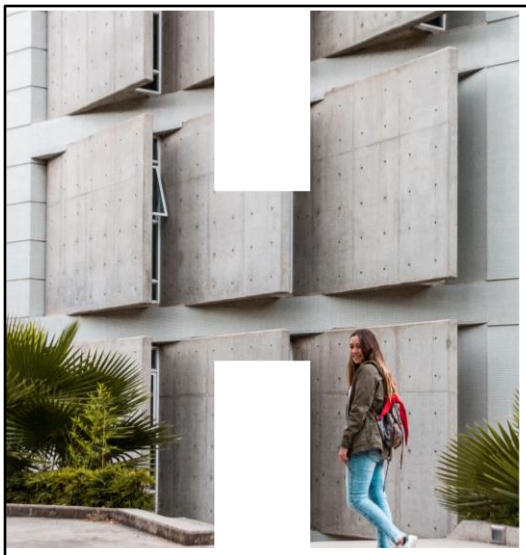


NEW

Cybersecurity

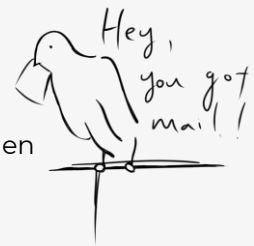
2020-2021

4. De kunst van het beschermen van geheimen

cisco

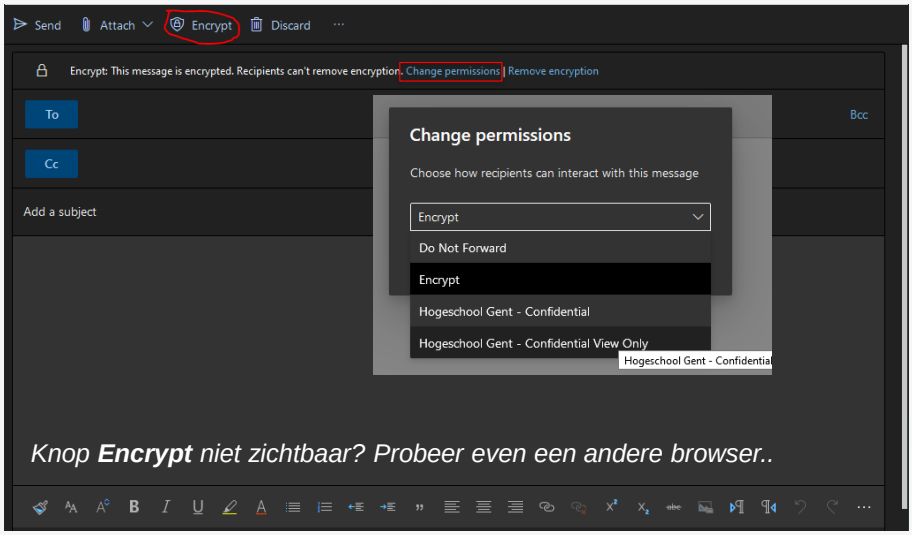
HO GENT

Vooraf...



- Verstuur via webmail.hogent.be enkele e-mails naar je eigen HOGENT adres, gebruikmakend van volgende opties:
  1. Encrypt
  2. Confidential
  3. Confidential View Only
- Je kan ook je persoonlijk (extern) e-mailadres toevoegen als extra ontvanger
- Bekijk het resultaat, zowel in de browser als via een mailclient (smartphone, e-mailprogramma op laptop, ...)
  - Kan je via de browser de e-mail rechtstreeks lezen? Kan je hem doorsturen?
  - Idem via e-mailclient?

