Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

Del 7: Brukerautentisering

Oppgave 1: Passord

a. Hvorfor bør passord ikke lagres i klartekst på autentiseringstjeneren?
b. Hva menes med passordsalting, og hva er hensikten med det?
c. Hvilken kjent tjeneste på internett brukes for å sjekke om en bruker-ID (og passord) kan være stjålet. Sjekk om en av dine egne bruker-ID-er kan være stjålet, og endre passordet hvis den er det.
d. Nevn en grunn til at passord aldri bør gjenbrukes..

Løsningsforslag

a. Autentiseringstjenere må lagre passord på en eller annen måte. En mulig trussel er at passorddatabasen blir stjålet eller lekket. Det rapporteres stadig om slike hendelser. Hvis passordene lagres i klartekst er det en enkel sak å gjøre identitetstyveri av alle som har en bruker-ID i databasen. For å gjøre identitetstyveri vanskeligere bør databaser ikke lagre passord i klartekst.
b. At passord lagres som saltet hash betyr at passordet kombineres med en tilfeldig verdi (som kalles salt) og deretter hashes. Både hashverdien og saltet lagres i databasen. På den måten vil brukere alltid ha forskjellige hash selv om de har samme passord. Saltet hash gjør også at angripere ikke kan benytte forhåndsgenererte hashtabeller for å gjenfinne passord i databasen, fordi det ville kreve en separat tabell for hvert salt, noe som ikke er praktisk mulig.
c. Nettsiden som alle benytter er https://haveibeenpwned.com/
Det er ikke spesielt overraskende hvis en eller flere av dine kontoer er eksponert gjennom en lekket database. Hvis du kjenner igjen kontoen er det viktig å endre passordet. Hvis du har sterke passord er det som regel uproblematisk at en konto er eksponert, fordi angripere da ikke vil være i stand til å cracke passordet.
d. Hvis du gjenbruker passord på to eller flere kontoer, og hackere cracker passordet på en av kontoene, vil de lett kunne angripe andre kontoer som har samme passord.

Oppgave 2: Biometri

a. Forklar hvordan kvaliteten på et system for biometrisk autentisering kan uttrykkes med EER (Equal Error Rate).
b. Hvis et biometrisk system konfigureres med svært lav FMR (False Match Rate), hva er konsekvensen for FNMR (False Non-Match Rate)?
c. Se for deg et system som er konfigurert med svært lav FMR. I hvilken grad gjør det at systemet er robust mot tilsiktet forfalskning (eng. presentation attack)?

Løsningsforslag

a. Biometrisk autentisering har to typer feilrate som kalles FMR (False Match Rate) og FNMR (False Non-Match Rate). En rate er det samme som en prosentandel, men uttrykt i intervallet [0,1] i stedet for [0,100]. FMR er raten av uekte brukere som feilaktig blir godtatt. FNMR er raten av ekte brukere som feilaktig blir avvist. Hvis terskel for å godta brukere justeres opp vill FMR synke og FNMR øke, og omvendt. Terskelen kan justeres slike at FMR = FNMR, som da kalles EER (Equal Error Rate). Det er ønskelig at systemet gjør så lite feil som mulig, som betyr at det er ønskelig at EER er lav. Jo lavere EER, desto bedre kvalitet har systemet.
b. Hvis systemet konfigureres med svært lav FMR er det svært liten sannsynlighet for at en uekte bruker blir godtatt, men det medfører også at det blir en relativt stor sannsynlighet for at en ekte bruker blir avvist.
c. Lav FMR betyr **ikke** at systemet **ikke** kan lures. FMR reflektere kun raten av uekte brukere som feilaktig blir godtatt uten forsøk på forfalskning. Andel av vellykket tilsiktet forfalskning kan ikke måles som en rate. Hvis noen f.eks. klarer å lage et perfekt falskt fingeravtrykk vil de lykkes hver gang. Da ville FMR = 1, som er en meningsløs måleparameter.

Oppgave 3: Veileder for autentisering

a. Hva er formålet med å ha en veileder/forordning for e-autentisering?
b. Hvilken veileder/forordning for e-autentisering gjelder for Norge?
c. Nevn norske autentiseringstjenester som tilfredsstiller krav til høyeste autentiseringsnivå.

