Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

Teori 1 (Del 1): Grunnleggende sikkerhetsbegreper

Oppgave 1: Tilgangsautorisering

a. X.800 er en standard for sikkerhetstjenester i OSI (Open Systems Interconnection). Søk og finn X.800-standarden, eller besøk
https://www.itu.int/rec/T-REC-X.800-199103-I/en
Les definisjonene av konfidensialitet, integritet og autorisering i X.800. Er definisjonene av konfidensialitet og integritet fra X. 800 meningsfulle i forhold til hvordan autorisering er definert? Hvorfor eller hvorfor ikke?
b. Hvordan er autorisering definert på Wikipedia?
https://en.wikipedia.org/wiki/Authorization
c. Forklar om definisjoner av konfidensialitet, integritet og tilgjengelighet (KIT) i standardene X.800 og ISO/IEC 27000 gir mening på bakgrunn av Wikipedias definisjon av autorisering..

Løsningsforslag

a. X.800 definerer «autorisering» med to forskjellige betydninger, både som
1) å spesifisere tilganspolicy (*granting of rights*), og
2) å gi tilgang (*granting of access*).
Definisjonene på konfidensialitet og integritet i X.800 er meningsløse når autorisering defineres som at man blir autorisert ikraft av at man får tilgang, dvs. i betydning (2). Da ville en angriper med et stjålet passord være autorisert, uten brudd på konfidensialitet, som er meningsløst. Konfidensialitet og integritet gir mening når autorisering kun defineres i betydning (1).
Det er bare meningsfult å si at et system gir tilgang basert på autorisasjonspolicy som på forhånd er definert av en autoritet (et menneske) eller delegerte. Å autorisere tilgang er en policy-prosess som foregår under konfigurasjonsfasen av IAM (identitets- og tilgangshåndtering) før brukeren får tilgang til systemet. Autoriseringsprosessen består av å definere tilgangsrettighetene som brukeren skal ha i henhold til jobbrolle.
b. Wikipedia definerer "autorisering" som *"det å spesifisere brukernes tilgangsrettigheter til dataressurser"*.
c. Ved å klart skille mellom det å **spesifisere** tilgansrettigheter (tilgangsautorisering) og å **håndheve** tilgangsrettigheter (tilgangskontroll) gjør Wikipedias definisjon på autorisering at ISO og X.800 sine definisjoner på 'konfidensialitet', 'integritet' og 'tilgjengelighet' blir meningsfulle. Uten dette skillet ville definisjonene bli meningsløse.

Oppgave 2: Eksempler på angrep som kan gi brudd på KIT

Beskriv eksempler på angrep som kan forårsake sikkerhetsbrudd for hvert KIT-sikkerhetsmål, og mulige tiltak som kan forhindre angrepene. Angrepsbeskrivelsene skal være svært abstrakte, som f.eks. *«en hacker stjeler et passord og overtar brukerkontoen til en annen person»*.

a. Konfidensialitet
b. Integritet
c. Tilgjengelighet

Løsningsforslag

a. Konfidensialitet.

Eksempel 1:
En uetisk student får tak i passordet til en foreleser som har laget eksamensoppgaver på en eksamensplattform. Studenten logger seg inn og får tilgang til eksamensoppgavene før eksamen. Dette er brudd på konfidensialitet. Et mulig tiltak er at foreleseren bruker et bedre passord og passer bedre på passordet sitt, eller at universitetet innfører tofaktor-autentisering. Et annet tiltak er å styrke etikk og sikkerhetskultur blant studentene, slik at ingen finner på å jukse.

Eksempel 2:
Phishing epost som ber brukeren logge på en konto, med lenke til falsk nettside for kontoen. Hvis brukeren lar seg lure får angriper tak i det hemmelige passordet, som i seg selv er brudd på konfidensialitet. Dette angrepet er ID-tyveri, og gjør angriperen istand til videre angrep. Mulige tiltak er styrking av sikkerhetskultur og bevissthet rundt denne typen angrep, slik at brukeren ikke så lett lar seg lure.

b. Integritet.

Eksempel 1:
En uetisk student som har gjort det dårlig på eksamen får tak i passordet til en administrator som legger karakterene inn i systemet. Studenten logger seg inn på systemet og gir seg selv karakter A, som er brudd på integritet. Et mulig tiltak er tofaktor-autentisering som gjør at det ikke er tilstrekkelig å bare stjele et passord for at en angriper skal få uautorisert tilgang. Et annet tiltak er å styrke etikk og sikkerhetskultur blant studentene, slik at ingen finner på å jukse.

Eksempel 2:
Et angrep på dataintegritet er f.eks. en falsk wifi-ruter som er man-in-the-middle mellom nettleser/klient og webtjer som kommuniserer med ukryptert http-forbindelse, der den falske ruteren endrer på informasjon fra webtjeneren som vises i nettleseren. Mulig tiltak er kryptering av forbindelsen med VPN.

