Region Nordjylland

Teknisk kursus, dag 2

UCN act2learn

9. juni 2023

Ib Helmer Nielsen
UCN act2learn Erhverv

Agenda for dag 2

1

REST og SOAP

Grundlæggende Netværk

Sikkerhed/Authentication

4

Databaser

Sikkerhed/Authentification

- CIA
- Kryptering
- Authentification
- Firewall
- Active Directory

UCN act2learn

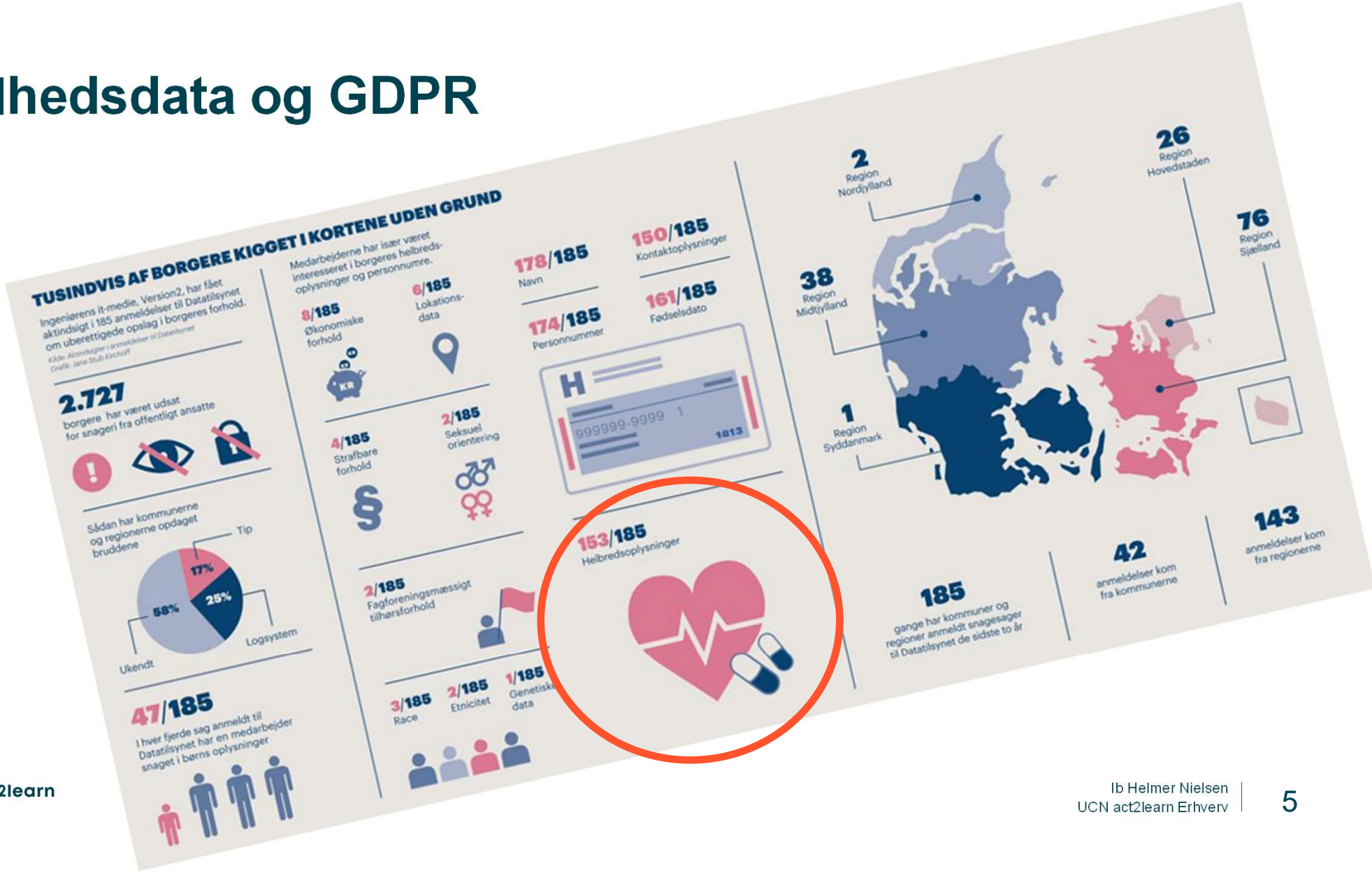
9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

Hvorfor sikkerhed og hvad vil det sige?

UCN act2learn

9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

Sundhedsdata og GDPR



GDPR forordningen

Artikel 9

2. Stk. 1 finder ikke anvendelse, hvis et af følgende forhold gør sig gældende:

h) Behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson og underlagt de betingelser og garantier, der er omhandlet i stk. 3.

(53) Særlige kategorier af personoplysninger, som bør nyde højere beskyttelse, bør kun behandles til sundhedsmæssige formål, når det er nødvendigt for at opfylde disse formål til gavn for fysiske personer og samfundet som helhed, navnlig i forbindelse med forvaltning af sundheds- eller socialydelser og -systemer, herunder administrationens og centrale nationale sundhedsmyndigheders behandling af sådanne oplysninger med henblik på kvalitetskontrol,

Sikkerhedstrusler

UCN act2learn

9. juni 2023

Ib Helmer Nielsen
UCN act2learn Erhverv

Sikkerhedstrusler i moderne IT-systemer

- De største sikkerhedstrusler i moderne IT-systemer er konstant i udvikling, efterhånden som teknologi og angrebsteknikker bliver mere sofistikerede.
- Her er nogle af de mest betydelige trusler, som organisationer står over for i dag:
  - Phishing og Social Engineering:Angriberne bruger falske e-mails, beskeder eller websites til at narre brugere til at afsløre følsomme oplysninger som loginoplysninger eller finansielle data. Phishing-kampagner er ofte meget målrettede og svære at opdage, især når de kombineres med social engineering-teknikker.
  - Ransomware:Ransomware-angreb krypterer en virksomheds data og kræver løsesum for at gendanne adgangen. Disse angreb kan lamme virksomhedens operationer og medføre store økonomiske tab samt skade virksomhedens omdømme.

Sikkerhedstrusler mod moderne IT-systemer

- Malware:Malware, som kan være virus, trojanske heste, spyware osv., bruges til at stjæle data, overvåge brugeres aktiviteter, eller få uautoriseret adgang til systemer. Malware kan spredes gennem inficerede filer, usikre downloads, eller kompromitterede websites.
- Insidertrusler:Medarbejdere, tidligere ansatte, eller andre med intern adgang kan bevidst eller ubevidst kompromittere sikkerheden. Insidertrusler kan være svære at opdage, fordi de ofte involverer personer, der allerede har tillid og adgang til virksomhedens ressourcer.
- Distributed Denial of Service (DDoS) Angreb:DDoS-angreb overbelaster et system, netværk eller service med en overflod af forespørgsler, hvilket gør dem utilgængelige for legitime brugere. Dette kan føre til driftsafbrydelser og betydelige økonomiske tab.
- Zero-Day Sårbarheder:Disse er ukendte sikkerhedssårbarheder i software, som endnu ikke er opdaget eller rettet af udviklere. Hackere kan udnytte zero-day sårbarheder til at infiltrere systemer og stjæle data, før en patch er tilgængelig.

Sikkerhedstrusler i moderne IT-systemer

- Supply Chain Angreb:Hackere målretter sig mod tredjepartsleverandører for at infiltrere en organisations systemer. Disse angreb udnytter ofte tilliden mellem en virksomhed og dens leverandører og kan sprede sig til mange andre virksomheder via den samme kompromitterede kilde.
- Credential Stuffing:Hackere bruger stjålne loginoplysninger fra et sikkerhedsbrud til at få adgang til andre konti. Da mange brugere genbruger deres adgangskoder, kan dette føre til kompromittering af flere konti på tværs af forskellige tjenester.
- Cloud Security Issues:Efterhånden som flere virksomheder flytter til skyen, opstår der nye trusler, såsom forkert konfigurerede cloud-tjenester, manglende synlighed i dataflow, og uautoriseret adgang til cloud-resourcer.
- Internet of Things (IoT) Sikkerhedsrisici:IoT-enheder, der er forbundet til nettet, kan være sårbare over for angreb, hvis de ikke er korrekt sikret. Svage adgangskoder, manglende softwareopdateringer, og dårlig enhedsadministration kan føre til, at IoT-enheder bruges som indgangspunkter til større netværksangreb.

CIA

- Confidentiality,
- Integrity,
- Availability

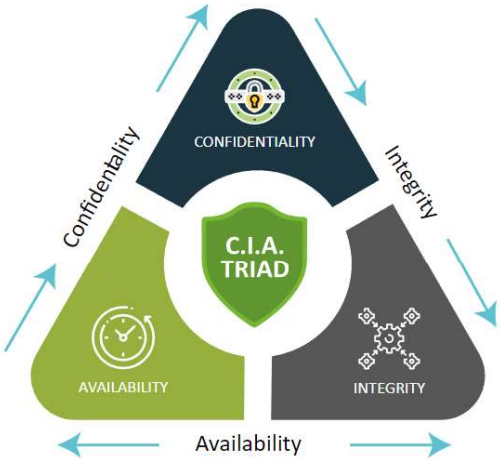
UCN act2learn

9. juni 2023

Ib Helmer Nielsen
UCN act2learn Erhverv

CIA-Triaden

- CIA-triaden er en grundlæggende sikkerhedsmodel inden for informationssikkerhed, der repræsenterer tre centrale mål:
  - fortrolighed (confidentiality),
  - integritet (integrity) og
  - tilgængelighed (availability).



CIA-Triaden Fortrolighed

- Fortrolighed handler om at sikre, at oplysninger kun er tilgængelige for de autoriserede parter.
- Dette indebærer at beskytte data mod uautoriseret adgang, læsning, kopiering eller videregivelse.
- Kryptering, adgangskontrol og sikkerhedspolitikker er nogle af de metoder, der anvendes til at opnå fortrolighed.

CIA-Triaden Integritet

- Integritet handler om at sikre, at data forbliver uændrede, autentiske og pålidelige.
- Det indebærer beskyttelse mod uautoriseret ændring, manipulation eller ødelæggelse af data.
- Metoder som datavalidering, hashfunktioner og digital signering bruges til at sikre integriteten af data.

CIA-Triaden Tilgængelighed

- Tilgængelighed handler om at sikre, at autoriserede brugere har rettidig adgang til de nødvendige ressourcer og informationer, når de har brug for dem.
- Det indebærer at forhindre nedbrud, afbrydelser eller utilgængelighed af systemer og data på grund af fejl, angreb eller tekniske problemer.
- Redundans, backup, fejlfinding og kapacitetsstyring er nogle af de tilgængelighedsrelaterede metoder.

Andre forhold vi gerne vil kunne sikre (Non-repudiation)

- Non-repudiation (ikke-benægtelse) betyder at en person eller enhed ikke kan benægte ægtheden af deres underskrift eller det faktum, at de har sendt en besked.
- Det giver bevis for oprindelsen og integriteten af data, hvilket forhindrer nogen i senere at benægte, at de har sendt dataene eller været involveret i transaktionen.I praksis implementeres ikke-benægtelse ofte gennem kryptografiske metoder, såsom digitale signaturer.
- Her bruger afsenderen en privat nøgle til at underskrive en besked eller et dokument. Modtageren eller en tredjepart kan derefter bruge afsenderens offentlige nøgle til at verificere, at beskeden eller dokumentet faktisk blev underskrevet af afsenderen og ikke er blevet ændret.
- Dette sikrer, at afsenderen ikke kan benægte deres involvering, fordi underskriften er unikt knyttet til dem. Ikke-benægtelse er afgørende i mange sammenhænge, herunder online transaktioner, e-mail kommunikation og juridiske aftaler, hvor det er vigtigt at have uomtvistelige beviser for, hvem der gjorde hvad og hvornår.

Kryptering

- Kryptering er processen med at omdanne almindelige tekst eller data til en uforståelig form ved hjælp af en algoritme og en nøgle.
- Det formål, det tjener, er at beskytte fortroligheden og integriteten af information, så kun autoriserede parter kan læse og forstå dataene.
- Kryptering spiller en afgørende rolle i informationssikkerhed og bruges til at sikre kommunikation, beskytte følsomme oplysninger og verificere dataintegritet.

Cæsarkryptering

- Cæsarkryptering er en simpel form for substitution kryptering, hvor hvert bogstav i en besked erstattes med et bogstav, der er en fast skiftning længere nede i alfabetet.
- Det er opkaldt efter Julius Cæsar og blev brugt til at sende hemmelige beskeder i det gamle Rom. Cæsarkryptering er en let at bryde metode og anvendes sjældent i moderne kryptografi.
- Nøgle 3
- Plain text : Hej RN -> Cipher text: Khm#UQ

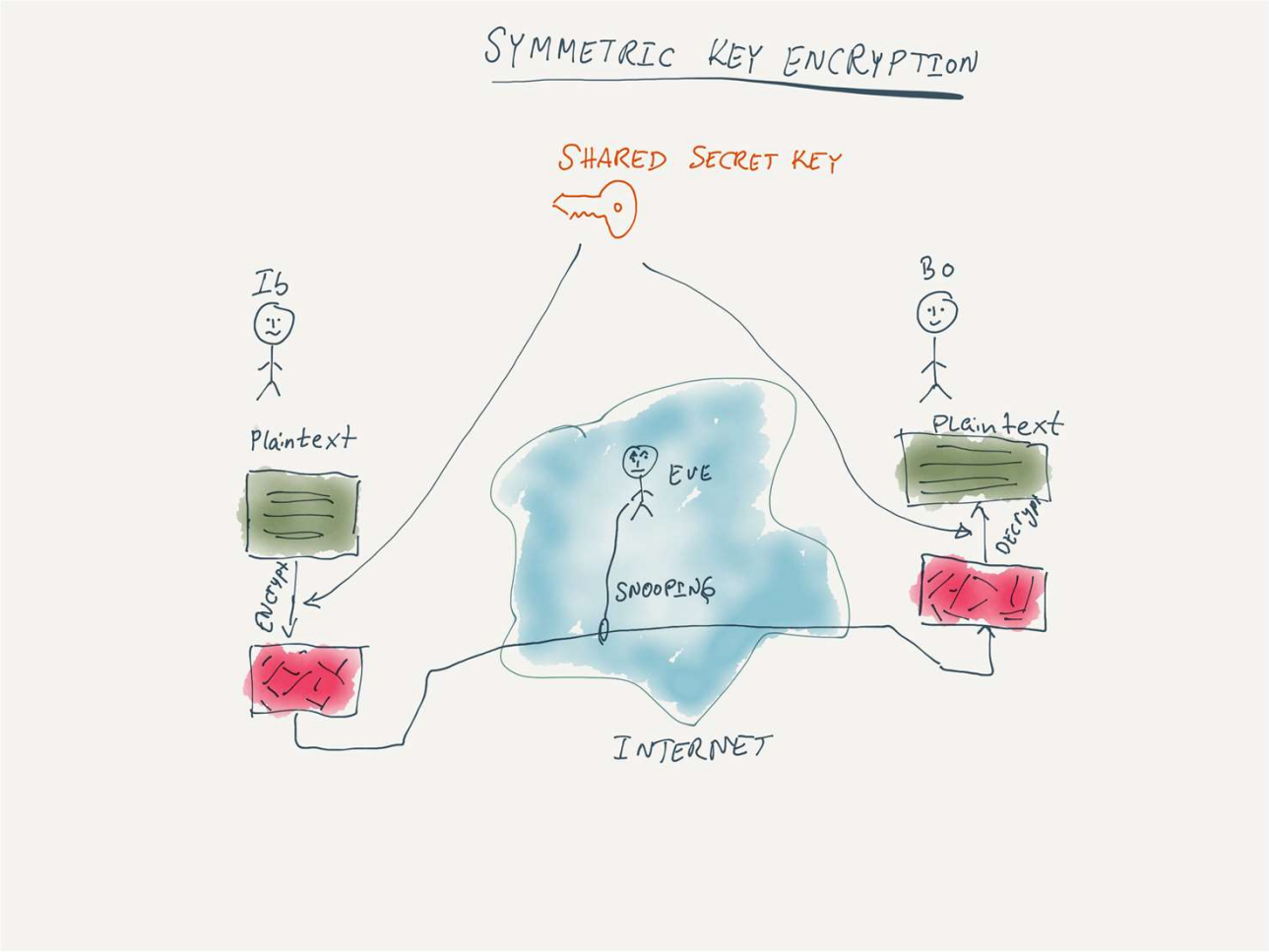
Kryptering (5 min)

