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

OWASP
15.11.2012

The OWASP Foundation
http://www.owasp.org

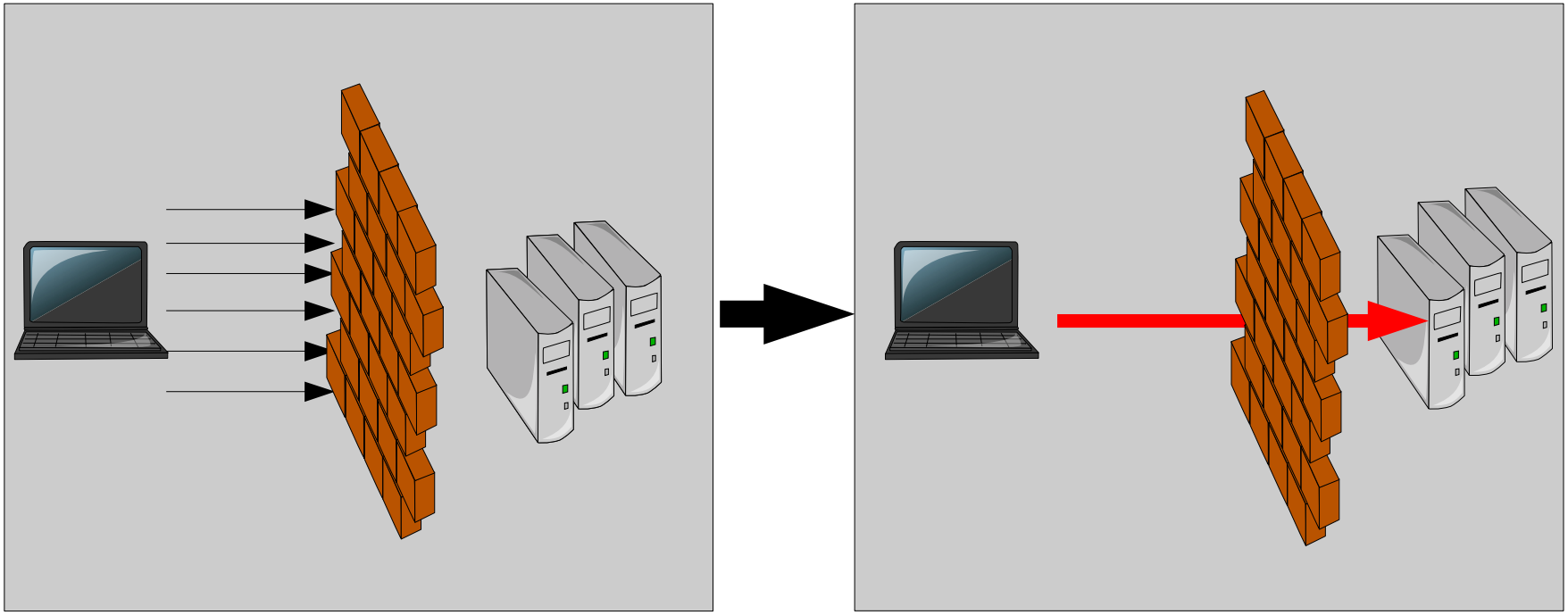
Motivation for WEB-SPA

- 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

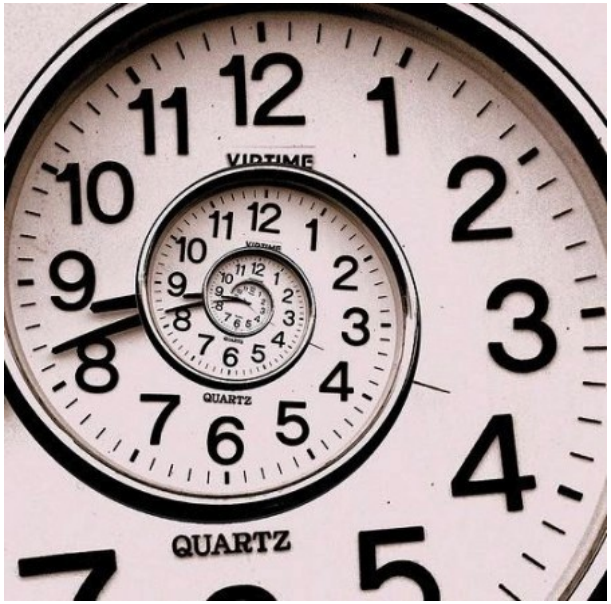
