol Analysis
- Network Surveying
- Network Attack Analysis and Visualization

Distributed Agent Function

- Integration with Distributed Firewall
- Integration with Distributed IDS
- Integration with HoneyNet
- Integration with the System Monitor
- Remote Network Forensics

Tools

- TcpDump/Windump
- Snort
- Ethereal
- VisualRoute
- SamSpade
- Nmap

Characters

- Adaptive
- Intelligent
- Cooperative
- Agent-based
- Distributed
- Integrative

Challenges

- Custody of Chain
- Privacy Protection vs Traffic Monitor
- Encrypted Traffic
- Traffic Volumes
- Covert Channel
- IP Spoof/Compromise Hops
- Anti Sniff

Web Site

- DFRWS
- IJDE (International Journal of Digital Evidence)
- JDI (Journal of Digital Investigation)
- National Center for Forensic Science
- Economic Crime Institute (ECI)
- SANS institute
- Global Information Assurance Certification
- FIRST
- CERT Coordination Center
- CERIAS

Reference

- Ren Wei, “On The Reference Model of Distributed Cooperative Network Forensics System”, Proceeding of The Sixth International Conference on Information Integration and Web-based Application & Services (iiWAS2004), Jakarta, Indonesia, 2004, Austrian Computer Society.
- Ren Wei, “On A Conceptual Model of Network Forensics System for Information Security”, Proceeding of The Third International Conference of Information Systems Technology and its Applications (ISTA2004), Salt Lake City, UT, USA, Lecture Notes for Informatics, Germany.
- Gary, P. “A Road Map for Digital Forensic Research”, Technical Report DTRT0010-01, DFRWS, November 2001.
- Brian Carrier. “Defining Digital Forensics Examination and Analysis Tools”. In Digital Forensics Research Workshop II, 2002.

Acknowledgement

Dr. Hai Jin

Cluster and Grid Computing Lab,
School of Computer Science,
Huazhong University of Science and Technology,
Wuhan, P.R.China

Q&A

renw@public.wh.hb.cn