A Proposed Intrusion Detection System for Encrypted Computer Networks

by

Nesreen Kamel

IT Dept., Faculty of Computers & Information, Cairo University
Agenda

1. Network Security & Intrusion Detection

2. NIDS Deployment in Encrypted Computer Networks

3. Key Recovery Encryption Systems

4. The Proposed Intrusion Detection System

5. Conclusion & Future Work
Network Security

- Systems are becoming more vulnerable
- Attackers are getting smarter, stealthier, and more bold
- Different security mechanisms used to enforce security properties
Network Security

Attack Prevention
- Methods of preventing attacks before affecting the target
- Examples: Access Control, Firewalls

Attack Avoidance
- Methods of modifying information to make it unusable for the attacker
- Examples: Encryption

Attack Detection
- Methods report that a malicious activity is found
- Examples: Intrusion Detection Systems

A second line of defense should be identified...
Network Intrusion Detection Systems (NIDS)

Classical Detection Techniques

- Misuse Detection
  - Models well-known attacks as patterns
  - Scans the system for occurrence of such patterns

- Anomaly Detection
  - Models typical or expected behavior
  - Observes significant deviations from the reference model
In the late 1990s new mechanisms appeared designed in a more practical fashion. They don’t follow the classical techniques. The two commonly known:

- **Signature detection**
  - Observe the data stream for a match to an attack pattern.

- **Protocol anomaly detection**
  - Models normal Internet protocols’ usage based on published standards.

- **Stateful Protocol Anomaly Detection**
  - Monitors all the events within a protocol session.
Network Intrusion Detection Systems (NIDS)

NIDS Challenges

- Network Packet Reassembly
  - IP fragmentation evades NIDS

- Packet Loss on High Speed Networks
  - NIDS drops packets as speed increases especially under heavy loads

- Encryption
  - Attack detection is not applicable when encryption is employed in the network
Network Packet in Cipher text form

Network Packet in plain text form

Packet “headers” (TO, FROM, TYPE OF DATA, etc.)

Packet “payload” (data)

Perform packet inspection (Payload + Header)

Encryption

Undetected Attack

OK

http://www.freesurf.com/downloads/Gettysburg

Attack
Two possible solutions

- Preserve encryption keys on the router (encrypt/decrypt on the fly)
  - Hard to manage the keys
  - A compromised router exposes all the company traffic

- Use a distributed NIDS with micro agents on mission critical hosts (reading the data stream post decryption)
  - Agents are dependent on the host platform
  - Agents affect the performance of the hosts
Idea of Proposed Solution

- Providing an authorized decryption capability to the NIDS
- This can be done by the so called key recovery encryption systems
Key recovery encryption systems (Unlike traditional encryption systems) provide an authorized decryption capability.

- Allow authorized persons to obtain the keys & decrypt the cipher text.
- By sending the session secret key with each ciphered session.
- The session secret key is formatted in a special field (Data recovery field DRF).
Key Recovery Encryption Systems

User Security Component

Data Recovery Component

Recovery Keys & other information

Plaintext Data

Key K

Encrypt

DRF + Cipher text

Key K

Decrypt

Determine Key K

Decrypt

Plaintext Data
Key recovery provides an authorized decryption capability to the NIDS

By attaching an Intrusion Detection Access Field (IDAF) to encrypted data
The Proposed Intrusion Detection System

**Key Recovery (USC)**

- **Client**: Application Encryption → Cipher text Data → IDAF Cipher text Data → Encrypted Packet
- **Server**: Cipher text Data → IDAF → Cipher text Data → Key Recovery (USC)

**USC Attaches Intrusion Detection Access Field (IDAF)**

NIDS sniffs packets from the network media

**Monitoring Data after Decryption**

- Key Recovery (DRC)
- IDAF Decode, Data Decryption

**Apply NIDS Techniques to Plain Text Data**

**Recovery Agent (RAC)**

- Recovery Keys
Performance Evaluation

Network Traffic Overhead

Percentage of Network Traffic Overhead

RSA Key Length in Bits

- 512: 7.4%
- 1024: 13.5%
- 2048: 25.9%
## Performance Evaluation

### Processing Time Overhead

<table>
<thead>
<tr>
<th>RSA Key Length (bits)</th>
<th>Processing Time Overhead (Milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>196.8</td>
</tr>
<tr>
<td>1024</td>
<td>256.2</td>
</tr>
<tr>
<td>2048</td>
<td>273.9</td>
</tr>
</tbody>
</table>
Conclusion & Future Work

- Application of key recovery procedures
  - Provides the NIDS an authorized decryption capability
  - Allows encryption & NIDS to be used side by side
    - Provided with a little overhead (Network & Processing overheads)
  - Restricts the avenues available to attackers to hide their abuse using encryption
The proposed approach provides a set of benefits

- Detection of attacks in application-level protocols embedded in encrypted sessions
- Application of protocol anomaly detection approach
  - Detection of known & unknown attacks
- Application of statistical & stateful inspection techniques
  - Support session & application-level intrusion detection
- Attack detection in FTP sessions
Future Work

- Use of state transition analysis in protocol specification implementation
  - Develop a protocol state machine
  - Use Markov chains to learn transition probabilities

- Use of covert channels to add key recovery information
  - Interoperability
  - Filterability

- Intrusion prevention support
  - Working inline to prevent attacks by dropping packets
  - Deflect attacks against any part of the protected system
Thanks

Questions?