

# Samenvatting Info Sec

## CIA-driehoek

Deze driehoek is de basis voor information security en beveiligingsmaatregelen rond IT-gerelateerde zaken. Het doel is om de CIA te waarborgen. CIA staat voor:

- 1) **Confidentiality**: De gegevens zijn vertrouwelijk en enkel de nodige gegevens mogen opgezocht worden door personen die hiertoe bevoegd zijn of recht hebben op deze gegevens.
  - a. Militaire classificatie
    - i. **Top secret**: de gebruiker heeft een need to know (heel groot gevaar voor de nationale veiligheid)
    - ii. **Secret**: data met beperkte toegang (kritisch gevaar)
    - iii. **Confidential**: eigendomsdocumenten (ernstig gevaar)
    - iv. **Sensitive but unclassified (SBU)**: intern gebruik (FOUO)
    - v. **Unclassified**: brengt geen schade toe
  - b. Commerciële indeling
    - i. **Confidential** (bedrijven)/private (individueel): heel erg gevoelig (grote impact)
    - ii. **Sensitive**: intern gebruik (kleine impact)
    - iii. **Public**: publiek toegankelijk (geen impact)
  - c. Technologie
    - i. **Encryptie**
- 2) **Integrity**: De gegevens zijn correct en volledig (betrouwbaarheid).
- 3) **Availability**: De gegevens zijn beschikbaar voor iedereen die daar recht op heeft wanneer het nodig is.
  - a. **RAID: redundant array of independent disks (inexpensive)**
  - b. Netwerk, authenticatie, dedundante hardware, back-up, ...

Een aantal voorbeelden van een schending van de CIA-driehoek zijn:

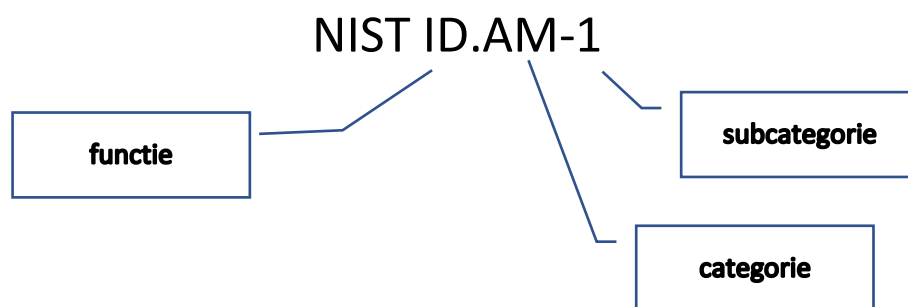
|   |
|---|
| Een agent controleert het vervallen van de groene verzekeringskaart van een chauffeur na een aanrijding.  |
| Een agent controleert het vriendje van zijn dochter in de politiedatabase.  |
| Geldautomaat <ul style="list-style-type: none"> <li>▪ Confidentiality: two-factor authentication               <ul style="list-style-type: none"> <li>▪ Zowel kennis als een bezit nodig</li> </ul> </li> <li>▪ Integrity: bankverrichtingen worden real-life uitgevoerd</li> <li>▪ Availability: altijd beschikbaar (ook als de bank gesloten is)</li> </ul> |
| Identiteitskaart: <ul style="list-style-type: none"> <li>▪ Confidentiality: zelf verantwoordelijk</li> <li>▪ Integrity: Informatie moet kloppen op de chip (medische records etc)</li> <li>▪ Availability: altijd, code voor sommige dingen, kaartlezer</li> </ul>  |

**Non-repudiation (onweerlegbaarheid)**: is de waarborg dat ontvangst en/of verzending van een contract of een bericht niet kan worden ontkend door de beide betrokken partijen, respectievelijk de ontvanger en de verzender (alles kan worden bevestigd en gecontroleerd, logs).

## Hoofdstuk 1

### NIST

- **N**ational **I**nstitute of **S**tandards and **T**echnology
- Dit is een Amerikaans framework die richtlijnen geeft over hoe organisaties cyber security kunnen implementeren.
- Bestaat uit 5 functies
  - o Identify (ID)
  - o Protect (PR)
  - o Detect (DE)
  - o Respond (RS)
  - o Recover (RC)



## Hoofdstuk 2

- Waarom beveiliging van fysieke infrastructuur nodig?
  - ➔ Zonder fysieke beveiliging is er geen beveiliging.
- Physical security: a system of **inclusion** and **exclusion** for assets
  - o Exclude non authorized people
  - o Include authorized persons
- Cybersecurity
  - o involves securing physical access to property, systems and equipment ports
  - o securing electronics, optical and information access tot he system's data and controls
- infrastructure security: when physical security initiatives are applied to providing security for the basic physical and organizational structures needed for the operation of an enterprise, an organization, or society
- Drie lagen om fysieke beveiliging te plannen
  - o **The Outer Perimeter:** Securing this space involves controlling who can move (walk, drive, fly) across the legal or physical line that marks this perimeter. Examples of typical physical outer perimeters include property lines or the exterior walls of a building or complex.
  - o **The Inner Perimeter:** This perimeter typically involves physical barriers such as walls, doors, and windows—either exterior or interior, depending on the context of the outer perimeter.
  - o **The Interior:** This is the innermost level of security and consists of the interior of the building, office, cubicle, etc. that is surrounded by the inner and outer perimeters.
  - o **(Logische perimeter:** grenzen tussen netwerken, local hosts, ...)
- Bij elke laag zijn er twee concepten aan het werk

- **Natural Access-Control Methods:** Natural access control involves using natural design elements, such as structures and landscaping, to guide people as they enter and exit spaces.
- **Territorial Reinforcement:** Territorial reinforcement employs structures, systems, and devices to prevent unauthorized entry and create a clear difference between what is public and private.
- Drie basisregels infrastructuur
  - **Access-control and monitoring** systems (H2)
  - **Video surveillance** systems (H3)
  - **Intrusion-detection** and reporting systems (H4)
- **Tailgating:** an unauthorized person slips past the locking door closely behind someone who is authorized to pass through it.
- Access-control
  - Om fysieke toegang te vermijden (schade, vernietiging, diefstal)
    - Ingress (recht om ergens binnen te gaan)
    - Egress (recht om ergens buiten te gaan)
    - Regress (recht om ergens opnieuw binnen te gaan)
  - Voorbeelden
    - Outer perimeter
      - Natuurlijke elementen
        - Hagen
        - Paadjes
        - Bomen
        - Waterlopen
        - **CPTED**
          - Crime Prevention Through Environmental Design
          - Ontwerp van een gebouw en de omgeving ontmoedigt criminelen



- Territorial reinforcement
  - Apparaten (access-control, camera's, intrusion-detection, poorten)

- Borden
- Schuif- en draaipoorten (met motor)
  - Kaartenlezer (copy card)
  - Radiosignalen (capture the signal)
  - Numerieke toetsen (code beter regelmatig veranderen)  
((thermal) camera)
- Inner perimeter
  - Muren, deuren, vensters en andere openingen
  - Sloten: manueel (sleutel) of elektronisch (magnetisch)
    - Solenoid: verschillende configuraties mogelijk
      - Sluit automatisch na het binnengaan (tailgating)
      - Sluit automatisch af wanneer de stroom uitvalt (emergency exit)
    - Cijferslot
      - Persoonlijke toegangscode vereist (keypad)
- Interior
  - Alarm systemen (detectie)
  - Een receptionist
    - Vragen naar de aard van bezoek
    - Opvallend gedrag waarnemen
  - Security guard
    - Kunnen inschattingen maken en beslissingen nemen
  - Een bewakingsagent (kan beslissingen nemen en tijdig ingrijpen)
  - Authenticatie (wie ben jij – basis voor autorisatie)
    - Knowledge: wat de gecontroleerde persoon weet (pin code)
    - Possession: wat de gecontroleerde person bezit (bankkaart)
    - Inheritance: rol van t de gecontroleerde person  
(verantwoordelijkheden)
    - Plaats: waar de gecontroleerde persoon is (containerpark)
    - Magnetische strip lezers (magnetische data op de strook)
    - RFID: chip is not powered; powered by radio signal
    - Biometric scanners
    - Smart card
      - Identiteitskaart: PII (personally identifiable information)
      - Zichtbaar:
        - Rijksregisternummer
        - label 'identiteitskaart'
        - geldigheidsperiode
        - plaats van uitgave
        - familienaam en voornamen
  - Identiteitskaart
    - Zichtbaar:
      - Nationaliteit
      - Geslacht
      - Geboorteplaats
      - Geboortedatum
      - Foto

- Verborgen op de chip:
  - adres (hoofdverblijfplaats)
  - identificatiecertificaat (eID in card reader)
  - handtekeningcertificaat (digital signing)
- chip moet na een aantal jaar vervangen worden
  - chip is read only
  - update van software nodig
- Remote-access monitoring
  - Remote-access monitoring systems are used to notify supervisory security personnel when an unauthorized access is attempted.
  - The notification can come in the form of a visual notification on a security control panel, a call via telephone, an instant messenger notice, or a text message to a smart phone. The notification can also involve activating strobe lights and high intensity sirens to call attention to the intrusion attempt.
  - **Locked-Condition Monitoring:** Locked monitoring is a feature that allows the security supervisor to confirm that a door is locked. In addition to monitoring the locked status of a door or gate, the condition-monitoring system can also provide details as to how long and during what time periods the door or gate has remained locked.
  - **Unlocked-Condition Monitoring:** The condition-monitoring system can record and signal each time a specific gate or door is unlocked (granting access) and what type of access was granted. Unlocked monitoring can also identify who was granted access.
  - **Time-of-Day Settings:** Most automated access-control systems base decisions about valid or invalid entry requests, also called transactions, on preconfigured time-of-day settings. This is normal because any entry request that does not fit the predefined time profile or time schedule of an identified user is subject to suspicion.

