SPAM over Internet Telephony

and how to deal with it

Rachid El Khayari, Nicolai Kuntze, Andreas U. Schmidt,
Fraunhofer Institute for Secure Information Technology SIT,
Darmstadt, Germany

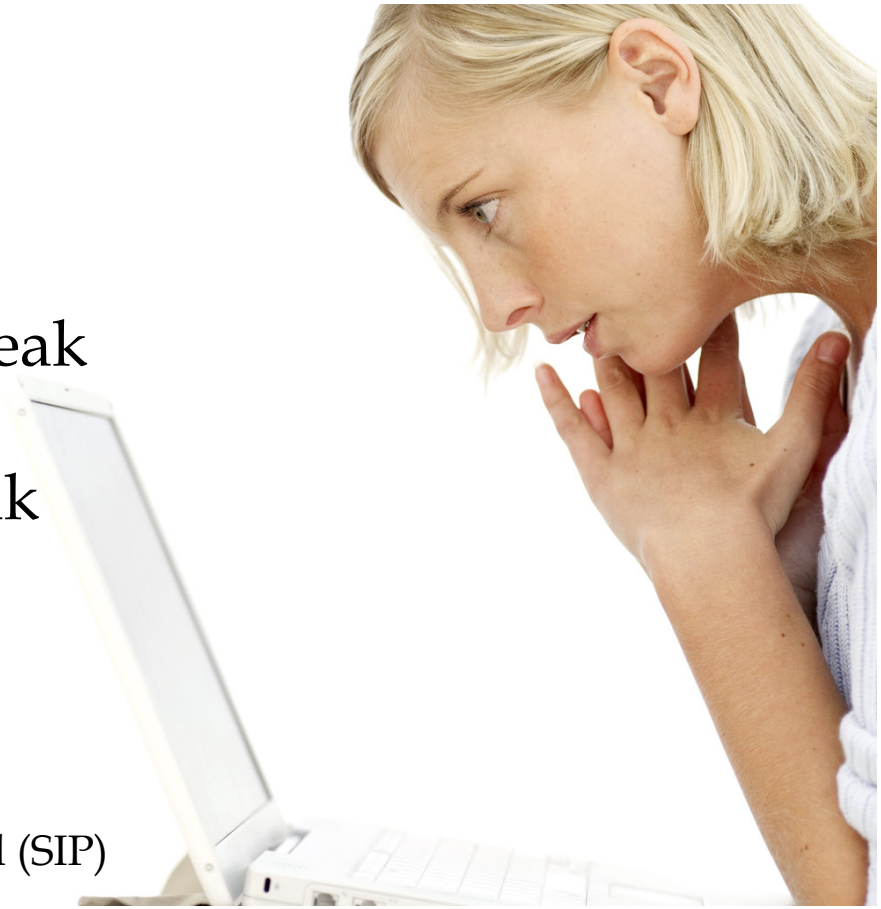
Special thanks to the presenter by proxy:
Alapan Arnab, T-Systems South Africa, Midrand

Introduction bird's eye view

- email spam is considered 80-90 % of email traffic
- threat can spread out on VoIP world
- SPAM over Internet Telephony (SPIT) even more fatal (higher disturbance)
  - email at 4 p.m. vs. call at 4 p.m!

Introduction
Agenda

- What is SPIT?
- What are state of the art SPIT countermeasures?
- Do the countermeasures have weak points?
- How can an attacker exploit weak points ?



Note:
Discussion is based on Session Initiation Protocol (SIP)

What is SPIT?

A first approach

What is SPIT?

- SPIT vs. SPAM
- Similarities:
  - both are unwanted messages
  - attackers use Internet to target victims
- Differences:
  - email is an asynchronous service
  - VoIP is a synchronous service
  - email contains content within the message
  - VoIP content is exchanged after! session initiation

What is SPIT?
SPIT vs. SPAM

- Consequences of Differences:
  - email spam recipient can decide whether to read emails or not or read them later
  - SPIT recipient doesn't have this freedom, as phone rings immediately
  - email spam content can be analyzed before a message is delivered
  - SPIT content can't be analyzed before phone rings

If the phone rings, it's too late for SPIT prevention and the phone rings immediately!

Now we know what SPIT is not

and not what SPIT is!

