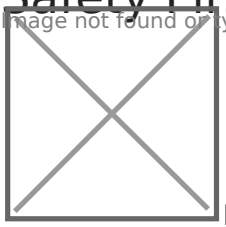
STRIDE

Safety First?



Niet altijd 'safety first'. Er moet een goede balans zijn tussen veilig en usability.

Daarnaast geldt dat als je het te ingewikkeld maakt voor gebruikers dat het dan onveiliger kan worden. Bijvoorbeeld als je een wachtwoord niet meer kan onthouden dan moet je het wel opschrijven.

Uit een Berceley University Study blijkt dat:

- 70% van de gebruikers vergeet hun wachtwoord
- 90% van de gebruikers die het wachtwoor dniet meer weten lopen weg van de site
- 40% van de gebruikers schrijft hun wachtwoorden op
- Wachtwoorden worden door een gemiddlede gebruiker 7-9 keer opnieuw gebruikt op andere sites

> Advies: gebruik een goede wachtwoord manager en gebruik voor elke site een uniek wachtwoord.

Liefst geen bekende/bestaande woorden. We zullen later nog zien waarom niet.

STRIDE

Bij ontwerp van veilige software moet je aan de volgende zaken denken:

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure

- **D**enial of Service
- **E**levation of Privilige

> Let op, STRIDE moet je kennen voor je cijfer voor it keuzevak.

Spoofing

Spoofing is je voordoen als iemand anders. Dat kan als je iemand zijn password op een of andere manier achterhaald. Dat kan op vele manieren: keyloaggers, phissing, camera's plaatsen, social engineering, brute force attack, ...

Tampering

Tampering is het veranderen van data. Dat kan bijvoorbeeld door SQL injection (data in de database veranderen), maar ook door achterdeurtjes te gebruiken om op een systeem binnen te komen en daarna gegevens te veranderen. Door spoofing toe te passen (je voordoen als iemand anders) kun je ook gegevens aanpassen.

Repudiation

"*I did not do that*!", is iets doen en dan zeggen dat jij het niet gedaan hebt. Bijvoorbeed geld opnemen en dan tegen de bank zeggen dat jij het niet hebt gedaan. De bank heeft dan bijvoorbeeld video-opnamen om te bewijzen dat jij het wel bent geweest.

Non repudiation betekent dat je een systeem zo maakt dat iemand niet of heel moeilijk kan ontkennen dat hij iets heeft gedaan. Log files kunnen daarbij heel handig zijn.

Information Discluse

Geheime of gevoelige informatie blootleggen. Denk aan Wiki leaks of aan het Facebooks Cambridge-Analytica schandaal.

Denial of Service

De 'bekende' DDOS aanvallen. Dit betekent zoveel verkeer genereren dat een webserver 'omvalt'. Dit wordt meestal met BOTs uitgevoerd. Dit is een virus dat op vele (miljoenen) computers is verspreid en dat op commando verkeer naar dezelfde site stuurt.

Jouw computer zou deel uit kunnen maken van een BOT netwerk, daar merk je over het algemeen weinig van.

Elevation of Privildge

Jouw rechten verhogen. Dus je bent een gewone gebruiker en je weet jezelf de rechten van de administrator of in een Unix-omgeving van root eigen te maken.

Revision #4
Created 17 September 2019 15:15:07 by Admin
Updated 21 September 2019 09:17:16 by Admin