## Hoofdstuk 3

- PIR: passive infrared
- Some systems are based on coaxial cable for component connectivity, while others are IP-based and rely on wireless Wi-Fi communications or traditional network cabling.
- CCD camera (Charged Coupled Device) (dit is een alternatief van CMOS, maar wel heel oud)
  - Hoge resolutie
  - Weinig licht nodig
  - Weinig temperatuurafhankelijk
  - Hoge betrouwbaarheid
- IP camera (Internet Protocol)
  - Kan overal bekeken worden (internet)
  - PoE
  - Notificaties
  - Cloud back-up
  - Geen bijkomende hardware nodig (DVR)
  - Kan met een NVR verbonden worden (network video recorder)
- Analoge camera
  - Resolutie is lager
  - Beter in lagere lichtomstandigheden (lux rating)

- Beste prestatie met coax-kabel
  - Geen PoE
  - Kan op een lange afstand geplaatst worden van videorecorder (tot 1,5 kilometer)
  - Geen encryptie, geen VPN, geen datacompressie
- Analoge en digitale camera's (CCTV)
  - CCTV = Closed circuit TV
  - Uses a DVR (digital video recorder)
  - Beeldscherm nodig om video te kunnen bekijken
- Belangrijkste specificaties voor camera
  - lichtgevoeligheid
    - lux waarde
      - hoe lager, hoe beter de camera objecten kan zien in het donker
  - resolutie
    - analoog: aantal horizontale lijnen
    - digitaal: aantal pixels
- Lenzen
  - Hoe groter de lens (en dus ook de brandpuntsafstand), hoe smaller het beeld maar ook minder gedetailleerd
  - Soorten
    - Varifocale lens: zoom mogelijk, maar herfocussen elke keer
    - Vaste focale lens: één vast focuspunt
    - Breedbeeld lens: breder beeld
    - Tele- of zoomlens: zoom met automatische focus
    - Fisheye lens: zie een hele kamer, maar met vervorming
    - Pinhole lens: verborgen opnames
- Zwart-wit vs kleur
  - Zelfde kwaliteit
  - Kleur: meer beschrijvend (kleur auto, kledij, ...)
- IR-verlichting
  - Weinig licht: infrarood LED-verlichting
    - Niet zichtbaar voor mensen (beter verborgenheid van de camera's)
- Toepassingen camera's
  - Binnen/buiten (weerbestendig of niet)
  - Dag/nacht
  - Vast/pan/tilt
  - Bewegingsdetectie
  - Sequencing (wisselen tussen camera's)/multiplexing (alle camera's gelijktijdig)
  - Time lapse
  - ...
- Video recorders
  - Tegenwoordig digitaal (DVR ipv VCR)
  - Hoge hoeveelheid aan opslagruimte nodig
    - Internal storage (HDD in een videorecorder)
    - Peripheral storage (extern met HDD via USB to DVR)  
= DAS (direct-attached storage)
    - Network storage (NAS en SAN)  
NAS = network attached storage  
SAN = storage area network

## Hoofdstuk 4

### Intrusion-detection

- Bestaat uit drie zones
  - o Perimeter
    - Bescherming van openingen in de perimeter: deuren, ramen, garages, ...
  - o Interior
  - o Fire
- Basisconfiguratie
  - o Controller (met back-up batterij)
    - PCB (printed circuit board)
    - Processor
    - Telefoonlijn inputs en outputs
    - Terminals (schroeven voor sensor input)
    - Back-up batterij
  - o Toetsenborden
  - o Binnensensors
  - o Alarmsignalen
  - o Autodialer naar telefoonlijn (sms of stem)
  - o Autodialer naar bewakingsfirma
  - o (optioneel) rookmelders
  - o (optioneel) perimeter sensoren (venster, deur, ...)
- Zones
  - o Groep van sensoren die bij elkaar horen
  - o Voorbeelden
    - Een aantal bewegingssensoren in een gang
    - Beweging sensoren in een traphal
  - o Gesloten loop van schakelaar waar een kleine stroom moet doorheen lopen (current loop). Wanneer dit onderbroken wordt zal de controller dit detecteren. Dit is beter dan een normaal open circuit omdat daarbij het doorknippen van een kabel niet kan worden gedetecteerd
- Sensors
  - o Magnetische contact switches
  - o Glasbreuk sensors
    - Acoustische sensor
    - Trilling sensor
  - o Bewegingsmelder
    - PIR = passive infrared (does not emit any energy)
  - o Voertuigdetectie
    - Photoelectric beam devices
    - Microwave beam devices
  - o Druksensoren
  - o Brandmelders
    - Warmtesensoren
    - Rookmelders
- Output devices
  - o Visual notification

- Audible annunciators
- Remote messaging

## Hoofdstuk 5

- Meerdere factoren spelen een rol bij authenticatie
  - Kennis (wat de persoon weet)
  - Bezit (wat de persoon heeft)
  - Erfelijkheid (wat de persoon is)
  - Locatie
- Bij two-factor authenticatie gebruik je een combinatie van twee van deze vormen
- Een open en gesloten conditie is niet hetzelfde als een vergrendeld en ongegrendeld conditie

## Hoofdstuk 6

### Local host Security in the real world

- Gaat over toestellen die data kunnen verzamelen: local host
  - smartphone, ip camera, ...
  - Local host are all devices except for a server or sharing device
- **CSO**: chief security officer
- Risk assessment met NIST
  - NIST identification
    - Hardwareinventaris
    - Softwareinventaris
    - Data flow
    - Infrastructuur
    - Kwestbaarheden
  - NIST protect
    - Wie mag inloggen op het systeem en wie niet
    - Hoe de zwakke plekken beschermen?
    - Remote access
    - Communicatie input en output
  - NIST detect
    - Genomen maatregelen monitoren
    - Welke apparatuur heb je nodig voor monitoring?
      - Machine zelf
      - Personeelsactiviteiten
  - NIST respond
    - Procedures om een aanval te behandelen
      - Lagen in lekken
  - NIST recover
    - Welke schade moet hersteld worden?
    - Backup
    - Redundant hardware?



## Hoofdstuk 7

- De drie zones van beveiliging
  - Outer perimeter: behuizing en hardware (H7)
  - Inner perimeter: operating system + programma's (H8)
  - Interior: data opgeslagen op het toestel (encryptie?)

### Secure the local host





















- Infrastructuur
  - Dekstop in een gesloten kast
  - Kabelslot
  - docking station with lock
- Er zijn drie plaatsen waar de data beschermd moet worden
  - geheugen (RAM – memory dump)
  - storage (HDD, SSD, USB-stick, SD-kaart, ...)
  - tijdens transfer van een plaats naar een andere (communicatie )(input/output)
- Hoe kunnen ze aan deze data?
  - Via toetsenbord, muis, touchpad, touchscreen, UTP-poort, ...
- **BIOS**: Basic Input/Output System
  - Geeft basis hardwarebeveiligingsopties
    - Wachtwoord om toegang te krijgen tot het systeem (bij opstarten nog voor OS wordt geladen)
  - **UEFI** (Unified extensible firmware interface)
    - Is met grafische interface
  - Drie taken
    - hardware componenten opstarten
    - functionaliteitscheck
    - Bootloader opstarten
  - BIOS/UEFI security
    - Wachtwoord instellen
      - **CMOS** setup utility (complementary metal-oxide-semiconductor)
      - Anders toegang tot de inner perimeter en interior
        - Poorten (boot order) om toegang te krijgen tot de storage
      - Wachtwoord vergeten?
        - CMOS-batterij verwijderen
        - Jumpers op het moederbord verplaatsen
        - Soldeernaden lossen (oudere PC's)
        - Daarom behuizing beveiligen achter slot zodat niet iedereen dit kan doen
    - Updaten!
  - BIOS of UEFI is de eerste plaats waar software wordt gebruikt. Dit is dan ook de beste plaats om te starten als een hacker
- Local system hardening
  - **Hardening** = een computersysteem beveiligen
    - Hardware wordt beveiligd door BIOS
  - Waar begint een hacker? Bij de firmware.

