IN1020 - Datasikkerhet og nettverkskommunikasjon: Løsningsforslag gruppetime 6 (uke 40)

1. Passord som autentiseringsfaktor:

   (a) Et godt passord bør: Være så langt som mulig (vanskeligere å knekke i brute-force angrep), være unikt, ikke være enkelt å gjette (f.eks. en vanlig setning eller ord, sekvens av etterfølgende nummer, kun bestå av en eller to bokstaver), ikke kunne assosieres med deg eller tjenesten passordet gjelder for.

   (b) Skriv dem gjerne ned! Men oppbevar notatet som en verdigjenstand. Ikke klistre legg den under tastaturet på kontoret :-) Bruk kanskje en passordbank?

   (c) En vanlig person har i dag brukerkontoer på så mange ulike steder at de fleste nok velger å bruke samme passord flere steder. Selv om dette gjør jobben enklere for deg som bruker, vil det også gjøre deg mer sårbar. Hvis en tjeneste hackes og uvedkommende får tak i brukernavnet og passordet ditt vil de garantert prøve den samme kombinasjonen alle på andre kjente tjenester eller plattformer. Og plutselig sitter de med tilgang til store deler av ditt digitale liv.

   (d) Sikkerheten overlates ofte til brukeren selv, ved at vedkommende selv får bestemme hva passordet skal være. Til tross for at mange tjenester/plattformer setter krav til lengden av passord, til bruk av bokstaver, tegne, tall osv., kan du som bruker likevel velge et dårlig passord, f.eks. noe som er sterkt assosiert med deg som person, med tjenesten passordet fungerer til, osv.

2. Refleksjonsoppgave uten fasitsvar.

3. Det spesielle med bankkort (og mange andre typer adgangskort) er at både identifikatoren og autentifikatoren "sitter" i kortet. Bankkortet *presenterer* et kontonummer (identifikator), samtidig som det *autentiserer* med elektronikken innebygget i kortet. I de tilfellene du også må taste kode benyttes 2FA (kombinasjon av noe du har o noe du vet).

4. Tilgangskontroll

   (a) Autorisering = å **spesifisere** tilgangrettigheter.

   Tilgangskontroll = å **håndheve** tilgangsrettigheter.

   Autorisasjon er altså det som gjøres når en bestemmelse (policy) om hvem eller hva som skal ha tilgang til en ressurs nedfelles. Autorisering defineres som det å spesifisere tilgangsrettigheter til dataressurser.

   Tilgangskontroll defineres som det å håndheve disse tilgangsrettighetene i et datasystem hver gang et subjekt (bruker, prosess, maskin, ol.) ønsker å utføre en handling (lese, endre, slette, etc) på et objekt (en ressurss, f.eks. datafil eller et dataprogram/tjeneste). Å skulle utføre tilgangskontroll for kombinasjonen subjekt, handling, ressurs vil dermed kreve at subjektet er autentisert (vi vet hvem det er), og at forespørselen kan kontrolleres mot et forhåndsbestemt regelverk (autorisasjonen, policyen) og enten godkjennes eller avvises.

   (b) Noen eksempler på tenkelige (men ikke nødvendigvis ønskelige!) handlinger:

   - Student ønsker å levere en oppgave

- Student ønsker å se en medstudents innlevering
- Student ønsker å se tilbakemelding
- Retter vil laste ned en students oppgave
- Retter vil slette en students innlevering
- Retter vil godkjenne en students innlevering

(c) For å implementere policyer for autorisasjon i et datasystem er det nødvendig med tilgangskontroll. Tilgangskontroll krever autentisering, samt et system/program/applikasjon som har som oppgave å kan kontrollere og enten godkjenne eller avvise en forespørsel fra et subjekt om å utføre en gitt handling på et objekt.

5. Trusler mot autentisering

   (a) Angripere kan gjette passord fordi svake passord er tillatt eller det ikke finnes begrensninger på antall forsøk. Med cracket passord kan angriper logge inn.

   (b) Biometrisk autentisering kan manipuleres på grunn av svak beskyttelse mot presentasjonsangrep (f.eks. å bruke gummifinger, eller å vise bilde av ansikt)

6. Trusler mot tilgangskontroll

   (a) Identitetstyveri fører til at noen som ikke skulle hatt tilgang likevel får tilgang (eks. stjålet brukernavn/passord)

   (b) Autentiserte brukere får uautorisert tilgang til ressurser fordi policy/regler for tilgangskontroll ikke håndheves korrekt og sikkert av systemet.