HO GENT

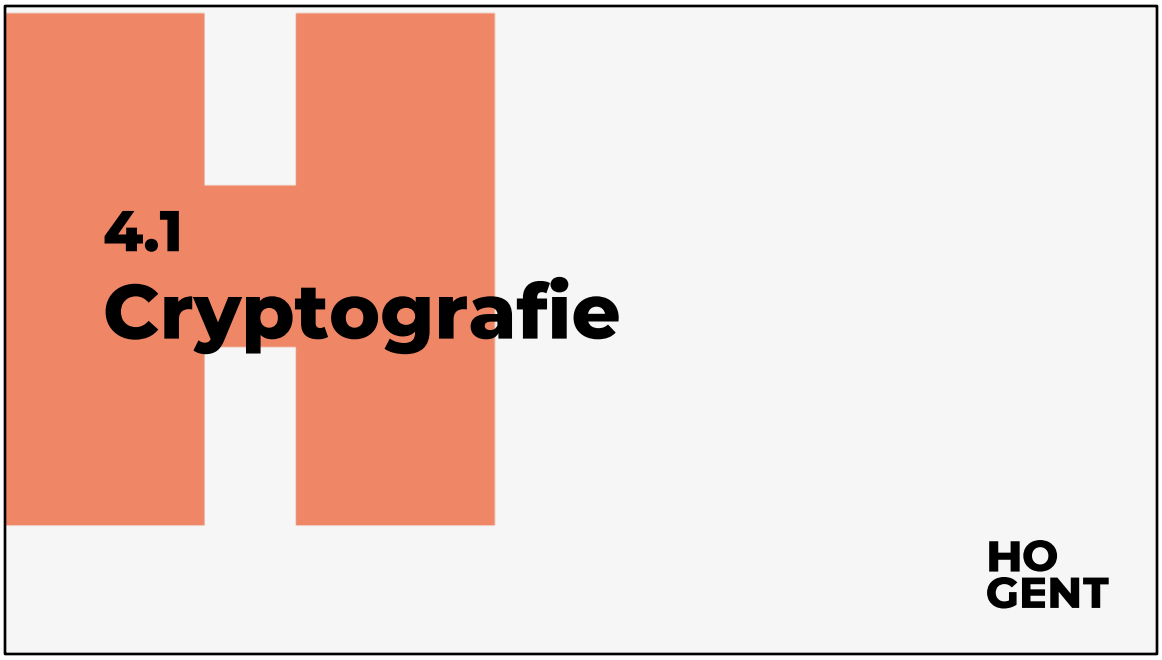


*Knop **Encrypt** niet zichtbaar? Probeer even een andere browser..*

HO GENT

4. De kunst van het beschermen van geheimen

4.1 Cryptografie
4.2 Toegangscontrole
4.3 Data verduisteren


4.1
Cryptografie
HO
GENT

4.1 Cryptografie

Overzicht

- Cryptologie: wetenschap maken en breken geheime codes
- Cryptografie: manier om gegevens op te slaan en te verzenden, zodat alleen de ontvanger deze kan lezen
  - Moderne cryptografie: gebruik van algoritmen om gevoelige data te beschermen
  - Cryptografie is veel ouder dan computers (duizenden jaren)! Belangrijk middel voor uitwisselen berichten in diplomatieke kringen
- Berichten encrypteren/decrypteren
  - Specifiek algoritme (cijfer/cipher) met aantal goed gedefinieerde stappen
  - Verschillende technieken:
    - Transpositie (omzetting)
    - Substitutie (vervanging)
    - One-time pad

HO GENT

Cryptologie is de wetenschap van het maken en breken van geheime codes. **Cryptografie** is een manier om gegevens op te slaan en te verzenden, zodat alleen de beoogde ontvanger deze kan lezen of verwerken. Moderne cryptografie maakt gebruik van computationeel beveiligde algoritmen om ervoor te zorgen dat cybercriminelen niet gemakkelijk beschermde informatie kunnen compromitteren.

De geschiedenis van cryptografie begon duizenden jaren geleden in diplomatieke kringen. Boodschappers van het hof van een koning brachten versleutelde berichten naar andere rechtbanken. Af en toe probeerden andere rechtbanken die niet bij de communicatie betrokken waren, berichten te stelen die waren verzonden naar een koninkrijk dat zij als een tegenstander beschouwden. Niet lang daarna begonnen militaire commandanten encryptie te gebruiken om berichten te beveiligen.

Elke versleutelingsmethode gebruikt een specifiek algoritme, een cijfer genaamd, om berichten te versleutelen en te ontsleutelen. Een cijfer is een reeks goed gedefinieerde stappen die worden gebruikt

om berichten te versleutelen en ontsleutelen. Er zijn verschillende methoden om cijfertekst te maken:

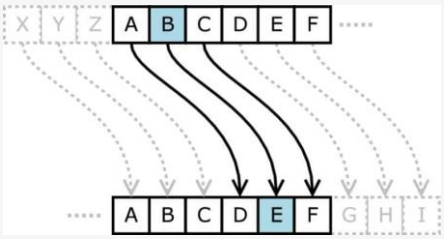
- Transpositie (omzetting)
- Substitutie (vervanging)
- Eenmalige pad

Message: JAMESBONDNEEDSBACKUP
Code: JEONDAUASNESCPMBDEBK

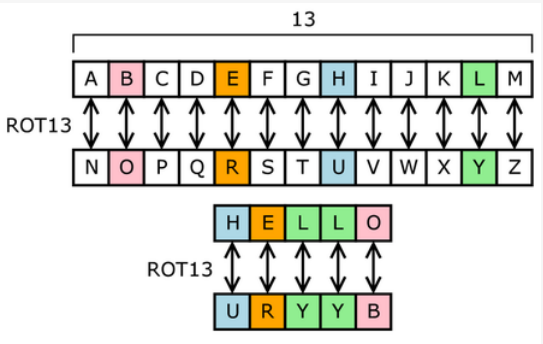
J	E	O	N	D	A	U
A	S	N	E	S	C	P
M	B	D	E	B	K	

Eenvoudig voorbeeld transpositie waarbij de volgorde van de karakters wijzigt
(cfr. transpositie van een matrix, A^T)