- Andere paden naar de inner perimeter zijn
  - fysieke poorten
    - Zowel input als output nodig (resultaat van opdrachten bekijken)
    - Input geeft toegang tot de interne communicatie bussen zoals databus, geheugen en interne opslag (chipset)
      - Chipset = IC's die de connectie tussen randapparatuur, de CPU en het geheugen verzorgen
      - Twee IC's vormen samen chipset: Northbridge en Southbridge
        - Northbridge
          - Heel snel
          - Moet meegaan met de snelheid van de CPU
          - Is dus afhankelijk van welke CPU is gebruikt
          - Kan ook verbinden met PCIe
          - Taak: verbinden van CPU met RAM en andere snelle perifera's
        - Southbridge
          - Is trager
          - Is niet rechtstreeks verbonden met de CPU
      - BIOS en OS bepalen wat wel is toegestaan met deze chipset
  - Softwarepoorten op netwerkaart (draadloos of UTP) (H12)





#### Fysieke poort

- USB-poort (Universal Serial Bus)
  - Daisy chains met USB-hub
  - Indien rechtstreeks op mobo, uit te schakelen in CMOS setup
  - **Hot-swapping**: toevoegen of verwijderen wanneer het systeem actief is
  - IDE (Integrated Drive Electronics) (nu PATA genoemd = Parallel Advanced Technology Attachment): zorgt voor transport van data tussen ROM en RAM; tegenwoordig wordt SATA gebruikt (Serial ATA)



| USB 1.0  | USB 2.0  | USB 3.0<br>USB 3.1 Gen 1<br>USB 3.2 Gen 1  | USB 3.1 Gen 2<br>USB 3.2 Gen 2  | USB 3.2 Gen 2x2   |
|--|--|--|---|---|
| 12 Mbit/s  | 480 Mbit/s   | 5 Gbit/s   | 10 Gbit/s   | 20 Gbit/s   |
|             |             |             |           |            |
| <br>Type A  | <br>Type A  | <br>Type A  | <br>Type A | <br>Type-C |
| <br>Type B  | <br>Type B  | <br>Type B  | <br>Type-C |   |
| <br>Mini-A  | <br>Mini-A  | <br>Mini-B  |   |   |
| <br>Micro-A | <br>Micro-A | <br>Micro-B |   |   |

- 
- Type A vooral gebruikt waar kabel permanent bevestigd is (muis, toetsenbord, ...)
- Type B vooral gebruikt waar kabel verwijderbaar is (printer, Arduino, ...)
- USB 3.0 vaak blauw

|   | Version | Speed                             | Bits/sec            | HD movie 25GB |
|---|---------|-----------------------------------|---------------------|---------------|
|    | USB 1.1 | Low speed (LS)<br>Full speed (FS) | 1.5 Mbps<br>12 Mbps | ~9.25 hours   |
|   | USB 2.0 | High speed (HS)                   | 480 Mbps            | ~14 mins      |
|  | USB 3.0 | SuperSpeed (SS)                   | 5 Gbps              | ~70 sec       |
|  | USB 3.1 | SuperSpeedPlus (SSP)              | 10 Gbps             | ~35 sec       |

- 
- FireWire en Thunderbolt
  - FW is opvolger van SCSI
  - TB is een vervanger voor oudere SCSI, SATA, USB, FireWire, PCI-e

| Bandbreedte van USB, FireWire en Thunderbolt |              |               |
|--|--------------|---------------|
| USB 1.0                                      | 1,5 Mbit/s   | 0,19 MB/s     |
| USB 1.1                                      | 12 Mbit/s    | 1,5 MB/s      |
| USB 2.0                                      | 480 Mbit/s   | 60 MB/s       |
| USB 3.0                                      | 4,8 Gbit/s   | 600 MB/s      |
| USB 3.1                                      | 10 Gbit/s    | 1.250 MB/s    |
| FireWire 400                                 | 400 Mbit/s   | 50 MB/s       |
| FireWire 800                                 | 800 Mbit/s   | 100 MB/s      |
| FireWire 3200                                | 3,2 Gbit/s   | 400 MB/s      |
| Thunderbolt                                  | 2× 10 Gbit/s | 2× 1.250 MB/s |
| Thunderbolt 3                                | 2× 20 Gbit/s | 2× 2.500 MB/s |

○



- 
- DE-15 heb je in 2 rijen of 3 rijen
- M = male; F = female
- BNC connector



- ○ eSATA
  - External SATA (serial Advanced Technology Attachment) om aan de interne SATA-bus te koppelen
  - Directe toegang tot een bus (gevaarlijk)



- ○ POST: Power On Self Test

## Hoofdstuk 8

- Inner perimeter
  - Operating system
  - Application programs
- Operating system

- Intermediate software tussen de hardware en de applicaties
- Taken:
  - Resource management (RAM, disk, printer, ...)
  - Multi-user access
  - Programma-uitvoer
  - Geheugenbeheer
  - Disk management
  - File Management System (FMS)
  - ...
- Disk operating system (DOS)
  - = Een collectie van programma's die gebruikt worden om algemene operaties van een computer te controleren vanuit een schijf-gebaseerd systeem, oftewel een besturingssysteem voor apparaten met schijfstations
- Voorbeelden: Microsoft Windows, Apple MAC OS X, Linux
- Bestaat uit vier secties
  - **Boot files** nemen controle van het systeem over na BIOS/UEFI (laden kernel-bestanden)
  - **Kernel files** zorgen voor de communicatie met de CPU
  - **File management files** zetten data in het RAM-geheugen, waar de CPU de data en instructies kan ophalen
  - **Utility files** waarmee de gebruiker de resources kan beheren, het systeem kan troubleshooten en configureren
- Soorten operating systems
  - Standalone OS (Windows, OS X, Android, ...)
  - Client OS (in een netwerkomgeving; maken gebruik van een master computer = server)
    - Thick clients
      - Hebben zelf wel veel power en zouden lokaal kunnen werken
      - Maken gebruik van enkele services op de server
      - Heeft lokaal geheugen
    - Thin clients
      - Volledig functionele PC maar zonder geheugen voor opslag (HDD)
      - Alle data en software wordt op de server bewaard en uitgevoerd
    - Terminal clients
      - Gewone terminals, heel dom, weinig geheugen, ...
      - Hebben zelf geen OS
  - Server OS
    - Server OS is basis om network te beveiligen (hoofdstuk 14)
  - NOS (network operating system)
    - Voor communicatie en data-uitwisseling tussen verschillende DOS
    - Windows Server OS, Linux server distributions, Unix
    - Combinatie van disk management voor verschillende toestellen
  -
- Operating systems aanvallen gebeurt vaak op twee manieren:
  - Kernel manipuleren
  - File management system aanvallen
- Kernel manipuleren
  - Door geheugen manipulatie

- Waarde van een variabele aanpassen
  - Return adres van een functie aanpassen
  - Pointer naar uitvoerbare code wijzigen
  - Malicious code toevoegen aan het geheugen
- NX bit (No eXecution) of eXecute Disable (XD)
  - Storage-only memory (voor specifieke instructieblokken) om het geheugen te beschermen waar geen data geplaatst kan worden
  - Instructies kunnen daar niet worden bewaard
  - Bescherming tegen buffer overflow attack waar code wordt geïnjecteerd
- DEP mode (Data Execution Prevention)
  - Elke applicatie krijgt een geïsoleerd stukje geheugen dat als virtueel geheugen gezien kan worden
  - Enkel de applicatie zelf kan in de virtueel afgeschermd zone werken
- File system security
  - Uitermate belangrijk
    - Beschadiging leidt tot denial of access
    - Data stelen als iemand toegang heeft tot het file system
  - Hoe kunnen we file system en bestanden beschermen?
    - => ACL (access control list)
      - Gebruikers hebben wel of geen toegang tot data (lezen, schrijven, wijzigen, verwijderen, uitvoeren)
      - Bij een OS: ACL beschermt objecten zoals TCP/UDP en I/O (user kan dan een process zijn)
      - Unix en Linux: Mandatory Access Control (MAC)
        - Gebruik administrator policy als bron
        - Werkt met access rights
      - Windows: Role-Based Access Control (RBAC)
        - Gebruikt rollen van gebruikers als bron
        - Dit wordt vaak gebruikt in grote bedrijven
        - Werkt met permissies
      - Werkt enkel op het bijpassende OS. Door bijvoorbeeld Kali Linux te gebruiken kan je in deze lijst kijken -> encryptie van lijst nodig
  - POSIX
    - Portable operating system interface
    - Standard voor Linux-achtige systemen om ACL te delen
  - Encryptie
    - Meeste OS hebben een vorm van encryptie in hun file management system (bijvoorbeeld BitLocker)
    - Kan worden gedaan bij opslag van data of bij vervoeren van data
      - NIST
        - PR.DS-1 data at rest
        - PR DS-2 data in transit
    - Kan op verschillende niveaus worden toegepast
      - Toestel
      - Disk/partitie/volume
      - Mappenstructuur
      - Bestand

