NTNU

Norges teknisk-naturvitenskapelige universitet

Får vi lov til å beskytte internett?

Hva gjør revisjonen av eIDAS-forordningen?

Kristian Gjøsteen, Institutt for matematiske fag

IDentitet 2024, 19. april 2024

En programerklæring?

Vi må legge til grunn at folk er ærlige og redelige.

En norsk statsråd, januar 2024

En programerklæring?

Sertifikater

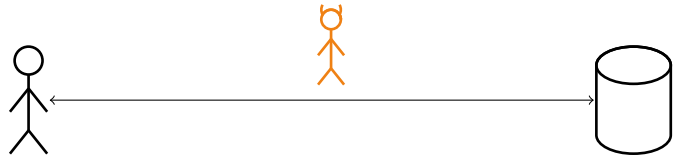
Sikkerhet

eIDAS

Konsekvenser

Problemet

Jeg ønsker å snakke med et nettsted via internett.



Hvordan vet jeg hvem jeg snakker med?

- Problemet er ikke nytt, men det blir mer akutt med internett.

Problemet

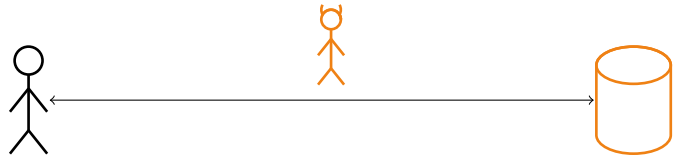
Jeg ønsker å snakke med et nettsted via internett.

Hvordan vet jeg hvem jeg snakker med?

- Problemet er ikke nytt, men det blir mer akutt med internett.
- Problemet er *ikke* om jeg kan stole på den jeg snakker med.
  - Hvordan vet vi hvem som er (eller vil bli) skurker?

Problemet

Jeg ønsker å snakke med et nettsted via internett.

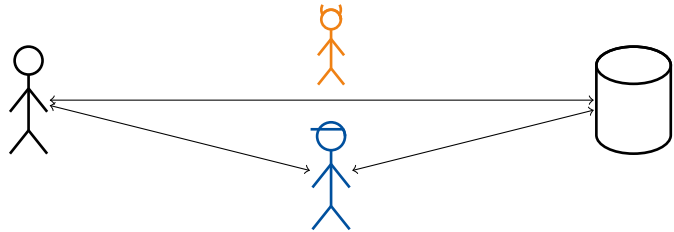


Hvordan vet jeg hvem jeg snakker med?

- Problemet er ikke nytt, men det blir mer akutt med internett.
- Problemet er *ikke* om jeg kan stole på den jeg snakker med.
  - Hvordan vet vi hvem som er (eller vil bli) skurker?
  - Skurker kan bryte seg inn på noen andres nettsted.

Problemet

Jeg ønsker å snakke med et nettsted via internett.



Hvordan vet jeg hvem jeg snakker med?

- Kryptografi garanterer at den jeg snakker med er i besittelse av en bestemt nøkkel.
- En *offentlig-nøkkel-infrastruktur* forteller meg hvem nøkkelen tilhører.

Økonomi

I en offentlig-nøkkel-infrastruktur går *sertifikatutstedere* god for hvem nøklene tilhører.

Økonomi

I en offentlig-nøkkel-infrastruktur går *sertifikatutstedere* god for hvem nøklene tilhører.

- Tidlig på 90-tallet var sertifikater dyre og sertifikatutstedere mye verdt.
- Sertifikater ble stadig billigere.
  - Det har sammenheng med at sertifikatutstederne stilte færre krav.

Økonomi

I en offentlig-nøkkel-infrastruktur går *sertifikatutstedere* god for hvem nøklene tilhører.

- Tidlig på 90-tallet var sertifikater dyre og sertifikatutstedere mye verdt.
- Sertifikater ble stadig billigere.
  - Det har sammenheng med at sertifikatutstederne stilte færre krav.
- Nå om dagen kan du betale. Eller få sertifikatene gratis.
  `letsencrypt.org` er mest kjent. Det finnes også norske leverandører.

Praksis

Nettleseren viser oss adressen til nettsiden vi snakker med.

Adressen er bare løselig knyttet til hvem nettsiden tilhører.