HO GENT



Voorbeelden substitutie waarbij karakters vervangen worden door andere karakters



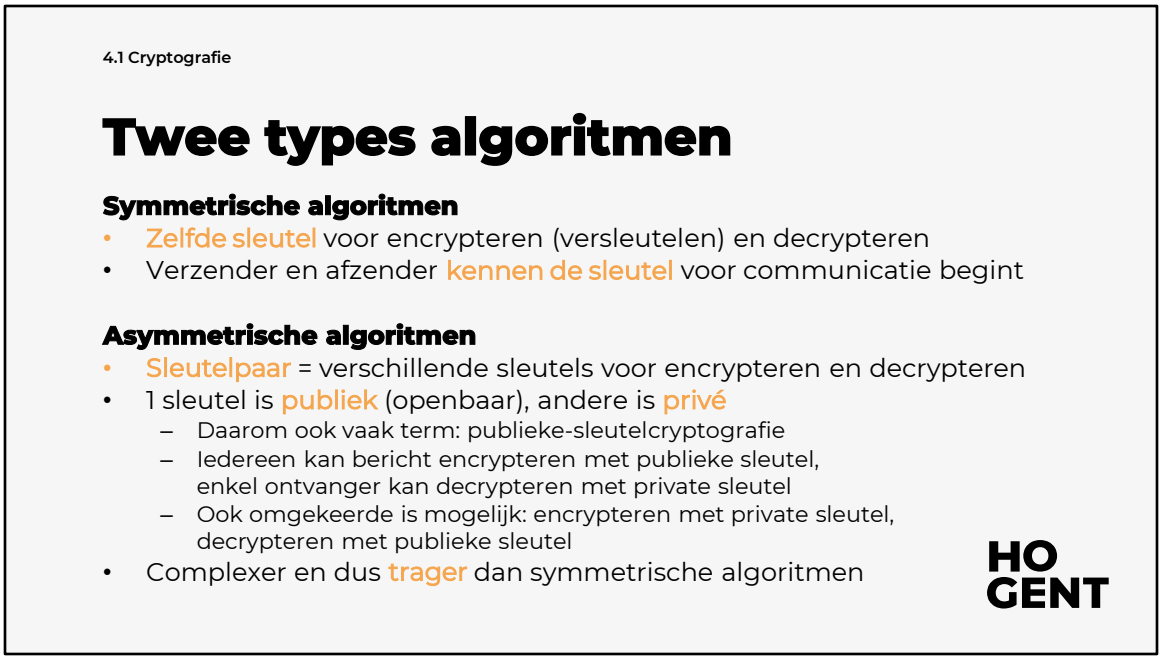
HO GENT

Voorbeeld one-time pad waarbij een random sleutel (=pad) opgeteld wordt bij de plaintext en vervolgens wordt het resultaat omgezet naar een getal van 2 cijfers

HO GENT

HO GENT

Video: https://www.youtube.com/watch?v=FlIG3TvQCBQ

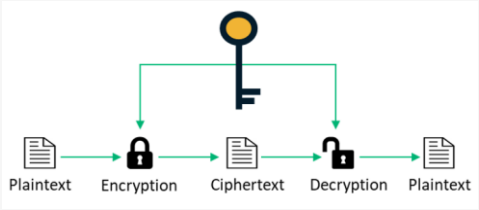


Er zijn twee soorten versleutelingsalgoritmen:

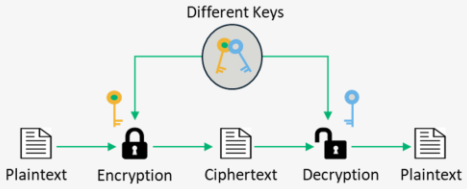
Symmetrische algoritmen gebruiken dezelfde vooraf gedeelde sleutel, ook wel een geheim sleutelpaar genoemd, om gegevens te encrypteren (versleutelen) en te decrypteren (ontgrendelen). Zowel de afzender als de ontvanger kennen de vooraf gedeelde sleutel voordat er gecodeerde communicatie begint.

Asymmetrische algoritmen gebruiken één sleutel om gegevens te encrypteren/versleutelen en een andere sleutel om gegevens te decrypteren/ontgrendelen. De ene sleutel is openbaar en de andere is privé. In een coderingssysteem met openbare sleutel kan elke persoon een bericht coderen met de openbare sleutel van de ontvanger, en de ontvanger is de enige die het kan decoderen met zijn privésleutel. Partijen wisselen beveiligde berichten uit zonder een vooraf gedeelde sleutel nodig te hebben. Asymmetrische algoritmen zijn complexer. Deze algoritmen zijn arbeidsintensief en trager uit te voeren.

Twee types algoritmen



symmetrisch algoritme



asymmetrisch algoritme

HO GENT

Symmetrische algoritmen gebruiken een vooraf gedeelde sleutel om gegevens te encrypteren en decrypteren, een methode die ook bekend staat als versleuteling met een privésleutel. Talrijke versleutelingssystemen gebruiken symmetrische versleuteling. Enkele van de algemene coderingsstandaarden die symmetrische codering gebruiken, zijn onder meer:

- 3DES (Triple DES): Digital Encryption Standard (DES) is een symmetrische blokversleuteling met een 64-bits blokgrootte die een 56-bits sleutel gebruikt. Triple DES versleutelt gegevens driemaal en gebruikt een andere sleutel voor ten minste één van de drie passages, waardoor het een cumulatieve sleutelgrootte krijgt van 112-168 bits.
- IDEA: Het International Data Encryption Algorithm (IDEA) gebruikt 64-bits blokken en 128-bits sleutels. IDEA voert acht transformatieronden uit op elk van de 16 blokken die het resultaat zijn van het verdelen van elk 64-bits blok. IDEA was de vervanging voor DES, en nu gebruikt PGP (Pretty Good Privacy) het.
- AES: De Advanced Encryption Standard (AES) heeft een vaste

blokgrootte van 128 bits met een sleutelgrootte van 128, 192 of 256 bits. Het National Institute of Standards and Technology (NIST) keurde het AES-algoritme in december 2001 goed. De Amerikaanse overheid gebruikt AES om geheime informatie te beschermen.

Asymmetrische codering, ook wel codering met openbare sleutel genoemd, gebruikt één sleutel voor codering die verschilt van de sleutel die wordt gebruikt voor decodering. Een crimineel kan de decoderingssleutel niet binnen een redelijke tijd berekenen op basis van kennis van de coderingssleutel en vice versa. De asymmetrische algoritmen zijn onder meer:

- RSA (Rivest Shamir-Adleman): gebruikt het product van twee zeer grote priemgetallen met een gelijke lengte tussen 100 en 200 cijfers. Browsers gebruiken RSA om een veilige verbinding tot stand te brengen.
- Diffie-Hellman: biedt een elektronische uitwisselingsmethode om de geheime sleutel te delen. Beveiligde protocollen, zoals Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH) en Internet Protocol Security (IPsec), gebruiken Diffie-Hellman.
- ElGamal: gebruikt de Amerikaanse overheidsstandaard voor digitale handtekeningen. Dit algoritme is gratis te gebruiken omdat niemand het patent heeft.

