Lab 5: PKI och TLS

Översikt

Den här labben handlar om säkerhet över Internet speciellt krypterad ansluting med HTTPS.

Referenser

- Cryptographic Right Answers (https://gist.github.com/tqbf/be58d2d39690c3b366ad)
- Bild på TLS handshake med förklaringar (https://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/tls/tls.html)

Grunduppgift

Gör om första laborationen i kursen, “Gissa talet jag tänker på”, fast nu med HTTPS anslutning. Skapa ett certifikat antingen med hjälp av keytool och sätt upp en ny keystore i din projektmapp eller använd den fria tjänsten let's Encrypt (https://letsencrypt.org/) för att skaffa en gratis men riktigt certifikat. Det kan vara så att det redan finns en keystore i din hemmamapp, men det är antagligen ingen bra ide att modifiera den. Modifiera sedan koden du skrev i laboration 1 så att nu väntar servern på en HTTPS-anslutning. Efter det så ska du bara behöva koppla upp dig med en webbläsare (firefox eller chrome) och efter att ha accepterat det självsignerade certifikatet så ska du kunna koppla upp dig säkert.

Din webbläsare (beroende på version) kan fortfarande visa att din anslutning inte är säker då du har ett självsignerat certifikat. Men om du klickar på i:et/hänglåset vid adressen så ska du kunna se ditt certifikat bland menyerna.

Specifika krav

1. SSLSockets måste användas.
2. Din kod måste vara ordentligt kommenterad.
3. Du måste förstå alla nyckelord i koden.

Tips

1. JSSE reference guide är VÄLDIGT hjälpsam för alla stegen i labben.
2. Om du använder dig av eclipse sa måste certifikatet placeras i projektmappen och inte i SRC eller BIN.
3. JSSE guide (http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html)

Bonus

I bonusuppgiften är fokus på teorin. Skriv frågorna och svaren i en fil med pdf-format. Ladda upp filen sedan på Cnavsa. Vi kommer i första hand kolla igenom inlämnade svar på Canvas och godkänna men vid behov kontaktar vi er för att diskutera inlämnade svaren.

Frågorna

1. Förklara hur PKI fungerar, ge en övergripande bild av infrastrukturen
2. Vad löser PKI för centralt problem på webben?
3. Förklara innehållet i ett certifikat. Viktigast är fälten relaterade till autentisering och verifiering av att certifikatet är korrekt
4. Förklara hur ett verifikat valideras från en teknisk synvinkel. Vilka algoritmer används på vilka fält och i vilken ordning? Här är de små detaljerna väldigt viktiga.
5. Hur levereras root-certifikaten till din dator?
6. Vad är en trust chain?
7. Är det säkert att lagra lösenord till certifikat i din kod? Varför/Varför inte?
8. Förklara HELA TLS-handskaket.
9. När används symmetrisk kryptering?
    1. När används asymmetrisk kryptering?
    2. Vad innehåller en cipher suite?
    3. Förklara nyckelorden nedan (de är även bra att kolla på för övriga frågor)
        - X.509
        - TLS/SSL
        - Signatur
        - RSA
        - Private key
        - Public key
        - Cipher suite
        - HTTPS
        - MD5/SHA
        - AES