Løsningsforslag

a. Formålet med veileder/forordning for e-autentisering er at forvaltning av offentlige online tjenester underlegges et felles sett med krav til brukerautentisering.
b. Fra 2008 gjaldt *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor*, som spesifiserte 4 autentiseringsnivåer, der nivå 4 var høyest. Det europeiske eIDAS fra 2014 inneholder også et rammeverk for e-autentisering, som i prinsippet erstatter det norske rammeverket fra 2008. eIDAS er under revidering. I 2022 publiserte DigDir *Veileder for identifikasjon og sporbarhet*, som erstatter rammeverket fra 2008. Den nye veilederen spesifiserer 3 autentiseringsnivåer (kalt sikkerhetsnivåer) som er LAVT, BETYDELIG, og HØYT.
c. Autentiseringsnivå HØYT er høyeste nivå i den norske veilederen. Det tilsvarer autentiseringsnivå 4 i det gamle rammeverket fra 2008. Autentiseringsløsninger på nivå HØYT er f.eks. BankID, BankID-app, Buypass og Commfides.

Oppgave 4: Passordpolicy

a. Et passord regnes vanligvis som en autentikator basert på noe du vet. Diskuter om dette fortsatt er tilfelle når passordet er skrevet ned på papir eller et annet sted.
b. Sjekk typiske retningslinjer for passord, f.eks. UiOs beregning av kompleksitet i passord: https://www.uio.no/tjenester/it/brukernavn-passord/passordtjenester/hjelp/kompleksitet.html eller passordveileder fra NIST SP800-63B (*Section 5.1.1.2 Memorized Secret Verifiers* og *Section 10.2.1 Usability of Memorized Secrets*) https://pages.nist.gov/800-63-3/sp800-63b.html
   i) Hva sier retningslinjene om lengde og kompleksitet av passord?
   ii) Hva sier retningslinjene om krav til bytte av passord?
c. I hvilken grad følger UiOs passordpolicy NIST sin veileder?
d. Gi et eksempel på kortest mulig passord i henhold til passordpolicyen for UiO.
e. Hvorfor er det ofte anbefalt å huske passord, og ikke å skrive ned passord?
f. Anta at du ikke er enig med (e), foreslå og diskutere alternative metoder.

Løsningsforslag

a. Et passord som nedskrevet på papir kan betraktes som noe du vet i den forstand at du vet hvor papiret er lagret. Ellers må det betraktes som noe du har, det vil si at papiret/mediet der passordet er lagret er noe du har.
b. Retningslinjer for passord:
   i) Retningslinjer krever typisk at passord må å ha tilstrekkelig lengde og/eller kompleksitet. NIST-veilederen anbefaler at selvvalgte passord må ha minst 8 tegn (Section 5.1.1.2) som er temmelig kort. UiO sin policy fokuserer på lange passord.
   ii) UiO sin policy sier intet om krav til å endre passord, men alle som har brukerkonto på UiO opplever at USIT krever bytte av passord omtrent annethvert år. NIST-veilederen sier at virksomheter ikke bør tvinge brukere til å bytte passord, bortsett fra ved mistanke om kompromittering (Section 10.2.1). At passord i utgangspunktet kan forbli uendret er en relativt moderne trend i passordpolicyer. Bakgrunnen for denne trenden er forståelsen av at krav om passordbytte kan skape dårlige vaner hos brukere.
c. UiOs policy (sist endret 19. mai 2023) synes å være inspirert av NIST politikk om å ikke sette strenge kompositt-regler. Men UiOs policy avviker fra NIST sin policy om minimum lengde og anbefaling om å sjekke typiske svakheter i passord. UiOs passordkompleksitet er basert på et poeng-system hvor akseptable passord må score minst 32 poeng. Et passord på 18 identiske tegn (f.eks. 111111111111111111) får 33 poeng og vil bli godtatt.
   NIST anbefaler ≥ 8 tegn, og fraråder å kreve "kompositt-regler" dvs. å kreve tegn fra ulike kategorier, i motsetning til mange passordpolicyer som anbefaler nettopp det. NIST anbefaler å sjekke passord for typiske svakheter
d. UiO krever at et passord får **minst** 32 poeng. De korteste mulige passord som gir 32 poeng har 12 tegn. For eksempel, passordet «aaAA11111111» får 32 poeng, og vil bli godtatt..