What is SPIT?
Intuitive SPIT definition

- Some SPIT definitions:
  - unwanted or bulk or unsolicited call
  - unsolicited advertising calls
  - transmission of bulk unsolicited messages and calls
  - a bulk unsolicited set of session initiation attempts, attempting to establish a voice, video, instant messaging, or other type of communications session
- Problem with these definitions:
  - either to specific or to general
  - don't cover all facets of SPIT

What is SPIT?
SPIT analysis

- How can we find a better definition?
  - What is the goal of an attacker?
    - establish a communication session with as much victims as possible in order to transfer a message to any available endpoint
  - How can he achieve this goal?
    1. Systematic gathering of contact addresses of victims
    2. Establishment of communication sessions to the victims
    3. Media transfer

Fundamental 3 Steps of SPIT

What is SPIT?
Step 1 – Information gathering

- We differ two type of contact addresses:
  1. Temporary SIP URIs
     (e.g. <sip:someone@192.0.2.5>)
  2. Permanent SIP URIs
     (e.g. <sip:someone@example.com>)
- Scan attack:
  - Attacker scans network to find out:
    - Temporary URIs
    - Permanent URIs
    - Or both

What is SPIT?
Step 1 – Information gathering

- Scan attack (permanent URIs):
  - Attacker has knowledge about numbering scheme of a provider (e.g. 555XXXX)
  - Attacker sends INVITE request to all possible targets (e.g. 5550000-5559999)
  - Answer is '404 Not found'
    - Number unassigned
  - Answer is '480 Temporarily unavailable'
    - Number is assigned, user offline
  - Answer is '200 OK'
    - Number is assigned, user available
  - Silent version of this attack:
    - Send 'OPTIONS' request or other adequate SIP request

What is SPIT?
Step 1 – Information gathering

- Scan attack (temporary URIs):
  - Same procedure as with permanent URIs
    - Additionally extract IP Address from 'Contact' header of SIP response
  - What if IP address is not submitted?
    - Brute force
  - Attacker has knowledge, that provider assigns IP addresses from range 192.0.2.5-192.0.2.155
    - Send 'INVITE' requests to UDP Port 5060 to all IP addresses of range
    - Try out all possible numbers (e.g. 5550000-5559999)
  - Last method is exhaustive but excludes SIP Proxy

What is SPIT?
Step 2 – Session establishment

- Two ways possible for session establishment:
  - SPIT via Proxy
    - Attacker uses permanent URIs as target
    - Advantage: Permanent URIs are easy to collect
    - Disadvantage: Attacker needs valid accounts, because SIP Proxy/Registrar is involved
  - Direct IP SPIT
    - Attacker uses temporary URIs as target
    - Advantage: Attacker doesn't need valid accounts
    - Disadvantage: Temporary URIs are harder to collect

What is SPIT?
Step 2 – Media transfer

- What kind of media is sent, depends on SPIT Scenario:
  - Call center:
    - Computer establishes calls
    - Dispatches call to call center agent
    - Agent talks with callee
  - Calling bots:
    - prerecorded messages are sent
  - Ring tone SPIT:
    - Ring tone is a message or
    - Goal of attacker is simply to disturb victim

Now we know what SPIT is exactly.

So, what has been done against it so far?

SPIT Countermeasures Overview

- Device Fingerprinting
- White-, Black-, Grey Lists
- Reputation Systems
- Turing Tests/Computational Puzzles
- Payments at Risk
- Intrusion Detection/Honey phones

SPIT Countermeasures Device Fingerprinting

- Assumption:
  - Attacker can be differed from ‘normal’ caller, as he uses special attack tools
- Passive fingerprinting:
  - Check order and presence of SIP header fields of e.g. ‘INVITE’
  - If header fingerprint doesn’t match standard clients -> classify as SPIT
- Active fingerprinting:
  - Challenge caller with unexpected SIP messages (e.g. ‘OPTIONS’)
  - If reaction doesn’t match behavior of standard clients -> classify as SPIT

SPIT Countermeasures
Device Fingerprinting - Weakness

- Passive fingerprinting:
  - Attacker simply needs to order SIP headers like a standard Client
- Active fingerprinting:
  - Attacker simply needs to behave like a standard Client
- Attack can be called Device Spoofing

