Security of Distributed Software

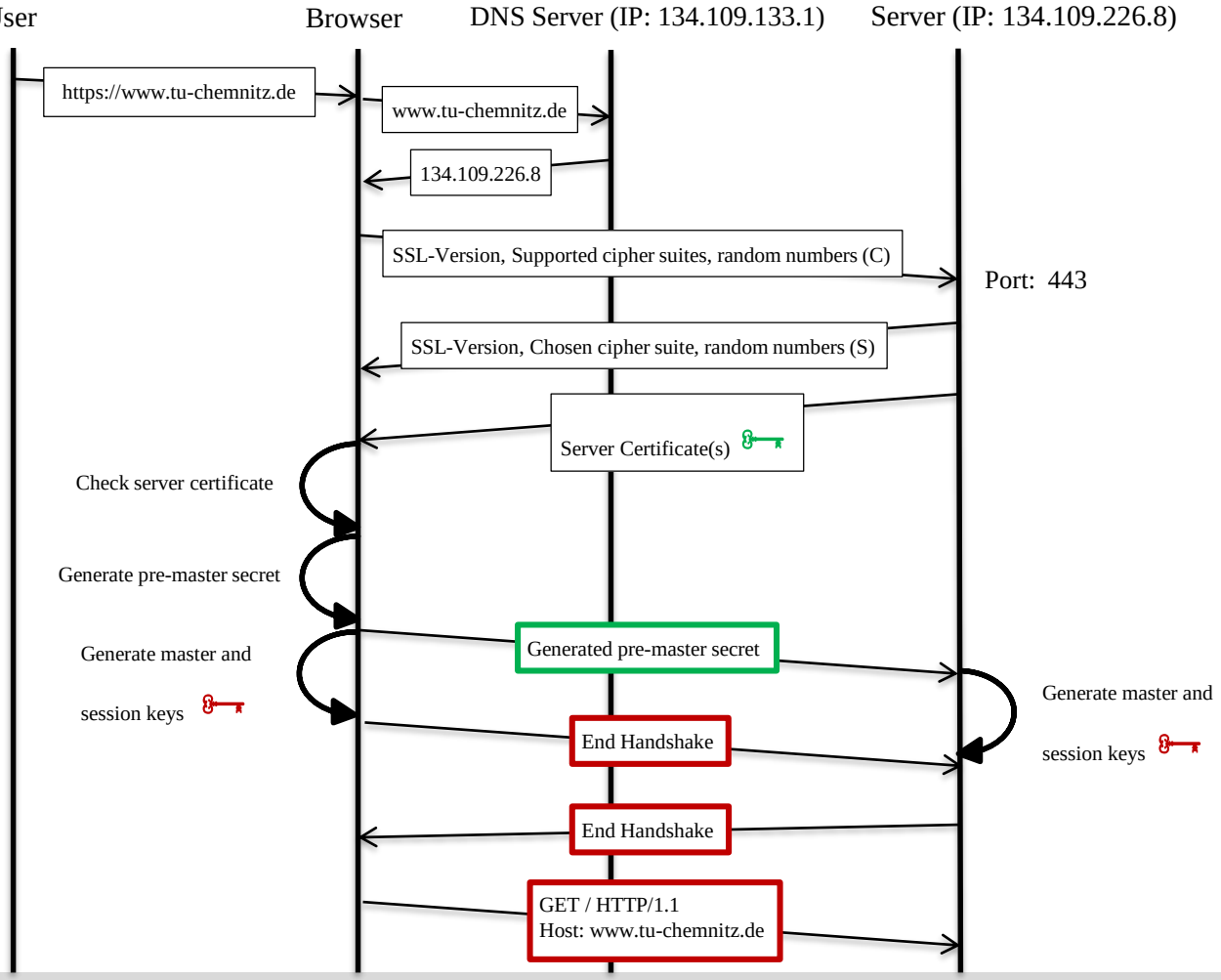
SS 2019 – 7. Tutorial

Valentin Siegert M.Sc.

Dang Vu

*VSR.Informatik.*TU-Chemnitz.*de*

Task 1


User
Browser
DNS Server (IP: 134.109.133.1)
Server (IP: 134.109.226.8)
https://www.tu-chemnitz.de
www.tu-chemnitz.de
134.109.226.8
SSL-Version, Supported cipher suites, random numbers (C)
Port: 443
SSL-Version, Chosen cipher suite, random numbers (S)
Server Certificate(s)
Check server certificate
Generate pre-master secret
Generate master and
session keys
Generated pre-master secret
Generate master and
session keys
End Handshake
End Handshake
GET / HTTP/1.1
Host: www.tu-chemnitz.de

a. Which goals does SSL/TLS have?

- Confidentiality
- Authenticity
- Integrity

Which risks exist despite of usage of SSL/TLS?

- Out-of-scope

b. How does server decide, which certificate should be shown if several virtual hosts exist?

- Server Name Indication (SNI)
- Wildcard-Certificates
- Multidomain-Certificates

Task 2

- Prevent phishing
- No password storage at apps
- Prevents chosen-plaintext attacks
- Prevents replay attacks

- Many security options are optional
- man-in-the-middle attack
- Prevents strong hash algorithm

3. What would a client send as a response to the following server message, if his username would be „Max“ and his password - „Secure123“?

Request:

```
GET /index.html HTTP/1.1
Host: localhost
```

Response:

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Secured Area",
nonce="aer95b7fg2dd2hhe8b11d0f6f7afb0c14v"
Content-Length: 0
```

HA1 = MD5(username:realm:password)

HA2 = MD5(method:digestURI)

response = MD5(HA1:nonce:HA2)

Task 3

Inform yourself about Public Key-Authentication in SSH Authentication Protocol.

1. Create key pair for a user
2. Transfer the public key to the server
3. Configure the ssh service to use Public Key-Authentication
4. Test the authentication using the newly created keys

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*