Single Packet Authorization on the WEB -- WEB-SPA

Dr. Markus Maria Miedaner
Syracom Consulting AG
Dr. Yiannis Pavlosoglou
USB AG

markus.miedaner@syracom.de
yiannis@owasp.org

15.11.2012

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
Motivation for WEB-SPA

- Ubiquity of web servers
- Active defense against 0-Days
- Easy to access
- Urge to experiment
- Include the mobile world
- Consider deferred timeouts
- No latency issues
- Break the network layer boundary
Previous Work
Port Knocking

- Established pre 2000 to open ports in firewalls
- Susceptible to replay attacks
- Limited to the network level
Port Knocking takes its time

- Port field in TCP Headers: 16 bit
- Simple cipher text: 128 bit
- 8 Packets required
- 4 Seconds required

Example (64 bit hash)

- CRC32("pwd") = 32FB1181

  to binary and chunked into pieces of 16 bits

  0011100000110001 – 0011000100110001 – 0100011001000010 - 0011001100110010

  Portnumber: 14385 12593 17986 13106
Single Packet Authentication

- New protocol – first established in 2005
- Extends Port Knocking
- Mitigates some vulnerabilities
- Combines authentication and authorization

hash(username+passwd+date)
Port Knocking, SPA and Security

- Defence in depth
  - An additional layer?
  - Detectability?

- Exploitability of the server
  - Direct packet inspection
  - Log file analysis

- Exploitability of the client

- Client identification

- Timeouts
Problems with Port Knocking and SPA

- Logfile pollution
- Flow vs. IP-based authentication
- IDS/IPS detection
- Anonymity → TOR
- Password rotation
- Slow

© wuala.com
Attacks against Port Knocking and Single Packet Authorization
Attacks

- Latency
- Denial of Service
- Replay
- Man in the middle
- Brute force
- Weak cryptography
The WEB

- Various authentication / authorisation schemes
- Various 2 factor authentication methods
- Strict separation of layers
  - Network
  - Transport
  - Application
  - Storage
WEB-SPA – The principle – STEP 1

One packet to a complex url

OR

Stolen from pluzzi.com
WEB-SPA – The principle - STEP2

2.

Use the service you activated
WEB-SPA 0.4 – How does it work?

http://localhost/web-knock/date-hash/version/user-hash/action-hash/message/uuid/final-hash

sha1sum{datetime + salt}

sha1sum{user + pass + datetime}

plaintext message

sha1sum{date-hash + user-hash + action-hash + salt}

version (e.g. 0.4)

sha1sum{action + datetime}

52826fb0-cfa5-448e-9fae-fc0192445f01

pre-defined property for client & server
Example URL: http://localhost/%CF%87/OKSNmjNF-...

Host
http://localhost/%CF%87/OKSNmjNF-4kcY5HeUCuXhyGmEPw/

Knock

DateHash

Version
0.4/RHfD0fT5xQwR2yqJSzVe2XoFWVw/VGnb45xSWAqkYEQ1NyRvvfEWUZg/

UserHash

ActionHash

Message
Tm90IG5vdw/7172134f-6eec-4026-8b9e-f0ee77e79c81/FVKt_Y-R1DIF5VWMylGuBxa1gU/

UUID

FinalHash
Configuration Example for WEB-SPA

- **User Configuration**
  - Username:Password:Action
  - john:smith:msg
  - chris:cooper:linuxssh

- **Action Configuration**
  - ActionName~#~StartCommand~#~StopCommand~#~Timeout
  - linuxssh~#~service ssh start~#~service ssh stop~#~7
Outlook

- QR-Codes
  - Easy configuration of mobile devices
  - DB – backend for configuration

- Configurable Hashing / Public Key Cryptography
  - Non-repudiation of origin
  - Higher level of security
  - Longer URL
Summary

Web-SPA is:

- SIMPLE
- SECURE
- HIGHLY CONFIGURABLE
QUESTIONS

© allthingsd.com