SIP Digest Access Authentication
RELAY-ATTACK for Toll-Fraud

Humberto J. Abdelnur
Humberto.Abdelnur@loria.fr

Radu State
Radu.State@loria.fr

Olivier Festor
Olivier.Festor@loria.fr

Madynes team
http://madynes.loria.fr
LORIA-INRIA Lorraine

November 2, 2007
Outline

1. RFC 3261 Overview
   - Direct Call
   - re-INVITE Request
   - Authenticated Call

2. Known Authentication Attacks
   - MITM Attack
   - Replay Attack

3. Unknown Attack
   - Relay Attack
RFC 3261 Overview
Direct Call from user B to A

User A
SIP-URI: Alex@PBX.1

INVITE sip:Alex@PBX.1
100 Trying
180 Ringing
200 OK
ACK

User B
SIP-URI: Bob@PBX.2

Media Data
re-INVITE Request

re-INVITE overview

“This modification can involve changing addresses or ports, adding a media stream, deleting a media stream, and so on. This is accomplished by sending a new INVITE request within the same dialog that established the session. An INVITE request sent within an existing dialog is known as a re-INVITE.”

1RFC 3261 Section 14 Modifying an Existing Session
Authenticated Call

Call from User B to User A via a Proxy using Digest Access Authentication (RFC 2617)

User A
SIP-URI: Alex@PBX.1

User B
SIP-URI: Bob@PBX.2

Registrar/Proxy
URI-Domain: PBX.2

INVITE sip:Alex@PBX.1
180 Ringing
200 OK
ACK sip:Alex@PBX.1

INVITE sip:Alex@PBX.1

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

Proxy-Authorization: Digest username="Bob",realm="domain.org",
url="sip:Alex@PBX.1",
response="4cc8a1de5a60306c760bba828abed155",
nonce="1d78fb72", algorithm=MD5
Known Authentication Attacks

RFC 2617 Section 4.5 Replay Attacks
Man in the Middle Attack

User A
SIP-URI: Alex@PBX.1
Registrar/Proxy
URI-Domain: PBX.2

INVITE sip:Alex@PBX.1
180 Ringing
200 OK
ACK sip:Alex@PBX.1

INVITE sip:Alex@PBX.2
(Authentication Response)
180 Ringing
200 OK
ACK sip:Alex@PBX.1

Man in the Middle Attacker

INVITE sip:Alex@PBX.2
100 Trying
401 Authentication required
(Authentication Challenge)
ACK sip:Alex@PBX.2

INVITE sip:Alex@PBX.2
100 Trying
401 Authentication required
(Authentication Challenge)
ACK sip:Alex@PBX.2

INVITE sip:Alex@PBX.2
(Authentication Response)
486 Busy
ACK sip:Alex@PBX.2

User B
SIP-URI: Bob@PBX.2
Replay Attack

INVITE sip: Alex@domain
401 Authentication required
(Authentication Challenge)
ACK

INVITE sip: Alex@domain
(Proxy-Authentication)
180 Ringing
200 OK
ACK

User A
SIP-URI: Alex@PBX.1
INVITE sip: Alex@PBX.1
180 Ringing
200 OK

Registrar
URI-Domain: PBX.2

Registered user

Attacker

INVITE sip: Alex@domain
(Proxy-Authentication)
180 Ringing
200 OK
ACK
Unknown Authentication Attack to SIP
Relay Attack

Trigger a re-INVITE on User B in order to request him to authenticate.

"The UAC uses the remote target and route set to build the Request-URI and Route header field of the request."
RFC 3261 12.2.1.1 Generating the Request (Requests within a Dialog)