- Elliptic Curve Cryptography (ECC): gebruikt elliptische curven als onderdeel van het algoritme. In de VS gebruikt de National Security Agency ECC voor het genereren van digitale handtekeningen en het uitwisselen van sleutels.

4.1 Cryptografie

Symmetrische vs. asymmetrische codering

Symmetrisch	Asymmetrisch
Snel	Niet nodig om beide sleutels te delen
Verbruikt weinig resources	Kan gebruikt worden voor encryptie en validatie (=handtekening)
Kan gebruikt worden voor korte en lange berichten	Gebruikt veel resources
Sleutel moet op veilige manier gedeeld worden	Enkel bruikbaar voor relatief kleine berichten

Asymmetrische codering vaak gebruikt om een (tijdelijke) sessiesleutel voor symmetrische encryptie uit te wisselen!

HO GENT

Het is belangrijk om de verschillen tussen symmetrische en asymmetrische versleutelingsmethoden te begrijpen.

- Symmetrische versleutelingssystemen zijn efficiënter en kunnen meer gegevens verwerken. Sleutelbeheer met symmetrische versleutelingssystemen is echter problematischer en moeilijker te beheren.
- Asymmetrische cryptografie is efficiënter in het beschermen van de vertrouwelijkheid van kleine hoeveelheden gegevens, en de grootte en snelheid ervan maken het veiliger voor taken zoals elektronische sleuteluitwisseling, wat een kleine hoeveelheid gegevens is in plaats van grote blokken gegevens te versleutelen.

4.1 Cryptografie

Toepassingen

- Eenmalig wachtwoord genererend token = hardware apparaat om een eenmalig wachtwoord te genereren (cfr. online banking)
- Elektronische betalingssector gebruikt 3DES
- Oudere besturingssystemen: DES om gebruikersbestanden en systeem gegevens te beschermen met wachtwoorden *(niet meer veilig in 2020!)*
- De meeste versleutelde bestandssystemen, zoals NTFS, gebruiken AES

HO GENT

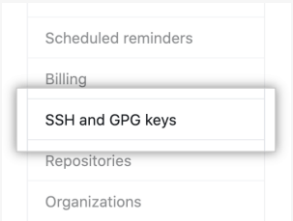
Er zijn veel toepassingen voor zowel symmetrische als asymmetrische algoritmen.

- Een eenmalig wachtwoord genererend token is een hardware-apparaat dat cryptografie gebruikt om een eenmalig wachtwoord te genereren. Een eenmalig wachtwoord is een automatisch gegenereerde numerieke of alfanumerieke reeks tekens die een gebruiker verifieert voor slechts één transactie van één sessie. Het nummer verandert elke 30 seconden of zo. Het sessiewachtwoord verschijnt op een display en de gebruiker voert het wachtwoord in.
- De elektronische betalingssector maakt gebruik van 3DES.
- Oudere besturingssystemen gebruikten DES om gebruikersbestanden en systeem gegevens te beschermen met wachtwoorden.
- De meeste versleutelde bestandssystemen, zoals NTFS, gebruiken AES

4.1 Cryptografie

Protocollen (Asymmetrisch)

- **Internet Key Exchange** (IKE), fundamenteel onderdeel IPSec (VPN)
- **Secure Socket Layer** (SSL), gebruikt in browser (HTTPS)
- **Secure Shell** (SSH), remote inloggen op Linux toestel
- **Pretty Good Privacy** (PGP), gebruikt voor o.a. e-mail en encrypteren bestanden
  - GPG = GNOME (Linux) implementatie van PGP
  - Weinig gebruikt in praktijk?
  - Je kan GPG sleutel toevoegen in GitHub om *commits* en *tags* digitaal te ondertekenen!



Vier voorbeelden van protocollen die asymmetrische sleutelalgoritmen gebruiken:

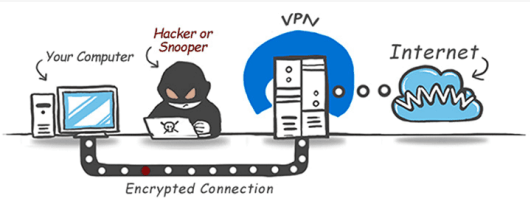
- Internet Key Exchange (IKE), een fundamenteel onderdeel van IPsec Virtual Private Networks (VPN's).
- Secure Socket Layer (SSL), een manier om cryptografie in een webbrowser te implementeren. HTTPS maakt gebruik van SSL.
- Secure Shell (SSH), een protocol dat een veilige verbinding voor externe toegang tot netwerkapparaten biedt.
- Pretty Good Privacy (PGP), een computerprogramma dat cryptografische privacy en authenticatie biedt om de beveiliging van e-mailcommunicatie te vergroten.