   4 poeng for første tegn
   + 14 poeng (2 poeng hver) for de neste 7 tegn (tegn 2-8)
   + 6 poeng for de neste 4 tegnene (1,5 poeng hver for tegn 9-12)
   + 8 bonuspoeng hvis passordet har minst 2 tegn hver av 3 kategorier
   = 32 poeng

e. En memorert passord kan ikke lett bli mistet eller stjålet, hvis det er virkelig memorert (ikke glemt) og ikke er gjettbart for noen andre.
f. Vi samler flere og flere online-kontoer. Det er for mye å forvente at vi memorere et sterkt og unikt passord for hver konto. Brukerne må kunne lagre dem eller skrive dem ned et sted. Lagring av passord på papir er OK hvis du oppbevarer det trygt. Lagring av passord i en elektronisk enhet må gjøres med forsiktighet, det vil si at passordene alltid skal være krypterte. Hvis den er lagret i klartekst, må enheten være offline, dvs. ikke koblet til internett. Å benytte en passordbank har økende popularitet. Det kan virke paradoksalt at det faktisk kan være en sikker løsning å la en 3.part håndtere dine passord i skyen. Sjekk review av passordbanker: https://password-managers.bestreviews.net/
Selv om det forenkler håndtering av passord skaper det et ekstra ledd som kan ha sikkerhetssårbarheter, se f.eks.
https://password-managers.bestreviews.net/faq/which-password-managers-have-been-hacked/

Oppgave 5: Biometrisk autentisering og identifisering

a. Gi en kort og konsis beskrivelse av hva et biometrisystem er.
b. Et biometrisystem kan virke i enten autentiseringsmodus eller identifiseringsmodus. Forklar kort prinsippene for begge moduser.
c. Si hvilken av disse modusene er minst/mest effektive, dvs. som krever minst/mest prosessering, og forklare hvorfor.
d. Beskriv kort hvilken modus (autentisering eller identifisering) som brukes i) for pass og ii) for kriminalteknisk etterforskning.

Løsningsforslag

a. Et biometri-system er en automatisert metode å autentisere eller identifisere en person basert på en fysiologisk eller atferdsmessige karakteristika.
b. I autentiseringsmodus vil brukeren først oppgi sin identitet. En ny biometriprøve tas og sammenlignes med den lagrede biometri-malen som tilsvarer brukerens identitet. En beslutning om å avvise eller godkjenne brukeren gjøres basert på sammenligningsskåringen i forhold til en terskelverdi. I identifikasjonsmodus trenger ikke bruker å oppgi en identitet. En ny biometriprøve tas, sammenlignes med alle biometrimaler lagret databasen for å finne den beste skåringen.
c. Identifiseringsmodus er mindre effektiv siden det krever 1:N sammenligning i stedet for bare 1:1 sammenligning i autentiseringsmodus.

c. Modusene for bruk med pass og for kriminalteknisk etterforskning:
   i) Autentiseringsmodus brukes til ID-kontroll ved grenseoverganger. Pass lagrer den biometriske prøven i kryptert form, som kan hentes ut av det utstedende landet (men ikke av andre land) og sammenlignes med fingeravtrykkprøven som personen gir ved grensekontrollen. Noen land (f.eks. USA) sentraliserte databaser med fingeravtrykk / ansikt til personer som passerer grensene, slik at de ikke trenger de krypterte fingeravtrykkene som er lagret i passene.
   ii) Identifikasjonsmodus brukes til kriminalteknisk etterforskning. Etterforskerne må sammenligne prøven som er samlet inn på åstedet med prøver fra en database med potensielle mistenkte.

Oppgave 6: Optimalisering av biometrisk autentisering

a. Skåring ***s*** kvantifiserer likheten mellom innhentede biometriprøve og lagret mal av biometriprøve. Forklar hvordan skåring ***s*** og terskel ***T*** brukes til å bestemme om prøvene er *like par* eller *ulike par*, som fører til henholdsvis *aksept* eller *avvisning*.
b. Terskelen ***T*** kan justeres for å gi den optimale balansen mellom FMR (False Match Rate) (raten av feil aksept) og FNMR (False Non-Match Rate) (raten av feil avvisning). Forklar hvordan terskelen ***T*** bør justeres som funksjon av kostnadene forbundet med henholdsvis tilfeller av feil aksept og feil avvisning.

Løsningsforslag

a. Sammenligning av et par biometriske prøver genererer skåring ***s***. I tilfellet ***s ≥ T*** er konklusjonen *like par* (dvs. at de tilhører samme person), og dermed aksept. I tilfelle ***s < T*** er konklusjonen *ulike par*, og dermed avvisning.
b. Høy ***T*** verdi gir høy FNMR (feil avvisning) og lav FMR (feil aksept), som er økonomisk rasjonelt når det er høye kostnader forbundet med feil aksept. Lav ***T*** verdi gir høy FMR (feil aksept) og lav FNMR (feil avvisning), som er økonomisk rasjonelt når det er høye kostnader forbundet med feil avvisning.

