Zukunft der Netze, 20.03.2009

SPAM over Internet Telephony (SPIT) und Abwehrmöglichkeiten

Dirk Hoffstadt (Uni Duisburg-Essen)

Christoph Sorge (NEC)

Yacine Rebahi (Fraunhofer FOKUS)
Outline

- Introduction
  - From SPAM to SPIT
  - The SPIT problem in more detail

- SPIT detection and prevention
  - University of Duisburg-Essen
    • VoIP Honeypot system
    • SPIT Protection Filter
  - NEC
    • VoIP SEAL: 5 stage SPIT protection framework
  - Fokus
    • Spider: SPam over Internet Detection sERvices

- Conclusions
Introduction –
From SPAM to SPIT

- SPAM generally refers to any unsolicited communication
  - Ranging from marketing advertisements to fraud, phishing and attempts to spread malware
  - Content of SPAM messages information is useless for the majority of people
  - SPAM creates significant effort and cost for recipients

- Spammers seek for low cost and widely used tools
  - Few years ago facsimile was used
  - Currently email, SMS and phone are used
  - In the future, Voice over IP is the appropriate tool
    - No or low cost,
    - universal reachability due to voice / data convergence

⇒ SPAM over Internet Telephony (SPIT)
SPAM over Internet Telephony (SPIT) – The problem in more detail

- **Automated SPIT**
  - Hardware or software generating calls / messages automatically
  - Any SIP client is able to generate a huge number of simultaneous calls
  - Interactive Voice Response (IVR) is used to deliver pre-recorded voice messages

- **SPIT generation by humans**
  - Professional telemarketers or call centers
    - make phone calls for advertising products
  - This category is annoying
    - But its potential volume is very limited compared to the volume of automated spit generation
SPAM over Internet Telephony (SPIT) –
The problem in more detail (2)

Can also be used for DoS

Make SPIT call

Internet
SPAM over Internet Telephony (SPIT) – The problem in more detail (3)

- **Focus on SIP based VoIP**
- **SPIT detection**
  - Major protocol changes not feasible
    - Only additional (filtering) mechanisms viable
  - E-Mail is a preferred target for spammers
    - One can learn how email spam was addressed
- **Difficult to find out the origin of SPIT calls**
  - Spoofed identities are used
  - Anonymity services are used
- **Insecure third party relays**
  - SIP open relay servers (e.g. Asterisk in default configuration)
    - Unauthorized third party relays
    - Used by spitters to route large volumes of unwanted SIP messages
Does SPIT really exist? – VoIP Honeypot system (1)

- VoIP Honeypot project
  - Modified VoIP server attached to the Internet
    - Accepting and logging incoming calls from the internet
      - SPIT detection
    - Handling and logging Register attempts
      - Toll Fraud detection (unauthorized toll calls)

- Short field test
  - Duration about 2 months
    - Honeypot was found and attacked without further publishing activity

- Publication of a specific SIP URI on web site
  - SIP URI was found and attacked
Does SPIT really exist? – VoIP Honeypot system (2)
Does SPIT really exist? – VoIP Honeypot system (3)

- Result for SPIT in VoIP Honeypot field test
  - Only one series of 11 SPIT calls to SIP URI published on web page
    - From the same IP address (located in Bulgaria)
    - About 30 minute interval between calls
  - SIP header fields obviously forged (e.g. SIP ID indicating Peru)

- SPIT is obviously a potential problem
  - But no real problem on a large scale yet

- Some SPIT experiments performed
  - What effort does it take to produce SPIT?
  - What effort does it take to protect against SPIT?
    - In both infrastructure and P2P scenarios
Effort to produce SPIT – SPIT generator based on Asterisk

- Automated calls can be made by using a „call file“
- Simple scripts can be used to repeat calls with varying parameters
- Execution of scripts can be performed in parallel
  - Performance only limited by outgoing bandwidth
    - Estimated 11 SPIT calls in parallel on 16 Mbit/s ADSL access (→ Upstream!)

```
[call-file-SPIT]
exten => 10,1,Answer()
exten => 10,2,Wait(1)
exten => 10,3,Playback(spit_audio)
exten => 10,4,Wait(1)
exten => 10,n,Hangup()
```

```
Channel: SIP/302
MaxRetries: 10
CallerID: 333333
RetryTime: 60
WaitTime: 45
Context: call-file-SPIT
Extension: 10
```
Effort to produce SPIT – Extension for Phishing

```plaintext
[call-file-Phishing]
exten => 10,1,Answer()
exten => 10,n,Wait(1)
exten => 10,n,Playback(information)
exten => 10,n,Background(req_accountno)
exten => 10,n,Read(ano)
exten => 10,n,Background(req_bc)
exten => 10,n,Read(bc)
exten => 10,n,Background(req_PIN)
exten => 10,n,Read(PIN)
exten => 10,n,Background(req_TAN)
exten => 10,n,Read(TAN)
exten => 10,n,Playback(thanks)
exten => 10,n,System("echo '${bc}${ano}${PIN}${TAN}' >> d.txt")
exten => 10,n,Hangup
```