- File System Attacks
  - Race condition attacks
    - Tussen twee events voert een hacker malicious code in
    - Bv. Wanneer een besturingssysteem een tijdelijk bestand aanmaakt, checkt het OS eerst of de te gebruiken bestandsnaam al bestaat, daarna maakt die het bestand effectief aan (twee events). Hacker voert in tussentijd malicious code in met de gecheckte filename. Dat bestand kan adminrechten hebben.
  - Alternative data streams (bestanden verbergen)
    - ADS of alternative data streams op NTFS
    - Voor het verbergen van rootkits
    - Bestaat voor support met HFS (Hierarchical File System van Mac) dat bestanden wel eens forked (opsplitst) in meerdere bestanden
    - Wordt ook toegepast op bestaande OS-bestanden, waarin malicious code geplaatst wordt
    - Enkel opspoorbaar met gewijzigde timestamp
  - Directory traversals
    - Backtracking, directory climbing attacks, canonicalization attacks
    - Slecht geschreven software of slecht beveilige (web)servers
      - Toegang verwerven tot een map met geen beperking, daarna opklimmen in de structuur
- Verschillen tussen OS'en
  - Microsoft Windows
    - GUI-gebaseerd
    - Werkt met x86 32-bit en x86 64-bit processors
    - Heeft ondersteuning voor NX-bit en XD-bit
    - Basic file system formats
      - FAT/FAT16/FAT32
        - File Allocation Table
        - Nog veel gevonden op USB-sticks, SD-kaarten, ...
      - NTFS
        - New Technology File System
        - Wordt nu als standaard gebruikt in Windows
        - Heeft ACLs en EFS toegevoegd (encrypting file system)
      - ISO 9660 (CDFS)
        - Compact Disk File System
        - Voor op cd's
      - UDF
        - Universal Disk Format
        - Opvolger van CDFS
        - Vooral gebruikt op Dvd's
    - Encryptie
      - Bestanden en mappen door EFS
      - Volledige schijf door BitLocker
    - Firewall maakt gebruik van packet filtering
  - Unix
    - Veel variaties
      - BDS (Berkeley Software Distribution)

- Verschillende distributies maken gebruik van verschillende file system formats
  - UFS
    - UNIX File System
    - Originele file system
    - Boomstructuur
  - NFS
    - Network File System
    - Bestanden benaderen over het netwerk
- Encryptie
  - Vroeger: crypt
    - Is makkelijk te kraken
  - DES
    - Data Encryption Standard
  - PGP
    - Pretty Good Privacy
  - PEFS
    - Private Encrypted File System
    - Voor bestanden
  - GELI en GBDE
    - voor schijven
- heeft ook firewall
- Linux OS Distributions
  - Open-source
  - Veel verschillende distributies
  - Heeft ondersteuning voor NX-bit op sommige systemen
  - File system types
    - Ext/ext2/ext3/ext4
      - Extended File System
      - Primair file system voor Linux
      - Ext2/3 ook veel pop SD kaarten en andere flash schijven
    - ReiserFS
      - Alle veranderingen worden bijgehouden in een log bestand (journal)
      - Heeft permissies en ACLs, maar geen encryptie
    - Linux OS
      - Heeft vaak ook ondersteuning voor ISO9660, FAT en UDF
  - Encryptie
    - Via pakket: eCryptfs
  - Ingebouwde firewall: Netfilter
    - Maakt ook gebruik van packet filtering
    - Maar ook filtering voor network address translation (NAT) en port address translation (PAT)
- Apple OS
  - Werkt met x86 32-bit en x86 64-bit processors
  - Heeft ondersteuning voor NX-bit
  - Ondersteuning voor ISO9660, FAT, NFS, UFS en UDF



- Ondersteuning voor FMS standaard
  - HSF/HSF+
    - Hierarchical File System
    - Gemaakt door Apple
  - SMBFS/CIFS
    - Server Message Block File System of ook bekend als Common Internet File System
    - Voor gebruik van gemeenschappelijke toegang tot bestanden
- Encryptie
  - FileVault voor encryptie van schijven
- iOS
  - heeft veel kenmerken van macOS maar kan die applicaties niet draaien
  - gebruikt RISC (Reduced Instruction Set Computing)
  - ARM (Acorn RISC Machines)
    - Gebruiken veel minder energie en produceren veel minder warmte dan x86 CISC (Complex Instruction Set Computing)
    - Execute Never (XN) ondersteuning
  - Encryptie
    - Toestel gebaseerde encryptie
- Android OS
  - Gebaseerd om Linux OS kernel
  - Open source
  - ARM
    - XN ondersteuning
  - Speciale versies die op x86 draaien
    - Ondersteuning voor XD-bit en NX-bit
  - Verschillende toestellen ondersteunen verschillende file systems
  - Er zijn wel enkele gemeenschappelijke file systems voor flash die vaak worden gebruikt
    - exFAT
      - extended File Allocation Table
      - van Microsoft
    - F2FS
      - Flash-Friendly File System (version 2)
      - van Samsung
      - open-source
    - JFFS2
      - Journal Flash File System (version 2)
      - Vervanging van YAFFS2 (Yet Another Flash File System)
    - Ext2/Ext3/Ext4
      - Vervanging voor F2FS en JFFS2
  - Vaak ook ondersteuning voor FAT
  - Encryptie
    - Schijf encryptie van flash geheugen: dm-crypt
- Operating System Security Choices
  - Microsoft Windows is het vaakste het doel van criminelen

- **Grayware:** irritante ongewilde software
- Security tools en OS
  - Nadat het OS is opgestart moeten stappen worden ondernomen om niet-geauthentiseerd toegang tegen te houden
    - Local login-vereisten
      - Gebruiker en groeps accounts
      - Wachtwoord policies
        - Wachtwoorden
          - Hoofdletters (A, B, C, D, ...)
          - Kleine letters (a, b, c, d, ...)
          - Getallen (0, 1, 2, 3, ...)
          - Speciale tekens (?, !, &, |, ...)
        - Wachtwoordentechnieken
          - Lengte: hoe langer hoe beter
          - Vervanging: jOrisg33ns
          - Toevoeging: jorisgeens123 <slecht wachtwoord>
          - Mnemonisch: UraGreet!
          - Afkorting: lhobtf (I have only begun to fight – Natalia)
          - Volle zin met vervanging: welk0m1nd3l3sv@nV@n6@@g
        - Goede praktijken met wachtwoorden
          - Gebruik een consistente naamconventie
          - Bv. Groentennamen met getallen en symbolen Prei38@w0rk!
          - Bij eerste gebruik verplicht laten wijzigen
          - Wachtwoorden niet opschrijven (awareness)
          - Geen standaardwachtwoorden
          - Train gebruikers in het maken van sterke wachtwoorden (2-factor)
          - Dwing een policy af
      - Lockout policies
        - Account lockout policies
          - Maximal aantal pogingen
          - Brute force attacks tegengaan
        - Computer locking
          - Na verloop van tijd automatisch
    - Bijkomende authenticatie
      - Kaart of vingerscanner (Biometrische scanners)
    - Lokale administratie tools
      - Event logging en audit
        - Windows: security log file (event viewer)
        - Windows: Administrative Tools > Local Security Policy
        - Linux: System log
      - Encryptie
      - Monitoren van application software security
    - Remote access-bescherming
      - Firewall (H9)

- Browser beveiligingsopties
- Bescherming tegen malicious software
- Security updates en patches

| Patch   | Update  |
|---|---|
| <ul style="list-style-type: none"> <li>• Richt zich alleen op security vulnerabilities</li> </ul>                     | <ul style="list-style-type: none"> <li>Update de applicatie, verandert functionaliteit en hoogt de versie op</li> </ul> |
| <ul style="list-style-type: none"> <li>• Verandert niets aan functionaliteit of dependencies</li> </ul>               | <ul style="list-style-type: none"> <li>Breekt vaak plugin/theme/extensie-dependencies</li> </ul>                        |
| <ul style="list-style-type: none"> <li>• Verandert de applicatie versie niet, compatibel met latere update</li> </ul> | <ul style="list-style-type: none"> <li>In de meeste gevallen niet veilig te automatiseren</li> </ul>                    |
| <ul style="list-style-type: none"> <li>• Veilig te automatiseren</li> </ul>   |   |

