Kristof Van Laerhoven
Thomas Janson

Freiburg, den 21. Mai 2015
Besprechung 5. Juni 2015

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2015

Blatt 4 (15 Punkte)

AUFGABE 1: 10 Punkte

Im Folgenden soll ein mit Wireshark abgefangener SSL-Stream untersucht werden. Öffnen Sie dazu folgende Wireshark-Aufzeichnung (`http://archive.cone.informatik.uni-freiburg.de/lehre/lecture/systeme-II-s15/uebung/trace-ssl.pcapng`) und filtern Sie nach SSL- und TLS-Nachrichten.

1. Untersuchen Sie eine Nachricht aus der Mitte der Aufzeichnung, welche als Info "Application Data" anzeigt.
   - Welchen "Content-Type" hat dieser Frame?
   - Welche TLS-Version wird verwendet?
   - Umfasst die Länge den "Record Layer Header" als auch den "Payload" oder nur den "Payload"?
2. Finden und analysieren Sie die Details der "Client Hello"- und "Server Hello"-Nachrichten inklusive der weiteren Details des "TLS Records".
   - Wie viele Bytes beinhaltet "Random Data" der "Hellos" von Client und Server und wofür wird es genutzt?
   - Welches Verschlüsselungsverfahren wurde vom Server verwendet?
3. Analysieren Sie als Nächstes die Details der "Certificate"-Nachricht.
   - Wie viele Zertifikate wurden gesandt?
   - Nennen Sie die Cipher-Suite, welche verwendet wurde, um das Pre-master-secret zu erzeugen
   - Wofür wird das Pre-master-secret verwendet?
   - Wie lang ist der öffentliche Schlüssel des Servers?
   - Welche kryptographische Hashfunktion wurde für die Signatur verwendet?
4. Analysieren Sie die Details sowohl der "Client Key Exchange"- als auch der "Change Cipher"-Nachrichten.
   - Wozu wird dieser Nachrichtenaustausch genutzt?
   - Welchen "Content-Type" besitzen diese Nachrichten?

- Wer sendet die “Change Cipher Spec”-Nachricht und was ist deren Inhalt?

5. Analysieren Sie die Details einer “Alert”-Nachricht.
   - Welchen “Content-Type” hat eine “Alert” Nachricht?
   - Werden die “Alert” Nachrichten verschlüsselt versandt, wenn nein: Was ist ihr Inhalt und was sagt er aus?

AUFGABE 2: 3 Punkte

Senden Sie sich selbst via *telnet* eine E-Mail mit der Nachricht: **Hello World!**
Dokumentieren Sie den Vorgang.

1. Nutzen Sie hierfür den SMTP Server: *smtp.informatik.uni-freiburg.de* auf Port *25*.
2. Bauen Sie vorher eine SSH-Verbindung mit dem Server: *login.informatik.uni-freiburg.de* auf. Dies ist notwendig, da der SMTP-Server (auf diesem Port) nur von wenigen Hosts im Universitätsnetzwerk erreichbar ist.
3. Als Empfänger müssen Sie ihre eigene E-Mail Adresse (<*user*>@*informatik.uni-freiburg.de*) verwenden!
4. Geben Sie die erhaltene E-Mail vollständig an, insbesondere auch alle Kopfzeilen.

AUFGABE 3: 2 Punkte

DNS-Anfragen

1. DNS-Server nutzen verschiedene Resource Record-Typen für unterschiedliche Anfragen. Für welche Anfragen werden die folgenden Resource Records benutzt?
   - A
   - CNAME
   - PTR
   - SOA
   - SPF
2. Was ist die IP-Adresse von uni-freiburg.de? Was für eine Anfrage wird gesendet, um diese Information zu erhalten?