- Practical Issues:
  - A lot of SIP User Agents exist (soft phones, hard phones)
  - Administrator must keep fingerprint list up to date
    - otherwise 'normal' calls will be blocked

SPIT Countermeasures
Black-, White-, Grey Lists

- Black Lists:
  - Calls from Identities, that are known as Spitters are blocked
- White Lists:
  - Only calls from ‘buddies’ are permitted, all others are blocked
- Grey Lists:
  - If caller calls first time and is not in White List, call is blocked
  - If he tries calling back within short time, call will be accepted
  - or callee consults grey list and decides, if he wants to accept future calls

SPIT Countermeasures
Black-, White-, Grey Lists - Weakness

- Black Lists:
  - If call is blocked, attacker simply needs to take on new identity
    - SPIT via Proxy: new Account is needed
    - Direct IP SPIT: SIP Identity Spoofing
- White Lists/Grey Lists:
  - Attacker needs to take on white listed identity
  - How to gather knowledge about white listed Identities
    - Direct IP SPIT: Brute force -> try out all possible Identities (exhaustive)
    - Distributed White Lists: Import White List with a valid account

- Practical Issues:
  - Black Lists can only be used to prevent future attacks from same identity
  - People usually get often calls from Identities, that are not white listed
    - e.g. call from bank employee (Introduction problem)
  - Grey List: decision basis for callee is just the phone number of caller
    - He must decide whether to accept future calls or not!

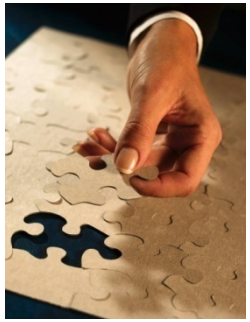
SPIT Countermeasures Reputation Systems

- After a call, callee can set a reputation value for caller
  - Spitters are e.g. marked with negative reputation value
  - Or 'normal' callers are marked positive reputation value
- User Feedback can be sent via SIP messages or additional headers
- Reputation value is displayed when a call is initiated
- Can be combined with Grey Listing in order to have a better decision basis

SPIT Countermeasures Reputation Systems

- User with a negative reputation value can be viewed as globally blacklistetd
  - obtain ‘fresh’ account to be able to place calls again
- Reputation value as SIP header can be spoofed in an Direct IP SPIT attack
- Ballot stuffing, Reputation Pushing:
  - User creates several accounts
  - Calls each other with this account
  - Feedbacks positively

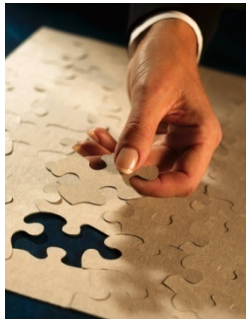
- Practical Issues:
  - Only future calls from caller with negative reputation are blocked
  - User must be classified often enough as Spitter in order to be blocked



SPIT Countermeasures
Turing Tests/Computational Puzzles

- Turing tests: Caller is given a challenge, that
  - human can solve easily
  - is hard to solve for a machine
- E.g. Audio CAPTCHA
  - IVR (Interactive voice response) system answers call
  - Challenges caller with a task (e.g. dial sequence '123')

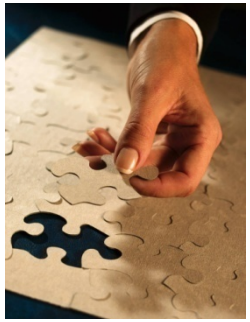
- Computational Puzzles:
  - User Agent (e.g. phone) of caller must compute a response to a challenge
  - E.g. finding a pre-image that will SHA1 hash to a correct image
  - Intention: Raise CPU costs



SPIT Countermeasures Turing Tests - Weakness

- Audio CAPTCHA can be relayed to human solver
- CAPTCHA Relay Attack:
  - If CAPTCHA is detected, dispatch call
  - pay cheap workers that are only hired for solving challenges
  - or set up a high traffic (e.g. toll free adult hotline) service and dispatch CAPTCHA to customers

- Practical Issues:
  - Very Intrusive
  - User Interaction is forced (e.g. every time a caller is not present in callee's white list)



SPIT Countermeasures Computational Puzzles - Weakness

- Attacker usually possess high CPU power
- Nothing except from CPU power is needed to bypass Computational Puzzles