- 
- Data encryptie
  - Symmetrische encryptie: zelfde sleutel voor encryptie en decryptie
  - Asymmetrische encryptie: twee verschillende sleutels
    - Private key (decryption) en public key (encryption)
    - Public key is afgeleide van private key
    - PKE: Public Key Encryption
  - Encryptie kan plaatsvinden op verschillende niveaus
    - File system-level (file and folder)
      - Windows: EFS (encrypting file system) langs Bestandsverkenner > Eigenschappen > Geavanceerd
      - Gewapend tegen **BIOS-kaping!**
      - Folders hebben ook list folder content permissie
    - Disk-level
      - Heel de schijf is encrypted
        - Ook OS bestanden
      - Kan via software of hardware
        - Software
          - Staat meestal al op OS
        - Hardware
          - TPM (trusted platform module): chip with for instance encryption keys
          - TPM chip is fixed on motherboard
          - Cannot be transferred to another main board
          - Controleert of er niks aan het OS is veranderd
    - Transport-level
      - USB-sticks met encryptie
      - Certificaten (https)

## Hoofdstuk 9

### Stappenplan tegen netwerkbedreigingen

1. Gebruik een beveiligde netwerkverbinding
  - Routers zorgen voor de beste eerste bescherminglaag

- Standaard admin-gebruikersnaam en wachtwoord wijzigen
  - Standaard SSID wijzigen
  - Configureer het hoogst mogelijke encryptieniveau
  - MAC-adresfilter (bv. 00:A0:C9:14:C8:29)
2. Pas een geconfigureerde **firewall** toe
    - **Controleert de data flow tussen computer en network**
    - Software of hardware (zie later)
    - Standaard staan alle poorten meestal open!
  3. Run één anti-malware-programma
    - Meerdere antimalwareprogramma's kunnen elkaar tegenwerken
    - Kan als suite of als aparte producten (antivirus, antispysware, firewall, ...)
  4. Verwijder onnodige software van de computer
    - Mogelijke slapende exploits
    - Weet je wat de software doet?
  5. Stop alle onnodige services op de computer
    - Weet je wat de service doet? Hoort die bij een bepaald programma?
    - Service altijd natrekken, kan een OS-service zijn
  6. Schakel onnodige OS-functionaliteiten (bv. webserver) uit
    - Bv. Autorun (DVD of USB met virus)
  7. Beveilig de webbrowser
    - (Cross-site) scripting
    - Onveilig browsen
    - Plug-ins
    - Security levels
    - Proxies
    - Cookies
      1. Sessions cookies: verdwijnen als de browser wordt gesloten
      2. Persistent cookies: blijven tot de vervaldatum is bereikt
  8. Voer updates en patches steeds uit
    - Dicht beveiligingslekken zo snel mogelijk
    - Op alle software op het toestel
  9. Gebruik sterke wachtwoorden
    - Drie verschillende soorten logons
      1. Lokaal niveau (machine zelf)
      2. Netwerkniveau (LAN/internet)
      3. Specifieke software (boekhouding)

#### Lokale bescherming

- 5 veel gebruikte tools
  - Lokale firewall
    - Software, bedoeld voor individuele computers met dial-up, LAN of andere rechtstreekse internetverbindingen
    - Beheert het inkomend en uitgaand dataverkeer
    - Bewaken poorten én services
      - 0 tot 1023: specifieke services
      - 1024 tot 49151: geregistreerde poorten
      - 49152 tot 65535: dynamisch en tussen computersoftware onderling
    - Well known ports and services

TABLE 9.1 Typical I/O Ports

| Service     | Well-Known Port Number |
|-------------|------------------------|
| FTP         | 20, 21                 |
| Telnet      | 23                     |
| SMTP Mail   | 25                     |
| HTTP (WWW)  | 80                     |
| POP3 (Mail) | 110                    |
| News        | 144                    |
| HTTPS       | 443                    |
| PPTP        | 1723                   |
| IRC         | 6667                   |

- - News: oude service in het verleden
  - IRC: Internet Relay Chat
  - POP: Post office protocol
- Inbraakdetectie
  - IDS (intrusion detection systems)
    - => Monitor system, logs key events and policy violations, alert reports
    - Network-based (NIDS)
      - Niet verder besproken
    - Host-based (HIDS)
      - Gebruikt twee strategieën
        - Signature analysis (patterns)
          - Kijkt voor verdacht patronen uit een lijst met verdachte patronen
        - Anomaly analysis
          - Statistische analyse van verkeer van data
            - Profile-based (rules)
              - ⇒ Zoekt naar ongewone patronen. Leert zelf wat “normal” is
            - Threshold-based (level)
              - ⇒ Als een bepaald event meerdere keren voorkomt
    - IPS (intrusion prevention systems)
      - Prevents the succeeding of intrusion
      - Ook wel IDPS genoemd
        - Intrusion Detection and Prevention System
- Browser beveiligingsopties
- Antivirus/anti-malware
  - Grayware: niet gewenst, maar moet niet kwaadaardig zijn
  - Malicious software: kwaadaardig
    - Virussen (dupliceren vanzelf met host programma en verspreiden zichzelf)

- Wormen (geen hostprogramma nodig, zoekt een exploit in het network en besmet alle computers, zodat er een hoge payload is op het network)
- Trojaans paard (lijkt een betrouwbaar programma te zijn, verspreid zichzelf niet)
- Rootkits (administratieve controle van het toestel verwerven, werken op rootniveau, nestelen zich bijvoorbeeld voor de bootloader)
- Ransomware (encryptie van data met vraag om losgeld)
- Spyware (probeert gevoelige data ongezien te stelen)
- Adware (toont ongevraagd gerichte reclame in de browser of andere applicaties)
- Logic bombs (delete data, zoals een trojaans paard met betrouwbare software, activeert zichzelf op een logisch moment, na x dagen, na het gebruik van x keer van het programma, malicious code zit in heel veel lijnen gewone code vervat)
- Zombies (voor DDOS-aanval – distributed denial of service)
- Botnets (vele zombies samen voor bijvoorbeeld spam uit te sturen)
- Antimalware
  - Antivirus (signatures en ongewoon gedrag)
  - Antispyware (twee soorten: één die opspoort en verwijdert, één die installatie tegenhoudt)
- Software updates en patches
  - Service pack
    - Grote hoeveelheid aan updates verpakt in één
    - Altijd eerst een back-up nemen vooraleer service pack te installeren (zou onstabiel kunnen zijn)
  - Patch
    - Kan ook als reactie op een virus zijn
  - Updates
    - Bevordert beveiliging, betrouwbaarheid of de voorkeur van een hacker/cracker voor een bepaald besturingssysteem
- Exploits
  - Weaknesses in software
  - Conflict bij het maken van software
    - Zo eenvoudig mogelijk in gebruik zijn voor eindgebruikers
    - Bullet proof, zodat er niets mee kan foutlopen
  - Buffer overflow -> kan systeem laten crashen -> Denial of Service (DoS)
- Soorten hackers/crackers
  - White hat [ethisch hacker mét contract]
  - Black hat [cracker of criminal hacker]
  - Grey hat [werkt vanuit overtuiging, overschrijdt wettelijke grenzen]
  - Red hat [valt black hats aan]
  - Scriptkiddies [werkt met bestaand material en scripts, geen kennis van zaken]

## Hoofdstuk 10

Overzicht + examenvragen

## Hoofdstuk 11

- IP = Intellectual Property

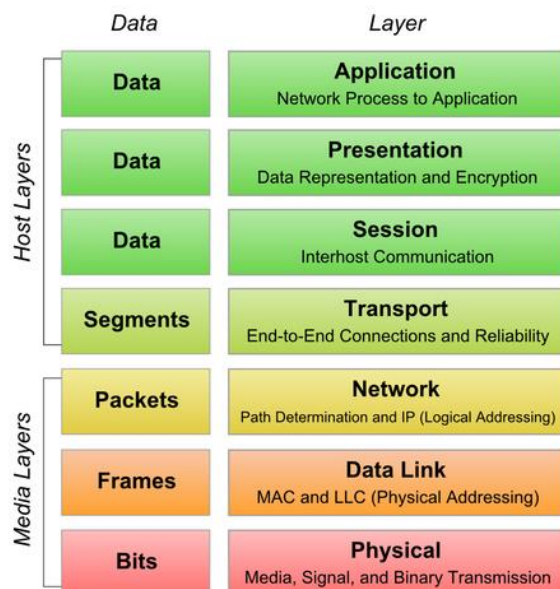
## Hoofdstuk 12

### Netwerken

- Twee basistypes van netwerken
  - o LAN (local area network)
    - Voor geografisch kleine gebieden (een huis, gebouw, ...)
  - o WAN (wide area network)
    - Voor geografisch grote gebieden
- Andere types van netwerken
  - o CAN (campus/corporate area network)
    - LANs die met elkaar verbonden zijn op campussen
  - o MAN (metropolitan network)
    - Zit tussen LAN en WAN
  - o WLAN (wireless local area network)
    - draadloos
  - o SAN (storage area network)
    - Voor dataopslag