Diskuter med siddemakker:

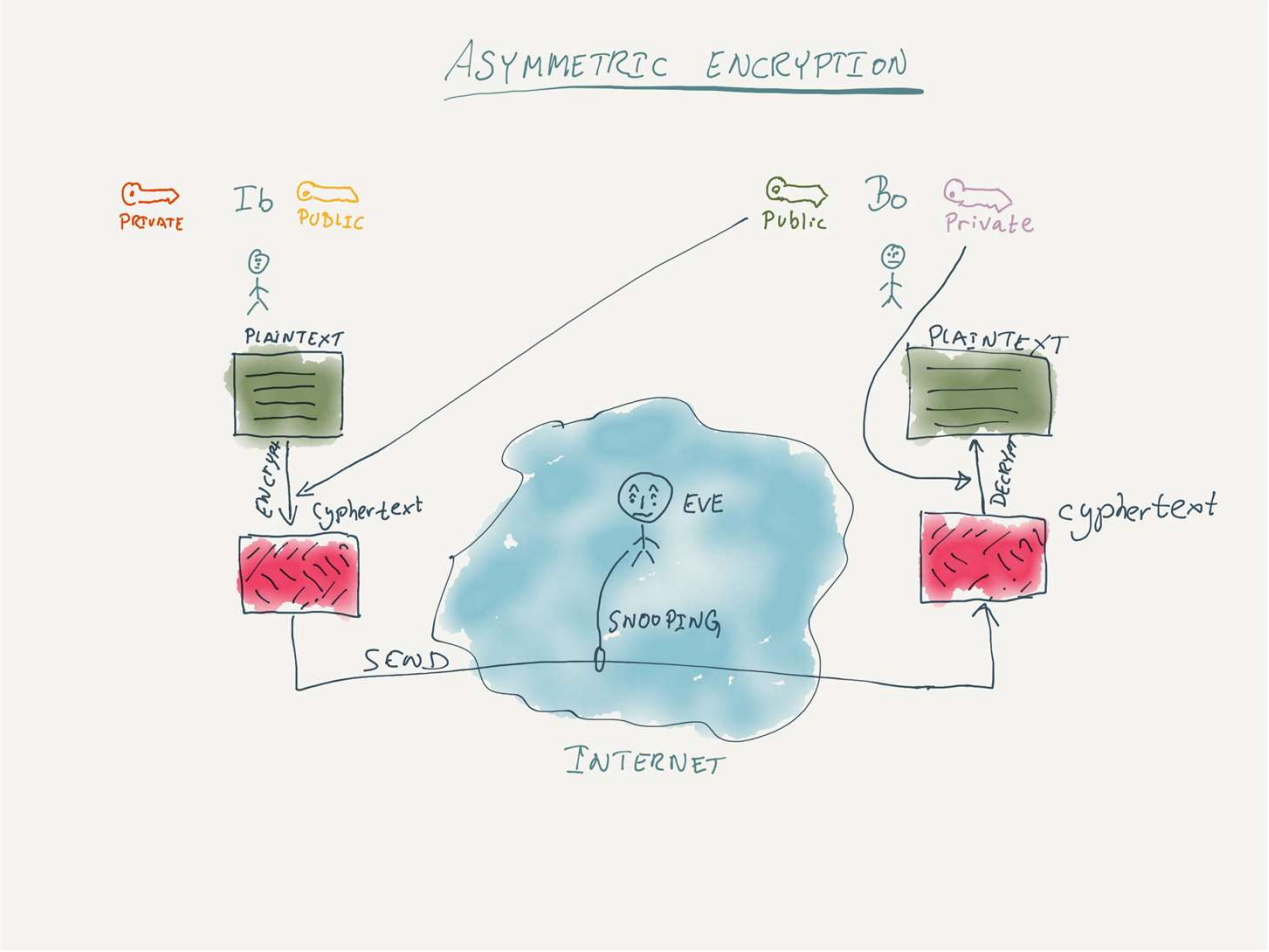
- Hvad er problemet med Cæsar kryptering ?
- Hvordan kan den let knækkes ?
- Hvordan kan den gøres bedre ?

Ib Helmer Nielsen
UCN act2learn Erhverv

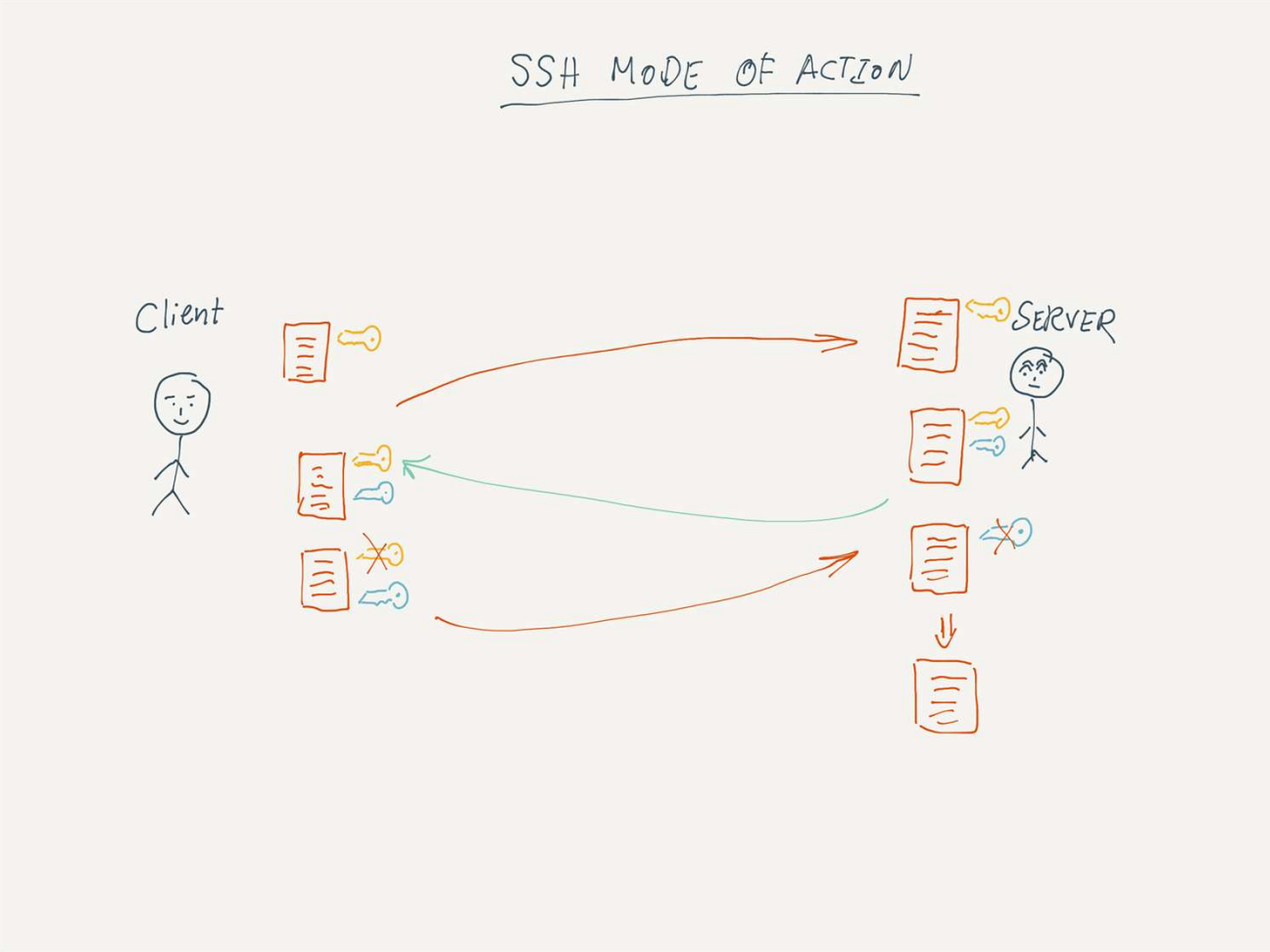
Symmetrisk kryptering



Asymmetrisk Kryptering

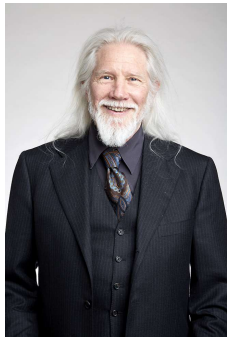


Andre måder at udveksle data krypteret på

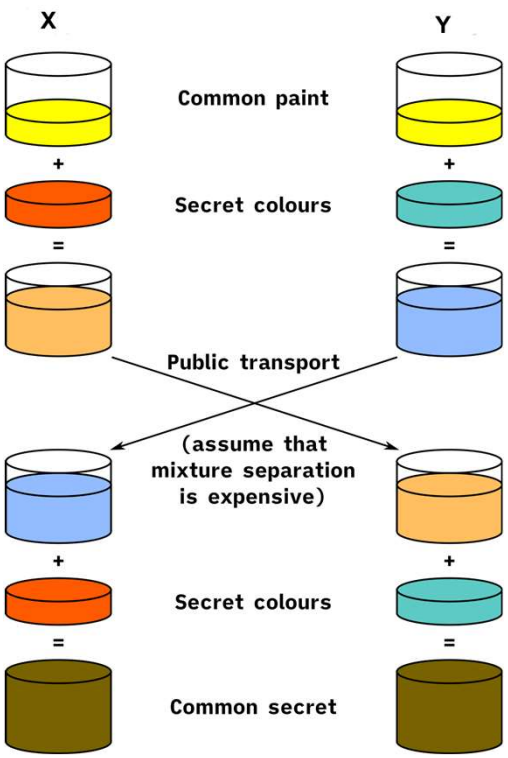


Diffie-Hellman key exchange

- Diffie-Hellman key exchange var den første udbredte metode til sikkert at danne og udveksle krypterings nøgler over en usikker kanal. Metoden tillader to parter, der ikke tidligere har mødt hinanden, på en sikker måde at etablere en nøgle, som de kan bruge til at sikre deres kommunikation.
- Faktisk udveksles nøglen ikke direkte, men i stedet information, der gør det muligt for begge parter at konstruere den samme nøgle ved at udveksle information.
- Diffie-Hellman-nøgleudveksling, også kaldet eksponentiel nøgleudveksling.
- I 1976 opfandt Whitfield Diffie og Martin Hellman metoden til, så folk altså kunne få adgang til den samme fælles nøgle selv over en en åben kanal. Ideen var baseret på et koncept af Ralph Merkle.

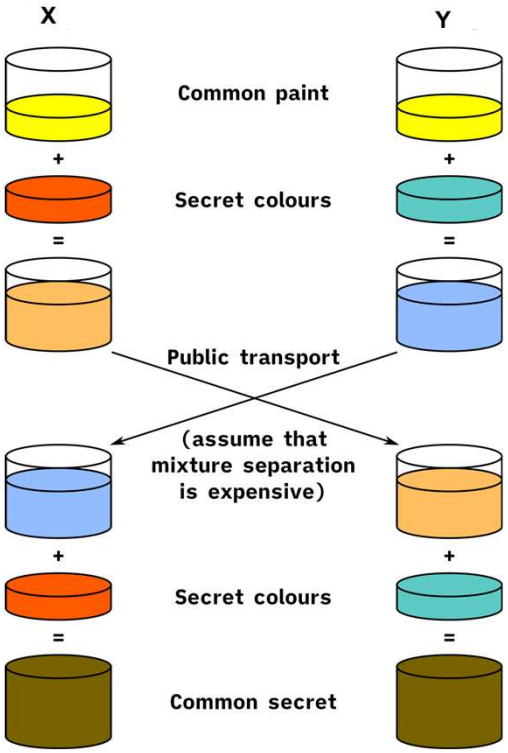


Princip behind DH



- Processen begynder med, at de to parter, Ib og Bo, offentligt bliver enige om en vilkårlig startfarve, som ikke behøver at holdes hemmelig (men som bør være forskellig hver gang). I dette eksempel er farven gul.
- Hver person vælger også en hemmelig farve, som de holder for sig selv – i dette tilfælde rød og blågrøn. Den afgørende del af processen er, at Ib og Bo hver især blander deres egen hemmelige farve med deres fælles delte farve, hvilket resulterer i henholdsvis orangebrun og lyseblå blandinger, og derefter udveksler de de to blandede farver offentligt.
- Endelig blander de hver den farve, de modtog fra modparten, med deres egen private farve. Resultatet er en endelig farveblanding (gulbrun i dette tilfælde), som er identisk med partnerens endelige farveblanding.

Princip behind DH



- Hvis en tredje part lyttede til udvekslingen af fælles farven, ville de kun kende den fælles farve (gul) og de første blandede farver (orangebrun og lyseblå), men det ville være svært for denne part at bestemme den endelige hemmelige farve (gulbrun).
- Hvis vi overfører analogien til en virkelig udveksling ved hjælp af store tal i stedet for farver, er denne beregning meget ressourcekrævende.
- Det er umuligt at beregne på en praktisk tidsskala, selv for moderne supercomputere.