Port Knocking

- 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



© thegivingdemocracy.com

- Example (64 bit hash)
  - CRC32(„pwd“) = 32FB1181

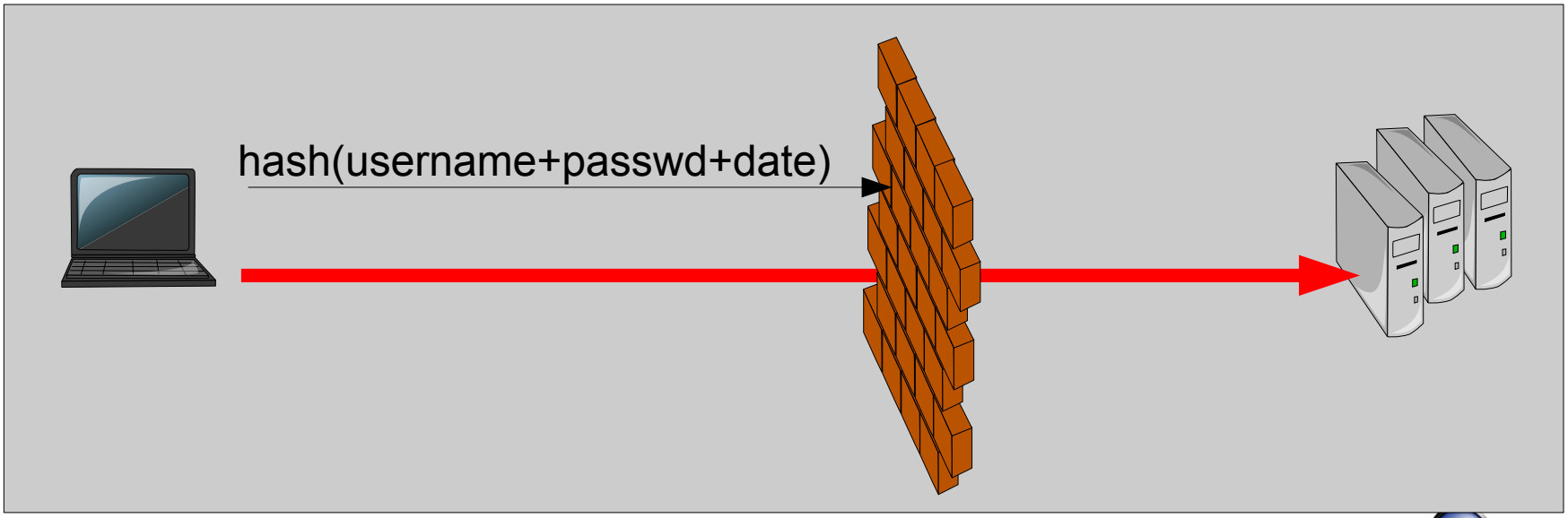
to binary and chunked into pieces of 16 bits