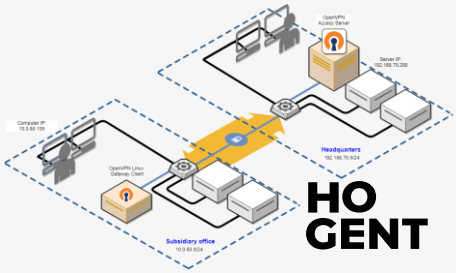
4.1 Cryptografie

Voorbeeld: Virtual Private Network (VPN)

VPN = privénetwerk over het internet, veilig communicatiekanaal tussen 2 eindpunten (bv. 2 kantoren op verschillende geografische locatie)

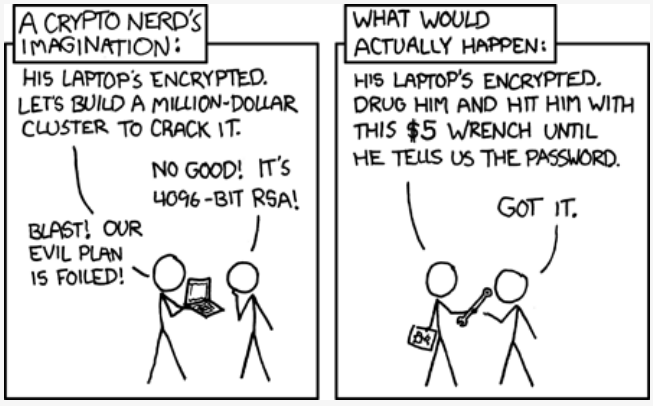
- Maakt gebruik van IPSec
- IPSec: authenticatie, integriteit, toegangscontrole en vertrouwelijkheid
- Hoofdzakelijk: encryptie (codering) en authenticatie (verificatie)
- Bescherming van data in beweging
- Veel varianten mogelijk!





Een VPN is een privénetwerk dat gebruikmaakt van een openbaar netwerk, meestal internet, om een veilig communicatiekanaal te creëren. Een VPN verbindt twee eindpunten, zoals twee externe kantoren via internet om de verbinding te vormen.

- VPN's gebruiken IPsec. IPsec is een reeks protocollen die zijn ontwikkeld om beveiligde services via netwerken te realiseren.
- IPsec-services maken authenticatie, integriteit, toegangscontrole en vertrouwelijkheid mogelijk.
- Met IPsec kunnen externe sites gecodeerde en geverifieerde informatie uitwisselen.
- Data in gebruik zijn voor veel organisaties een groeiende zorg. Data heeft tijdens gebruik geen enkele bescherming meer omdat de gebruiker de gegevens moet openen en wijzigen.
- Systeemgeheugen bevat gegevens die in gebruik zijn en kan gevoelige gegevens bevatten, zoals de coderingssleutel.
- Als criminelen gegevens die in gebruik zijn aantasten, hebben ze mogelijks toegang tot gegevens in rust én gegevens in beweging.



Bron: https://xkcd.com/538/

HO GENT


4.2
Toegangscontrole
HO
GENT

Soorten toegangscontrole

- **Fysieke toegangscontroles** zijn daadwerkelijke barrières die worden ingezet om direct contact met systemen te voorkomen. Het doel is om te voorkomen dat onbevoegde gebruikers fysieke toegang krijgen tot faciliteiten, apparatuur en andere bedrijfsmiddelen. Fysieke toegangscontrole bepaalt wie kan binnenkomen (of verlaten), waar ze kunnen binnenkomen (of verlaten) en wanneer ze kunnen binnenkomen (of verlaten).
- **Logische toegangscontrole** omvat hardware- en softwareoplossingen die worden gebruikt om de toegang tot bronnen en systemen te beheren. Deze op technologie gebaseerde oplossingen omvatten tools en protocollen die computersystemen gebruiken voor identificatie, authenticatie, autorisatie en verantwoording (accountability).
- **Administratieve toegangscontroles** zijn beleid en procedures die door organisaties gedefinieerd zijn om alle aspecten van het controleren van ongeautoriseerde toegang te implementeren en af te dwingen. Administratieve controles zijn gericht op personeel

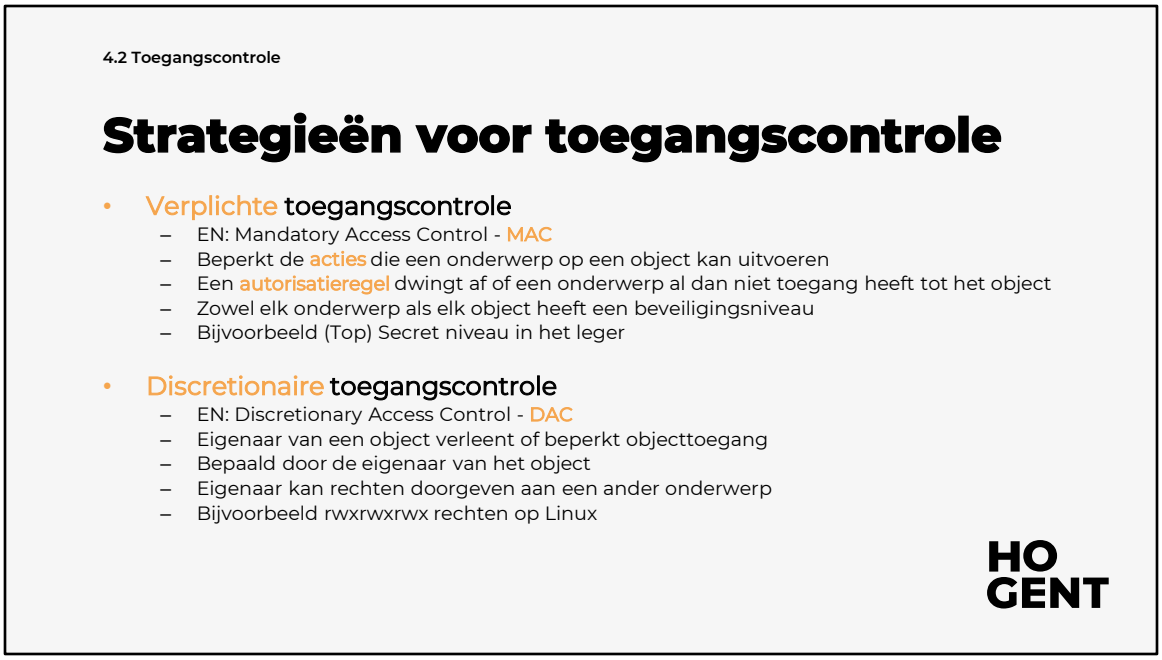
en zakelijke praktijken.