### OSI-model

- Open systems interconnection
  - o To standardize communications (data handling) between network components



- Lagen

- o **Laag 1: fysieke laag**
  - Transmissie media (elektrische of lichtsignalen)
  - Activatie van de media
  - Communicatiepoorten
- o **Laag 2: data link**

- Frames voor datapakketten aanmaken en verzenden tussen communicatiepunten
- Error detection en correctie
- Media access protocols
- Bestaat uit twee sublagen
  - LLC (Logic Link Control) sublaag is de overgang met de OS (drivers)
    - Communicatie tussen software en fysieke hardware
    - Hier kan niet veel worden veranderd en wordt bepaald door OS
  - MAC (media access control) sublaag gaat over de software op fysieke controller (netwerk kaart)
    - Is verantwoordelijk voor het encapsuleren van de data die afkomstig is van de bovenliggende lagen
    - Deze zal encapsulation doen (toevoegen van de Ethernet header met onder andere de MAC adressen) en de-encapsulation (verwijderen van de Ethernet header). Wanneer een frame wordt verstuurd over een router zal deze router de het destination ip adres bekijken, in de routing table (waarin routes door het netwerk staan vermeld aan de hand van ip adressen) kijken naar welk ip adres dit moet worden doorgestuurd, in de arp table kijken welk mac adres hierbij hoort, en het nieuwe destination mac adres toevoegen aan het packet
    - Verschillende toestellen op hetzelfde netwerk identificeren met een MAC adres: 48 bits, 12 hexadecimale getallen
- **Laag 3: netwerk**
  - Routing van datapakketten over netwerknodes, netwerksegmenten en media.
  - **Multiplexing (muxing)**: samenvoegen analoge of digitale signalen tot 1 enkel signal
  - **Demultiplexing (demux)**: scheiden van 1 signal in meerdere signalen
  - Samenstellen van berichten
  - Connecties opzetten en verbreken
- **Laag 4: transport**
  - End-to-end data flow met foutcorrectie en recovery
- **Laag 5: session**
  - Sessions beheren tussen applicaties
  - Starten en stoppen van datatransfers
  - Data flow tussen applicaties
  - Security
  - Authenticatie en tunneling protocols (**SSH**: secure shell, **IPsec**: internet protocol security, **PPTP**: point-to-point tunneling protocol, ...)
- **Laag 6: presentation**
  - Hoe ziet de data er bij ontvangst uit?
    - Encryptie
    - Datacompressie
- **Laag 7: application**
  - Data voor de eindapplicaties behandelen



- Browser, e-mail (gebruikersnaam en wachtwoord)
- Laag 1-3: **media layers**
- Laag 4-7: **host layers**
- Data transmissie pakketten
  - Encapsulatie: header toegevoegd in elke laag

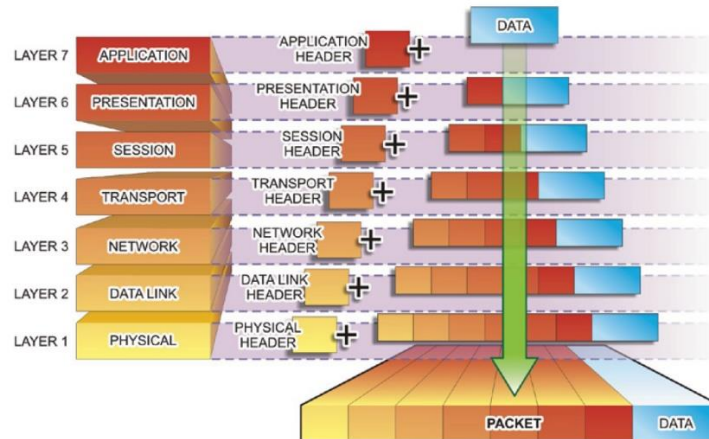


FIGURE 12.2 Building Transmission Packets

- OSI layer security
- Zit doorheen elke laag verweven

TABLE 12.1 OSI Layer Security

| OSI LAYER             | Network Security Model  | Exploit Type                           | Security Focus                |
|-----------------------|-------------------------|--|-------------------------------|
| 1) Physical Layer     | 7) Physical Level       | Physical Tampering/<br>Break-in        | Physical Security             |
| 2) Data Link Layer    | 6) VLAN Level           | Network Scanning<br>Local/Internal     | Access Security               |
| 3) Network Layer      | 5) ACL Level            | Network Scanning<br>Complete/Internal  | Domain Security               |
| 4) Transport Layer    | 4) Software Level       | Software Specific<br>Exploits          | Port Security                 |
| 5) Session Layer      | 3) User Level           | Social Engineering<br>– Users          | Authentication/<br>Encryption |
| 6) Presentation Layer | 2) Administrative Level | Social Engineering<br>– Administrators | Authentication                |
| 7) Application Layer  | 1) IT Department Level  | Social Engineering<br>– IT Staff       | ID/Authentication             |

- Three-layered rings of security
  - Bestaat op twee toestellen: zender en ontvanger
    - Het medium verbindt de hun outer perimeters (kabel, luchtgolven, ...)
  - Outer perimeter
    - Laag 1 (fysieke laag)
    - Beveiligen van datakabels en netwerkapparatuur
  - Inner perimeter
    - Laag 2 (data link)
    - Data kan hier aanvaard worden, geweigerd of doorgestuurd op basis van de identiteit
  - Interior perimeter
    - Laag 3-7
    - Bijvoorbeeld: laag 4 met het blokkeren van poorten

laag 7 is de meest aangevallen laag (zie later)

### Netwerktopologieën (laag 1)

- Bus
  - o Met centrale communicatielijn (ethernet) ofwel bus
  - o **Nodes** of stations met uniek adres
  - o Iedere node kan informatie op de bus zetten en juiste informatie eraf halen
- Ring
  - o Communicatielijn is gesloten in een cirkel
  - o Repeater stuurt info door vanuit elke node
  - o Geen collisions
  - o Risico: één node plat betekent netwerk plat -> meerdere redundante paden leggen
- Ster
  - o Communicatie langs een centrale component (switch)
  - o Geeft elke node een tijdsvenster om informatie mee te verzenden
    - Indien het bericht te lang is voor het tijdsvenster, zal het in stukken worden opgedeeld
- Mesh
  - o Elke node heeft een rechtstreekse verbinding met elke andere node
  - o Telefonie, Bluetooth, LoRaWAN, ...
- Hybride
- Logische topologie
  - o Niet elke getekende topologie komt met de interne circuits overeen met de visuele topologie
    - In een router zitten alle poorten als een bustopologie

### Labo

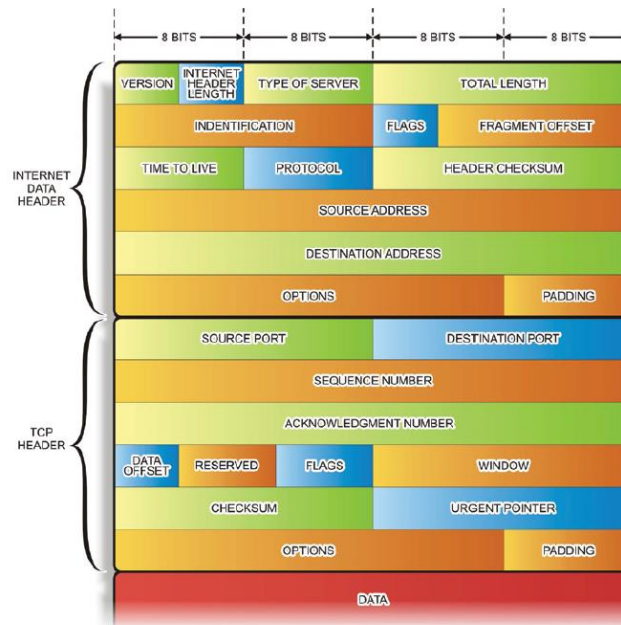
- Enkele protocollen
  - o Authentication Headers (AH)
    - Data integriteit
    - Origin authentication
    - Beschermt tegen replay attacks
      - Een opgenomen bericht wordt opnieuw verzonden om toegang te kunnen krijgen
    - Gebruikt ESP (Encapsulating Security Payloads)
  - o Security Associations (SAs)
    - Key exchange
    - Authentication
  - o Internet Key Exchange (IKE)
    - Wordt gebruikt om een beveiligde verbinding op te zetten met IPsec
      - IPsec werkt in laag 3
      - Verschilt van SSL omdat SSL op de browser werkt (laag 4/6/7)
      - Twee modes
        - o Transport mode: only IP payload is encapsulated
        - o Tunnel mode: the entire IP packet is encapsulated