- `hurtigruten.no` eller `hurtigruta.no`?
- Hvem er `trdmk.no`? `mknu.no`?

Praksis

Nettleseren viser oss adressen til nettsiden vi snakker med.

Det har vært mange forsøk på forbedringer.

- *Extended validation*-sertifikater var et forsøk på å:
  - knytte sertifikater sterkere til eieren; og
  - vise forståelig informasjon til brukeren (bl.a. grønne adresser).

Praksis

Nettleseren viser oss adressen til nettsiden vi snakker med.

Det har vært mange forsøk på forbedringer.

- *Extended validation*-sertifikater var et forsøk på å:
  - knytte sertifikater sterkere til eieren; og
  - vise forståelig informasjon til brukeren (bl.a. grønne adresser).
- Det ble tidlig klart[1] at EV-sertifikater ikke hadde noen sikkerhetseffekt.
- EV-sertifikater kan tolkes som et forsøk på å øke prisen på sertifikater.

[1] F.eks. Collin Jackson, Daniel R. Simon, Desney S. Tan, Adam Barth: An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. Financial Cryptography 2007: 281-293

Praksis

Nettleseren viser oss adressen til nettsiden vi snakker med.

Det har vært mange forsøk på forbedringer.

- *Extended validation*-sertifikater var et forsøk på å:
  - knytte sertifikater sterkere til eieren; og
  - vise forståelig informasjon til brukeren (bl.a. grønne adresser).
- Det ble tidlig klart[1] at EV-sertifikater ikke hadde noen sikkerhetseffekt.
- EV-sertifikater kan tolkes som et forsøk på å øke prisen på sertifikater.
- EV-sertifikater døde hen ca. 2018.

[1] F.eks. Collin Jackson, Daniel R. Simon, Desney S. Tan, Adam Barth: An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. Financial Cryptography 2007: 281-293

Praksis

Nettleseren viser oss adressen til nettsiden vi snakker med.

Et sertifikat for et nettsted sier nå bare at *eieren av nøkkelen kontrollerer nettstedet*.

Praksis

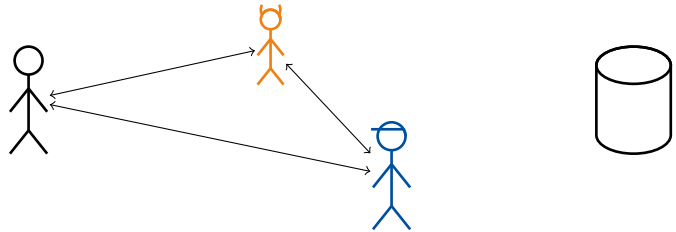
Nettleseren viser oss adressen til nettsiden vi snakker med.

Et sertifikat for et nettsted sier nå bare at *eieren av nøkkelen kontrollerer nettstedet*.

Min påstand er at det *ikke er noen sikkerhetseffekt* av dyre sertifikater for nettsteder.

Angrep

Med et falskt sertifikat og kontroll over nettverket kan du angripe brukerne til nettstedet.



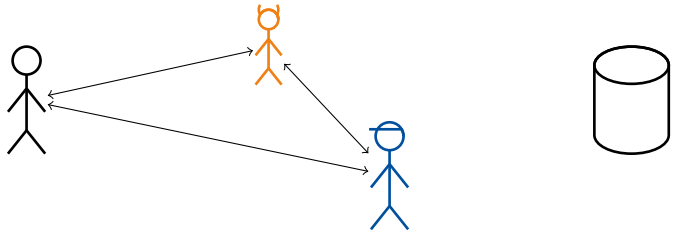
Vi må stole på sertifikatutstederne. Google-nettsteder er populære angrepsmål.

- I 2010 angrep Iran en nederlandsk sertifikatutsteder og utstedte falske sertifikater.
- I 2015 utstedte et kinesisk selskap falske sertifikater.

I 2010 var målet iranske borgere, hovedsaklig. Det virker uklart hva målet var i 2015.

Angrep

Med et falskt sertifikat og kontroll over nettverket kan du angripe brukerne til nettstedet.



Vi må stole på sertifikatutstederne. Google-nettsteder er populære angrepsmål.