7. Linjesvitsjing settes det opp en dedikert linje som brukes under hele kommunikasjonen, denne er statisk, og kan ikke endre seg. Den er tilkoblingsorientert, hvilket vil si at kommunikasjonen må først settes opp igjennom hele nettet før kommunikasjonen kan begynne. Når kommunikasjonen er ferdig kobles linjen ned.

   Beskjed-svitsjing er Tilkoblingsløs, beskjeden trenger ikke nødvendigvis følge samme vei hver gang, og det er ingen dedikert linje mellom sender og mottaker.

   Internett i dag bruker pakkesvitsjing, som ligner veldig mye på beskjed-svitsjing.

8. En protokoll er regler for hvordan kommunikasjonen mellom maskiner skal foregå. Protokoller er nødvendig for at man skal kunne kommunisere med flere forskjellige typer maskiner på forskjellige kontinenter.

9. De mest vanlige vi har rundt oss er Stjerne- eller tre-topologi med kablet nettverk (Ethernet) og Broadcast-nettverk (WiFi, 4G, 5G)

10. Diskuter I gruppetimen. Dere bør være innom behovet for å begkytte kommunikasjonen (for eksempel med kryptering) i broadcast nettverk.

    Dere kan også også snakke om behoved for å beskytte kommunikasjonen i kablet nettverk. Selv om dette vil være sikrere enn trådløs kommunikasjon.

11. Det enklest er å tvinge bruker til å lage passord som er lange, samt tillate av det berukes såkalte passord-setninger (setninger som består av flere ord, og kan inkludere mellomrom/space). Man kan også vurdere å bruke autentiseringsløsninger fra en tredjepart, f.eks. med 2FA via Google, microsoft eller ID-portalen. Evt. andre idéer? Å ha en løsning med sikkerhetsspørsmål til brukeren er ofte ikke så lurt (lett å finne ut av for noen som kjenner deg eller søker opp informasjon om deg på nett f.eks) og spesielt ikke med såkalte passordhint. (Hvis man kommer ut for en løsning der man som bruker blir påtvunget sikkerhetsspørsmål og det spørres om hint bør man egentlig skrive noe tilfeldig :-)).

12. Case-oppgave:

    Alle sider av informasjonssikkerhet må vurderes, men spesielt konfidensialitet, integritet, autentisitet og sporbarhet (etterprøvbarhet).

    Skal alle alltid ha tilgang til all informasjon selv om man jobber på samme prosjekt? Hvis alle kan bruke en ulåst pc vet man ikke hvem som har endret/lagt til/slettet informasjon. Hvilke konsekvenser vil dette få, og for hvem? (Arbeidsplassen, deg selv, andre brukere) Kan du få problemer dersom en kollega bruker din pc til å utføre handlinger som ikke er tillatt? F.eks. spre informasjon som ikke skal spres, laste ned filer ulovlig eller utført andre handlinger i strid med intern sikkerhetsinstruks.

13. Case-oppgave:

    (a) Persondata. Mange selskaper er interessert i å få tak i e-mail telefonnummer og ordrehistorikken til folk. Kundeklubb-poengene er også en verdi, siden disse kan byttes inn i rabatter.

    (b) Folk som vil selge kundeinfo videre, kunder som vil jukse til seg flere poeng.

    (c) Konfidensialitet bør prioriteres for å følge GDPR. Integritet er viktig for at kunders info alltid er korrekt. Uavviselighet kan være bra, slik at kunder ikke kan nekte for å ha brukt poeng eller annet.

    (d) Tilgangskontroll via innlogging, Integritet og uavviselighet kan opprettholdes via loggføring. Hash-algoritmer også for integritet (men dette har de ikke lært om ennå).

14. Case-oppgave:

    (a) Alt av info om spillet er en verdi. Fans vil være veldig interessert i å se konsept-tegninger, level-design, spoilere, animasjoner... etc... etc. I noen tilfeller kan det være en verdi å vite hvem som jobber med spillet, men dette er ikke så ofte hemmelig. Konkurrenter vil også være interessert i å se hvordan ting gjøres.

    (b) Fans av spillet vil ønske å få tak i alt de kan. Folk som hater spillet kan forsøke å sabotere. Ansatte kan lekke info. Konkurrenter kan ønske å stjele deler av arbeidet.

    (c) Integritet. Det verste som kan skje er nok at arbeid mistes. Konfidensialitet er også bra, slik at selskapet kan kontrollere markedsføringen selv.

    (d) Separat backup av all data. Tilgangskontroll og loggføring, slik at man kan kontrollere hvem som har tilgang til hva og hvem som har gjort hva.