DH how to implement

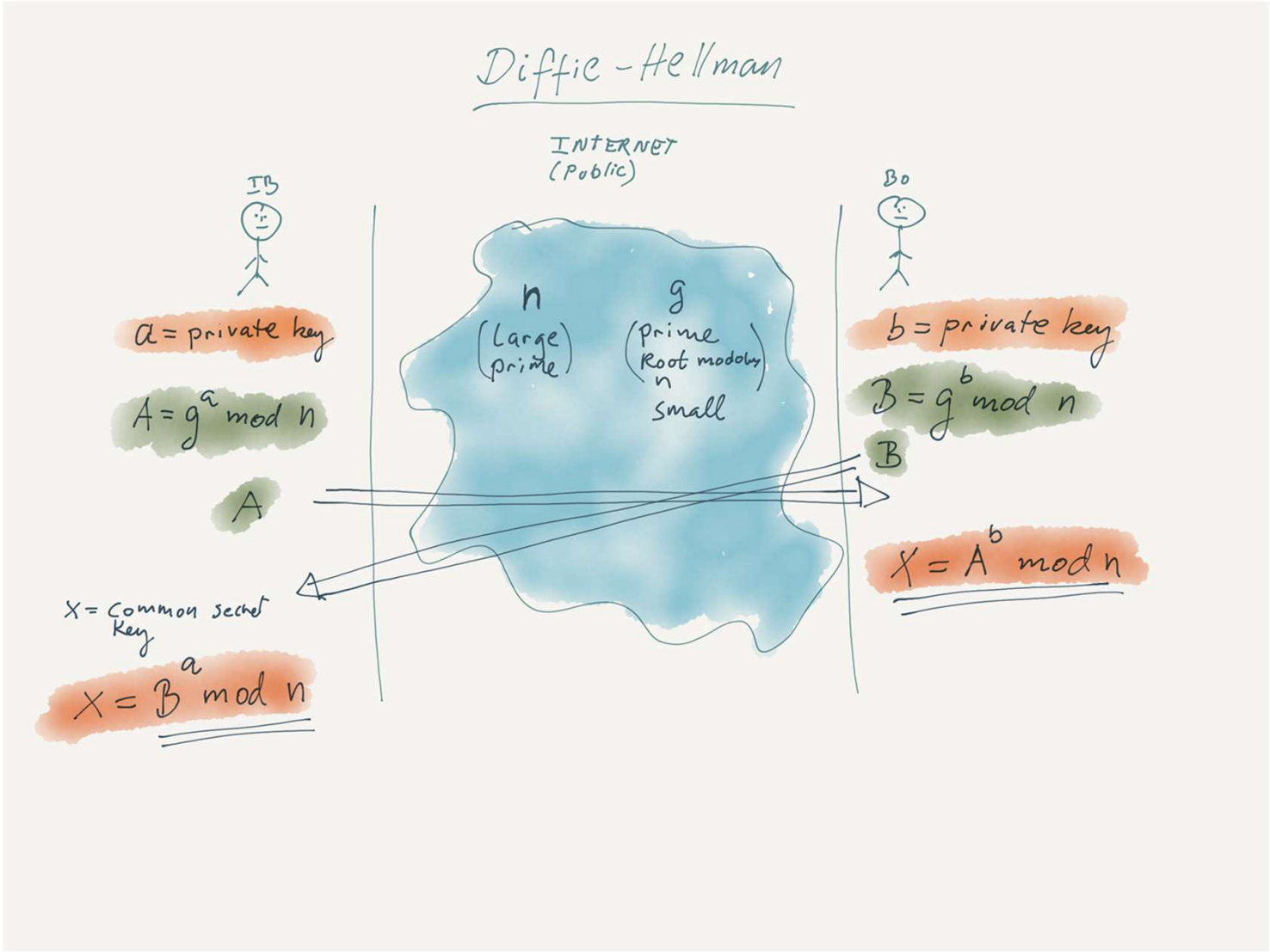
- To implement Diffie-Hellman, the two end users Ib and Bo, mutually agree on positive whole numbers n and g, such that n is a prime number and g is a generator of n. The generator g is a number that, when raised to positive whole-number powers less than n, never produces the same result for any two such whole numbers. This webpage (http://www.bluetulip.org/2014/programs/primitive.html) can be used for finding the numbers. The value of n may be large but the value of g is usually small.
- Once Ib and Bo have agreed on n and g, they choose positive whole-number personal keys a and b, both less than the prime-number modulus n.

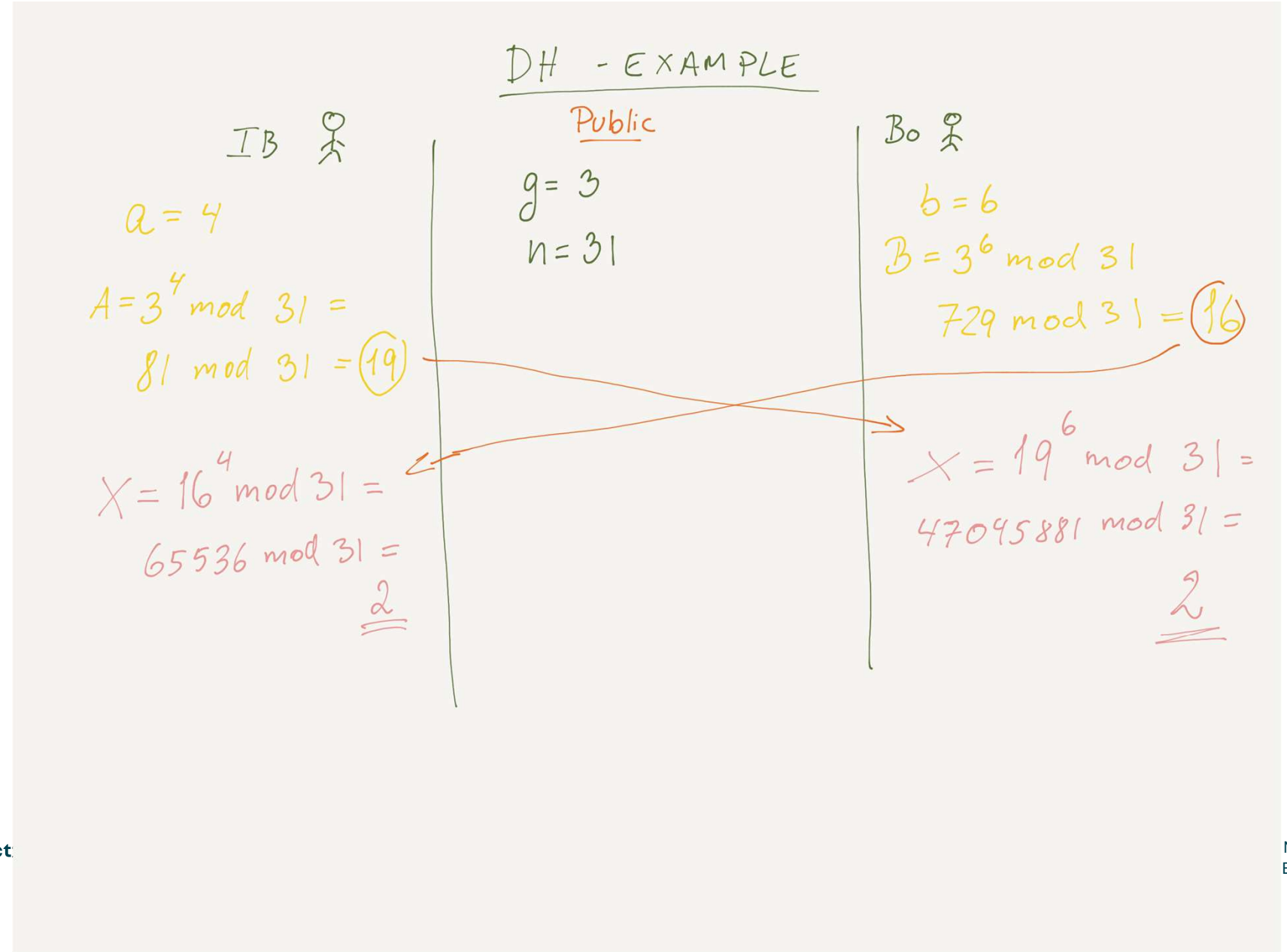
DH how to implement

- Neither user divulges their personal key to anyone; ideally they memorize these numbers and do not write them down or store them anywhere. Next, Ib and Bo compute public keys A and B based on their personal keys according to the formulas:
- A $= g^a \ mod \ n$ (Ib's formula)
- B $= g^b mod \ n$ (Bo's formula)
- a = Ib's personal keys
- b = Bo's personal keys

DH how to implement

- From the public keys, the secret number X can be generated by either user on the basis of their own personal keys a and b. Ib's computes x using the formula:
- $X = B^a \ mod \ n$
- Bo's computes X using the formula:
- $X = A^b \ mod \ n$


Diffie-Hellman
INTERNET
(Public)
IB
Bo
a = private key
A = g^a mod n
A
n
(Large prime)
g
(prime Root modolu n small)
b = private key
B = g^b mod n
B
X = A^b mod n
X = Common secret Key
X = B^a mod n


DH - EXAMPLE
Public
IB
Bo
g = 3
n = 31
a = 4
A = 3^4 mod 31 =
81 mod 31 = 19
b = 6
B = 3^6 mod 31
729 mod 31 = 16
X = 16^4 mod 31 =
65536 mod 31 =
2
X = 19^6 mod 31 =
47045881 mod 31 =
2

DH and it’s limitation

- The most serious limitation of Diffie-Hellman in its basic or "pure" form is the lack of authentication.
- Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium.
- Diffie-Hellman is well suited for use in data communication but is less often used for data stored or archived over long periods of time.

SSL and TLS Encryption

UCN act2learn

9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

How Does SSL/TLS Encryption Work?

- SSL (Secure Sockets Layer) encryption, and its more modern and secure replacement, TLS (Transport Layer Security) encryption, protect data sent over the internet or a computer network.
- This prevents attackers (and Internet Service Providers) from viewing or tampering with data exchanged between two nodes—typically a user's web browser and a web/app server.
- Most website owners and operators have an obligation to implement SSL/TLS to protect the exchange of sensitive data such as passwords, payment information, and other personal information considered private.

How Does SSL/TLS Encryption Work?

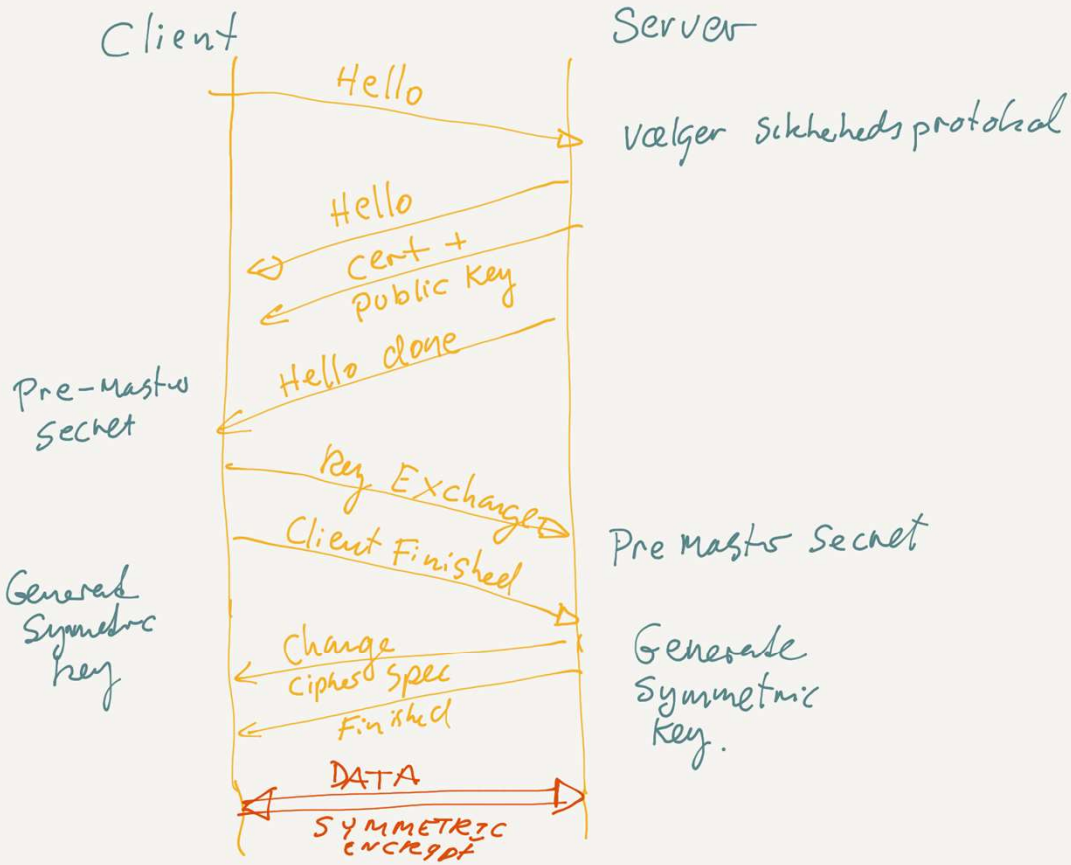
- SSL/TLS uses both asymmetric and symmetric encryption to protect the confidentiality and integrity of data-in-transit.
- Asymmetric encryption is used to establish a secure session between a client and a server, and symmetric encryption is used to exchange data within the secured session.
- A website must have an SSL/TLS certificate for their web server/domain name to use SSL/TLS encryption.
- Once installed, the certificate enables the client and server to securely negotiate the level of encryption.

How Does SSL/TLS Encryption Work, step by step

1) The client contacts the server using a secure URL (HTTPS…).
2) The server sends the client its certificate and public key.
3) The client verifies this with a Trusted Root Certification Authority to ensure the certificate is legitimate.
4) The client and server negotiate the strongest type of encryption that each can support.
5) The client encrypts a session (secret) key with the server's public key, and sends it back to the server.
6) The server decrypts the client communication with its private key, and the session is established.
7) The session key (symmetric encryption) is now used to encrypt and decrypt data transmitted between the client and server.

Both the client and server are now using HTTPS (SSL/TLS + HTTP) for their communication. Web browsers validate this with a lock icon in the browser address bar. HTTPS functions over Port 443.

TLS - Handshake



Hvad er et certifikat egentligt ?

- Et certifikat er et digitalt dokument, der fungerer som en elektronisk identitetsattest. Det bekræfter identiteten af en enhed, enten en person, en organisation, en computer eller en webside, i en digital kommunikation. Certifikater anvender kryptografiske metoder og er udstedt af betroede enheder eller certifikatautoriteter (CA).
- Et certifikat indeholder flere vigtige elementer. Først er der identitetsoplysninger, der identificerer den enhed, certifikatet er udstedt til. Dette kan omfatte navn, organisation, e-mailadresse eller anden identifikator.
- Derudover indeholder certifikatet en offentlig nøgle, som er en del af et nøglepar, der består af en offentlig og en privat nøgle. Den offentlige nøgle bruges til kryptografiske operationer som kryptering, digital signering eller nøgleaftale. Den offentlige nøgle er knyttet til den enheds private nøgle og kan bruges til at verificere digital signatur og sikre kommunikation.

Hvad er et certifikat egentligt ?