- I 2010 angrep Iran en nederlandsk sertifikatutsteder og utstedte falske sertifikater.
- I 2015 utstedte et kinesisk selskap falske sertifikater.

I 2010 var målet iranske borgere, hovedsaklig. Det virker uklart hva målet var i 2015.

Ingen av disse utstederne finnes lenger.

Sikkerhetstiltak

Det stilles en rekke sikkerhetskrav til sertifikatutstedere, og særlig viktig er:

- *Certificate Transparency* lar oss sjekke at utstederne er ærlige.
- *Certificate Pinning* låser fast et kjent sertifikat, slik at forfalskning er bortkastet.

Mitt inntrykk er at Google har vært en særlig pådriver for dette.

Hvem får utstede sertifikater?

Grovt sett: Leverandører av nettlesere og operativsystemer bestemmer hvem som får lov til å utstede sertifikater.

- Google: Android, Chrome
- Apple: MacOS, iOS, iPadOS, Safari
- Microsoft: Windows, Edge
- Mozilla: Firefox
- Samsung: (nettleser for telefoner/nettbrett?)
- Opera: Opera (nettleser)

I praksis gir denne kabalen et akseptabelt resultat, særlig siden sertifikater er gratis.

Hvem får utstede sertifikater?

Grovt sett: Leverandører av nettlesere og operativsystemer bestemmer hvem som får lov til å utstede sertifikater.

- Google: Android, Chrome
- Apple: MacOS, iOS, iPadOS, Safari
- Microsoft: Windows, Edge
- Mozilla: Firefox
- Samsung: (nettleser for telefoner/nettbrett?)
- Opera: Opera (nettleser)

I praksis gir denne kabalen et akseptabelt resultat, særlig siden sertifikater er gratis.

Hva sier EU til dette?

Artikkel 45

Krav til kvalificerede certifikater for webstedsautentifikation

[…]

1a. De kvalificerede certifikater for webstedsautentifikation, der udstedes i overensstemmelse med denne artikels stk. 1, **skal anerkendes af webbrowserudbydere**. Webbrowserudbydere sikrer, at de identitetsdata, der attesteres i certifikatet, og yderligere attesterede attributter **vises på en brugervenlig måde**.

[…]

Hva betyr dette?

- Nettleserne (og dermed brukerne) skal stole på alle EU stoler på.

Artikkel 45

Krav til kvalificerede certifikater for webstedsautentifikation

[…]

1a. De kvalificerede certifikater for webstedsautentifikation, der udstedes i overensstemmelse med denne artikels stk. 1, **skal anerkendes af webbrowserudbydere**. Webbrowserudbydere sikrer, at de identitetsdata, der attesteres i certifikatet, og yderligere attesterede attributter **vises på en brugervenlig måde**.

[…]

Hva betyr dette?

- Nettleserne skal vise brukerne informasjon. Selv om vi vet det ikke virker.

Artikkel 45a

Forebyggende foranstaltninger vedrørende cybersikkerhed

1. Webbrowserudbydere må ikke træffe foranstaltninger i strid med deres forpligtelser fastsat i artikel 45, navnlig kravene om at anerkende kvalificerede certifikater for webstedsautentifikation og vise de opgivne identitetsdata på en brugervenlig måde.
2. Uanset stk. 1 og kun i tilfælde af begrundet mistanke om sikkerhedsbrud eller tab af integritet for et identificeret certifikat eller sæt af certifikater kan webbrowserudbydere træffe forebyggende foranstaltninger vedrørende det pågældende certifikat eller sæt af certifikater.

Hva betyr dette?

- Kan nettleserne stenge ute en sertifikatutsteder?

Artikkel 45a

Forebyggende foranstaltninger vedrørende cybersikkerhed

1. Webbrowserudbydere må ikke træffe foranstaltninger i strid med deres forpligtelser fastsat i artikel 45, navnlig kravene om at anerkende kvalificerede certifikater for webstedsautentifikation og vise de opgivne identitetsdata på en brugervenlig måde.
2. Uanset stk. 1 og kun i tilfælde af begrundet mistanke om sikkerhedsbrud eller tab af integritet for et identificeret certifikat eller sæt af certifikater kan webbrowserudbydere træffe forebyggende foranstaltninger vedrørende det pågældende certifikat eller sæt af certifikater.

