PKI i et nøtteskall

Asymmetrisk kryptering

- Privat nøkkel: Hemmelig. Bare eieren har denne.
- Offentlig nøkkel: Offentlig. Alle har tilgang på denne.
- Krypterer man tekst med den ene nøkkelen, så kan teksten kun dekrypteres med den andre.
- På den måten kan man sende hemmelige beskjeder til eier av privat nøkkel, eller verifisere at eier av privat nøkkel er opphavet til dataene (digital signering).

Når bruker man asymmetrisk kryptering?

- Til digital signering
- Til å utveksle hemmelig nøkkel for symmetrisk kryptering

Symmetrisk kryptering er billigere (krever mindre prosessering) enn asymmetrisk, så vi vil helst bruke symmetrisk kryptering når vi sender mange pakker frem og tilbake.

Utveksle hemmelig nøkkel for symmetrisk kryptering via asymmetrisk kryptering

- Klient genererer en tilfeldig streng med tall (hemmelig nøkkel)
- Klient krypterer denne med tjeners offentlige nøkkel
- Tjener dekrypterer med privat nøkkel
- Klient og tjener har nå en hemmelig nøkkel som ingen andre kjenner

- Dette er sånn man gjør det i HTTPS!

HTTPS (HTTP over TLS)

- Klient etterspør HTTPS-session hos tjener
- Tjener svarer med sertifikat (inneholder offentlig nøkkel)
- Klient genererer nøkkel, krypterer med tjeners offentlige nøkkel
- Klient sender denne til tjener
- Tjener dekrypterer den
- Sesjonen kan fra nå av krypteres med felles hemmelig nøkkel

Hva er problemet med dette?

- Man-in-the-middle-angrep:
  - En angriper med kontroll over en av ruterne langs veien kan bytte ut tjenerens offentlige nøkkel med sin egen offentlige nøkkel før pakken sendes videre til klient.
  - Angriperen fortsetter å være mellomledd. Motta hemmelig nøkkel fra klient, kryptere med tjeners offentlige nøkkel og sende videre, og deretter bare lytte passivt med den hemmelige "symmetriske" nøkkelen. Eventuelt endre meldinger enten ene eller andre veien. Full kontroll over kommunikasjonen.

Løsning?

- Forsikre seg om at det digitale sertifikatet med tjenerens offentlige nøkkel ikke har blitt endret på veien, ved at en "Certificate authority" signerer sertifikatet med sin private nøkkel.
- Klient kan da bruke CAens offentlige nøkkel for å bekrefte at dette sertifikatet virkelig er skrevet av CAen. CAen går god for all informasjonen i sertifikatet, som sier hvem sertifikatet gjelder for, og hva som er den offentlige nøkkelen deres.

Men hva med CAens offentlige nøkkel?

- Den ligger innbakt i nettleseren din. Så lenge installasjonen av nettleser er trygg og nettleseren beskytter disse nøklene skikkelig, så er ektheten til CAenes offentlige nøkler trygg.

Så hva er PKI?

- Det er bare en betegnelse på denne infrastrukturen som lar oss distribuere offentlige nøkler på en trygg måte. Nemlig hele dette systemet med CAer og sertifikater, og distribuering av offentlige CA-nøkler i nettlesere.
- Public Key Infrastructure (Offentlig nøkkel - infrastruktur).