- Certifikatet indeholder også oplysninger om udstederen, den enhed eller organisation, der udsteder certifikatet. Disse oplysninger kan omfatte navn, offentlig nøgle og eventuelle tilladelser eller certificeringsniveauer.
- Endelig har certifikatet en udløbsdato, der angiver, hvornår certifikatet ikke længere er gyldigt. Dette er vigtigt, da det sikrer, at certifikatet regelmæssigt bliver fornyet for at opretholde sikkerheden og tilliden.
- Certifikater anvendes bredt inden for digital kommunikation og internetbaserede tjenester. For eksempel bruges SSL-/TLS-certifikater til at etablere en sikker forbindelse mellem en webbrowser og en webside. Certifikater spiller en afgørende rolle i at etablere fortrolighed, integritet og autentifikation i elektroniske kommunikationssystemer og bidrager til at opretholde sikkerhed og tillid.

Authentification

- Hvordan ved jeg at jeg faktisk kommunikere med F.eks Danske Bank ?
- Hvordan ved jeg at den data jeg udveksler mellem en website og min browser er kryptertet ?

Ib Helmer Nielsen
UCN act2learn Erhverv

Et skridt videre - Multifactor authentication (MFA)

- Multifactor authentication (MFA) er en sikkerhedsforanstaltning, der kræver brugen af to eller flere forskellige metoder til at bekræfte en persons identitet.
- Traditionel autentifikation, der normalt er baseret på brugernavn og adgangskode, kan være sårbart over for phishing, hacking eller tyveri af legitimationsoplysninger.
- MFA øger sikkerheden ved at tilføje ekstra lag af autentifikation.

Et skridt videre - Multifactor authentication (MFA)

- Typisk involverer MFA følgende faktorer:
  - **Noget, du ved**: Dette er normalt noget, du kender, såsom en adgangskode, en pinkode eller svar på sikkerhedsspørgsmål.
  - **Noget, du har**: Dette er noget fysisk, som du besidder, f.eks. en smartphone, en nøgleviser eller et smartkort.
  - **Noget, du er**: Dette er en biometrisk faktor, der bruger dine unikke fysiske egenskaber, såsom fingeraftryk, ansigtsgenkendelse eller stemmeidentifikation.

Et skridt videre - Multifactor authentication (MFA)

- For at logge ind eller få adgang til en tjeneste med MFA skal brugeren levere flere autentifikationsfaktorer. For eksempel kan en bruger blive bedt om at indtaste sit brugernavn og adgangskode (noget, de ved), og derefter modtage en engangskode via en autentificeringsapp på deres smartphone (noget, de har), som skal indtastes for at fuldføre autentifikationen.

- MFA forhindrer effektivt uautoriseret adgang, da selv hvis en faktor bliver kompromitteret, vil angriberen stadig skulle overvinde yderligere faktorer for at få adgang. Det øger beskyttelsen af brugerkonti og følsomme data og er blevet mere udbredt som en best practice for at styrke sikkerheden i digitale miljøer.

Problem når andre får adgang til vores PC

- Åben cmd (commando prompth)
- Kør kommando, indsæt i stedet for ”WiFi name”, navn på et wifi du bruger med denne PC :

Netsh wlan show profile name=”Wi-Fi name” key=clear

- Hvad får du udaf dette ??
- Du kan også bruge kommandoen:

for /f "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles') do @echo %j | findstr -i -v echo | netsh wlan show profiles %j key=clear

- Hvad får du udaf denne commando ?

Ib Helmer Nielsen
UCN act2learn Erhverv

Beskyttelse af vores Computer

- I mange moderne Notebook findes en TPM-chip (Trusted Platform Module) som er en hardwarekomponent i computeren, der bruges til at forbedre sikkerheden ved at beskytte krypteringsnøgler, adgangskoder og andre følsomme data.

TPM 2.0

TPM-chippen tilbyder en række sikkerhedsfunktioner:

- Sikker opbevaring af krypteringsnøgler:TPM-chippen kan generere, gemme og beskytte krypteringsnøgler, hvilket gør det sværere for hackere at få adgang til de data, der er beskyttet af disse nøgler. Nøglerne opbevares sikkert i TPM'en og kan ikke nemt eksporteres fra chippen, hvilket giver et ekstra lag af sikkerhed.
- Platformintegritetsmålinger:TPM bruges til at verificere, at systemet ikke er blevet ændret af ondsindet software eller malware. Dette gøres ved at måle integriteten af systemets komponenter (såsom BIOS, bootloader og operativsystem) under opstartsprocessen og sammenligne disse målinger med kendte værdier.
- Diskkryptering (f.eks. BitLocker):I Windows bruges TPM-chippen ofte sammen med BitLocker til at tilbyde fuld diskkryptering. TPM-chippen gemmer krypteringsnøglen og frigiver den kun, hvis systemets integritet er intakt. Dette betyder, at selv hvis en angriber fjerner harddisken og forsøger at læse dataene på en anden computer, vil de ikke kunne dekryptere oplysningerne uden TPM-chippen.

TPM 2.0

TPM-chippen tilbyder en række sikkerhedsfunktioner:

- Autentificering:TPM kan bruges til at forbedre autentificeringsmekanismer ved at gemme biometriske data eller andre autentificeringsoplysninger på en sikker måde. Dette bruges ofte i forbindelse med multifaktor-autentificering for at forbedre sikkerheden.
- Digital signering:TPM kan bruges til at generere og gemme digitale signaturer, som kan bruges til at autentificere dokumenter eller software, hvilket sikrer, at de ikke er blevet ændret.

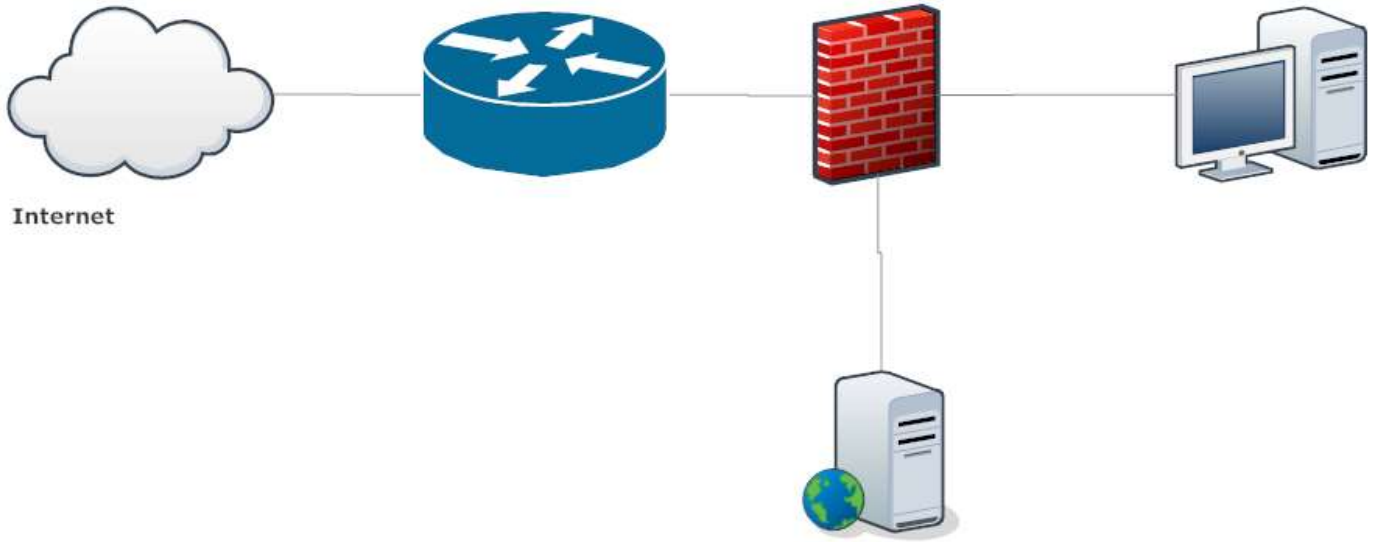
Firewall

UCN act2learn

9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

Grundlæggende virkemåde af en firewall.

- En firewall er en enhed (eller software) der anvendes til at styre flowet af data ind og ud af et netværk. Generelt installeres en firewall for at forhindre hackerangreb fra internettet og for at kontrollere den data der sendes ud fra et netværk.

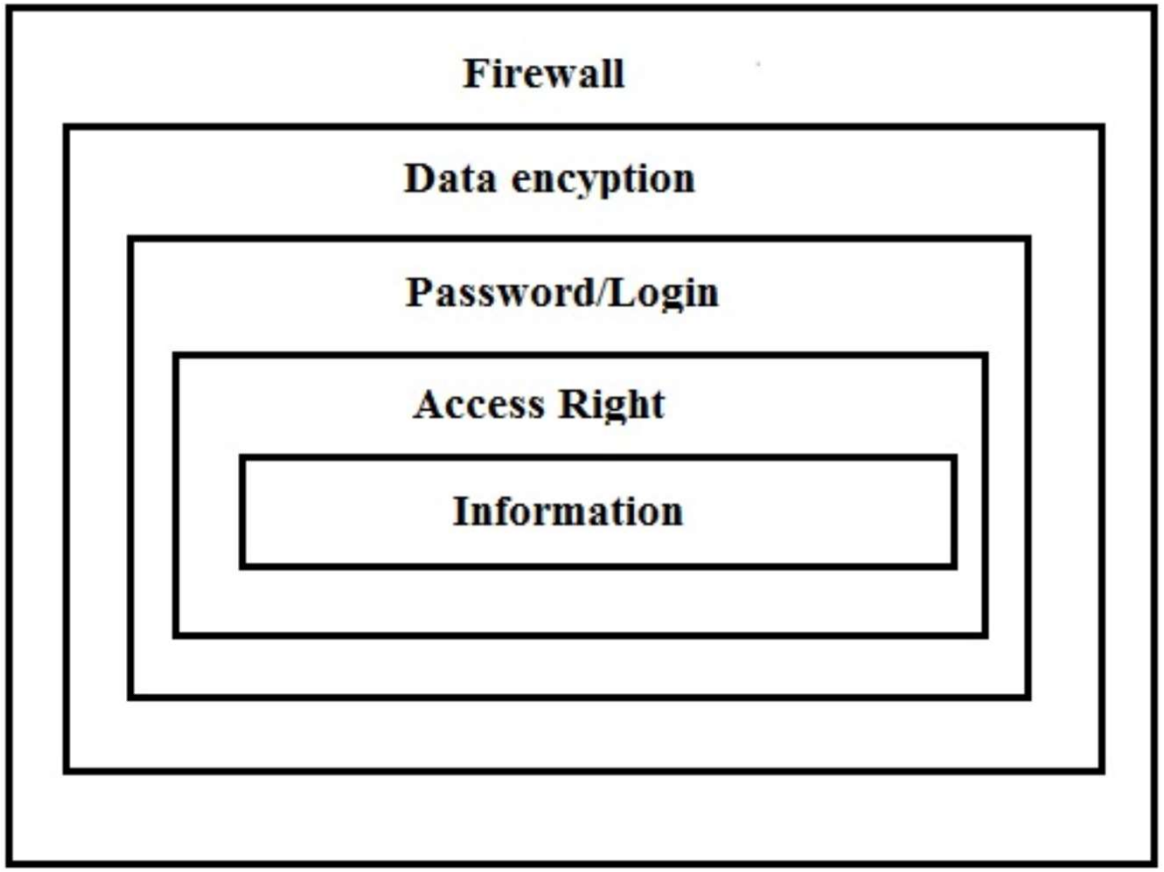


> A firewall is a computer traffic cop that permits or blocks data flow between two parts of a network architecture. It is the only link between parts.

Hvad er et ”hackerangreb”, nogle eksempler

- Port scanning for at få oplysninger om hvilke services der kører på netværk og på servere.
- Bevidst forsøg på at få en services eller en server til at gå ned.
- Forsøg på at få adgang til en computer for at bruge dens ressourcer
- Forsøg på at få adgang til de information der findes på computer.
- Forsøg på at ændre de informationer der findes på computer.

Sikkerhedsmodel for netværk og services



Firewalls enforce predetermined rules governing what traffic can flow

UCN act2learn

Ib Helmer Nielsen
UCN act2learn Erhverv

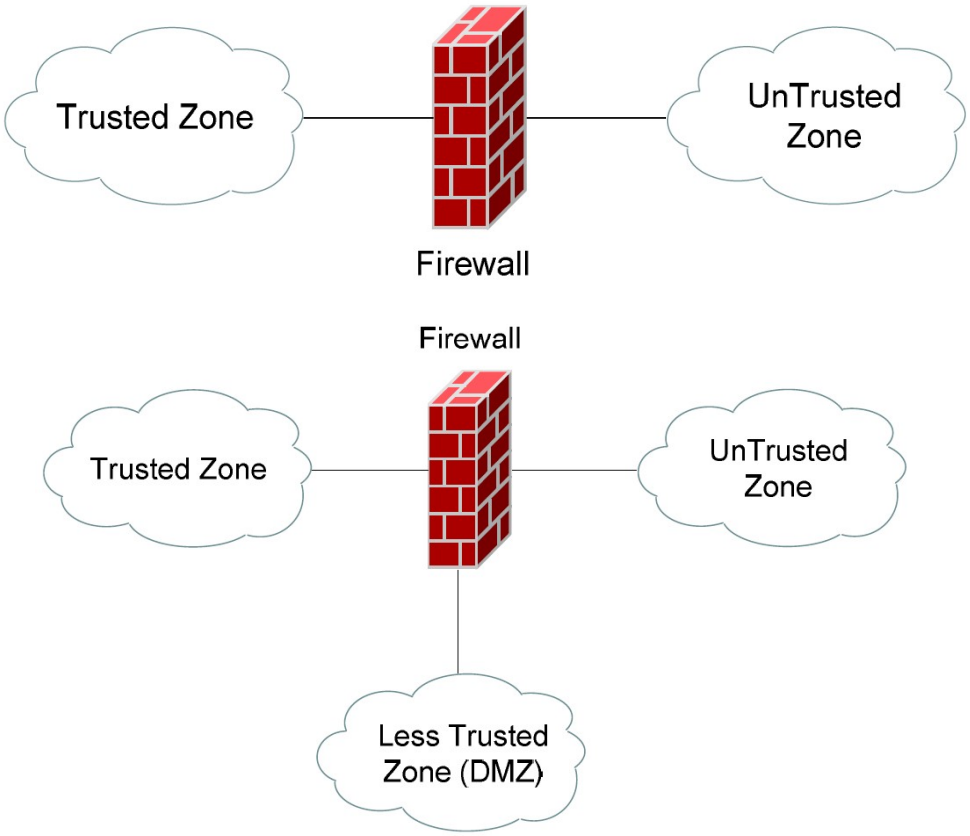
Hoved funktioner i standard firewall

Alle former for firewalls dele nogle generelle egenskaber og funktioner der sikre at firewallen kan løse den generelle opgave med at kontrollere datatrafik og sikre mod angreb.