Oppgave 7: Biometriske modaliteter

a. Enhver menneskelig fysiologisk eller atferdsmessige karakteristikk kan brukes som en biometrisk karakteristikk så lenge det tilfredsstiller syv grunnleggende krav. Beskriv kort disse syv grunnleggende kravene.
b. I hvilke situasjoner kan det være aktuelt å stille krav til trygghet ved bruk av biometri? Se f.eks. artiklene:
   http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm
   https://www.nytimes.com/2023/03/29/nyregion/indictments-nyc-gay-bars-homicide.html
c. Beskriv kort i hvilken grad hver av de følgende biometrimodaliteter oppfyller karakteristikkene og tilleggskrav du beskrev under spørsmål (a).
   • Fingeravtrykk
   • Ansiktsgjenkjenning
   For bakgrunnsinformasjon, se på artikkelen: "*An Introduction to Biometric Recognition*" http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Løsningsforslag

a. De grunnleggende kravene er:
   - Universalitet: hver person skal ha karakteristika for modaliteten;
   - Entydighet: alle personer skal være tilstrekkelig forskjellige i forhold til karakteristika for modaliteten;
   - Varighet: biometriske karakteristika bør være tilstrekkelig uendrede (med hensyn til kriterier for sammenligning) over en periode;
   - Målbarhet: biometriske prøver kan lett samles inn.
   - Ytelse: den oppnåelige gjenkjenningsnøyaktigheten og hastigheten, ressursene som kreves for dette, og de operative og miljømessige faktorene som påvirker nøyaktigheten og hastigheten.
   - Aksept: i hvilken grad folk er villige til å akseptere bruken av en bestemt biometrisk modalitet i hverdagen;

- Anti-spoofing: det skal være vanskelig å lure systemet med falsk biometri (gummifinger, bilde av ansikt, AI-generert stemme osv.). Imidlertid vil det alltid være praktisk mulig og relativt lett, hvis angriperen har tilstrekkelige ressurser.

b. Trygghet (beskyttelse av liv og helse): Hvis biometrisk autentisering åpner for tilgang til betydelige verdier eller sensitive opplysninger kan trusselaktører bli insentivert til å angripe brukere fysisk for å tvinge biometri fra dem. I slike tilfeller er det tilrådelig at biometriprøver må innhentes i en trygg omgivelse. Det har skjedd at en finger er blitt kappet og at folk er blitt dopet ned og drept for å misbruke deres biometriske egenskaper. Ved bruk av biometri i åpne (og potensielt utrygge) omgivelser for tilgang til betydelige verdier eller sensitive opplysninger bør biometri, eventuelt kombinert med en brukerenhet, ikke være eneste autentiseringsfaktor.

c. I artikkelen av Jain, Ross and Prabhakar (2004) oppgis følgende tabell. Fokortelsene H, M, L står henholdsvis for Høy, Middels og Lav. Det betyr at H alltid er best (f.eks., H for anti-spoofing betyr at det er vanskelig å lure systemet).

	Univer-salitet	Entyd-ighet	Varig-het	Målbar-het	Ytelse	Aksept	Anti-spoofing
Ansiktsgjenkjenning	H	L	M	H	L	H	L
Fingeravtrykke	M	H	H	M	H	M	H

- **Ansiktsgjenkjenning:** Denne metoden er ikke-invasiv og har god universalitet og aksept. Det finnes ulike metoder for å få en nøyaktig kvantitative prøver slik at kollektabiliteten er god. Kvaliteten på innsamlede prøver/bilder kan variere betraktelig med lys og visningsvinkel som påvirker varighet negativt. Ansiktsgjenkjenning i seg selv gir et tvilsomt grunnlag for identifikasjon, slik at entydighet og ytelse er vurdert relativt lavt. Dette påvirker også spoofing, spesielt hvis personen ikke samarbeider (for eksempel ved å presentere en annen profilvinkel).
- **Fingeravtrykk:** En liten andel av folk har ikke egnet fingeravtrykk for identifikasjon på grunn av genetisk, alder, miljø eller yrke. Derfor er universalitet bare middels. Fingeravtrykk er svært entydig og temmelig permanent. Fingeravtrykksskannere er billige og brukes i masseproduserte produkter. Å innhente fingeravtrykk kan virke invasivt og gir assosiasjoner til kriminell aktivitet, slik at aksept kan være noe lavere enn andre biometriske modaliteter. Det kan diskuteres om fingeravtrykk skårer høyt på anti-spoofing.