- Practical issues:
  - 'Normal' callers usually don't have high CPU power in their hard phones
  - Therefore 'normal' users are bothered much as call delays will happen

SPIT Countermeasures Payments at risk

- Demand Payment from unknown callers
- If User A wants to call User B
  - A pays small amount to B
  - If B classifies A as 'normal' caller after session initiation money is paid back to User A
  - otherwise money is kept
- Goal: Raise costs for SPIT callers
- Combinable with White List
  - If user is not in White List demand Payments at risk
- Combinable with Reputation system
  - If reputation value is e.g. high allow call
  - If reputation value is e.g. low block call
  - If value is in between demand payment

SPIT Countermeasures
Payments at risk - Weakness

- If Combined with White List:
  - Bypassed in same way as White List
- If Combined with Reputation system:
  - Bypassed in same way as Reputation system
- If Payment is demanded for every call
  - SIP Identity Hijacking Attack:
  - Attacker can impersonate other accounts and
  - dispatch costs to 'normal' users

- Practical issues:
  - relative high costs required for micropayment
  - inequities in the value of currency between sender and recipient

SPIT Countermeasures
Intrusion Detection Mechanisms

- Detect intrusive behavior within a system:
  - Differ ‘normal’ calls and SPIT calls by characteristics, such as e.g.:
    - request intensity
    - error response intensity
    - parsing error intensity
    - number of different destinations
    - max number of dialogues in waiting state
  - Intrusive behavior will be detected as it will differ in these variables

SPIT Countermeasures
Intrusion Detection Mechanisms - Weakness

- Attacker can align behavior with behavior of 'normal' callers
- Call Rate Adaption Attack:
  - Change call rate while attacking
  - e.g. begin attack with 5 calls per hour and vary it up or down
- Account Switching Attack:
  - Use different accounts and spread statistical values across them
  - Statistics can't be correlated if originated from different sources

- Practical Issues:
  - Border line between normal and intrusive behavior must be set precisley
    - Otherwise: false positives and false negatives are produced
  - Statistical values are based on assumption, that are not verified

SPIT Countermeasures Honey Phones

- Can be viewed as part of Intrusion Detection Systems
- Part of a VoIP network, that can't be accessed by 'normal' users
  - E.g. If any users calls unassigned numbers
  - this can be viewed as an attack
- Good against Scan attacks

SPIT Countermeasures
Honey Phones - Weakness

- SIP Identity Hijacking is effective against Honey Phones
- Attacker impersonates accounts of ‘normal’ users
- Assumption that only attackers access Honey Phones is lapsed

- Practical Issues:
  - Attacker who already possesses list of valid assigned account doesn’t access Honey Phones at all

SPIT Countermeasures Summary - Weaknesses

- Attacker who can perform following attacks:
  - Device Spoofing
  - SIP Identity Spoofing
  - SIP Header Spoofing
  - Reputation Pushing or Pulling, Ballot Stuffing
  - CAPTCHA Relay Attack
  - SIP Identity Hijacking
  - Call Rate Adaption
  - Account Switching
- can bypass presented mechanisms

Countermeasures have weaknesses!

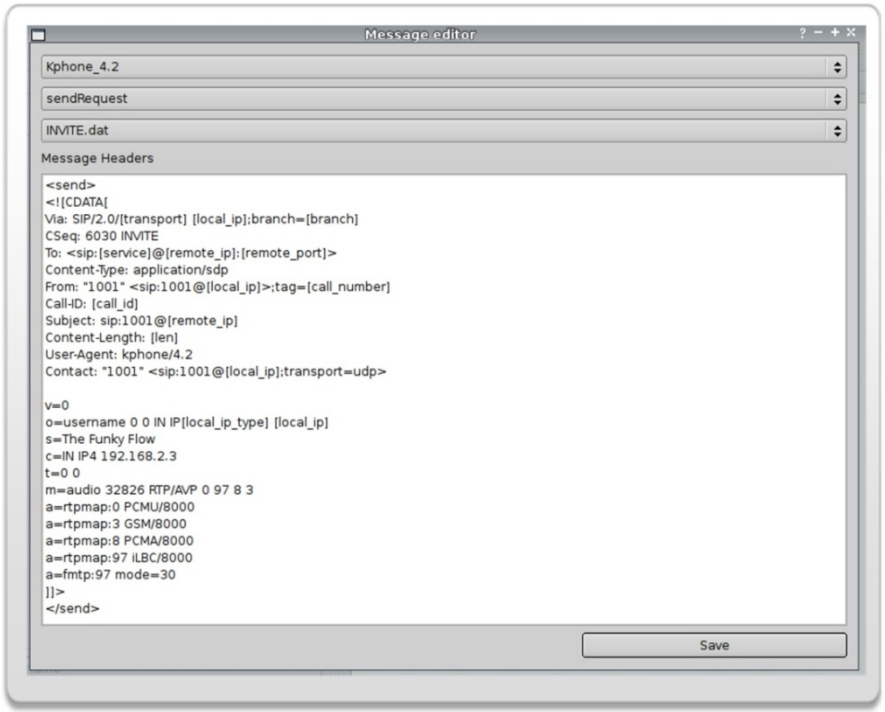
How can the attacks be put into practice?