Følgende er grundlæggende funktioner som de fleste firewall i større eller mindre grad kan udføre:

- Administration og styring af netværkstrafik
- Autentificere adgang
- Beskyttelse ressourcerne om uautoriseret adgang og forsøg på at hacke enhed
- Registrering og rapportering af hændelser
- Optræde som proxy

Begreber i forbindelse med en firewall's virkemåde



Policy

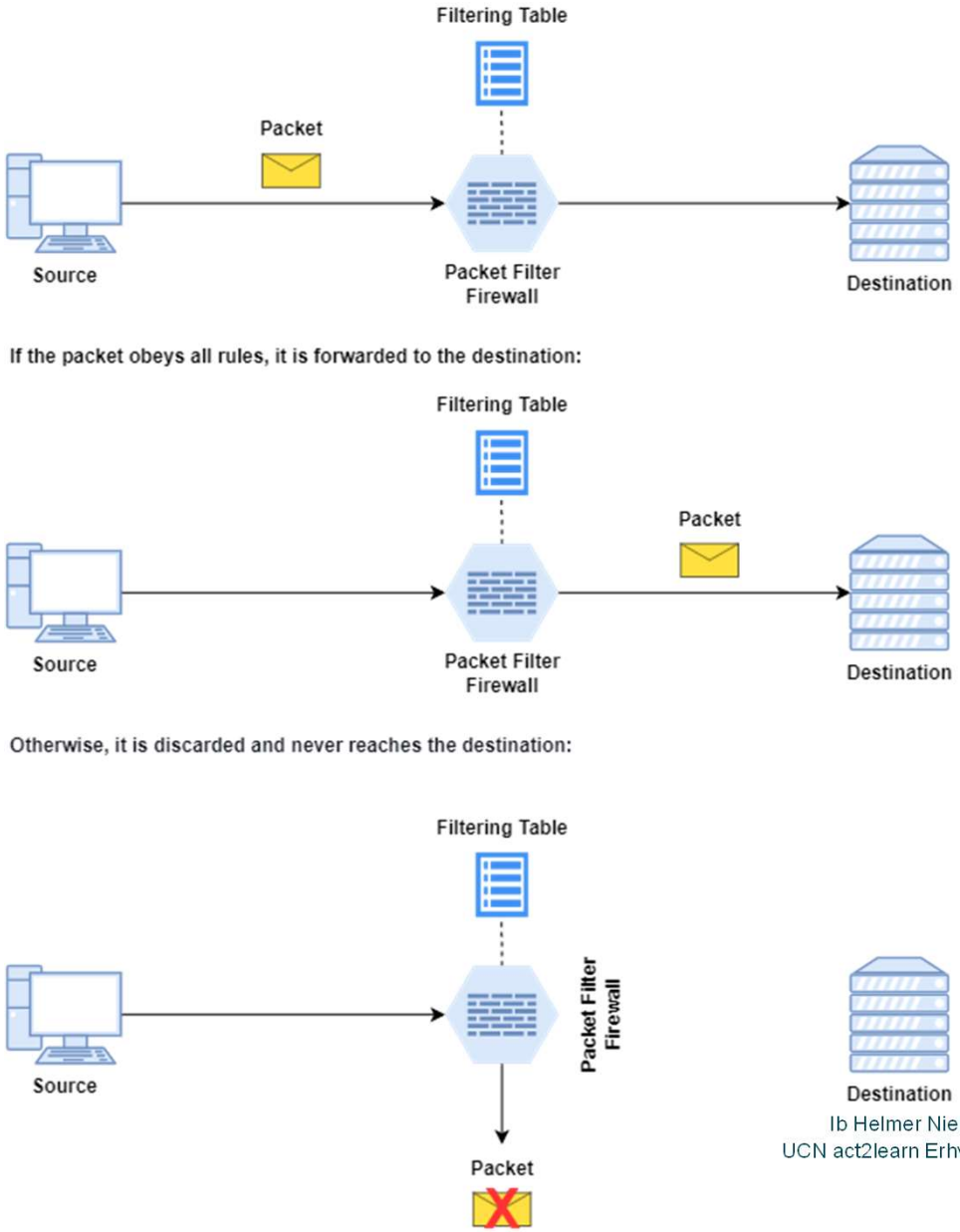
- A firewall implements a security policy, that is, a set of rules that determine what traffic can or cannot pass through the firewall.
- As with many problems in computer security, we would ideally like a simple policy, such as “good” traffic can pass but “bad” traffic is blocked.
- Unfortunately, defining “good” and “bad” is neither simple nor algorithmic.
- Firewalls come with example policies, but each network administrator needs to determine what traffic to allow into a particular network.

Example of firewall policy

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

Packet filtering firewall

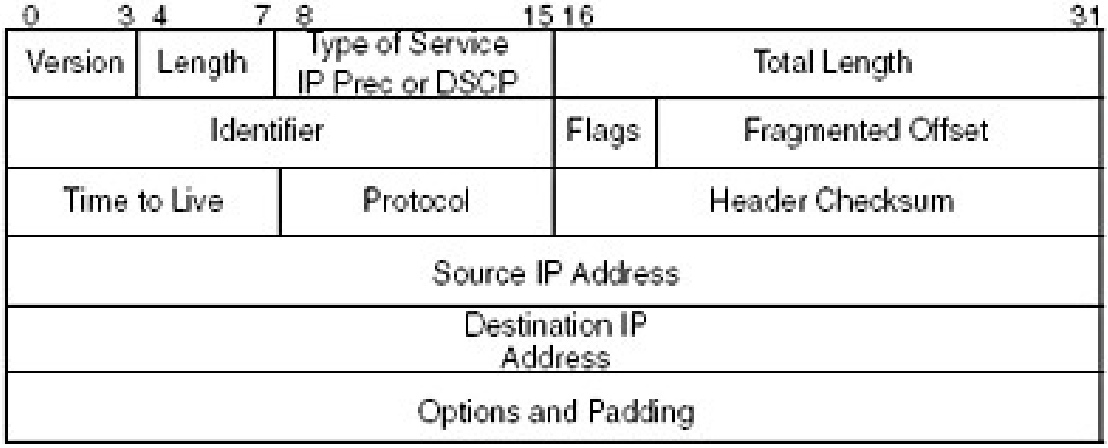
- Øverste tegning: Pakke sendt til destination med “lovlig” ip og port
- Miderste tegning: Pakke slipper gennem firewall
- Nederste tegning: Pakke sendt til ulovlig ip eller port smides væk.

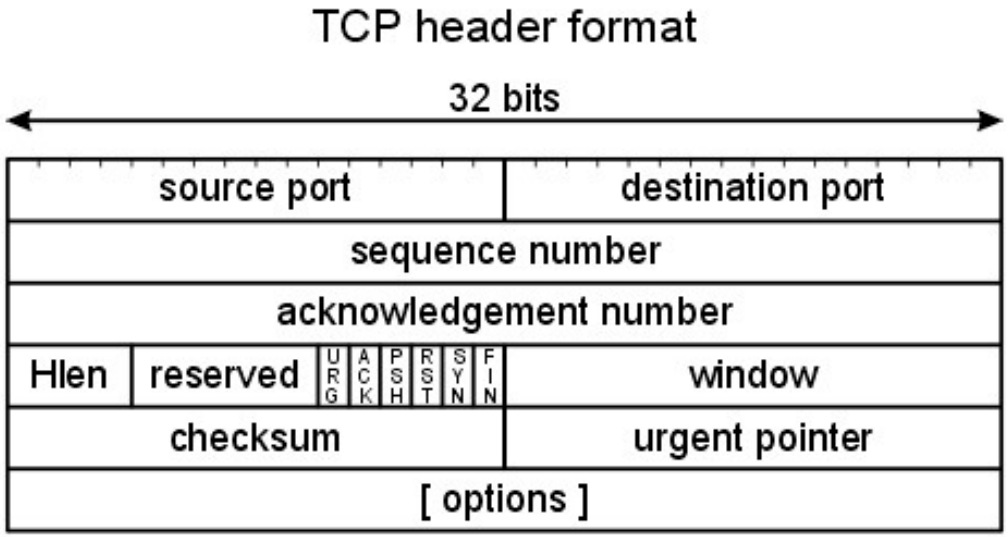


Packet Filtering

Foregår ved at undersøge de enkelte pakker der ankommer til firewallen udfra f.eks:

- Source address
- Destination address
- Protocol Type (IP, TCP, UDP, ICMP, ESP, etc.)
- Source Port
- Destination Port

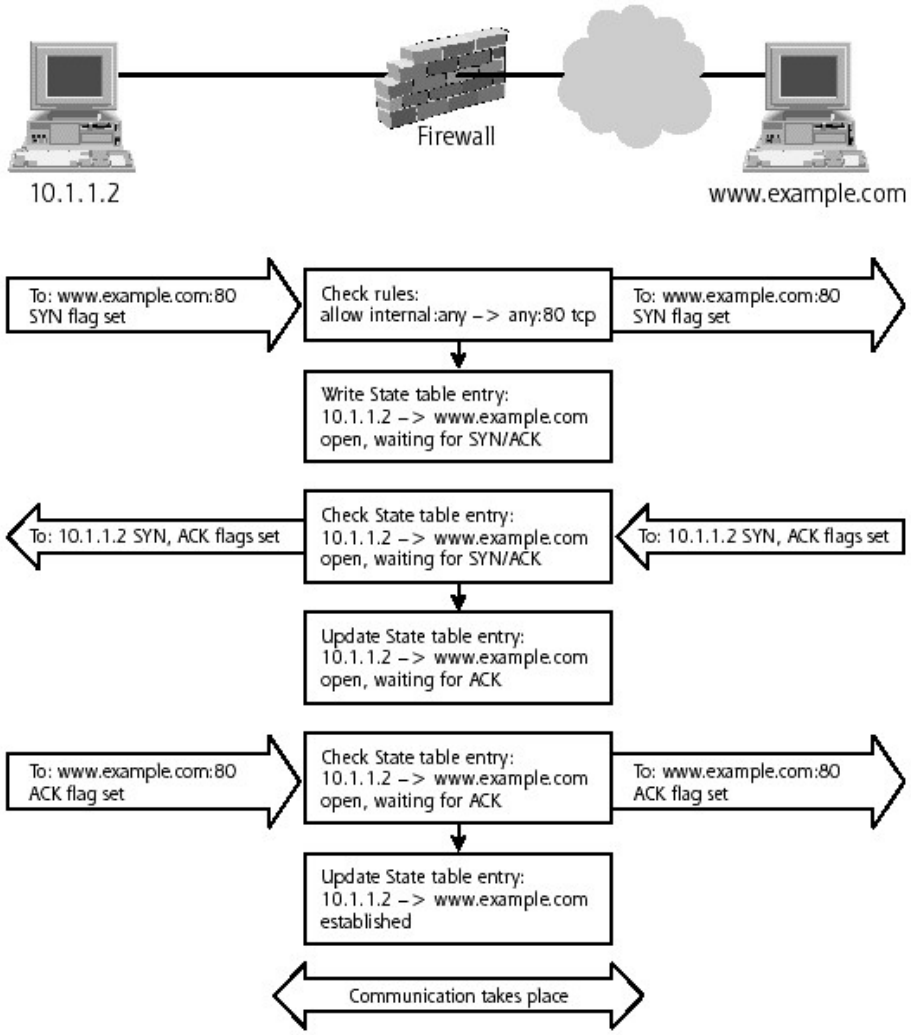




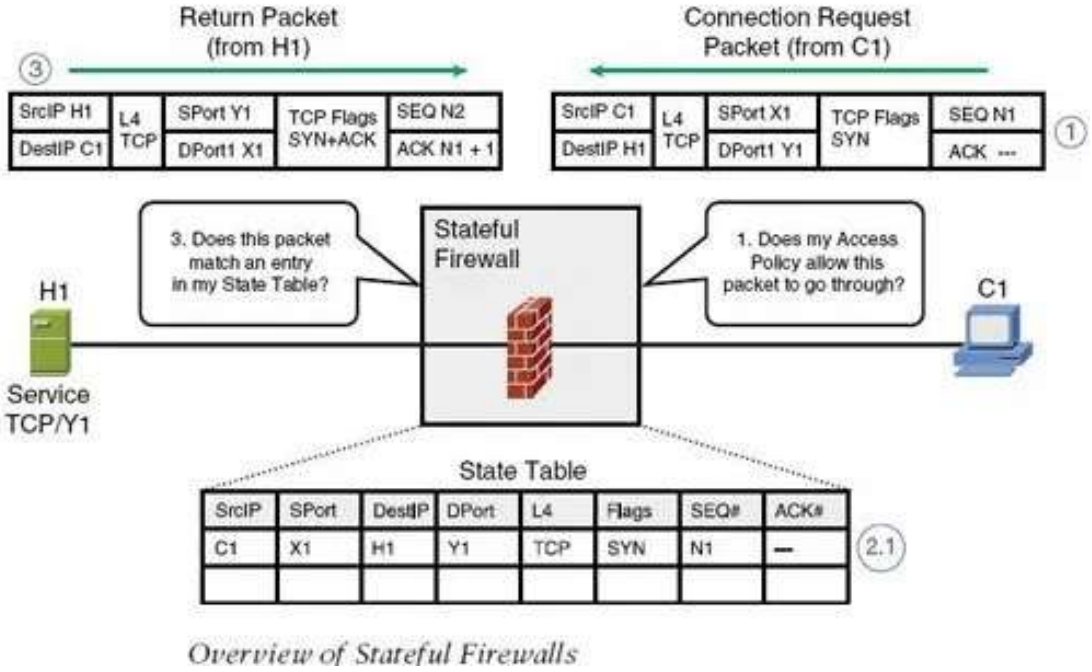
Packet Filtering

- Pakker der opfylder en bestem regel kan herefter enten accepteres eller forkastes (permitted or denied).
- De enkelte regler i firewallen opstilles i en prioriteret række og det er normal at den sidste regl i en firewall dropper hvad der ikke er fanget at regler tidligere:

Example


Firewall
10.1.1.2
www.example.com
To: www.example.com:80
SYN flag set
Check rules:
allow internal:any –> any:80 tcp
To: www.example.com:80
SYN flag set
Write State table entry:
10.1.1.2 –> www.example.com
open, waiting for SYN/ACK
To: 10.1.1.2 SYN, ACK flags set
Check State table entry:
10.1.1.2 –> www.example.com
open, waiting for SYN/ACK
To: 10.1.1.2 SYN, ACK flags set
Update State table entry:
10.1.1.2 –> www.example.com
open, waiting for ACK
To: www.example.com:80
ACK flag set
Check State table entry:
10.1.1.2 –> www.example.com
open, waiting for ACK
To: www.example.com:80
ACK flag set
Update State table entry:
10.1.1.2 –> www.example.com
established
Communication takes place

Stateful Packet Inspection

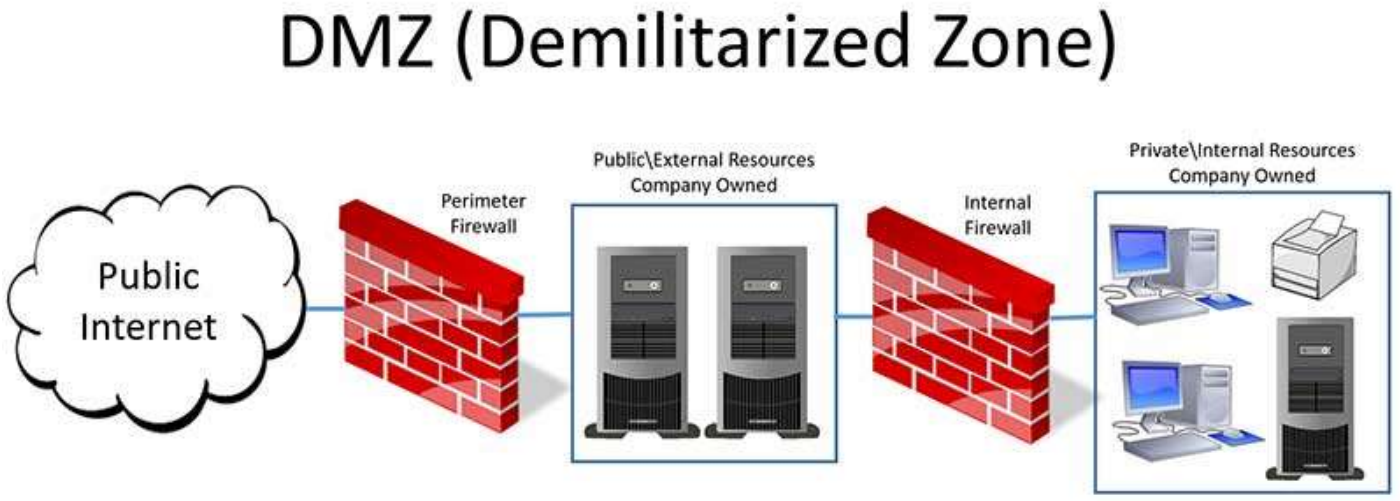


Overview of Stateful Firewalls

- ht

Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

DMZ (Demilitarized zone)



Her af navnet DMZ

Reflektion over DMZ (10min)

- Hvad er formålet med et DMZ
- Diskuter hvorfor det er en fordel ud fra et sikkerhed perspektiv at placere nogle services i en DMZ.
- Hvilke services kan med fordel placeres i et DMZ.
- Er der nogle ulemper ved at placere services i et DMZ ?