Onderwerp vs. object

- Onderwerp
  - EN: subject
  - Gebruiker of proces
  - Wil iets doen met een object
- Object
  - Bestand, poort of I/O apparaat
  - Onderwerp wil een object aanspreken

Toegangscontrole dwingt af of een onderwerp de nodige toegang heeft tot het object, en een bepaalde actie kan/mag uitvoeren.

HO GENT



Strategieën voor toegangscontrole

- Verplichte toegangscontrole (EN: Mandatory Access Control - MAC) beperkt de acties die een onderwerp op een object kan uitvoeren. Een onderwerp kan een gebruiker of een proces zijn. Een object kan een bestand, een poort of een invoer- / uitvoerapparaat zijn. Een autorisatieregel dwingt af of een onderwerp al dan niet toegang heeft tot het object.
- Discretionaire toegangscontrole (DAC) verleent of beperkt objecttoegang bepaald door de eigenaar van het object. Zoals de naam al aangeeft, zijn besturingselementen discretionair omdat een objecteigenaar met bepaalde toegangsrechten deze rechten kan doorgeven aan een ander onderwerp.
- Rolgebaseerde toegangscontrole (RBAC) is gebaseerd op de rol van het onderwerp. Rollen zijn functies binnen een organisatie. Voor specifieke rollen zijn machtigingen vereist om bepaalde bewerkingen uit te voeren. Gebruikers verwerven machtigingen via hun rol. RBAC kan werken in combinatie met DAC of MAC door het beleid van beide af te dwingen.

- Op regels gebaseerde toegangscontrole gebruikt toegangscontrolelijsten (EN: Access Control Lists - ACL's) om te helpen bepalen of toegang moet worden verleend. Een reeks regels is opgenomen in de ACL. De beslissing om al dan niet toegang te verlenen hangt af van deze regels. Een voorbeeld van zo'n regel is er een die stelt dat geen enkele werknemer buiten kantooruren of in het weekend toegang mag hebben tot het salarisdossier.

Strategieën voor toegangscontrole (cont.)

- Rolgebaseerde toegangscontrole RBAC
  - Role-based Access Control - RBAC
  - Gebaseerd op de rol (= functie binnen een organisatie) van het onderwerp
  - Voor specifieke rollen zijn machtigingen vereist om bepaalde bewerkingen uit te voeren
  - Gebruikers verwerven machtigingen via hun rol
  - RBAC kan werken in combinatie met DAC of MAC door het beleid van beide af te dwingen
- Op regels gebaseerde toegangscontrole
  - Rule-based Access Control
  - Toegangscontrolelijsten (EN: Access Control Lists - ACL's) om toegang te verlenen
  - Bijvoorbeeld: *geen enkele werknemer mag buiten kantooruren toegang hebben tot loondossiers*

HO GENT

Identificatie

Dwingt de regels af die zijn opgesteld door het autorisatiebeleid:

- een onderwerp vraagt toegang tot een systeembron (= object)
- de toegangscontroles bepalen of toegang moet worden verleend of geweigerd
- cybersecurity policies bepalen welke identificatiecontroles moeten worden gebruikt
- de gevoeligheid van de informatie- en informatiesystemen bepalen hoe streng de controles zijn
- de toename van datalekken heeft veel organisaties gedwongen hun identificatiecontroles te versterken

HO GENT

Authenticatiemethoden

- What You Know
  Wachtwoorden, wachtwoordzinnen of pincodes zijn allemaal voorbeelden van iets dat de gebruiker weet. Wachtwoorden zijn de meest populaire verificatiemethode.
- What You Have
  Smartcards en beveiligingssleutelhangers zijn beide voorbeelden van iets dat gebruikers in hun bezit hebben.
- Who you are
  Een uniek fysiek kenmerk, zoals een vingerafdruk, netvlies of stem, die een specifieke gebruiker identificeert, wordt biometrie genoemd.

Bij multi-factor authenticatie (ook gekend als 2FA) worden ten minste twee verschillende authenticatiemethoden gebruikt.
Een beveiligingssleutelhanger is een goed voorbeeld. De twee factoren zijn iets dat u kent, zoals een wachtwoord, en iets dat u heeft, zoals een beveiligingsdongle.

HO GENT

4.2 Toegangscontrole

Autorisatie

Bepaalt wat een gebruiker kan doen na authenticatie:

- Toegang tot welke (netwerk) bronnen?
  Wat kan de gebruiker doen met de bronnen?
  - Read, copy, create, delete
- Verzameling attributen beschrijven de toegang
  - Attributen worden vergeleken met authenticatiedatabase
  - Op basis hiervan vastleggen beperkingen (via autorisatieregels)
  - Resultaat doorgeven aan router waarop de gebruiker is aangesloten
- Een autorisatiebeleid legt de autorisatieregels vast voor het beheren van toegang. Bijvoorbeeld: *enkel senior administratoren hebben toegang tot de serverruimte*

HO GENT

Autorisatie bepaalt wat een gebruiker wel/niet kan doen na succesvolle authenticatie:

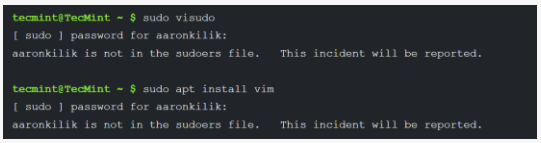
- Nadat een gebruiker zijn of haar identiteit heeft bewezen, controleert het systeem tot welke netwerkbronnen de gebruiker toegang heeft en wat de gebruikers met de bronnen kunnen doen.
- Autorisatie maakt gebruik van een set attributen die de toegang van de gebruiker tot het netwerk beschrijven.
- Het systeem vergelijkt deze attributen met de informatie in de authenticatiedatabase, bepaalt een reeks beperkingen voor die gebruiker en bezorgt deze aan de lokale router waarop de gebruiker is aangesloten.
- Het definiëren van autorisatieregels is de eerste stap bij het beheren van toegang, en een autorisatiebeleid legt deze regels vast.