SIP XML Scenario Maker

- At first a Tool is needed that can implement the attacks:
  - SIP XML Scenario Maker expands SIPp with the ability to quickly
  - Create custom SIP scenarios via a graphical user interface (GUI)
  - Execute created scenarios and evaluate the result with
  - Two different editing modes (Scenario Editor, Message Editor)
  - One execution mode

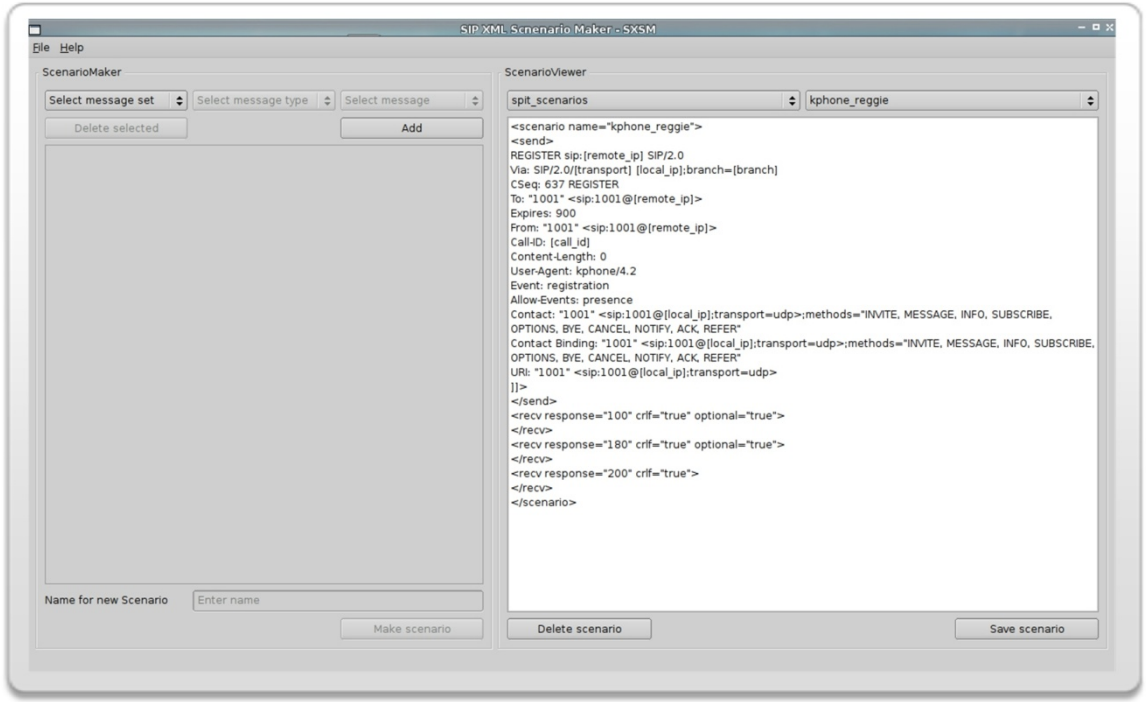
SXSM – Message Editor

- Create custom SIP messages
- Organize messages by type or by set



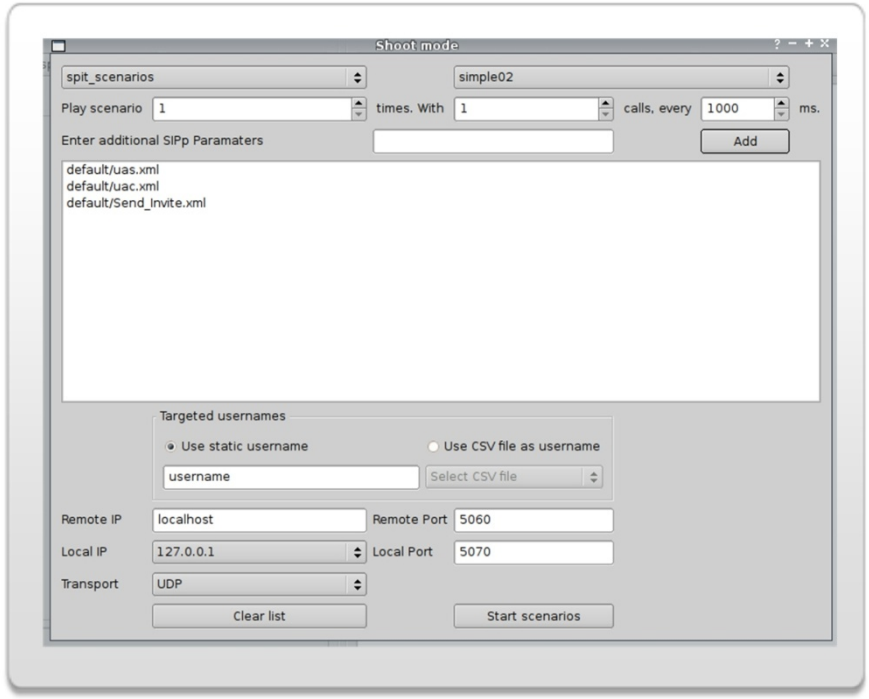
SXSM – Scenario Editor

- Create Sequence of SIP Messages as a Scenario
- Create complex scenarios within few clicks



