VOIP INTRUSION DETECTION SYSTEM WITH SNORT

Pavol Číž
Ondrej Lábaj
Pavol Podhradský
Juraj Londák

Presentation by Juraj Blichár
Introduction

- Proposal of protection model
  - focused on signaling DoS attack
- Detection of malfunction of the software exchange Asterisk
- Serve as a base during creation, testing and evaluation of security policies in "HBB-NEXT" project
VoIP & security...why together?!

- Circuit switched domains had/has easily predictable issues in security manner
- There was only limited set of services in legacy systems.
- NOW – Migration to packet based domains is here...
  - Voice is going to be transmitted only via IP networks
VoIP & security…why together?!

- It brings more service oriented BUT also complex voice systems based on Next Generation Networks.
Threats classification

- Social Threats
  - Mispresentation
  - Spam of Call – SPIT
  - Phishing
- Man in the Middle
  - Eavesdropping
  - Packet spoofing
  - Replay attack
- Service abuse

- Denial of Service
  - Signaling DoS Attacks
  - Media DoS Attacks
  - Physical DoS Attacks
What is IDS/IPS?

- **IDS** – Intrusion Detection System
  - Well known from IP networks
  - Proactive identification of potential security attacks
- **Detection techniques:**
  - anomaly detection
  - misuse detection
- **IPS** – Intrusion Prevention System
  - Extension of IDS
  - Actively prevent/block malicious attacks
Protection model

- Components
  - Sip server: Asterisk 10.0.0
  - IDS: Snort 2.9.1
  - Traffic generator: SIPp 3.1
  - OS: Debian 6.0.2
- SIPp
  - free Open Source test tool / traffic generator
- Snort
  - free, open source network intrusion detection and prevention system
Experiment

DoS Attacker
SIPp

INVITE flooding

PBX Asterisk

Server unreachable

VoIP Phones

IDS Snort

Attack Detection
Scenario

- UAC scenario
  - SIPp – client, INVITE flooding attack
    - INVITE ----> 
    - 100  < -----
    - 180  < -----
    - 183  < -----
    - 200  < -----
    - ACK ----> 
    - Pause [0ms]
    - BYE ----> 
    - 200  < -----
  - Snort as a IDS, sends defined alert message
Results

- two tasks
  - cause malfunction of the exchange
    - 70 second and 65462 messages were sent
    - only 6524 processed
    - server unreachable
  - detect a DoS attack

```plaintext
[**] [1:10000001:0] DoS [**]
[Priority: 0]
02/08-15:20:42.295606 147.175.178.83:138 -> 147.175.178.255:138
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:256 DF Len: 228
```
What next?

- find other variants of DoS rules or rules of other types of attack
- results will be used in HBB-NEXT project
  - as a base during creation, testing and evaluation of security policies enforced by security manager
Acknowledgement

This paper also presents some of the results and acquired experience from various research projects such as

- **HBB-NEXT, FP7-ICT-2011-7, No. 287848,**
- NGNlab.eu project,
- LdV IntEleCT project,
- Slovak National basic research project VEGA No. 1/0720/09,
- European Celtic-EURECA project Netlab
Thank you for your attention!