A Framework of Distributed Agent-Based Network Forensics System

By
Ren Wei

Presented At
The Digital Forensic Research Conference
DFRWS 2004 USA  Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
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
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


Acknowledgement

Dr. Hai Jin

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