4.2 Toegangscontrole

Verantwoording (Accountability)

Herleidt een actie naar een onderwerp (gebruiker of proces):

- Organisatie kan dit gebruiken voor audits of facturering
- Verzamelde gegevens kunnen zijn:
  - Inlogtijd gebruiker
  - Succesvol aangemeld?
  - Welke bronnen gebruikt?
- Laat toe om acties, fouten en vergissingen te traceren
- Implementatie via technologieën, beleid, procedures en opleidingen
- Logbestanden: gedetailleerde informatie op basis van gekozen parameters



HO GENT

Verantwoording herleidt een actie terug naar een persoon of proces dat de wijziging in een systeem aanbrengt, verzamelt deze informatie en rapporteert de gebruiksgegevens:

- De organisatie kan deze gegevens gebruiken voor bijvoorbeeld audits of facturering.
- De verzamelde gegevens kunnen de inlogtijd voor een gebruiker omvatten, of de gebruiker zich succesvol aangemeld heeft, en tot welke netwerkbronnen de gebruiker toegang heeft gehad.
- Hierdoor kan een organisatie acties, fouten en vergissingen tijdens een audit of onderzoek traceren.
- Het implementeren van verantwoording bestaat uit technologieën, beleid, procedures en opleidingen.
- Logbestanden bieden gedetailleerde informatie op basis van de gekozen parameters.

4.2 Toegangscontrole

Soorten beveiligingsmaatregelen

- Preventieve maatregelen voorkomen dat er iets gebeurt
  - Preventieve toegangscontrole voorkomt dat ongewenste of ongeautoriseerde activiteiten plaatsvinden.
- Afschrikmiddel ⇔ beloning
  - Beloning moedigt mensen aan om het goede te doen
  - Afschrikmiddel weerhoudt hen ervan het verkeerde te doen
  - Enkel afschrikmiddelen vaak niet voldoende
- Detectieve maatregelen om iets te ontdekken
  - Bij toegangscontrole: ontdekken ongeautoriseerde activiteiten
  - Eenvoudige detectiesystemen: bv. bewegingsmelder of bewaker
  - Complexere detectiesystemen: bv. inbraakdetectiesysteem

Soorten beveiligingsmaatregelen

- Preventieve maatregelen voorkomen dat er iets gebeurt. Preventieve toegangscontrole voorkomt dat ongewenste of ongeautoriseerde activiteiten plaatsvinden.
- Een afschrikmiddel is het tegenovergestelde van een beloning. Een beloning moedigt mensen aan om het goede te doen, terwijl een afschrikmiddel hen ervan weerhoudt het verkeerde te doen. Cybersecurityprofessionals en -organisaties gebruiken afschrikmiddelen om een actie of gedrag te beperken of te verzachten. Afschrikmiddelen stoppen deze acties echter niet altijd.
- Detectieve maatregelen: detectie is de handeling of het proces waarbij iets wordt opgemerkt of ontdekt. Detectie bij toegangscontrole identificeert verschillende soorten ongeautoriseerde activiteiten. Detectiesystemen kunnen heel eenvoudig zijn, zoals een bewegingsmelder of bewaker. Ze kunnen ook complexer zijn, zoals een inbraakdetectiesysteem.
- Corrigerende maatregelen gaan iets tegen dat ongewenst is.

Organisaties voeren corrigerende toegangscontroles in nadat een systeem een bedreiging heeft ondervonden. Corrigerende controles brengen het systeem terug naar een staat van vertrouwelijkheid, integriteit en beschikbaarheid. Ze kunnen ook systemen herstellen naar normaal nadat er ongeautoriseerde activiteiten hebben plaatsgevonden.

- Herstelmaatregelen - Herstel is een terugkeer naar een normale toestand. Toegangscontroles voor herstel herstellen bronnen, functies en mogelijkheden na een schending van een beveiligingsbeleid. Herstelcontroles kunnen schade herstellen, naast het stoppen van verdere schade. Deze controles hebben meer geavanceerde mogelijkheden dan corrigerende maatregelen.
- Compensatieve maatregelen - Compenseren betekent iets goedmaken. Compensatieve maatregelen bieden opties voor andere controles om de handhaving ter ondersteuning van een beveiligingsbeleid te versterken. Een compenserende controle kan ook een substitutie zijn die wordt gebruikt in plaats van een controle die onder de gegeven omstandigheden niet mogelijk is.

Soorten beveiligingsmaatregelen (cont.)