0011100000110001 – 0011000100110001 - 0100011001000010 - 0011001100110010

Portnumber : 14385 12593 17986 13106

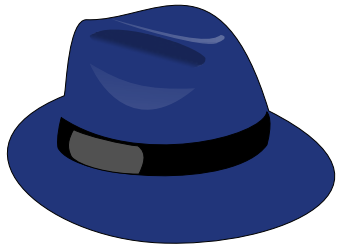
Single Packet Authentication

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



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



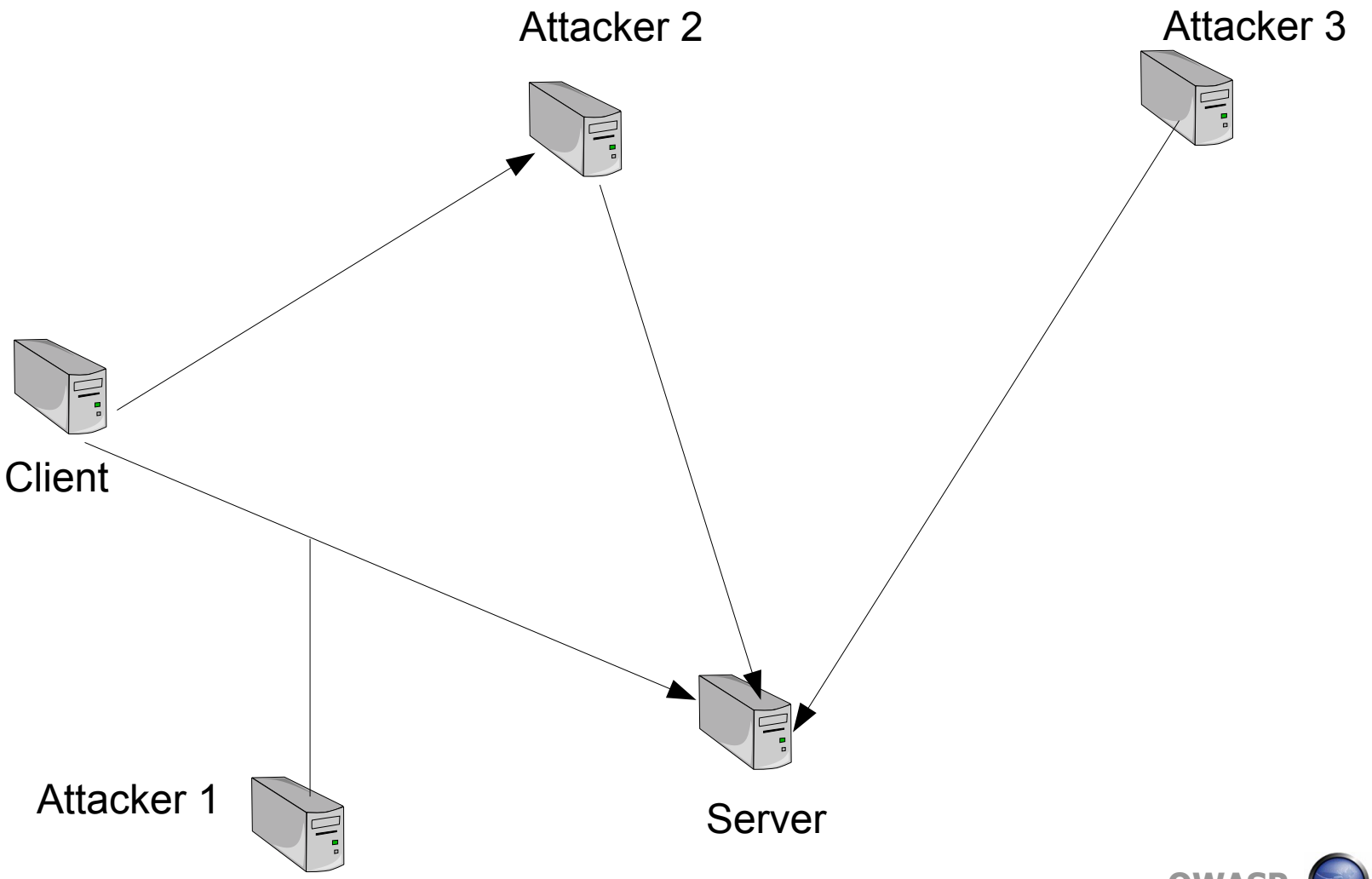
Problems with Port Knocking and SPA

- Logfile pollution
- Flow vs. IP-based authentication

© wuala.com

- IDS/IPS detection
- Anonymity → TOR
- Password rotation
- Slow

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

Ripped of from: iStockphoto/ktsimage

WEB-SPA – The principle – STEP 1

One packet to a complex url

1.

OR

```
Web-Spa-Client _v0.4 (subere@uncon.org)
Welcome to Web Single Packet Authorisation

Please enter your login
[username] :user

Enter your password
[password] :

Enter the action you want to execute on the server
[windowsmsg] :sshd

Enter the (optional) message you want to send
[AYBABTU] :yahoo

Finally, please enter the host
[http://localhost/] :http://my-site.com:8080

Web Knock : %CF%87
Date Hash : MNAV4egW0LUPGEcS313mLwwBKz0
Version   : 0.4
User Hash : 93ahnu7TZtV7H6DXBeojffue28k
Action    : Y28gjYEMgAnh8s0fcyOvK-8CJJQ
Message   : eWFob28
Unique ID : a5cba8df-81f6-481a-824f-f0c561452b0d
Final Hash: BExGbcVxrgrlT0e4q9fUo93Nv4w

http://my-site.com:8080/%CF%87/MNAV4egW0LUPGEcS313mLwwBKz0/0.4/93ahnu7TZtV7H6DXBeoj
ffue28k/Y28gjYEMgAnh8s0fcyOvK-8CJJQ/eWFob28/a5cba8df-81f6-481a-824f-f0c561452b0d/BE
xGbcVxrgrlT0e4q9fUo93Nv4w/

Copy the above URL to the clipboard?
[yes] :
```

1.