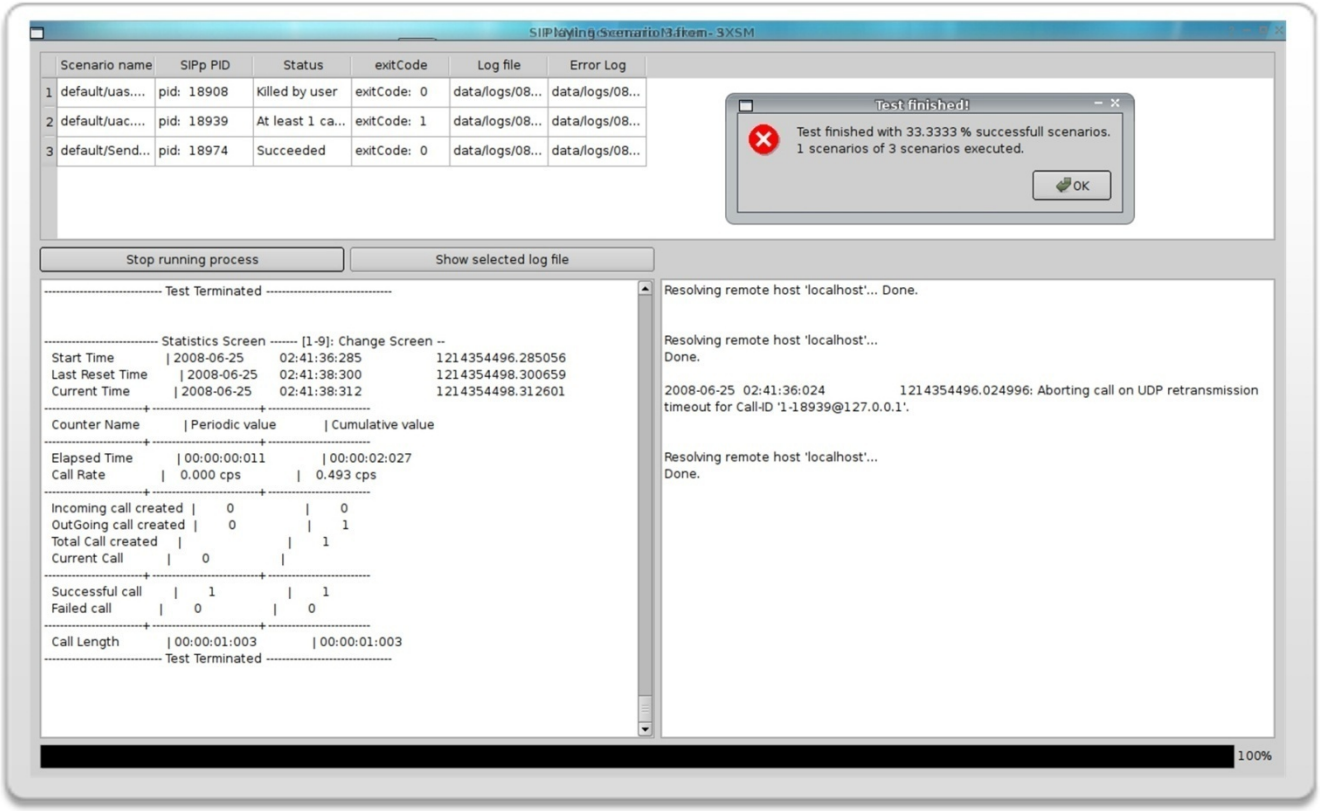
SXSM – Shoot Mode

- Execute created Scenarios in a batch
- Adjust parameters such as targets, call rate



SXSM – Shoot Mode

- Evaluate output of executed Scenarios
- Call Success Rate is displayed, Log files



SIP XML Scenario Maker Device Spoofing

- Passive Device Spoofing
  - Analyze SIP message layout of a standard client (e.g. KPhone)
  - Create a new message set in Message Editor for this client
  - Create new SIP message with exact same layout in Message Editor
- Active Device Spoofing
  - Analyze standard client's behavior to probes
  - Create custom scenario, that handles all messages
  - Scheme If message X is received jump to section Y (scenario with branch points)

SIP XML Scenario Maker
SIP Identity Spoofing

- Change SIP message headers in Message Editor
  - Enter wished values for ‘From’ and ‘Contact’ header
- Change SIP message headers in detail view of Scenario Editor
- Inject values from a CSV File
  - From: [field0 file=“caller.csv”] <sip:[field1 file=“caller.csv”]@[local ip]:[local port]>;
  - CSV File can contain several accounts that are used

SIP XML Scenario Maker
SIP Header Spoofing

- Header fields and their values can be manipulated
  - Within Message Editor
  - Within Scenario Editor

- In Direct IP SPIT Scenario any header field or value can be set
- In SPIT via Proxy only acceptable values

SIP XML Scenario Maker
Reputation Pushing/Ballot Stuffing

- Create two scenarios
  - Scenario one calls with identity that should be pushed