- Corrigerende maatregelen gaan iets tegen dat ongewenst is
  - Worden ingevoerd nadat een systeem een bedreiging heeft ondervonden
  - Corrigerende controles brengen het systeem terug naar een staat van vertrouwelijkheid, integriteit en beschikbaarheid
  - Ze kunnen ook systemen herstellen naar een normale toestand nadat er ongeautoriseerde activiteiten hebben plaatsgevonden
  - Bv. virusscanners
- Herstelmaatregelen zorgen voor terugkeer naar een normale toestand
  - Toegangscontroles voor herstel herstellen bronnen, functies en mogelijkheden
  - Herstelcontroles kunnen schade herstellen, naast het stoppen van verdere schade
  - Meer geavanceerde mogelijkheden dan corrigerende maatregelen
  - Bv. backupsystemen
- Compensatieve maatregelen proberen iets goed te maken
  - Bieden opties voor andere controles om beveiligingsbeleid te versterken
  - Compenserende controle kan substitutie zijn voor andere controle die niet mogelijk is
  - Bv. het is niet altijd mogelijk om een waakhond te hebben, dus wordt er in de plaats daarvan een bewegingsdetector met een spotlamp en speaker met blafgeluid geplaatst

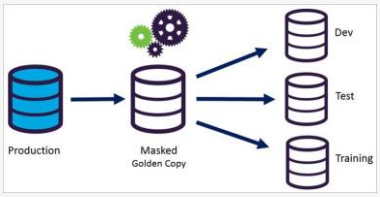
HO GENT


4.3
Data verduisteren
HO
GENT

4.3 Data verduisteren

Gegevensmaskering (masking)

- Gevoelige data vervangen door niet-gevoelige data
- Niet-gevoelige versie ziet eruit en gedraagt zich als het origineel
  - Geen wijzigingen nodig aan applicaties of dataopslagfaciliteiten
- Vaak: vervangende gegevenssets distribueren voor testen en analyse
- Verschillende technieken om gegevens te wijzigen, maar zinvol te houden:
  - Vervanging vervangt gegevens door authentiek ogende waarden (garanderen anonimiteit)
  - Shuffling leidt een vervangingsset af uit de gegevens die een gebruiker wil maskeren
    - Werkt goed voor bijvoorbeeld financiële data in een testdatabase



Datamaskering of gegevensmaskering is een technologie die gegevens beveiligt door gevoelige informatie te vervangen door een niet-gevoelige versie. De niet-gevoelige versie ziet eruit en gedraagt zich als het origineel. Dit betekent dat een bedrijfsproces gebruik kan maken van niet-gevoelige data en dat het niet nodig is om de ondersteunende applicaties of dataopslagfaciliteiten te wijzigen.

In het meest voorkomende geval beperkt maskering de verspreiding van gevoelige gegevens binnen IT-systemen door vervangende gegevenssets te distribueren voor testen en analyse.

Er zijn technieken voor gegevensmaskering die ervoor kunnen zorgen dat gegevens zinvol blijven, maar voldoende worden gewijzigd om ze te beschermen:

- Vervanging - vervangt gegevens door authentiek ogende waarden om anonimiteit toe te passen op de gegevensrecords.
- Shuffling - leidt een vervangingsset af uit dezelfde kolom met gegevens die een gebruiker wil maskeren. Deze techniek werkt

goed voor bijvoorbeeld financiële informatie in een testdatabase.

4.3 Data verduisteren

Steganografie

- Verbergt gegevens in een ander bestand
  - bv. grafisch, audio-, of ander tekstbestand
- Geheime boodschap valt niet op
  - Niemand zou ooit weten dat een foto daadwerkelijk een geheime boodschap bevatte door het bestand elektronisch of op papier te bekijken
- Verschillende componenten betrokken:
  - Ingebedde gegevens = geheim bericht
  - Omslagtekst verbergt gegevens die de stego-tekst produceren
    - Omslag en/of verborgen gegevens kunnen ook afbeelding of audio zijn
  - Stego-key regelt het verbergingsproces

HO GENT

Steganografie verbergt gegevens (het bericht) in een ander bestand, zoals een grafisch, audio- of ander tekstbestand.

Het voordeel van steganografie boven cryptografie is dat de geheime boodschap geen speciale aandacht trekt. Niemand zou ooit weten dat een foto daadwerkelijk een geheime boodschap bevatte door het bestand elektronisch of op papier te bekijken.

Er zijn verschillende componenten betrokken bij het verbergen van gegevens:

- Er zijn de ingebedde gegevens, dat is het geheime bericht.
- Omslagtekst (of omslagafbeelding of omslagaudio) verbergt de ingebedde gegevens die de stego-tekst produceren (of stego-afbeelding of stego-audio).
- Een stego-key regelt het verbergingsproces.

4.3 Data verduisteren

Gegevensverduistering (obfuscation)

Toepassen gegevensmaskering en steganografietechnieken

- Verduistering maakt de boodschap verwarrend, dubbelzinnig of moeilijker te begrijpen
- Systeem kan opzettelijk berichten door elkaar halen
- Softwarewatermerken:
  - Beschermen software tegen onbevoegde toegang of wijziging
  - Voegen een geheim bericht in het programma toe als bewijs van eigendom
  - Het geheime bericht is het softwarewatermerk
    Als iemand het watermerk probeert te verwijderen, is het resultaat een niet-functionele code

HO GENT

Gegevensverduistering is het gebruik en de praktijk van gegevensmaskering en steganografietechnieken in het beroep van cyberbeveiliging en cyberinformatie:

- Verduistering is de kunst om de boodschap verwarrend, dubbelzinnig of moeilijker te begrijpen te maken.
- Een systeem kan opzettelijk berichten door elkaar halen om ongeautoriseerde toegang tot gevoelige informatie te voorkomen.
- Softwarewatermerken beschermen software tegen onbevoegde toegang of wijziging.
- Softwarewatermerken voegen een geheim bericht in het programma toe als bewijs van eigendom.
- Het geheime bericht is het softwarewatermerk. Als iemand het watermerk probeert te verwijderen, is het resultaat een niet-functionele code.


HO
GENT