dSik - Threats and Pitfalls

Lukas Peter Jørgensen, 201206057, DA4

16. juni 2014

1 Sikkerhedsmål

CAA

CAA står for:

Confidentiality: Information skal holdes hemmelig for uvedkommende, gælder både under forsendelse, opbevaring og behandling af data

Authenticity: Informationen er autentisk, den er ikke blevet manipuleret af en uautoriseret person.

Availability: Systemer skal være tilgængelig når de skal bruges

Definition af et sikkert system

Det er typisk svært eller umuligt at bevise et system er sikkert. Tit bliver man nødt til at lave mange antagelser om angriberens muligheder for at bevise at et system er sikkert og disse antagelser er typisk forkerte.

Vi bruger udtrykket "sikret system"istedet for "sikkert system"da det blot indikerer at vi har sikret systemet mod nogle bestemte tilfælde. Disse tilfælde defineres ved en *Sikkerhedspolitik* på baggrund af en $Trusselmodel$, og implementerer herefter denne sikkerhedspolitik vha. nogle *Sikkerhedsmekanismer*. På den måde får vi, at et sikret system kan beskrives som:

$$Sikretsystem = Sikkerhedspolitik + Trusselsmodel + Sikkerhedsmekanismer$$

2 Klassificering af angreb

STRIDE

Kategorisering ud fra en angribers mål.

S poofing Identity: At angriberen får mulighed for at udgive sig for at være en anden.

T ampering: At angriberen får mulighed for at manipulere data uden at dette bliver opdaget.

R epudiation: At angriberen får mulighed for at kunne nægte at have gjort noget høn har gjort.

I nformation Disclosure: At angriberen får adgang til data han/hun ikke burde se.

D enial of Service:

E levation of privilege:

Nogle gange kan angriberen godt have et mål, men alligevel får angrebet andre konsekvenser end målet.

X.800

Meget begrænset og ufyldestgørende opdeling. Opdeling i hvordan angrebet bliver opnået:
Passive angreb:

Eavesdropping:

Traffic Analysis:

Aktive angreb:

Replay:

Modification:

EINOO

Opdeling i hvorfra og hvem der angriber, EI er "Hvem"og NOO er "Hvorfra"

E xternal attackers:

I nsiders:

N etwork attacks: Lytte og modificere netværkstraffik.

O ffline attacks: Uautoriseret adgang til der er permanent lagret i systemet.

O nline attacks: Angriberen bryder ing og overvåger systemet mens det kører, som f.eks. at aflæse hemmelig information fra RAM'en

TPM

Opdeling ud fra hvilket forsvar der har fejlet:

T hreat Model: Angrebet var muligt fordi vores trusselsmodel var ukomplet.

P olicy: Angrebet var muligt fordi vores sikkerhedspolitik kommunikerede noget andet end vi ønskede.

M echanism: Angrebet var muligt fordi angriberen kunne bryde uden om vore sikkerhedsmekanismer.

3 Buffer overflows

Dårlig programmering kan føre til at man kan overflowe en buffer og derved ændrer i noget det ikke var meningen man skulle ændre i.

4 Cross-Site Scripting

Injecte et script på en anden side gennem et bruger input. F.eks. for at stjæle cookie.

5 SQL Injections

Injecte noget SQL igennem input felterne som f.eks. brugernavnet.

6 Covert Channels

At kommunikere gennem kanaler man ikke burde kunne kommunikere igennem.