Ib Helmer Nielsen
UCN act2learn Erhverv

Overvågning og monitorering

UCN act2learn

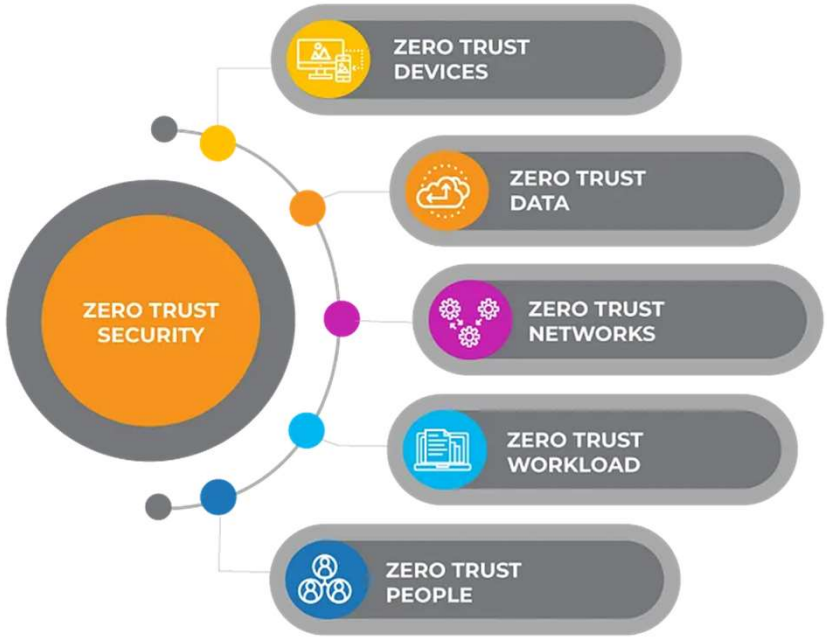
9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

Overvågning og beskyttelse af systemer internt

- Et NIDS (Network Intrusion Detection System) og et NIPS (Network Intrusion Prevention System) er begge sikkerhedssystemer designet til at overvåge netværkstrafik og beskytte mod ondsindede aktiviteter.
- NIDS (Network Intrusion Detection System): overvåger netværkstrafik i realtid og analyserer den for mistænkelig aktivitet. Den registrerer og advarer om potentielle sikkerhedstrusler baseret på et sæt af regler, signaturer eller en baseline. NIDS kan dog ikke aktivt forhindre trusler, men det kan logge hændelser og sende advarsler til sikkerhedsadministratoren, så der kan handles manuelt.
- NIPS (Network Intrusion Prevention System): udfører samme funktioner som et NIDS, men med den vigtige forskel, at det kan tage proaktive skridt for at forhindre trusler. Når en mistænkelig aktivitet, trussel eller anormalitet detekteres, kan et NIPS blokere eller afbryde den ondsindede trafik, inden den når målet, hvilket hjælper med at beskytte netværket mod angreb. Kort sagt, mens NIDS fokuserer på at opdage og rapportere trusler, går NIPS skridtet videre ved at forebygge dem aktivt.

Zero Trust

- Zero Trust er en IT-sikkerhedsmodel, der bygger på princippet om, at ingen brugere eller enheder, uanset om de befinder sig inden for eller uden for netværkets grænser, automatisk skal have tillid.
- I stedet skal alle brugere og enheder verificeres og autoriseres løbende, før de får adgang til ressourcer i netværket.



Kerneprincipperne i Zero Trust inkluderer:

- Verificér altid: Ingen implicit tillid. Alle brugere, enheder og applikationer skal gennemgå streng autentificering og autorisation, hver gang de forsøger at få adgang til ressourcer.
- Mindste privilegium: Giv kun adgang til de ressourcer, der er nødvendige for at udføre en bestemt opgave, og intet mere.
- Segmentering: Del netværket op i små segmenter for at begrænse, hvor langt en angriber kan bevæge sig, hvis de får adgang til et segment.
- Kontinuerlig overvågning: Aktiv overvågning og analyse af al trafik for at opdage og reagere på potentielle trusler i realtid.

Zero Trust-modellen hjælper med at beskytte organisationer mod moderne sikkerhedstrusler ved at minimere risikoen for insidertrusler og begrænse konsekvenserne af eventuelle sikkerhedsbrud.

Why Directory services?

Functions and Benefits of Active Directory
Components of Active Directory

UCN act2learn

9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

AD is a Directory Service

A directory service is:

> A service used by business to define, manage, access and secure network resources, including files, printers, people and applications for a group of users

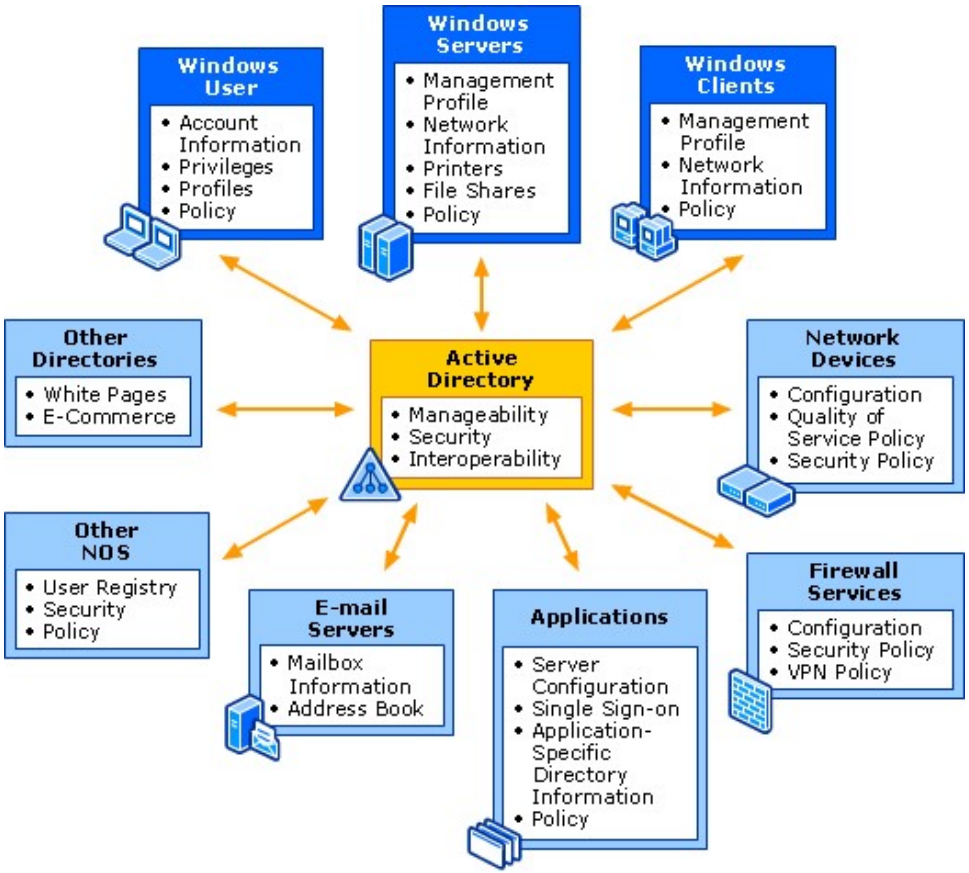
Ib Helmer Nielsen
UCN act2learn Erhverv

AD Benefits

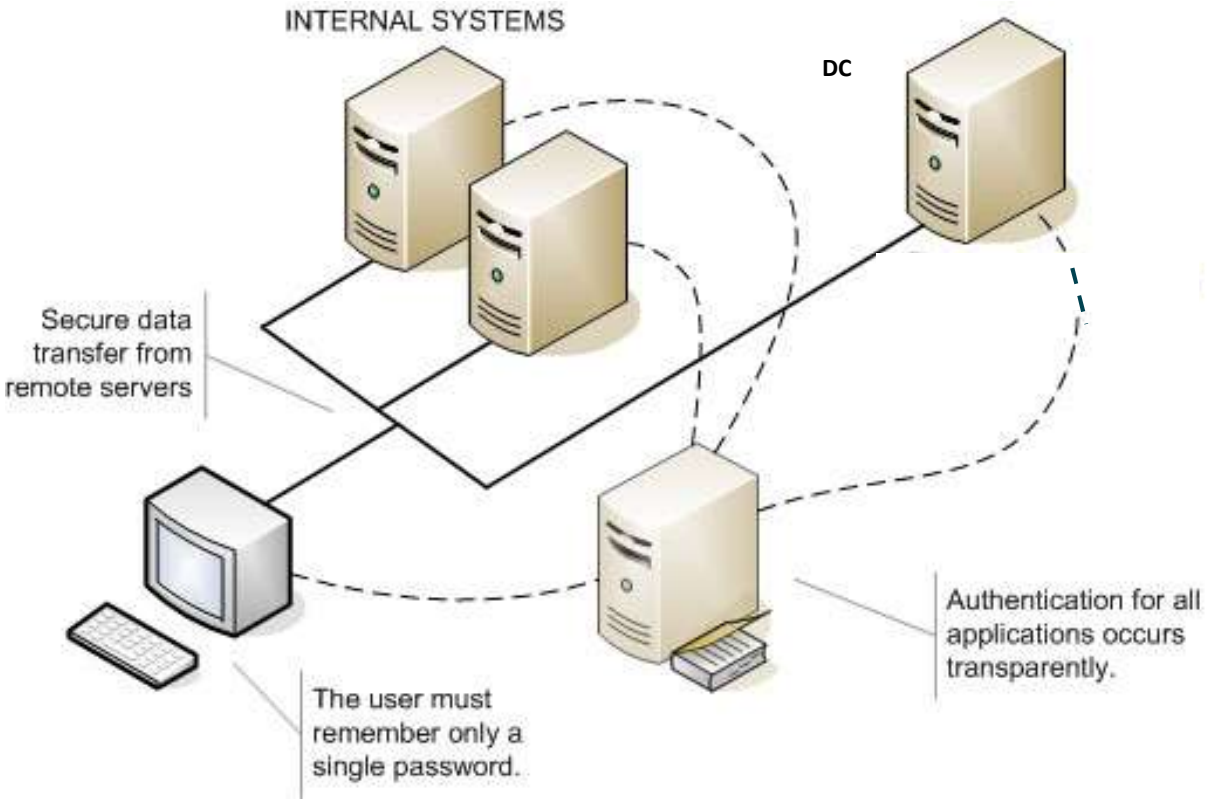
- Centralized Resource and Security Administration
- Single logon for access to network resources
- Fault tolerance and redundancy
- Simplified resource location

