Fraud detection with OpenSIPS 2.1
- workshop -

Vlad Paiu

OpenSIPS Developer

OpenSIPS Solutions

Fraud detection with OpenSIPS 2.1
- workshop -

Background

- account hijacking: classic issue with any VoIP platform
- no attempts have been made to standardize detection procedures

Fraud detection with OpenSIPS 2.1

- workshop -

- Actual stolen accounts
  - Weak passwords
- Badly configured phones
  - Unchanged default passwords

- Exploits in the phone software

- Traffic is valid, does not look like an attack until the user starts complaining about the bill

Fraud detection with OpenSIPS 2.1

- workshop -

<u>*Approaches to the problem of "detecting fraudulent calls"*</u>

- complex model (30+ day span) which detects changes in user dialing pattern
  - difficult to validate (false positives)

- event-based threshold alerting system which monitors a set of call-related parameters
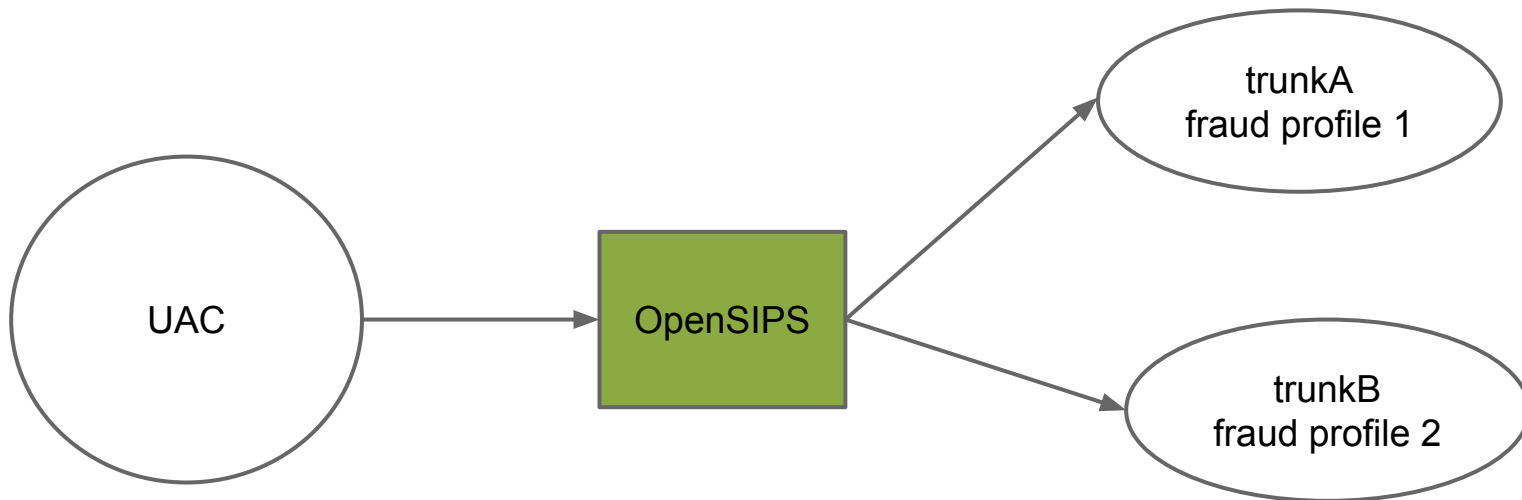
Fraud detection with OpenSIPS 2.1
- workshop -

New OpenSIPS module: fraud_detection

- closely monitors a set of five call-related parameters
  - CPM
  - call duration
  - sequential calls (to same destination)
  - concurrent calls
  - total calls
- above parameters are saved per each **[Subscriber, Destination]** pair

Fraud detection with OpenSIPS 2.1
- workshop -

Fraud detection with OpenSIPS 2.1
- workshop -

Resources

- fraud detection tutorial for OpenSIPS 2.1+
  - http://www.opensips.org/Documentation/Tutorials-FraudDetection-2-1

- fraud_detection module documentation
  - http://www.opensips.org/html/docs/modules/2.1.x/fraud_detection

- IRC / mailing list

Fraud detection with OpenSIPS 2.1

- workshop -

?