## Hoofdstuk 13

### Netwerkprotocol

- Een netwerkprotocol = een reeks aan regels voor communicatie tussen netwerkcomponenten
  - o Om met elkaar te communiceren, moeten ze hetzelfde protocol gebruiken
  - o OSI model
    - Lagen 1 – 2 (fysiek en data link: bekabelde, draadloze en optische netwerken)
      - Verschillende protocollen voor verschillende media
    - Lagen 3 – 4 (network en transport: routing schema's, e-mail, webapplicaties en beveiligde verbinding)
- **Ethernet**
  - o Netwerkprotocol (IEEE 802.3) (Institute of Electrical and Electronic Engineers)
    - Laag 1 (fysiek) en laag 2 (data link)
    - <> draadloos!
    - CAT5-kabel: 100 Mbit/s (0,1 Gbit/s)  
CAT5e-kabel: 1000 Mbit/s (1 Gbit/s)  
CAT6-kabel: 10000 Mbit/s (10 Gbit/s)
  - o Verschillende protocollen voor verschillende media (draadloos, draad, ...)
- **NIC**
  - o NIC = network interface card
  - o Hardware-kant van een netwerkverhaal
  - o Insteekkaart die data omzet in elektrisch signaal (modulatie)
- **MAC-adres**
  - o Een MAC-adres = Media Access Control-adres
  - o Ook *physical address* genoemd
  - o 48-bit met zes paar hex (IPv4)
  - o 64-bit met acht paar hex (IPv6, Firewire, ZigBee, ...)
  - o Ingebakken in de NIC (the burned in address in chip, flash, ...)
  - o Uniek identificatienummer (zou moeten zijn)
  - o Oorspronkelijk Ethernet, nu ook WiFi, Bluetooth, ...
  - o Voorbeeld
    - MM:MM:MM:SS:SS:SS
    - 24 bits links = manufacturer (uitgereikt door IEEE)
      - 00:13:10, 00:25:9C en 68:7F:74 voor Cisco LinkSys
    - 24 bits rechts = specific device
      - 00:1D:7E:53:2B:09
  - o **Spoofing**
    - Wijzig je MAC-adres vanuit het OS
    - Om je eigen router op de werking ervan te controleren zit het wijzigen van het MAC in bijvoorbeeld Windows in
- **TCP/IP**
  - o Transmission Control Protocol/Internet Protocol
  - o Suite met protocols
  - o Geadopteerd in de IT-wereld door integratie in OS'en
  - o Toepasbaar op diverse technologieën (Ethernet, Token Ring, ...)

- Routable over diverse soorten netwerken (Windows, Apple, Linux, ...)
- Ontwikkeld door Amerikaanse overheid (geen proprietary)
- TCP = laag 4 (transport), IP = laag 3 (network)
- Package fragmentation en reassembly
  - Twee header fields (IP header en TCP header)
  - Data field



- Connecties opzetten (**three-way handshake**)
  - SYN (Synchronize)
  - SYN (Synchronize) en ACK (Acknowledge)
  - ACK (Acknowledge)

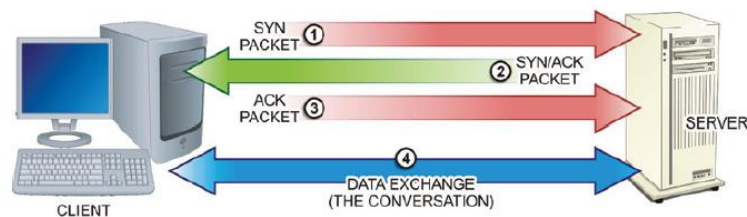
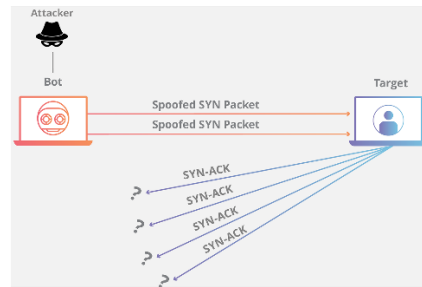


FIGURE 13.2 SYN/ACK Sequence

- Kwetsbaarheden
  - Attack of makeup of packets
    - Header manipulation
    - IP spoofing
      - Manipuleren van source en destination IP in header
  - SYN flood (denial of service) exploits three-way handshake
    - Hacker stuurt vele SYN requests naar een server en spoofs IP-adres of houdt ACK packet bij, waardoor er op de server allemaal connecties blijven openstaan en geheugen server volloopt



- **MAC en TCP/IP**
  - MAC = laag 2, TCP/IP = laag 3
  - **DHCP** (dynamic host configuration protocol) past **ARP** (Address Resolution Protocol) toe om een MAC-adres aan een IP-adres te koppelen
- **IP-adressen**
  - **IPv4-adressen**
    - 32-bits ( $2^{32} = 4.294.967.296$  adressen)
    - **Dotted decimal notation**
      - XXX.YYY.ZZZ.AAA (vier 8-bits velden of octetten)
    - Voorbeeld:
      - 10000111.10001011.01001001.00110110  
komt overeen met  
135.139.073.054
    - **MSO**      **LSO** (most en least significant octet)
    - **IPv4 classes**
      - Class A: laatste drie octetten duiden host aan
        - Range van 001.x.x.x tot 126.x.x.x (hele grote netwerken)
        - 17 miljoen nodes (hosts) in elk van de 126 netwerken
      - Class B: laatste twee octetten duiden host aan
        - Range van 128.x.x.x tot 191.254.0.0 (medium netwerken)
        - 65.534 nodes (hosts) in elk van de 16 384 netwerken
      - Class C: laatste octet duidt de host aan
        - Range: van 192.x.x.x tot 223.254.254.0
        - 254 nodes (hosts) in elk van de 2 miljoen netwerken
    - **Subnetting**
      - Beperk het aantal bruikbare ip-adressen voor hosts
        - Subnet mask verbergt of masks
          - 255.255.255.0 laat 10.0.1.1, 10.0.1.100, 10.0.1.255 toe, niet 10.0.2.5
        - Voordelen
          - Netwerk afscheiden
          - Efficiënt gebruik van IP-adressen
          - Eén IP-adres over meerdere fysieke locaties verdelen
  - **IPv6-adressen**
    - 128-bits ( $2^{128}$  of  $3,4 \times 10^{38}$  adressen)
    - 16 octetten (32 hexadecimale getallen)
      - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
    - Niet alle IPv6 kan je omzetten naar IPv4!
      - Er zijn meer IPv6 adressen dan IPv4

- Bestaat uit twee delen
  - Host = interface identifier
  - Netwerk = network address (bepaald door subnet mask prefix)
- In browser tussen vierkante haken
  - `http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]`
- aaneenliggende nullen weglaten met '::'

| RFC1918 name | IP address range              | Number of addresses | Largest CIDR block (subnet mask) | Host ID size | Mask bits | Classful description <sup>[Note 1]</sup> |
|--------------|-------------------------------|---------------------|----------------------------------|--------------|-----------|--|
| 24-bit block | 10.0.0.0 – 10.255.255.255     | 16 777 216          | 10.0.0.0/8 (255.0.0.0)           | 24 bits      | 8 bits    | single class A network                   |
| 20-bit block | 172.16.0.0 – 172.31.255.255   | 1 048 576           | 172.16.0.0/12 (255.240.0.0)      | 20 bits      | 12 bits   | 16 contiguous class B networks           |
| 16-bit block | 192.168.0.0 – 192.168.255.255 | 65 536              | 192.168.0.0/16 (255.255.0.0)     | 16 bits      | 16 bits   | 256 contiguous class C networks          |

- 
- **Ethernet**
  - Familie van standaards die oplegt hoe de signalen moeten worden verstuurd
  - Half-duplex: data kan in twee richtingen maar niet gelijktijdig
  - Hoe weten of datalijn in gebruik is?
    - **CSMA/CD** (carrier sense multiple-access with collision detection) protocol
      - Node luistert eerst of de LAN in gebruik is
      - Bij gelijktijdig zenden door twee nodes, wachten elk willekeurige tijd met opnieuw zenden