Ib Helmer Nielsen
UCN act2learn Erhverv

Centralized Resource and Security Administration

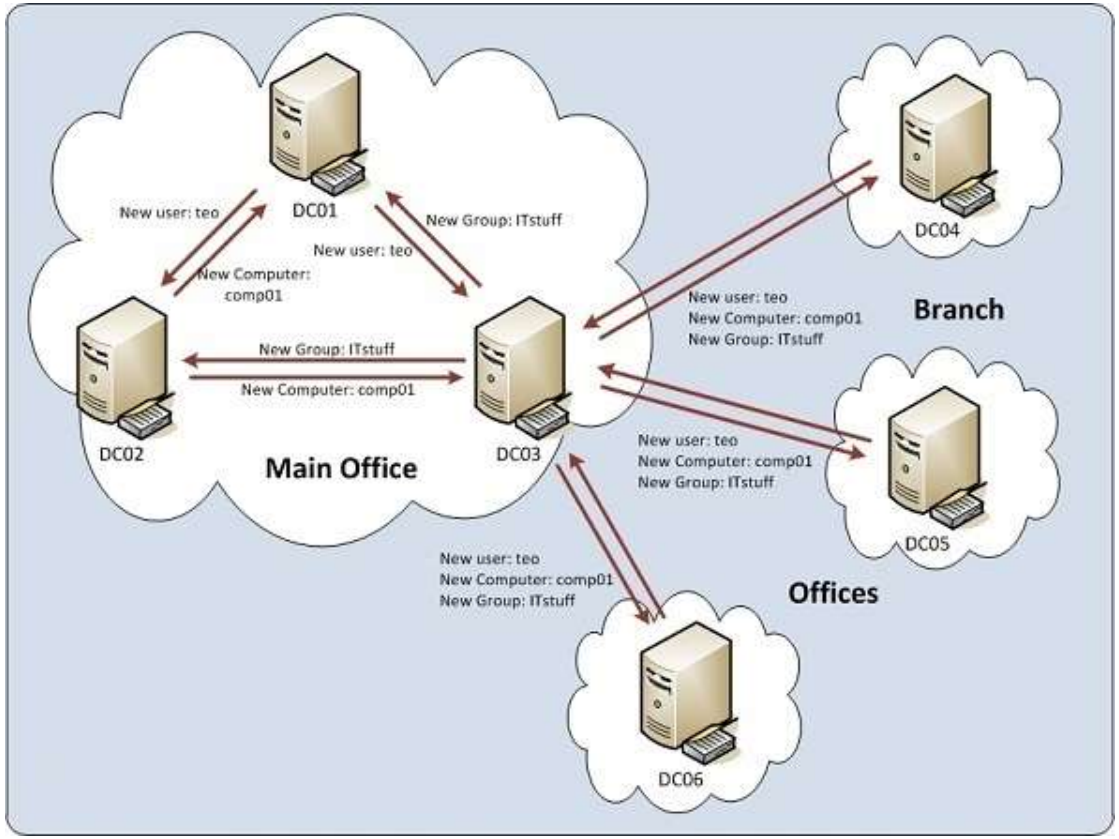


Single Logon for Access to Network Resources

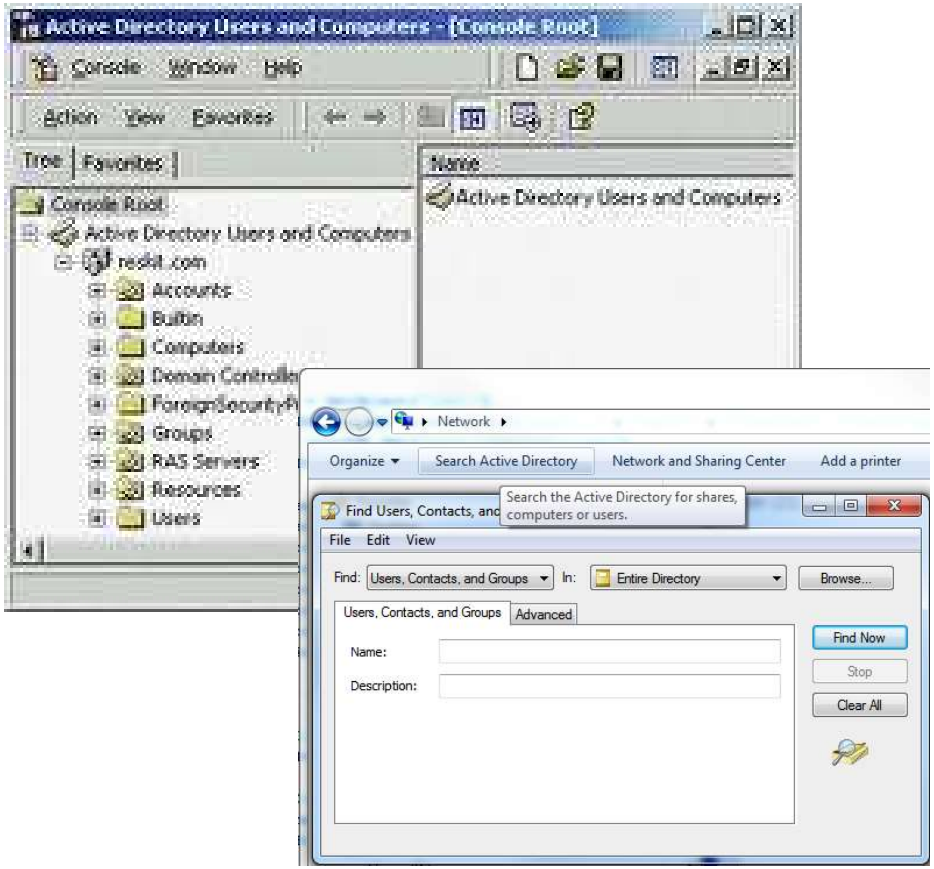


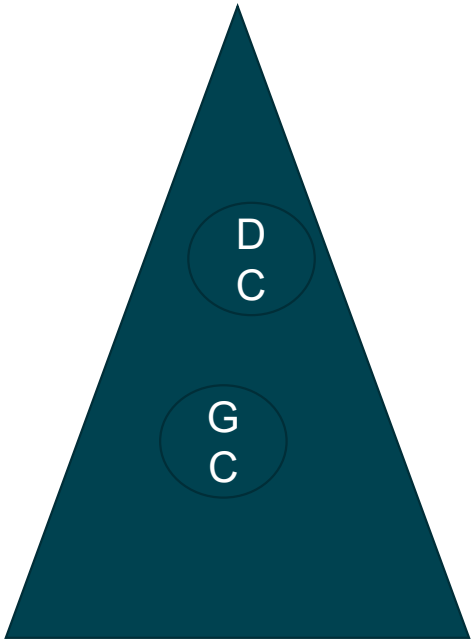
Ib Helmer Nielsen
UCN act2learn Erhverv

Fault Tolerance and Redundancy



Simplified Resource Location





Active Directory DS

Introduktion til AD DS

UCN act2learn

9. juni 2023
Ib Helmer Nielsen
UCN act2learn Erhverv

Active Directory Directory Services

- Microsoft Directory service
- Initially released in 1999
- Originally designed for Windows 2000 Server
  - Enhanced with Windows Server 2008
- Windows Server 2022 types
  - Workgroup model
  - Domain model

Workgroups

- Peer-to-peer network
- Decentralized management
  - Each computer has own database
    - User accounts, security privileges
  - Significantly more administration effort
- Practical for small networks
  - Few users
  - Simple to design, implement

Domains

- Client/server network with a shared database
- Domain - Group of users, servers, and other resources
  - Share centralized account and security information in a database
- Active Directory
  - Contains domain database with objects and attributes and schema
  - Makes it easier to organize and manage resources and security

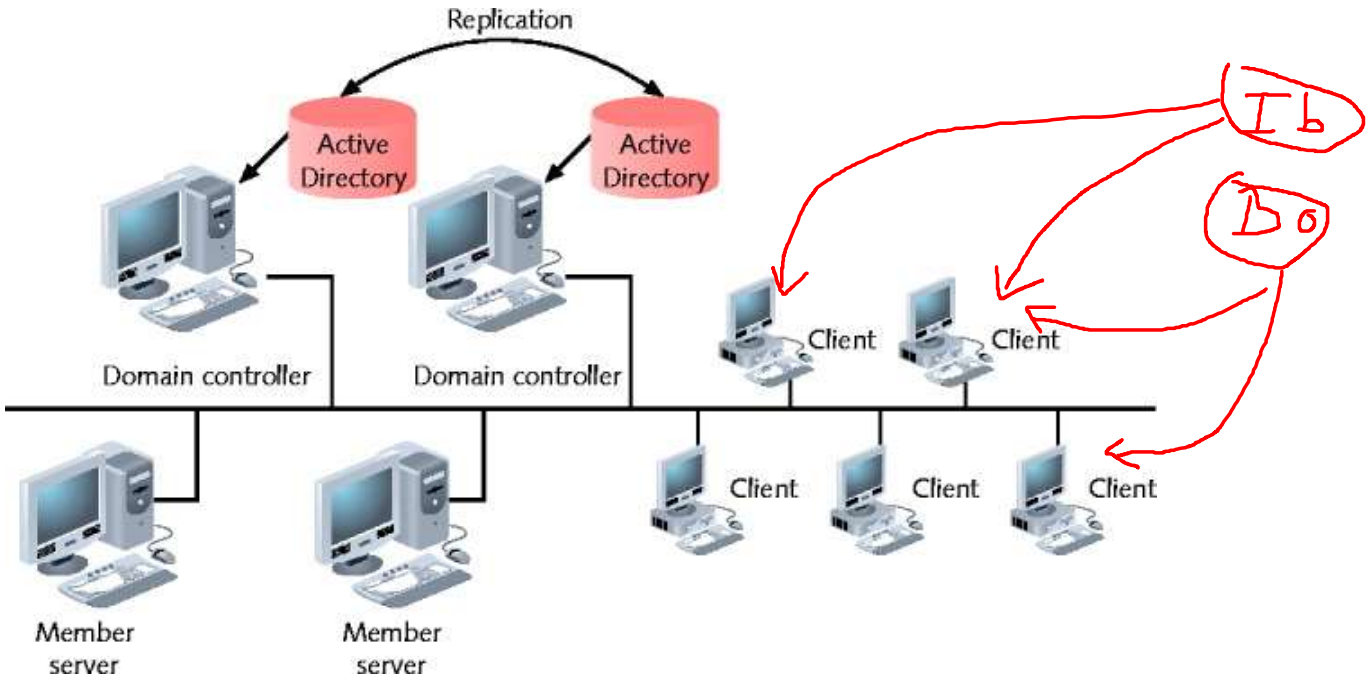
Active Directory - Domains

- Domain not confined by geographical boundaries
- Domain controller servers
  - Contains directory information about objects in a domain
- Member servers
  - Do not store directory information, can’t be used to authenticate users
- Replication
  - Process of copying directory data to multiple domain controllers

Active Directory
Directory Services– Domain Model

- Three main parts
  - Domain
  - Tree
  - Forest

Domains



Domain model on a Windows Server 2022 network

Active Directory

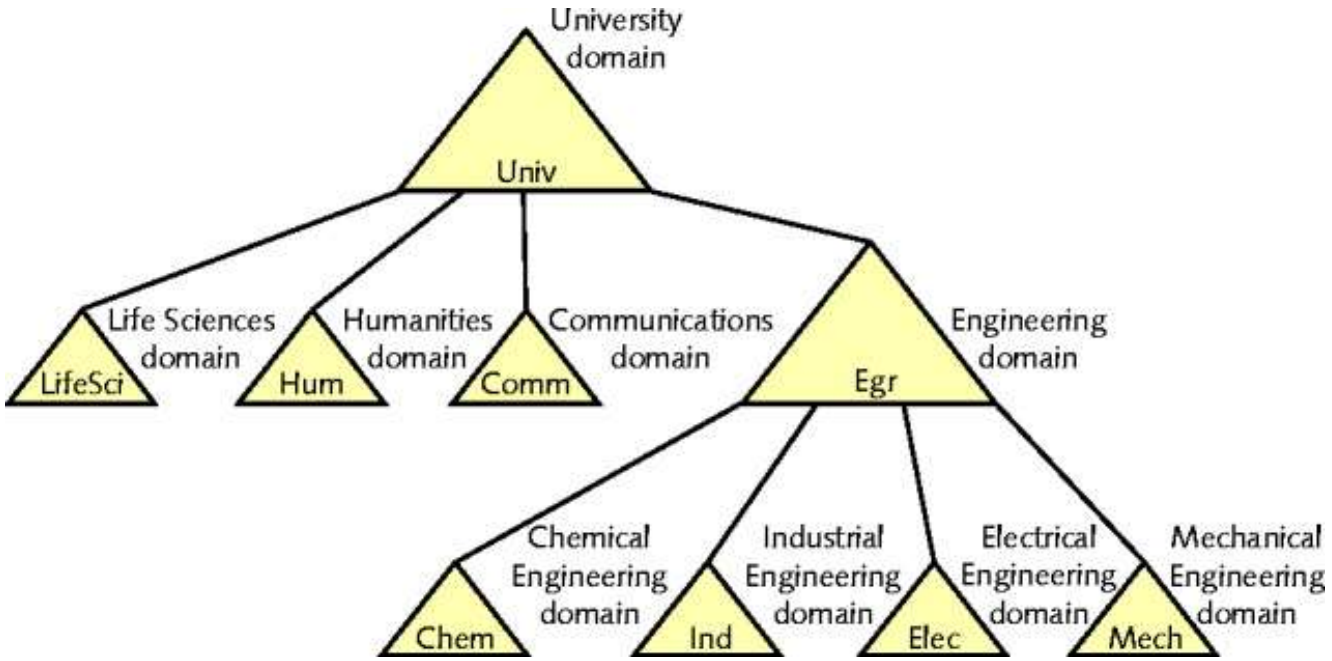
- Objects fall into two broad categories:
  - Resources (e.g., printers)
  - Security principals (user or computer accounts and groups).
    - Security principals are assigned unique security identifiers (SIDs)
    - This is where access rights are given
    - Users must have unique names – flat database

Ib Helmer Nielsen
UCN act2learn Erhverv

OUs (Organizational Units)

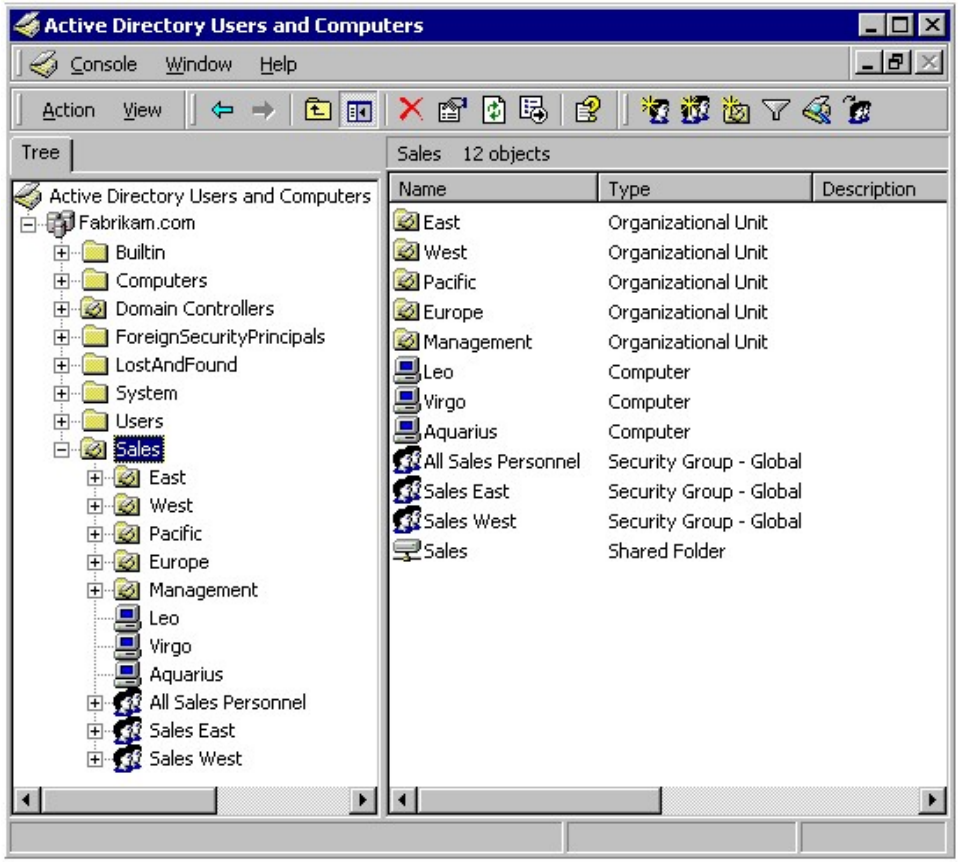
- Hold multiple objects having similar characteristics
  - Can be nested
  - Can contain other OUs or objects
- Provides simpler, more flexible administration
  - Apply policies to OU
  - Do not function as containers
  - Use users or groups for access permissions