  - Scenario two accepts calls from scenario one, terminates session and provides positive feedback
  - Repeat with enough identities for scenario two

SIP XML Scenario Maker CAPTCHA Relay Attack

- Make use of Third Party Call Control Feature
- Create a scenario, that does the following:
  - Call Victim
  - Call Human Solver
  - Refer victim to Human Solver
- When victim accepts the 'REFER' CAPTCHA will be solved

SIP XML Scenario Maker
SIP Identity Hijacking

- Create a scenario containing the following steps:

- Disable the legitimate user's registration by:
  - performing a DoS attack against the user's device or
  - deregistering the user or
  - Generating a registration race-condition
    attacker sends repeatedly 'REGISTER' requests in a shorter timeframe (such as every 15 seconds)

- Send a REGISTER request with the attacker's IP address instead of the legitimate user's

SIP XML Scenario Maker
Call Rate Adaption

- Adapt Call Rate within Shoot mode
- Play scenario e.g. 100 times with a rate of 10 calls per minute
- Put scenario several times into Shoot List
  - E.g. first with 100 calls per minute
  - Then with 50 calls per minute
- Call Rate can be adapted as wished

SIP XML Scenario Maker Account Switching

- Use CSV file for both calling and targeted identity
- Caller can be set within Scenario or Message Editor
- Target can be set within Shoot mode
- E.g. ten identities in caller.csv and hundred in callee.csv
- While the attack is performed in each step identities are switched automatically

Thank You!

Do You have any Questions?

- they may also be forwarded to the authors