On the Reliability of Current Generation Network Eavesdropping Tools

Second IFIP WG 11.9 International Conference on Digital Forensics
30 January 2006

Eric Cronin, Micah Sherr, Matt Blaze
Department of Computer and Information Science
University of Pennsylvania

http://www.cis.upenn.edu/~dsl/
Outline

- Background: Who are we? What are we doing?
- Some earlier results
- Challenges to reliable IP eavesdropping
- Evaluation of current tools
- Recommendations
Background: Who are we?

Trustworthy Network Eavesdropping and Countermeasures (TNEC) project

- NSF-funded research program to explore:
  - alternatives to cryptography for communications security
  - eavesdropping-resistant networks
  - eavesdropping-friendly networks
  - evaluation of existing interception technologies
    - In theory, unencrypted communication may be monitored.
    - but are practices susceptible to simpler (non-cryptographic) countermeasures that thwart eavesdropper?

- Unclassified, open-ended research project

- Focus primarily on Internet and emerging network technologies (e.g., sensor networks)

- Partly driven by lawful intercept requirements
Getting started: Evaluate state of eavesdropping

- Baseline of existing eavesdropping capabilities needed to evaluate new networks
- Look at general communications systems (not just computer networks)
  - Telephone network
  - Local area network
  - Internet

- Evaluation of telephone surveillance
- Number of previously known threats: detection, obfuscation (encryption), denial of service
- Identified several new threats specific to law enforcement wiretaps
  - Loop Extender systems are pretty hopeless
  - CALEA systems have subtle configuration vulnerabilities
IP Networks

- Newer network
- Very different design
- More eavesdropping (both lawful and unlawful)
- More awareness
  - General assumption: Anything you send will be seen
- More countermeasures
IP Complications

- Decentralized control
- Heterogeneous implementations
- “Best-effort” delivery (unordered, unreliable, duplication)
- Complex shared state
- Dynamic routing
- Lack of authentication
- Ambiguous protocols, implementations, configurations
Intercept fidelity

- Goal: perfect fidelity for captured communication
- But complications on previous slide make this impractical
  - Requires a perfect simulation of network/hosts
- Eavesdropper may suffer from *evasion*, missing legitimate communications
- Eavesdropper may suffer from *confusion*, recording non-existent communications
The Eavesdropper’s Dilemma

➡ To prevent against evasion, eavesdropper must increase its *sensitivity*
  - Increased sensitivity makes confusion easier

➡ To prevent against confusion, eavesdropper must increase its *selectivity*
  - Increased selectivity makes evasion easier

➡ See any problems?
Hot spots for study

![Diagram showing communication and remote attitude]

- **IDS evasion**
- **Cryptography**
What about in between?

Remote Attitude

Hostile  Apathetic  Cooperative

Limited  Arbitrary

IDS evasion  cryptography

IFIP WG 11.9 ’06 – Eavesdropping Tools – p. 11
Apathy doesn’t help the sender: IDS Evasion has already found most of the protocol loopholes
  - More diverse topologies
  - No deliberate normalization
Apathy doesn’t help the sender: IDS Evasion has already found most of the protocol loopholes
- More diverse topologies
- No deliberate normalization

But the eavesdropping tools are much worse...
How bad are the tools?

▸ Scenario:
  ◾ On a hostile LAN, sending e-mail to remote SMTP server
  ◾ Eavesdropper on LAN
  ◾ SMTP server does not support SSL/TLS

▸ Goal: Eavesdropper should not know contents of your e-mail

▸ Solution: [Ptacek and Newsham 98] + a few twists

▸ Result: 100% success, plus half the time a cover message seen instead
The guilty parties

▸ Open Source
  - Bro
  - Chaosreader
  - Ethereal
  - Snort
  - tcpick
  - tcptrace
  - tcpflow

▸ Commercial
  - CommView
  - NetworkActiv
  - Sniffem
**Technique 1: MAC confusion**

- Hosts on the same Layer 2 LAN addressed by MAC addresses
- If an IP address is not local, MAC of gateway used
- Noise/cover traffic generated with correct IP, incorrect gateway MAC
- Only packets with correct MAC reach server
- Eavesdropper ignores Layer 2 headers, only reconstructs on IP address
Technique 2: TTL confusion

- IP packets contain a “Time-to-live” field; each router decrements
- When TTL == 0, packet is dropped
- Noise/cover traffic generated with small TTL
- Only packets with larger TTL reach server
- Eavesdropper assumes all packets reached the server
Example result (real)

Hello Dr. Watson,

This is a very secret message. Please don't give the contents to anyone.

Sincerely,
Mr. Holmes
Example result (Ethereal)
Notable measurements

- One tool failed with no confusion simply by breaking packets into 1B
- Only three tools reported any kind of anomaly (2 IDS, 1 normal)
- Five tools interpreted cover text
- Reliability of actual SMTP session unharmed
What can be done?

- **Enhancing sensitivity**
  - Eavesdropping tools like to arrive at a single result for reconstructed communications
  - Essentially discards all other possible interpretations
  - High-speed links pose new problems

- **Enhancing detection and selectivity**
  - No heuristics employed to determine most likely reconstruction
  - No notification of suspicious traffic
  - No correlation of other network events (ICMP)

- **Active eavesdropping**

- **Deliberate placement**
  - The closer to the receiver (and farther from the confuser) the more accurate
Questions?