Encryptie Algoritme en Sleutel

Veel threads (=bedreigingen) die zijn beschreven in het STRIDE model kunnen worden tgengehouden of worden verminderd door encryptie teo te passen.

We gaan ons wat meer verdiepen in encryptie, we leren:

- Wat (symetrische) encryptie is;
- hoe werkt een brute force attack werkt;
- en hoe je een veilig wachtwoord maakt.

In deze les leren we wat een encryptie algorime is en wat een encryptie-sleutel is.

Algoritme

Encryptie werd al toegepast ver voordat de eerste computer er was. De meest eenvoudige encryptie werkt per karakter. Elk karakter wordt omgezet naar een ander karakter. Een a wordt bijvoorbeeld een b, een b een c , een c en d en ga zo maar door. Het algoritme in dit geval is: 'neem telkens het volgende karakter in het alfabet', en om d eboodschap terug te vertalen (te ontcijferen) zou het algrotme zijn: 'neem telkens het vorige karakter uit het alfabet'.

Nu kan je dat met een stap grootte van 1 doen (neem het voglende karakter), maar je kunt het ook met bijvoorbeeld 3 doen, dus a wordt dan d en b wordt e, c wordt f en ga zo maar door. Je kunt het ook met 12 doen, of met 23.

Dit verschuiven van de letters met een stapgrootte x, noemen we het algoritme. Dit is de *manier* waarop we gaan encrypten.

Sleutel

Dit getal, zeg maar de stap grootte, noemen we de sleutel. In principe is het algorime altijd bekend maar is de sleutel geheim.

> Vraag: hoeveel verschillende sluetels denk je dat er zijn bij het hierboven beschreven algoritme?

Het encryptie algoritme en de sleutel samen zorgen voor de encryptie.

Voordat we het algoritme gaan maken dat een boodschap kan coderen en decoderen volgens het hierboven beschreven algoritme moeten we even een stukje theorie behandelen. Dit doen we in het volgende hoofdstuk.

Revision #4
Created 2019-09-17 15:39:27 UTC by Admin
Updated 2019-09-21 09:18:07 UTC by Admin