Assurance, Autenticity and Anonymity (AAA)

Assurance, Autenticity and Anonymity (AAA)

Besläktade med CIA men relaterar lite annorlunda till varandra

Assurance: Kan vi lita på att system och människor beter sig som väntat?

Autenticity: Är uppgifter genuina?

Anonymity: Kan uppgifter kopplas till en specifik person?

Assurance

Inom datasäkerhet handlar detta om att hantera vem/vad vi litar på

Pålitlighet är svårt att mäta

men pålitlighet och hantering av pålitlighet är nödvändigt!

- Kan vi lita på att ett OS är buggfritt?
- Kan datorn lita på att användaren är den den säger sig vara?
- Kan en filmtjänst lita på att du inte kopierar filmen och distribuerar den vidare?
- Kan en dator lita på att den IP-adress den ser är korrekt?

Verktyg för assurance

För att säkra pålitlighet så behöver vi

Policies: Hur förväntar vi oss att användare och system beter sig?

Rättigheter: Vad för aktiviteter har användare och system rätt att göra?

Baserat på detta gör vi säkerhetsmekanismer: System som hanterar rättigheter

Autenticity

Autenticitet handlar om förmågan att avgöra om uppgifter och rättigheter är autentiska, om de är äkta

Inte samma sak som autentisering

Inte heller samma sak som integritet (integriteten hos data i ett system)

Terminologi: Non-repudiation

Repudiation betyder nekande.

Non-repudiation betyder oförmåga att neka att utföra en handling.

Det är skillnad på att säga ja och att inte kunna säga nej.

T.ex. att lämna en uppgift när man inte borde. Systemet vet inte vem som har rättigheterna och saknar spärrar.

Om det inte är möjligt att bevisa att något är äkta eller falskt så skall man inte anta att det är äkta. Äktheten nekas, "is repudiated".

"In general, non-repudiation involves associating actions or changes with a unique individual.".

Non-repudiation och accountability

Icke-avvisande och ansvar

Om det blir fel så vill vi kunna spåra vad som hände och vem som gjorde det

Den som gjorde fel skall kunna hållas ansvarig

- I förebyggande syfte: avskräck angripare
- När det händer: Reparera/betala skador
- Förbättring: Hjälp oss att stärka systemet

Verktyg för accountability: Audit trail och digitala signaturer

Audit trail = verifieringskedja

För att avgöra ansvar

Sekundärt mål: För att finna svagheter som möjliggjorde attacken

Ytterligare mål: Hitta och återställa ändringen

Digitala signaturer är ett verktyg för att knyta en person till en uppgift eller handling

Det tredje Aet: Anonymitet

Vår identitet knyts till våra onlineaktiviteter:

- medicinsk dokumentation
- inköp
- juridiska uppgifter
- E-post
- webhistorik

Det tredje Aet: Anonymitet

- Konfidentiell identitet
- Göm innehållet
- Att det finns ett meddelande, vem som var i kontakt med vem
- Analys av datatrafik används för att upptäcka kopplingar mellan personer

"Unlinkability"

Verktyg för anonymitet

• Online: Proxies. Pålitliga tjänster för att se till att en handling inte kan spåras till en individ.

• Pseudonymer

• Aggregering, kombinering av data från många individer så sammanräkningen inte kan kopplas till individer

Några fler koncept

Security policy

Formulering av säkerhetsmålen för en organisation

Vad är det som skall skyddas?

Hur skall detta göra?

För att formulera en "policy" så behöver du veta

- vad som skall skyddas
- hur det kan vara hotat
- vad som hotar
- hur hotet kan hindras

Security policy, exempel på fysisk access

Vem har tillgång till området?

Finns det områden med begränsat tillträde?

Kommer man in med nyckel, kort, vakt...?

Behöver du ha en ID-bricka?

Måste besökare ledsagas?

Kontrolleras väskor vid tillträde?

När låses byggnaden?

Vem har nycklar?

Security policy, exempel på lösenord

Hur långt skall lösenordet vara? ("Max 8 tecken")

Är ASCII-lösenord med enbart gemener tillåtna?

Görs ett test mot ordlista när lösenordet skapas, eller gör systemet detta rutinmässigt?

Hur ofta krävs nytt lösenord?

Terminologi: Hot och STRIDE

Ett hot är en möjlig negativ effekt på tillgångar

Dessa kan kategoriseras, e.g. STRIDE-modellen:

- Spoof identities = Bluffidentiteter
- Tampering with data = Ändringar i data
- Repudiation = Vägran att uppfylla löften
- Informationsläckor
- DOS, denial of service
- Elevation of priviligies = Ökade privilegier

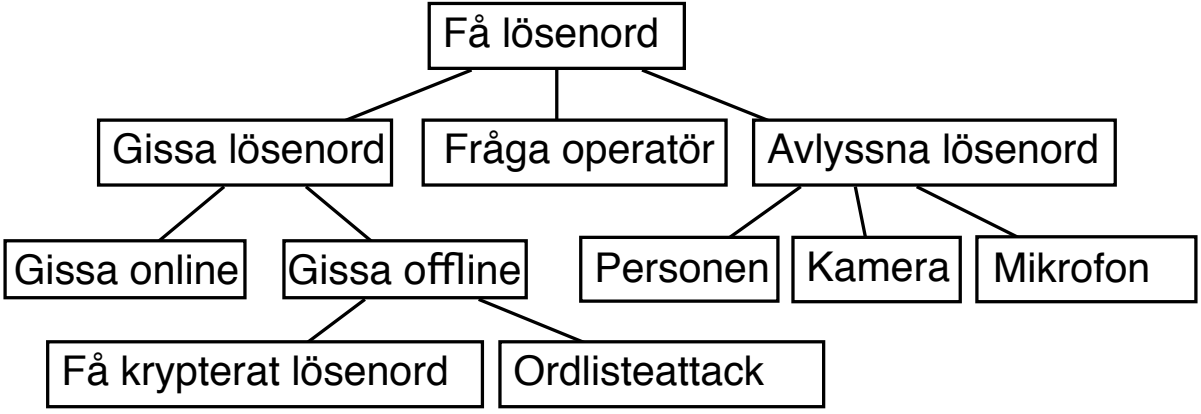
Ett alternativ är att identifiera hot efter källa

Attacksekvenser

En attack är en sekvens av steg som behövs för att genomföra hotet

Flera attacker kan behövas för att utföra hotet

Attacker är ofta strukturerade som träd:



Angriparens mål och metoder vs CIA

Ekonomisk vinning, ofta C-attacker

Skimming, phishing, industrispionage

För uppmärksamhet, ofta I-attacker

Skriva virus, sabotera websidor etc

Förstöra utrustning, ofta A-attacker

DDoS, systemkrascher etc

Uppföljning

Steget efter åtgärderna.

Hade åtgärderna önskad effekt?

Vad uppskattningarna korrekta?

Behöver strategin korrigeras eller kompletteras?

Har situationen ändrats sedan vi började? Vet vi mer?