Medical Records & Secure Connections:
Projektarbete i kursen Datorsäkerhet (EIT060)

EIT, Institutionen för Elektro och
Informationsteknik, Lunds Tekniska Högskola
Martin Hell

Adam Hansson Lyrén, C11 (dic11aha@student.lu.se)
Johan Bäversjö, C11 (dic11jba@student.lu.se)
Mergim Rama, C11 (dic11mra@student.lu.se)
Sven Elfgren, C11 (dic11sel@student.lu.se)

27 februari 2013

LUNDS
UNIVERSITET
Lunds Tekniska Högskola

Innehåll

1 Introduktion **2**

2 Bakgrund **2**
2.1 Socialstyrelsen 2
2.2 Läkare 2
2.3 Sköterska 2
2.4 Patienter 3

3 SSL/ TLS **3**
3.1 Handshake 3

4 Certifikat **3**

5 Säkerhetsutvärdering **3**

6 Referenser **3**

1 Introduktion

Projektet handlar till stor del om hur man kan upprätta en säker och krypterad anslutning mellan klient och server. För att kunna upprätta denna anslutning kommer vi använda oss av Secure Socket Layer (SSL) protokollet. Djupare teknisk beskrivning av SSL kommer senare i rapporten. Detta projekt kräver att man skapar en produkt som vi kan sälja vidare till myndigheter vilket visar projektets storlek. Koden till programmet kommer inte finnas med i rapporten. När vi använder oss av SSL protokollet kommer vi även använda oss av Java Secure Socket Extension (JSSE). Efter att ha skrivit klart programmet ska det säkerhetsutvärderas. Denna säkerthetsutvärdering täcker alla olika attacker som kan uppstå mot systemet och vilka attacker systemet kan skydda sig mot.

2 Bakgrund

Problemet som projektet grundar sig på är att skapa säkra medicinska journaler för ett sjukhus. Med säkra journaler menas i detta fall journaler som är sekretessbelagda så att inte vem som helst kan ha tillgång till dem, det vill säga att patienternas integritet skyddas. Eftersom systemet är en produkt framtagen för riktig användning måste det begränsas så att olika användargrupper på sjukhuset har olika behörigheter till journalerna. Personer som inte har någon behörighet kommer aldrig att kunna nå journalerna. De olika grupper som ska finnas med är:

1. Socialstyrelsen
2. Läkare
3. Sköterska
4. Patienter

2.1 Socialstyrelsen

Socialstyrelsen är det organ som bestämmer, det vill säga de har befogenheter till att kunna ta bort samt lägga till journaler.

2.2 Läkare

Läkaren kan däremot skriva och läsa färdiga journaler, förutsatt att han är den som tar hand om patienten. Han kan också läsa journaler som som finns på hans avdelning. Om patienten inte har någon journal har läkaren befogenheten till att skapa journalen. Kravet är då att läkaren själv är den som behandlar patienten.

2.3 Sköterska

Sköterskans rättigheter är att hon kan läsa och skriva till journalerna som hon är skriven på och att läsa alla journaler från hennes avdelning.

2.4 Patienter

Patienterna är berättigade till att läsa endast sina egna journaler vilket är en självklarhet. För att kunna spara allt som händer på journalerna ska en logg föras som visar vem som gjort vad i journalen samt vid vilken tidpunkt det hände.

3 SSL/ TLS

SSL är ett väldigt väl använt protokoll som man finner på nätet när en säker anslutning krävs. Med SSL förhindrar man tjuvlyssning på nätverket, vilket är en viktig faktor som gör protokollet säkert. Protokollet befinner sig mellan de två översta lagren i TCP/IP modellen, transportlagret och applikationslagret. Eftersom protkollet används för säkra anslutningar på nätet faller det i sin natur att SSL används mestadels i Hypertext Transfer Protocol (HTTP) [första referensen: http://docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html]. Många andra applikationer kan dra nytta av SSLs säkra anslutningar, några av dem är Telnet och FTP. SSL använder sig både av symmetrisk nyckel och asymmetrisk nyckel. De symmetriska nycklarna kan med hjälp av digitala signaturer göra datan som skickas över privat och på så sett tillgodoge data integritet. När SSL använder asymmetriska nycklar så görs detta för att kunna autentisera klienter respektive servrar. När protokollet gör detta betyder det att protokollet startar sin "handshakemetod. Utöver själva autentiseringen av server till klien så tillhandager "handshakeöckså:

1. Fastställa vilka algoritmer som ska användas
2. Förhandla om vilka nycklar krypteringen skall använda samt vilken MAC som skall användas
3. Autentisera klienten till servern, vilket inte är nödvändigt

Eftersom denna "handshake"kan bestå av delar eller hela meddelande cyklar, beskriver vi hur vårt system använder sig av dessa meddelanden i vår "handshademetod.

3.1 Handshake

4 Certifikat

Teknisk beskrivning av certifikat och vi använder det i vårt system.

5 Säkerhetsutvärdering

Säkerthetsutvärdering av systemet.

6 Referenser

Referenser till olika tekniska begrepp som kommer att nämnas.