Stolen from pluzzi.com

WEB-SPA – The principle - STEP2

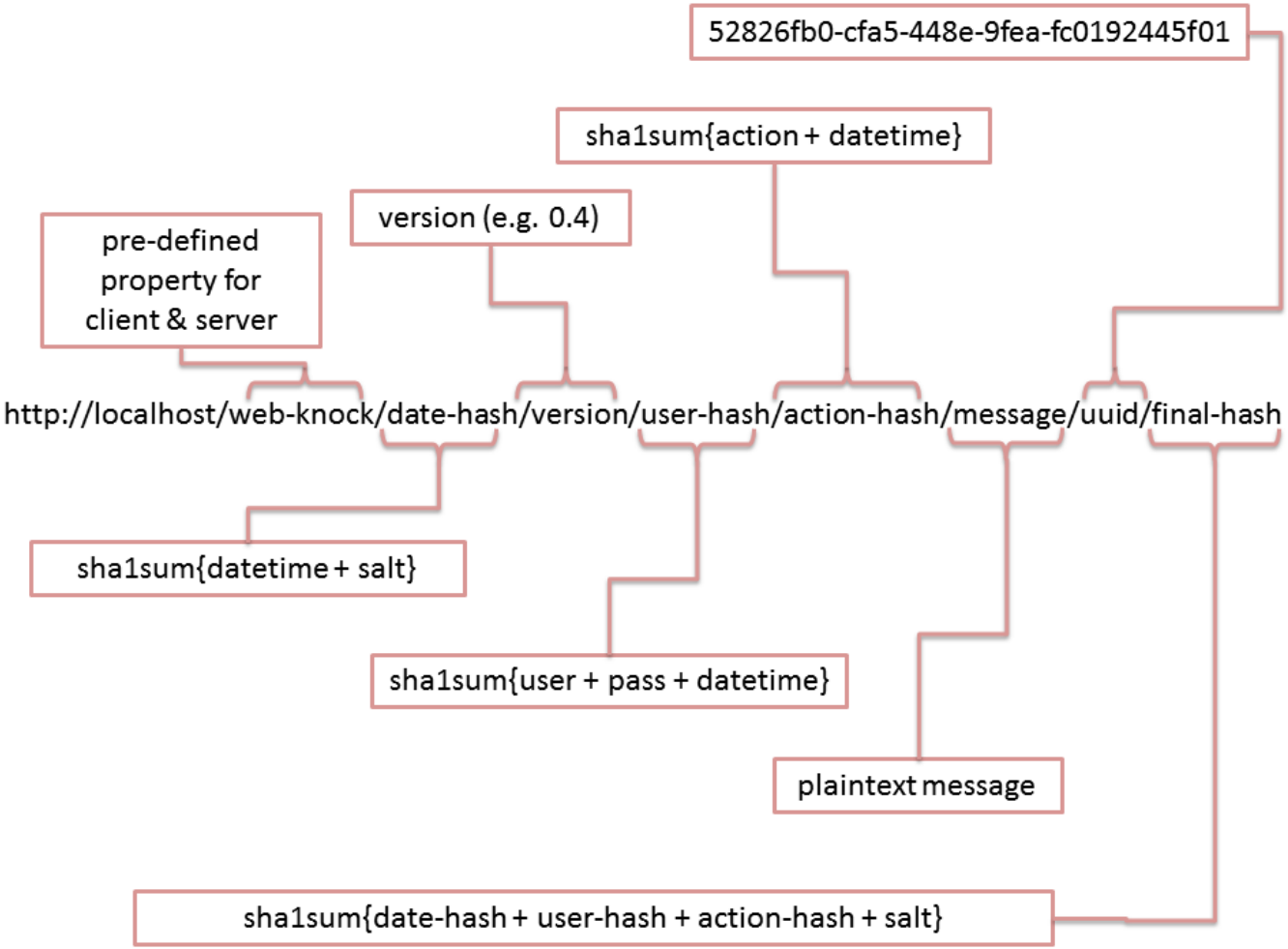
2.

2.

Use the service you activated

Stolen from pluzzi.com

WEB-SPA 0.4 – How does it work?



Example URL: http://localhost/%CF%87/OKSNmjNF-...

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

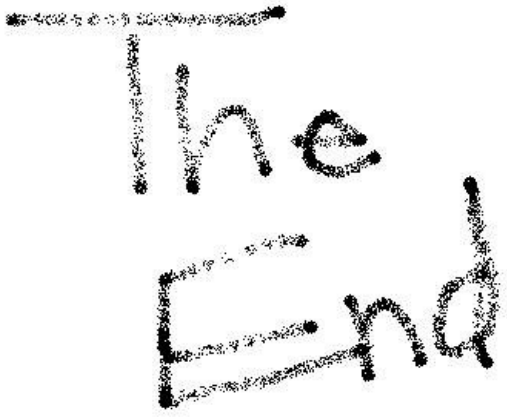
© searchengineland.com

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

© blogs.adobe.com

Summary

- Web-SPA is:
  - SIMPLE
  - SECURE
  - HIGHLY CONFIGURABLE



© http://jholverstott.files.wordpress.com/