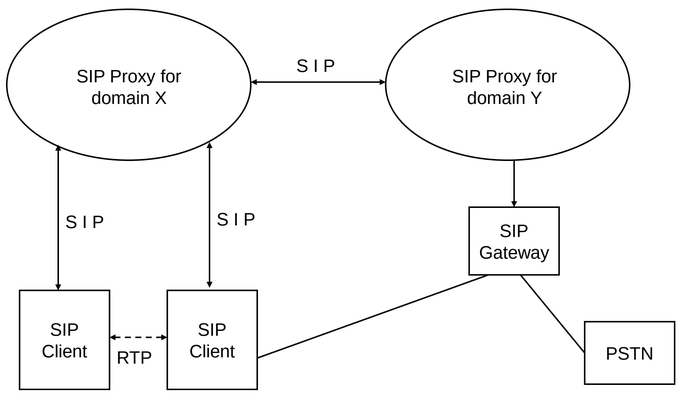
SCIDIVE : IDS for Voice-over-IP Environment

Dependable Computing System Lab

YuSung Wu, Ratsameetip Wita, Saurabh Bagchi

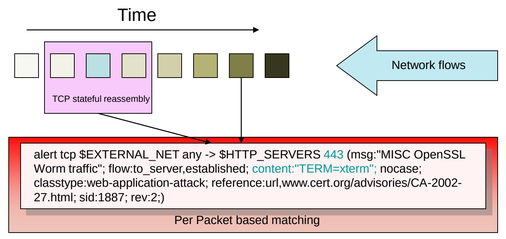
VoIP Overview



Motivation : Threats against VoIP System

- **Misrepresentation**
  - Presentation of a false caller ID name or number with the intent to mislead
  - False impersonation of the voice of a caller with the intent to mislead
- **Call Hijacking**
  - Through the Registrar (Tampering with the SIP Proxy server.)
  - Mid-session attacks (Re-invitation)
- **Theft of service**
  - Bypassing the SIP Proxy for billing
  - Unauthorized deletion or altering of billing records
- **Denial of Service**
  - Premature BYE to tear down connection
  - RTP based attacks to disrupt voice quality
- **SPAM/SPIT**
  - Telemarketing calls
- **Snooping & Call Tracking**

VoIP IDS : How's current IDS

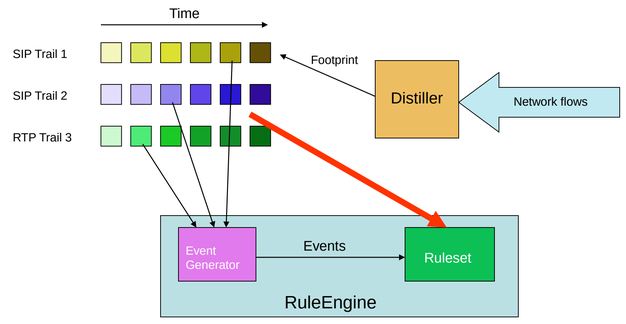


- Current IDS's not well suited for VoIP Intrusion Detection
- E.g.: Snort's ruleset is based on per packet pattern matching. It provides very limited matching capabilities across packets.
- Stateful detection is missing for VoIP. E.g., in Snort, the stream4 reassembly module only works for TCP

SCIDIVE IDS for VoIP

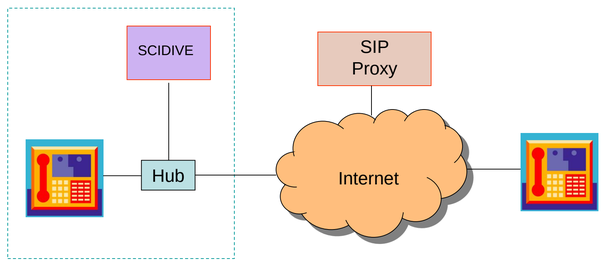
- Innovations
  - Cross-Protocol and Stateful detection
  - Can be operated in end-point only mode [Mode I]
  - Also support distributed detection when deployed on multiple points in the system [Mode II]

The Cross-Protocol & Stateful Methodology for detection



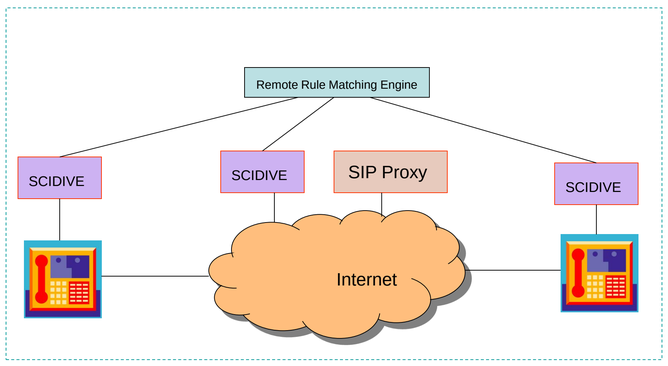
End-point only operation mode (mode I)

- A SCIDIVE-enabled-IDS engine sits on/close to the end-point and operates independently.
- It aims at protecting the end-point only.
- Simple and easy to maintain.



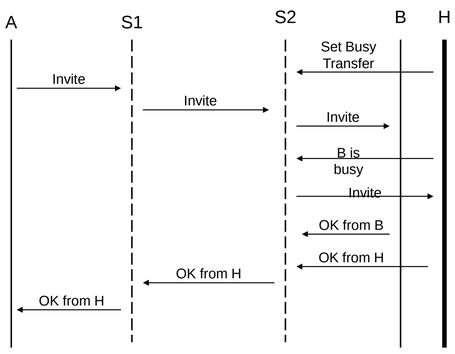
IDS Protected Area

Distributed detection mode (mode II)



IDS Protected Area

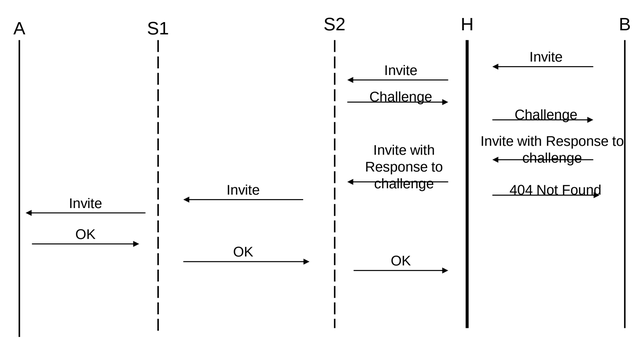
Call Hijacking (at start)



Detect Call Hijacking (at start)

- Mode I
  - SCIDIVE at S2 can observe the redundant OKs (OK from B and OK from H). However, A will not be alerted due to lack of collaboration with SCIDIVE on A.
  - SCDIVE at A can't detect this attack.
- Mode II
  - Check if the OK reply from B goes correctly all the way from B to A. The correlation is done across events at B, S2, S1, and A.

Man in the middle attack: intercepting outgoing calls



Detect Man In The Middle Attack

- Mode I
  - Can't detect this attack
- Mode II
  - This can be detected with an end-to-end matching rule for the OK message going correctly all the way from A to B through S1 and S2.

Future Work

- Collaborative IDS Engines deployed at endpoints, proxies, gateways and other network elements.
  - Potential to detect a broader set of attacks
  - Potentially lower false positives
- The SCIDIVE architecture can be extended to support other protocols and applications. It is potentially possible to become a general purpose IDS.
- Use machine learning to perform anomaly detection based on user profiles.