Playback welcome message

Query for account details

Store account details
SPIT Protection – SPIT protection filter

- **System behaviour** takes into account **SPIT Level (SL)**
- **Adaptation of SL** performed by filter system
  - Automated, based on metrics (e.g. call frequency, outcome of puzzle)
  - Based on user feedback
  - White- and blacklisting available

**Classes**

- **Class A**
  - Trusted, known in person, white-list
  - SL: 0 – 10
  - Regular signalling of incoming call

- **Class B**
  - Neutral, no rating, unknown or new caller
  - SL < 0
  - Signalling with SPIT indication

- **Class C**
  - "Potential SPIT" 
  - SL: 11 – 25
  - Signalling after completion of puzzle

- **Class D**
  - "Probably SPIT" 
  - SL: 26 – 50
  - No signalling, mailbox option available

- **Class E**
  - "Definitely SPIT" 
  - SL > 50
  - No signalling, mailbox option available
Effort to protect against SPIT
SPIT filter for Asterisk

- 3 PHP modules added
- Call acceptance module
  - Accept incoming calls
  - Check SL in data base
  - Create new data set for unknown caller
  - Activated by incoming call
- Rating module
  - Adapts SL based on
    - Metrics
    - User feedback
- Check module
  - Perform automated puzzle
- Support for signalling of SL with call
  - ISDN
  - SIP
Effort to protect against SPIT
SPIT filter system

Filter

Limited information (maybe forged) for several users

Has full information for many users

Internet

Make SPIT call

Filter

Limited information for one user
NEC VoIP SEAL: 5 stage protection framework

- **Stage 1:**
  - *Non-intrusive:* Filtering SIP messages without any user interaction
  - Examples: Blacklists, Whitelists, statistical analysis, …

- **Stage 2:**
  - *Caller interaction:* Interactively testing the trustworthiness of the caller
  - Example: CAPTCHA-tests

- **Stage 3:**
  - *Feedback before call:* Asking the callee regarding the identity of the caller

- **Stage 4:**
  - *Feedback during the call:* Indicating to the system that current call is unsolicited

- **Stage 5:**
  - *Feedback after the call:* Marking a call as unsolicited once the session has terminated
NEC
Research status and ongoing work

- **Product**
  - Statistical analysis approaches, blacklists, whitelists, ...

- **Prototype implementation**
  - All stages
  - Including
    - Simple honeypot system
    - Web-of-trust approach
    - Turing tests

- **Standardization**
  - E.g. introduction of Spam scores in SIP messages
  - Standardization work in IETF, ETSI TISPAN, 3GPP, ITU-T

- **Ongoing research**
  - Provider-level reputation systems
    - How trustworthy are Spam scores a provider adds to SIP messages?
  - Advanced statistical analyses
SPIDER-Project: Spam over Internet Detection sERvices

EU Research project for the benefit of SMEs

Design and prototype implementation of multilayered SPIT detection architecture

Main components
- Authenticated SIP (RFC 4474)
- Voice Captchas
- Offline Audio analysis (Mailbox spit detection)
- Passive traffic analysis
- White / Blacklists
- Proxy checker
SPAM over Internet Telephony (SPIT) und Abwehrmöglichkeiten
Conclusions

- Generation of SPIT is simple and requires limited effort
- Basically the same situation as for Malware and SPAM
  - Malicious activity already present
  - Escalation of the problems can be expected
    - P2P mode SIP (e.g. ENUM)
    - Home servers with SIP Registrar functionality
    - Large scale use of SIP
- Filter systems for different scenarios
  - IP-Phone (P2P)
  - Company SIP-Server
  - SIP-Provider
- Challenge: real-time SPIT detection (cf. E-Mail SPAM)
Thank you for your attention!