Die TLS Neuverhandlungsattacke

6. November 2009

T. Hildmann und T. Gebhardt

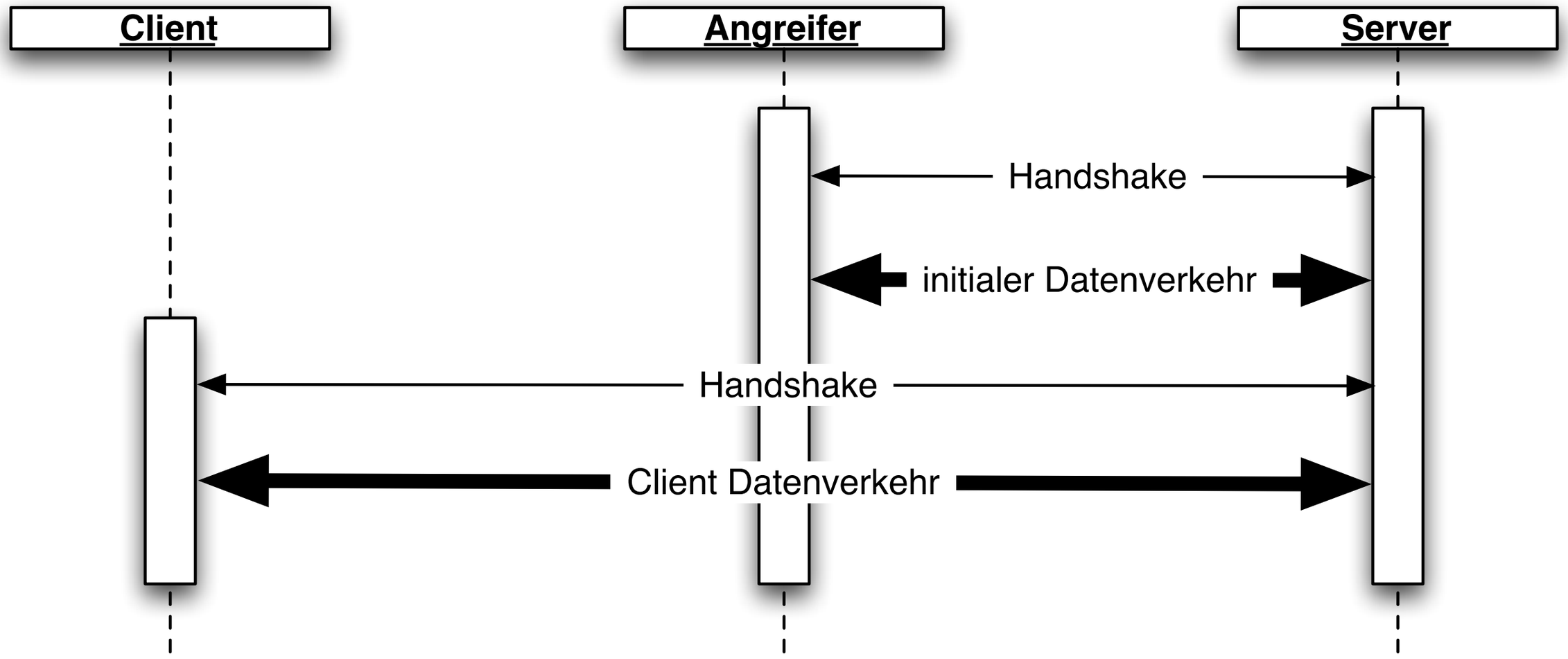
Problem

- Entwurfsfehler im TLS-Protokoll bezüglich Neuverhandlung (renegotiation)
- TLS erlaubt die Neuverhandlung von Verbindungseigenschaften in bestehenden Verbindungen (z.B. Client-Authentisierung oder veränderte Cryptoalgorithmen)

Authensierungslücke

- Lücke bezieht sich auf...
  - Authentizität des Servers
  - Authentizität des Clients
- Einschränkung: Für ein Neuverhandlungsvorgang

Prinzip der Attacke



Quelle: EKR, http://www.educatedguesswork.org/

Bedrohung

- Einschleusung von Inhalten, die vom Empfänger als authentisch angesehen werden (plain text injection).
- Grundannahmen auf Protokoll- und Anwendungsebene sind verletzt (SSH ist nicht betroffen)!
- Spezifische Angriffszenarien hängen vom Anwendungsprotokoll ab.

Beispiel: „Pizzaangriff“

Der Angreifer sendet:

```
GET /pizza?toppings=pepperoni;address=attackersaddress HTTP/1.1
X-Ignore-This:
```

and letzte Zeile ohne Return oder Linefeed senden. Danach folgt die Anfrage des Clients

```
GET /pizza?toppings=sausage;address=victimssaddress HTTP/1.1
Cookie: victimscookie
```

die zwei Anfragen zusammen:

```
GET /pizza?toppings=pepperoni;address=attackersaddress HTTP/1.1
X-Ignore-This: GET /pizza?
toppings=sausage;address=victimssaddress HTTP/1.1
Cookie: victimscookie
```

Quelle: EKR, http://www.educatedguesswork.org/

Potentielle Angriffsziele

- Server
  - indirekte Bedrohung (z.Zt. unkritisch)
- Daten
  - Integrität der Daten ist direkt bedroht
  - Beweisbarkeit von Transaktionen in Frage gestellt
- Benutzer
  - Fälschung von benutzerautorisierten Transaktionen

Gegenmassnahmen

- kurzfristig
  - Abschalten der Wiederverhandlung
    - OpenSSL ist bereits aktualisiert
- langfristig
  - Änderung des Protokollsdesigns und Implementierung (ist in Arbeit, IETF)

Konkrete Massnahmen

- OpenSSL aktualisieren, sobald von Distributoren angeboten!
- Alle eingesetzten SSL-Implementierungen ermitteln (Hard- und Software) und Neuverhandlung abschalten!
- Langfristig auf geändertes Protokoll umstellen!

Fazit

- Protokollfehler in TLS mit Auswirkung auf die meisten SSL/TLS-gesicherten Anwendungen.
- Angriff ist komplex und (noch) schwer generalisierbar / automatisierbar.
- Herstelleraktualisierungen abwarten / auf Aktualisierung drängen und umgehend aktualisieren!

Quellen

E. Rescorla: "Understanding the TLS Renegotiation Attack", http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html, Nov. 2009

M. Ray, S. Dispensa: "Renegotiating TLS", http://extendedsubset.com/?p=8, Nov. 2009

M.Rex: "MITM attack on delayed TLS-client auth through renegotiation", http://www.ietf.org/mail-archive/web/tls/current/msg03928.html, Nov. 2009

B.Laurie: "Another Protocol Bites The Dust", http://www.links.org/?p=780, Nov. 2009

Cox, et al. (OpenSSL Projekt Team): "Announcement: OpenSSL version 0.9.8l", http://www.openssl.org/news/announce.html, Nov. 2009

„SSH is not vulnerable to the SSL/TLS MITM attack“, http://djm.net.au/2009/11/6/ssh-is-not-vulnerable-to-the-ssl-tls-mitm-attack, Nov. 2009

Registriert unter CVE-2009-3555: https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2009-3555