A Survey of Connection-Chains Detection Techniques

Ahmad Almulhem and Issa Traore

Department of Electrical and Computer Engineering
University of Victoria

2007 IEEE Pacific Rim Conference on
Communications, Computers and Signal Processing

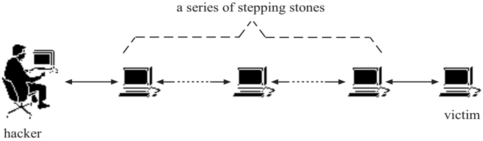
Outline

1. Introduction
2. Network-Based Approaches
3. Host-Based Approaches
4. System-Based Approaches
5. Summary

Outline

1. Introduction
2. Network-Based Approaches
3. Host-Based Approaches
4. System-Based Approaches
5. Summary

Connection Chains

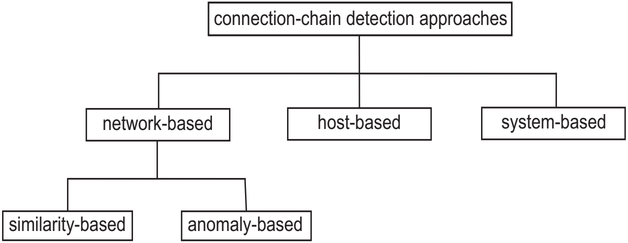


Connection chain

A set of tcp connections created by sequentially logging into a series of hosts, known as stepping-stones [Staniford-Chen 1995, Zhang 2000].

- Used to carry attacks indirectly.
- Avoid disclosing true origin of attack.
- Stay anonymous!

Taxonomy

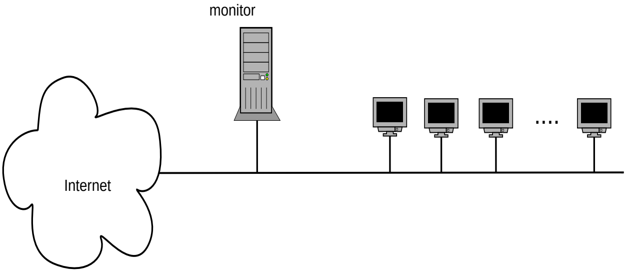


- Taxonomy is based on the location of analysis.
- Network-Based: analyze packets at network level.
- Host-Based: operates inside a host.
- System-Based: use network-based and host-based components.

Outline

1. Introduction
2. Network-Based Approaches
3. Host-Based Approaches
4. System-Based Approaches
5. Summary

Overview

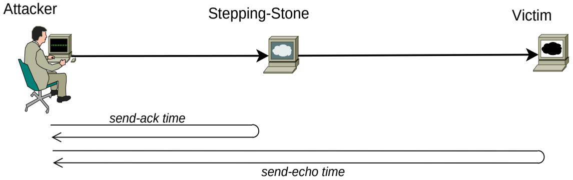


- Analyze packets/connections in a controlled network.
- Two types of network-based approaches:
    - Similarity-based: Find similarity between connections.
    - Anomaly-based: Analyze each connection alone.

Similarity-Based

- Apply similarity measures to compare the connections.
- Two types of similarity measures:
    - Content-based: analyze packets' contents (payloads).
        - Text Matching [Zhang and Paxon, 2000].
        - Compute character frequencies [Staniford-Chen and Heberlein, 1995].
    - Timing-based: analyze packets' timing.
        - Inter-packet delay [Wang et.al., 2002].
        - Typing pattern (On/Off) [Zhang and Paxon, 2000].

Anomaly-Based



[Yung, 2002]

- Compare send-ack time with send-echo time.
- send-echo time gets larger as the connection-chain gets longer.

Outline

1 Introduction

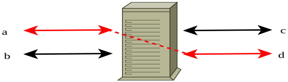
2 Network-Based Approaches

3 Host-Based Approaches

4 System-Based Approaches

5 Summary

Host-Based Approaches



- Link two connections at a host (a and d in the figure).
- Two types of host-based approaches proposed:
  - Search processes [Carrier and Shields (2004)], [Kang et.al. (2004)].
  - Modify OS [Buchholz and Shields(2002)].

Outline

1. Introduction
2. Network-Based Approaches
3. Host-Based Approaches
4. System-Based Approaches
5. Summary

System-Based Approaches

- Employ host-based and network-based components.

  Example: DIDS [Snapp et.al. 1991]
  - Monitors installed in every host.
  - A Director module receives data from the monitors for analysis.
  - Unique network user identifications (NID) used to track users.

Outline

1 Introduction

2 Network-Based Approaches

3 Host-Based Approaches

4 System-Based Approaches

5 Summary

Summary

- A connection chain refers to the set of connections created by sequentially logging into a series of hosts.
- Attackers use them to stay anonymous.
- Detection approaches: Network-based, Host-base and System-based.