## Hoofdstuk 14

### Understanding network servers

- Server = computersysteem dat services levert aan clients
- Server op uitschuifbare rails
  - In een rack
  - In een kast
- Soorten
  - Algemeen gebruik-server (KMO)
  - Applianceserver (met gerichte hard- en software)
  - Toepassingssoftwareserver (interactie met databases)
  - Mail server
  - Firewall server (internet gateway)
  - Proxy server (caching)
  - Webserver (website)
  - Database server (databases)
  - Terminal server (mainframes)
    - A terminal server enables organizations to connect devices with a serial port to a local area network
  - Gateway server (to other types of networks)
  - DNS server (converteren naar ip-adres)
  - Router server (shared resources van alle routers binnen het netwerk)
  - Bridge server (computergroepen verbinden)
  - FTP (file transfer protocol)
  - NAS (network attached storage)
  - SAN (storage area network)
  - RAS (remote access system: dial in op het LAN)
  - Print server (lokaal en remote)
  - DHCP (dynamic host configuration protocol)

- Beveiliging
  - Shared resources beperken in rechten
  - Firewall om servers te beschermen
  - Account gegevens (password) hashen (versleutelen)
  - Subnetting / meerdere routers
  - Auditing

## Hoofdstuk 15

### Network connectivity devices

- Switch
  - Verbindt apparaten binnen een LAN
  - Opvolger van hub
    - Hub stuurt alle gegevens naar iedereen door (broadcast)
    - Hub verdeelt maximale bandbreedte over alle aangesloten nodes
  - Switch verdeelt de datapakketjes gericht tussen zender en ontvanger (peer to peer)
  - Soorten
    - Verschillende soorten, verschil in routing
    - Layer 2 (data link) = basisswitch
      - MAC-adressen als routing
      - Data packet = frame
    - Layer 3 (network) = brouter (bridged router)
      - IP-adressen als routing
      - Gebruikt hetzelfde protocol als een router
    - Layer 4 (transport) = router
      - Kan NAT (network address translation) toepassen om data te routeren  
= omzetten van private ip-adressen naar gateway-ip-adres en omgekeerd
    - Layer 7 (application)
      - Kan http-protocol toepassen om data te routeren
        - Kijken naar URL, cookies, SSL session om pakketten sneller te routeren
  - VLAN
    - Virtual local area network
    - Beperkt de zichtbaarheid van delen van een netwerk
    - Communicatie langsheen geselecteerde poorten
  - Types
    - Unmanaged
      - Out-of-the-box: plug and play (PnP)
      - Geen setup nodig
    - Managed
      - Kan geconfigureerd worden voor een specifiek netwerk
      - Langs CLI (command line interface) of web based (SNMP = Simple Network Management Protocol)
    - PoE
- Router

- Verbindt twee netwerken (bv. LAN met provider)
- Routing met IP-adressen
- OS op routers
  - Cisco System's Internetwork Operating System (IOS)
  - Andere Linux/Unix gebaseerde OS
- Soorten (bekabeld en draadloos)
  - Edge
    - Communiceert tussen twee netwerken (ISP en LAN) (internet dus)
    - Staat op de rand (edge) van het netwerk)
  - Core
    - Communiceert binnenin een netwerk (op de backbone) voor high-performance
    - Verkeer tussen edge routers regelen
  - Virtual
    - Software routers
    - Voordeel: makkelijk schaalbaar
- Gateway
  - Toestel dat twee netwerken verbindt, die elk een ander protocol gebruikt
    - Hardware- en softwareprotocollen
- Bridge
  - Verbindt meerdere netwerksegmenten
  - Broadcasts gaan naar alle poorten (blijven dus niet in netwerksegment)
  - Voorloper van de switch
- Kwetsbaarheden
  - Fysiek beschermd (bv. server room, afgesloten kasten, ...)
  - Uitschakelen van niet-gebruikte services en programma's
  - MAC-adressen filteren
  - Configuratie van het toestel
- Aanvallen
  - Unauthorized access
  - Packet sniffing
    - ARP spoofing attacks
      - Vals ARP request sturen zodat IP naar fout MAC adres verwijst
    - MAC flooding
      - MAC address table vullen op switch zodat er geen nieuwe MAC adressen bijkunnen op switch en alle berichten moet gaan broadcasten naar alle poorten
    - Router flooding
      - Router overbelasten
    - Denial of Service (DoS)
      - Een systeem overbelasten waardoor het niet meer goed kan functioneren
      - DDoS (Distributed DoS)
        - DoS met meerdere remote systemen tegelijk
    - Session replay
      - Aanvaller bewaart een aantal IP pakketten, wijzigt deze en stuur ze dan weer uit om toegang te krijgen of andere ongewenste gevolgen



- Rerouting attack
  - Aanvallen die toegang heeft tot routing tables en ze aanpast
- Masquerade attack
  - Manipuleren van IP pakketten om vals IP adres te maken (valse identiteit) en daarmee toegang te krijgen tot het netwerk
- Netwerkdefensie
  - Data rate limiting
  - Delayed binding
  - Bogus IP address filtering
  - Access control list
  - Deep packet inspection
    - Zoeken naar signalen van virussen, spam of andere bedreigingen en zal bepalen op het pakket moet worden doorgestuurd of niet. Soms kan het zijn dat een verdacht pakket naar een speciale locatie wordt verzonden voor verder onderzoek.
  - Packet filtering
    - Pakketten filteren op basis van hun source/destination adressen, poorten of protocols
- Network hardening
  - Monitoring
  - Security policy
  - Alle netwerkkapparaten up-to-date
  - Servers in het juiste netwerksegment, subnet of beveiligingszone (bv. achter een extra router)
  - ACL's
  - Rollen nakijken

## NIST cybersecurity framework

- National Institute of Standards and Technology (NIST)
- Het framework bestaat uit drie delen
  - the Framework Core
    - A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements:
      - Functions
        - Identify
          - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
        - Protect
          - Develop and implement appropriate safeguards to ensure delivery of critical services.
        - Detect
          - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
        - Respond

- Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
  - Recover
    - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
- Categories
- Subcategories
- Informative References.
- the Framework Implementation Tiers
  - A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
  - Geeft aan in welke mate een organisatie het framework gebruikt en reageert op dreigingen (wachten tot er iets gebeurt, actief zoeken, ...)
  - Hoe hoger de tier, hoe beter
  - Tiers
    - Tier 1: Partial
      - Enkel iets doen als er een cybersecurity event plaatsvindt
    - Tier 2: Risk Informed
      - Risicomanagement is toegelaten, maar is geen policy in de organisatie. Men is bewust dat er iets kan gebeuren, maar zal geen voorzorgmaatregelen nemen in heel de organisatie.
    - Tier 3: Repeatable
      - Policy voor risicomanagement. Er worden regelmatig controles en updates gedaan. Iedereen in de organisatie is zich bewust van de risico's en weet welke rol die speelt hierin.
    - Tier 4: Adaptive
      - Organisatie is continu bezig om beveiliging te verbeteren. Er is een door iedereen gekende aanpak over hoe je met cybersecurity events moet omgaan.
- the Framework Profiles
  - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
  - Geeft aan in welke mate de huidige implementatie overeenkomt met de gewenste implementatie van het framework core (categorieën en subcategorieën).
    - Current profile
    - Target profile
- Stappenplan
  - Step 1: Prioritize and Scope.
    - Doelen vastleggen
  - Step 2: Orient.
    - Bekijken wat de opties zijn, oriënteren
  - Step 3: Create a Current Profile.

- Step 4: Conduct a Risk Assessment.
  - Wat is de kans dat een cybersecurity event plaatsvindt? En wat is de impact?
- Step 5: Create a Target Profile.
- Step 6: Determine, Analyze, and Prioritize Gaps.
  - Verschil tussen current profile en target profile bepalen. Vervolgens plan opstellen om deze verschillen op te lossen.
- Step 7: Implement Action Plan.

## Examen

- Open vragen
- Voor examen hoofdstuk ~~1—25~~ -> 1 t.e.m. 15
- Je krijg NIST op het examen: geeft 2 categorieën en subcategorieën + leg uit
  - Zijn screenshots van het boek
- Risk assesment (met NIST)
- Poorten kunnen herkennen, naam, waarvoor het wordt gebruikt, input or output, ...
- Wat is een firewall en wat doet het?
- Alle namen van de 7 lagen van het OSI model kennen + kunnen uitleggen
- Three-layered rings of security zeker kennen
- Ip en TCP header -> enkele voorbeelden kunnen geven van wat er in zit
- Verschillende types van switches kennen
- Mac address table
- Geef twee voorbeelden van besturingssystemen op routers
  - Cisco IOS
  - Andere Unix systemen
- 
- **H5, H10 en H17 zeker nakijken: samenvattingen + examenvragen**

## Opdracht

- Kernel attack slide 59
  - Kernel praat met CPU
  - Instructie die naar CPU gaan wijzigen
- 4 kernel attacks in linux
  - Welke commando's
  - Hoe kan je dan doen?
  - Hoe kan je code in geheugen zetten zodat kernel die gaat gebruiken?
  - ...
- In document
  - Naam
  - Groep
  - 4 titels (slide 59)
  - Gewoon copy-paste van internet + bronvermelding