Eksempel 3:
Et angrep på systemintegritet er dataormer som automatisk sprer seg ved å utnytte sårbarheter i systemer, og på den måten infiserer stadig nye systemer. Et infisert system er et system som har mistet deler av sin integritet. Systemet kan

fortsatt fungere til en viss grad, men med redusert integritet og pålitelighet. Mulige tiltak er å fjerne utrydde dataormen og fjerne sårbarhetene som utnyttes av dataormen slik at ikke systemet blir infisert igjen.

c. Tilgjengelighet.

   Eksempel 1:
   En uetisk student som ikke har forberedt seg til eksamen ønsker at hele eksamen skal bli avlyst. For få dette til leier han et bottnett og kjører et DDoS-angrep mot eksamensplattformen slik at ingen studenter får tilgang. Som følge av angrepet beslutter administrasjonen å avlyse eksamen og utsette den til en uke senere. Dette er et brudd på tilgjengelighet. Et mulig tiltak er å installere en moderne brannmur som klarer å filtrere bort DDoS-trafikk. Et annet tiltak er å styrke studentenes sikkerhetskultur, moralske dømmekraft og etikk slik at ingen finner på å sabotere eksamen.

   Eksempel 2:
   Et angrep på tilgjengelighet er løsepengevirus som f.eks. kommer inn via phishing e-post. Løsepengevirus krypterer filer slik at de ikke lenger er tilgjengelige for brukerne. I tillegg til å styrke sikkerhetskultur og bevissthet er et mulig tiltak å benytte antivirusprogramvare som detekterer og filtrerer bort løsepengevirus før det starter å kjøre. Et annet tiltak er å ha god backup.

Oppgave 3: Trusler mot IAM (Identitets- og tilgangshåndtering)

En enkel metode for å identifisere trusler er å spørre «Hva kan gå galt?» eller «Hvordan kan dette angripes?».

a. Nevn relevante trusler mot (trinnene i) konfigureringsfasen av IAM (identitets- og tilgangshåndtering).
b. Nevne relevante trusler mot (trinnene i) bruksfasen av IAM (identitets- og tilgangshåndtering).

Løsningsforslag

Å kartlegge mulige trusler (dvs. mulige trusselscenarier) kalles «trusselmodellering». Det går i hovedsak utpå å beskrive mulige og relevante (tilsiktede/utilsiktede) handlinger og hendelsesforløp som kan forårsake sikkerhetsbrudd.

a. Potensielle trusler mot konfigurasjonsfasen av IAM er f.eks:
   i. Brukeren registreres med feil navn.
   ii. Brukeren er riktig registrert, men autentikatorene (f. eks passord eller brikke) sendes til feil person.
   iii. Riktig registrering og klargjøring av autentikatorer, men det konfigureres altfor vid tilgangsautorisasjon, som ikke er i samsvar med autorisasjonspolicyen som gjelder for jobbrollen.
b. Potensielle trusler mot bruksfasen av IAM er f. eks:
   i. Angripere kan gjette passord fordi svake passord er tillatt eller det ikke fins begrensninger på antall forsøk. Med cracket passord kan angriper logge inn.
   ii. Biometrisk autentisering kan manipuleres på grunn av svak beskyttelse mot presentasjonsangrep (f.eks. å bruke gummifinger, eller å vise bilde av ansikt)
   iii. Autentiserte brukere får uautorisert tilgang til ressurser fordi policy/regler for tilgangskontroll ikke håndheves korrekt og sikkert av systemet.

Oppgave 4: Brukerautentisering og data-autentisering

En bruker har autentisert seg til et nettsted på Internett ved starten av en økt, og bruker tjenester på webtjeneren via klientcomputeren. Forklar mulige scenarier som gjør at nettsted/webtjener i løpet av økten mottar falske data fra brukerklienten, dvs. data som **ikke** er autentisk sent av brukeren, på tross av at brukeren er korrekt autentisert.

Løsningsforslag

Brukerautentisering gir ikke nødvendigvis sterk garanti for data/meldingsautentisitet, dvs. at alle data som oversendes gjennom økten er basert på brukerens genuine intensjon. Det er plausibelt at brukeren forlater klientcomputeren uten å låse den, f.eks. for å ta en kaffe eller gå på toalettet, og at en annen person urettmessig bruker computeren til å sende data til webtjeneren. En annen plausibel mulighet er at klientcomputeren er infisert med en trojaner som genererer og sender data til serveren uten brukerens viten, selv om brukeren kanskje fysisk sitter foran computeren.

Hvis økten mellom klient og webtjener **Ikke** er beskyttet med https/TLS (Transport Layer Security) eller noen andre VPN (Virtual Private Network)-løsning, så er det plausibelt at et mann-i-midten-angrep kan skje, som dermed kan endre eller slette data som utveksles mellom nettleser og webtjener.