Hva betyr dette?

- Kan nettleserne tilbakekalle alle sertifikatene fra en sertifikatutsteder?

Artikkel 45a

Forebyggende foranstaltninger vedrørende cybersikkerhed

3. Hvor en webbrowserudbyder træffer forebyggende foranstaltninger i medfør af stk. 2, underretter webbrowserudbyderen skriftligt og uden ugrundet ophold Kommissionen, det kompetente tilsynsorgan, den enhed, som certifikatet er udstedt til, og den kvalificerede tillidstjenesteudbyder, der har udstedt det pågældende certifikat eller sæt af certifikater, om sin mistanke sammen med en beskrivelse af de foranstaltninger, der er truffet for at afbøde denne mistanke. Når den kompetente tilsynsorgan modtager en sådan underretning, udsteder den en kvittering for modtagelsen til den pågældende webbrowserudbyder.

Hva betyr dette?

- Er det lurt å pålegge ekstra papirarbeid når man håndterer ting som kan haste?

Artikkel 45a

Forebyggende foranstaltninger vedrørende cybersikkerhed

4. Det kompetente tilsynsorgan undersøger spørgsmålene i underretningen i overensstemmelse med artikel 46b, stk. 4, litra k). Når resultatet af denne undersøgelse ikke fører til inddragelse af certifikatets status som kvalificeret, underretter tilsynsorganet webbrowserudbyderen herom og anmoder den pågældende udbyder om at bringe de forebyggende foranstaltninger, der er omhandlet i nærværende artikels stk. 2, til ophør.

Hva betyr dette?

- Nasjonale organer bestemmer hva nettleserne får lov til.

Konsekvenser?

Det er uklart for meg hva som blir de faktiske konsekvensene av dette.

- Det kan kanskje gi noen europeiske selskaper økt omsetning.

Konsekvenser?

Det er uklart for meg hva som blir de faktiske konsekvensene av dette.

- Det kan kanskje gi noen europeiske selskaper økt omsetning.
- Det er vanskelig å tenke seg hvordan dette kan bidra til økt sikkerhet.

Konsekvenser?

Det er uklart for meg hva som blir de faktiske konsekvensene av dette.

- Det kan kanskje gi noen europeiske selskaper økt omsetning.
- Det er vanskelig å tenke seg hvordan dette kan bidra til økt sikkerhet.
- Man kan tenke seg at nettleserne skrur av sikkerhetsfunksjonalitet i Europa.

Konsekvenser?

Det er uklart for meg hva som blir de faktiske konsekvensene av dette.

- Det kan kanskje gi noen europeiske selskaper økt omsetning.
- Det er vanskelig å tenke seg hvordan dette kan bidra til økt sikkerhet.
- Man kan tenke seg at nettleserne skrur av sikkerhetsfunksjonalitet i Europa.
- Forhåpentligvis blir den eneste konsekvensen at EU kaster bort tid og krefter.

Konsekvenser?

Det er uklart for meg hva som blir de faktiske konsekvensene av dette.

- Det kan kanskje gi noen europeiske selskaper økt omsetning.
- Det er vanskelig å tenke seg hvordan dette kan bidra til økt sikkerhet.
- Man kan tenke seg at nettleserne skrur av sikkerhetsfunksjonalitet i Europa.
- Forhåpentligvis blir den eneste konsekvensen at EU kaster bort tid og krefter.

EU burde ikke gjort noe.

Eventuelt, EU burde brukt de eksisterende mekanismene.

Konsekvenser?

Det er uklart for meg hva som blir de faktiske konsekvensene av dette.

- Det kan kanskje gi noen europeiske selskaper økt omsetning.
- Det er vanskelig å tenke seg hvordan dette kan bidra til økt sikkerhet.
- Man kan tenke seg at nettleserne skrur av sikkerhetsfunksjonalitet i Europa.
- Forhåpentligvis blir den eneste konsekvensen at EU kaster bort tid og krefter.

EU burde ikke gjort noe.

Eventuelt, EU burde brukt de eksisterende mekanismene.

Forøvrig: Bitcoin bør skrus av. Migrasjonen til kvantesikker kryptografi er viktig.