Domains



Multiple domains in one organization

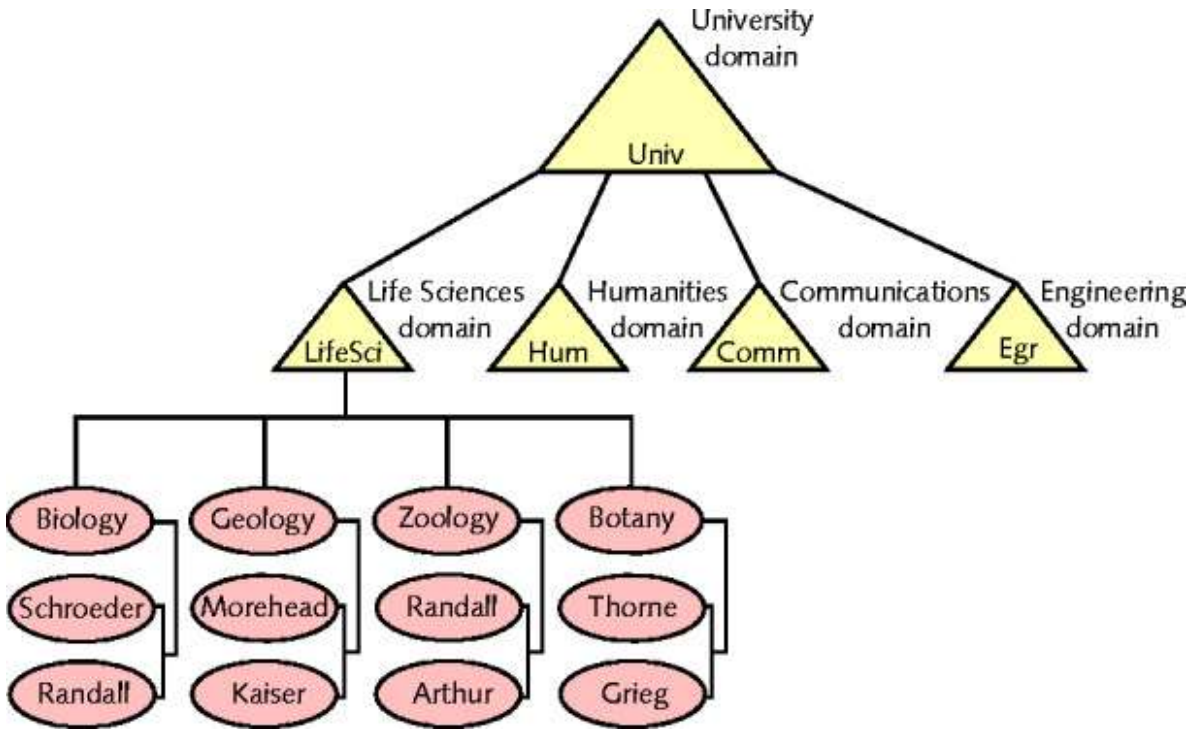
Domains


Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Sales 12 objects
Active Directory Users and Computers
Fabrikam.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
System
Users
Sales
East
West
Pacific
Europe
Management
Leo
Virgo
Aquarius
All Sales Personnel
Sales East
Sales West
Name
Type
Description
East Organizational Unit
West Organizational Unit
Pacific Organizational Unit
Europe Organizational Unit
Management Organizational Unit
Leo Computer
Virgo Computer
Aquarius Computer
All Sales Personnel Security Group - Global
Sales East Security Group - Global
Sales West Security Group - Global
Sales Shared Folder

Trees and Forests

- Directory structure above domains
  - Large organizations use multiple domains
- Domain tree
  - Organizes multiple domains hierarchically
- Root domain
  - Active Directory tree base
- Child domains
  - Branch off from root domain

Trees and Forests

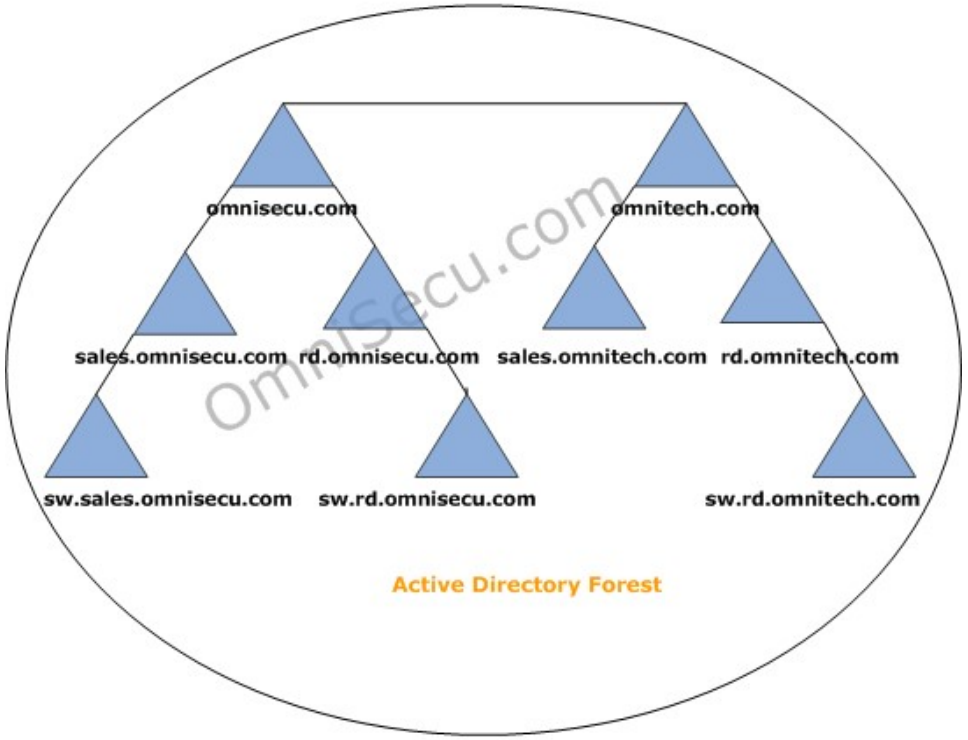


A tree with multiple domains and OUs

Trees and Forests

- Forest
  - A collection of one or more domain trees
  - Trees share common schema
- Domains within a forest can communicate
- Domains within same tree
  - Share common Active Directory database

Two Tree - Forest

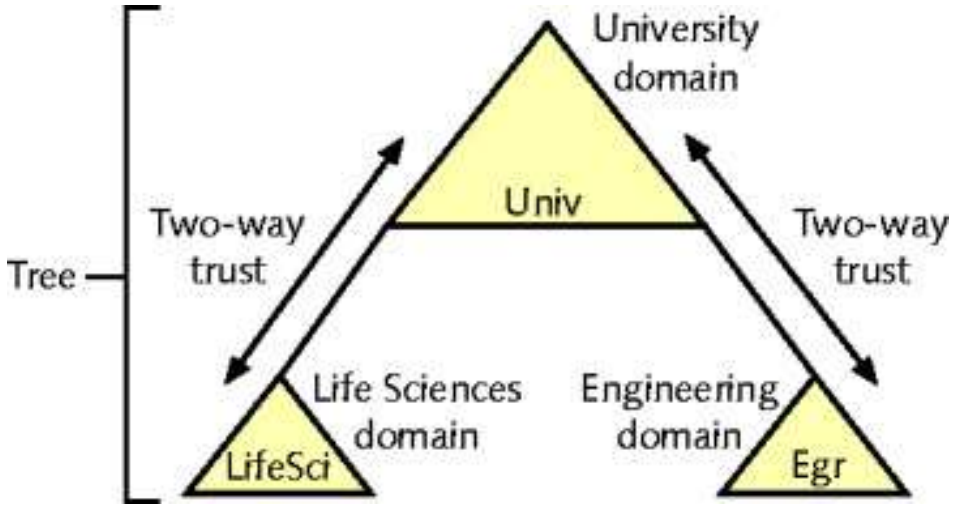


Ib Helmer Nielsen
UCN act2learn Erhverv

Trust Relationships

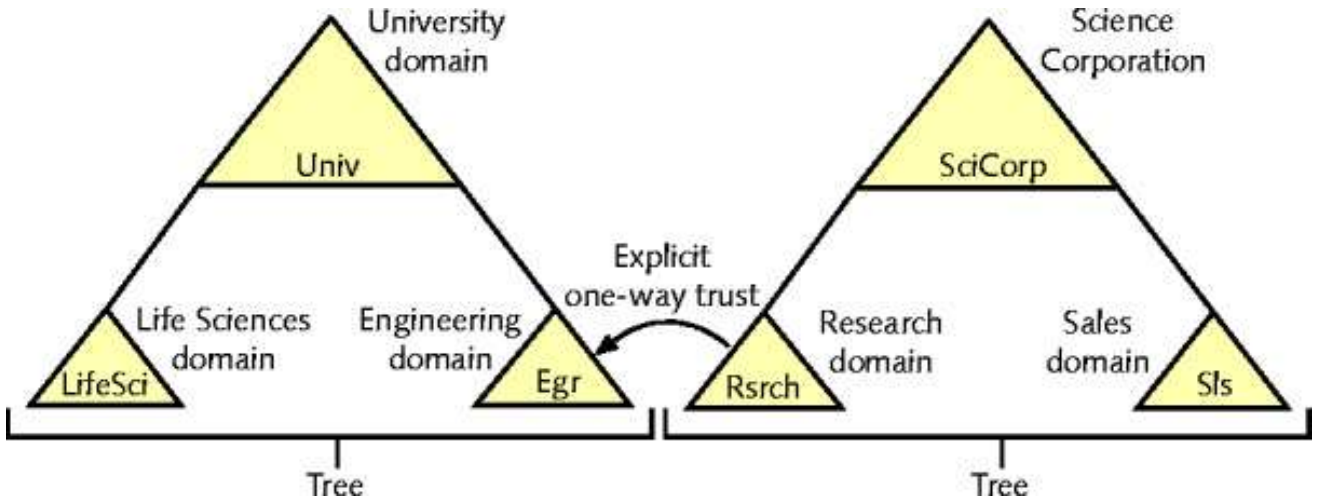
- Relationship between two domains
  - One domain allows another domain to authenticate its users
- Active Directory supports two trust relationship types – allows users to authenticate
  - Two-way transitive trusts
  - Explicit one-way trusts

Trust Relationships



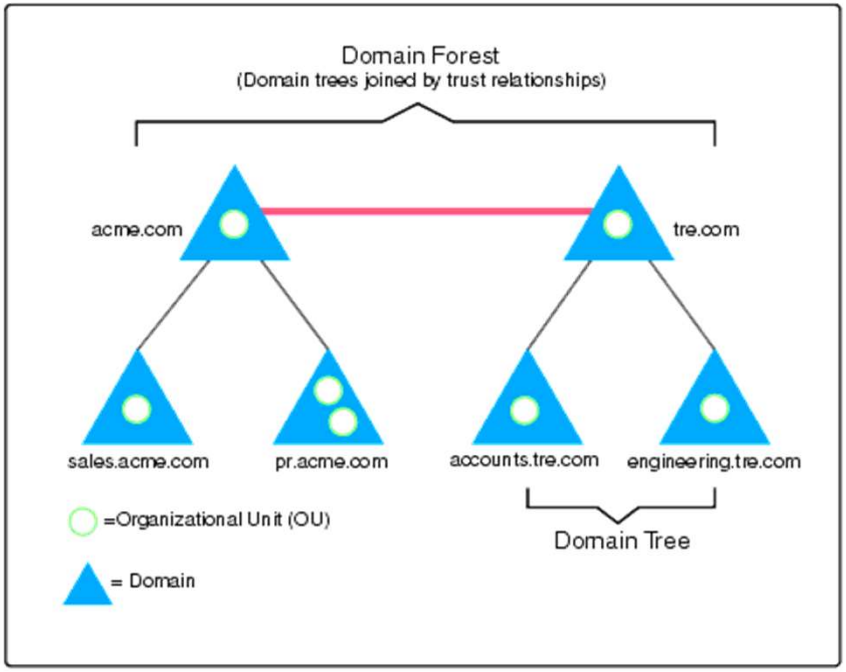
Two-way trusts between domains in a tree

Trust Relationships



Explicit one-way trust between domains in different trees

Trust Relationships



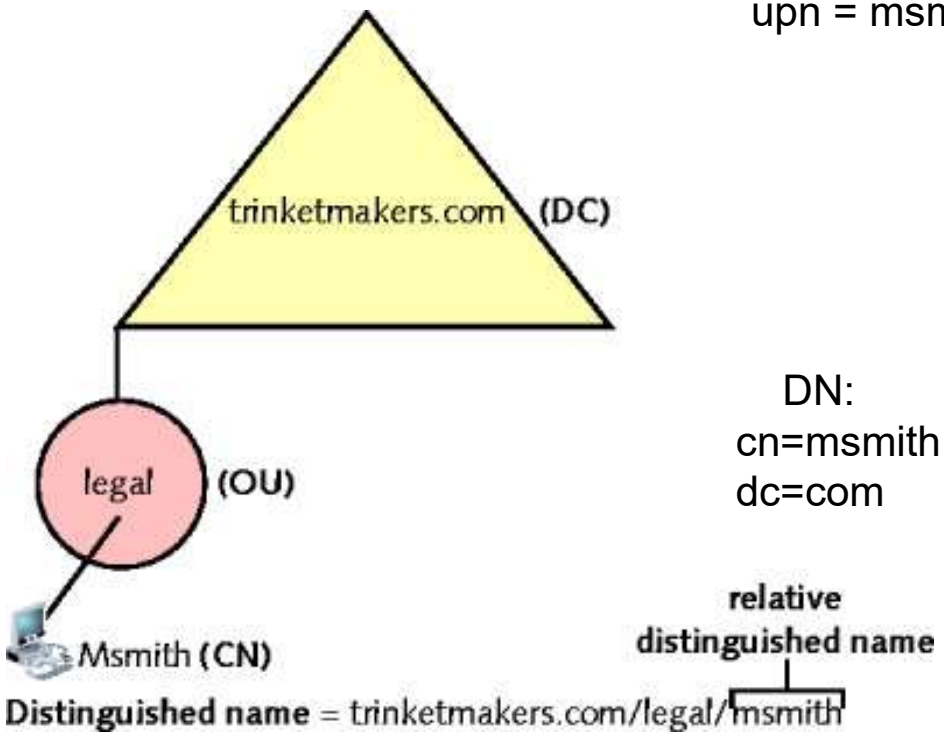
Naming Conventions

- Active Directory naming conventions (namespace)
  - Collection of object names and associated places in Windows Server 2016, Server 2019 network
  - Based on LDAP naming conventions
  - Follows the conventions of the internet namespace
    - Ex. dc=wright, dc=edu
    - Ex. cn=server1,dc=wright,dc=edu
    - Ex. cn=server2,ou=cse,dc=wright,dc=edu

Naming Conventions

- Windows Server 2022 network object
  - Three different names
    - DN (distinguished name): DC (domain component) and CN (common name)
    - RDN (relative distinguished name)
    - UPN (user principal name)
- GUID (globally unique identifier)
  - Each object has one
  - 128-bit number

Naming Conventions



upn = msmith@trinketmakers.com

DN:
cn=msmith,ou=legel,dc=trinketmakers,
dc=com

Distinguished name and relative distinguished name