Oppgave 8: Passnøkler

a. Hvordan utføres phishingangrep mot tradisjonell brukerautentisering?
b. Hva betyr det at en autentiseringsmetode er phishingresistent?
c. Hvorfor er passnøkler (FIDO/WebAuthn) phishingresistent?
   Se f.eks. https://m.youtube.com/watch?v=qMIAqdxNGpc&t=1258
d. Anta at passnøkler blir svært utbredt, slik at klassisk phishing ikke lenger kan benyttes for å stjele identiteter. Foreslå angrep mot phishingresistent brukerautentisering. Se f.eks. https://blog.talosintelligence.com/what-might-authentication-attacks-look-like-in-a-phishing-resistant-future/

Løsningsforslag

a. Phishingangrep mot autentisering betyr at offeret mottar en phishing-melding som lurer brukeren til å oppgi autentikatorer til angriperen. Phishing-meldingen inneholder typisk en lenke til en falsk nettside som f.eks. ser ut som nettsiden til en bank. Når offeret tror at hen logger inn med autentikatorer (f.eks. passord og engangskode) blir disse stjålet av angriperen som i sin tur bruker de samme autentikatorene til å logge inn til den ekte nettsiden.
b. Phishingresistent autentisering betyr at autentikatorene ikke kan stjeles eller ikke kan brukes mot andre nettsider enn den genuine nettsiden. Det skal ikke være mulig å oppgi autentikatorer til en falsk nettside. Det betyr typisk at autentikatorene er en funksjon av parametre lenger ned i internett-stacken som f.eks. URL (domenenavn) eller IP-adresse for det genuine nettstedet. Hvis brukeren blir lurt til å forsøke å logge seg på en falsk nettside, vil klientplattformen (f.eks. mobil eller laptopp) nekte å sende phishingresistente autentikatorer til den falske nettsiden fordi URL eller IP-adressen ikke stemmer med autentikatoren.
c. Passnøkler er kryptografiske nøkler som lagres på brukerens plattform og som benyttes for autentisering til ulike nettsteder som brukeren benytter. Passnøkler er phishingresistente fordi URL for hver passnøkkel er en funksjon av nettstedet nøkkelen brukes for autentisering. Hvis brukeren blir lurt til å forsøke å logge seg på en falsk nettside vil URL for det falske nettstedet ikke stemme med URL for det ekte nettstedet, slik at brukerens plattform vil nekte å bruke passnøkkelen for pålogging til det det falske nettstedet.
d. Det fins mange mulige angrep. Noen eksempler beskrives nedenfor.
    1. Sikkerhet ved passnøkler er avhengig av at plattformen håndhever policyen om at en passnøkkel bare skal brukes for autentisering mot nettstedet med samme URL som ligger i passnøkkelen. Et mulig angrep er at skadevare gjør at plattformen tillater bruke en passnøkkel til å autentisere seg mot andre nettsteder enn det nettstedet som har samme URL som passnøkkelen. Dermed kan det falske nettstedet autentisere seg videre mot det ekte nettstedet, og dermed spoofe brukeren.
    2. Angrep mot DNS kan gjøre at plattformen tror den er koblet til det ekte nettstedet, mens den egentlig er koblet til angriperens nettsted, og dermed blir lurt til å bruke passnøkkelen til å autentisere seg mot det falske nettstedet. Dermed kan det falske nettstedet spoofe brukeren på det ekte nettstedet.
    3. Brukeren vil som regel ha en alternativ måte å logge seg på. Et falsk nettsted kan gi beskjed til brukeren om at autentisering med passnøkler ikke virker, og at tradisjonelle passord må brukes i stedet. Med det stjålede passordet kan angriperen spoofe brukeren på det ekte nettstedet, og for eksempel opprette nye passnøkler, slik at brukeren blir lukket ut av sin konto.
    4. Angripere kan stjele brukerens plattform (mobiltelefon eller laptopp), og forfalske biometri for å åpne plattformen og bruke plattformens passnøkler for å spoofe brukeren på nettsteder.
    5. Plattformprodusenter tilbyr ordninger for å ha kopi av passnøklene i skyen. Tilgang til skyen må skje med en annen type autentikatorer enn passnøkler. Autentisering til skyen er dermed ikke phishingresistent. Angriperen kan utføre phishingangrep for å stjele slike autentikatorer for tilgang til skyen, og stjele brukerens passnøkler der.