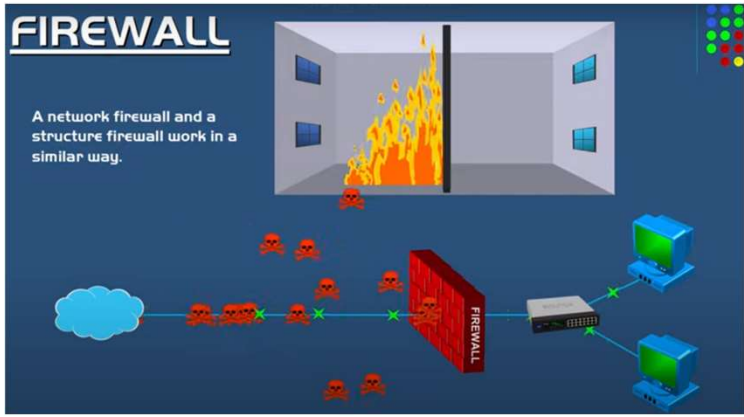
Operativ Systemer 11

Lavet af: Vivek Misra

Firewall

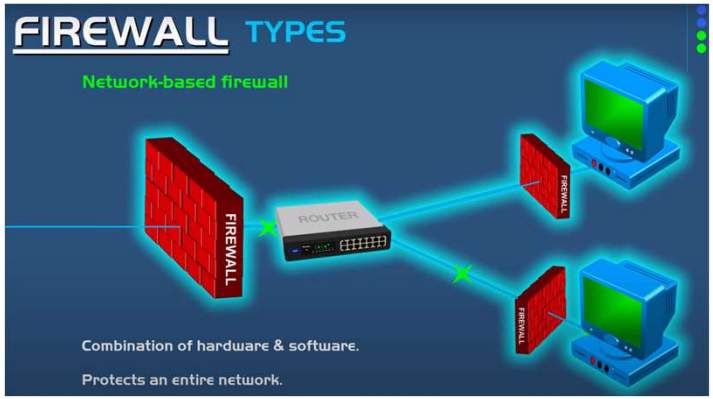
- En Firewall er et system, der forhindrer i at kunne beskytte fremmede adgang der tråder inde i et netværk.
- Dette er muligt ved, at Firewall filtrerer alt information der kommer fra Internettet.
- Derfor er det Firewallens hensigt i at kunne danne sikkerhedsgrænse mellem den lokale netværk og offentlig netværk.
- Firewall er brugt blandt mange virksomheder, især for at beskytte deres computere og data servere imod fremmede invasioner således at dataet ikke bliver væk.
- Begrebet Firewall er egentligt opstået fra et hus-koncept, hvor man opstiller et ”væg” eller et ”wall” som egentligt skal beskytte den ene del af huset hvis den anden del bliver flammeret med ild.
  - På denne måde sprede ilden ikke på den anden side.
- OBS: **Access Control List bestemmer er grænsevagten for, hvad der må passere / forlade igennem Firewall og ind i det lokale Netværk.**

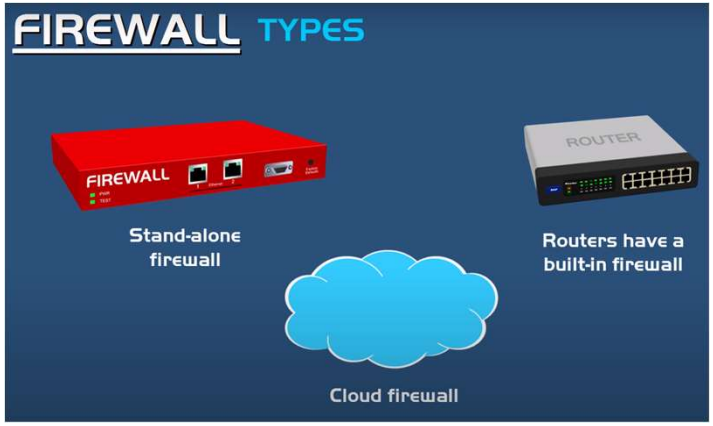


Permission	IP Address	Protocol	Destination	Port
ALLOW	162.213.214.140	TCP	ANY	80
ALLOW	54.21.66.112	TCP	ANY	80
DENY	40.55.130.66	TCP	ANY	80

Firewall Typer

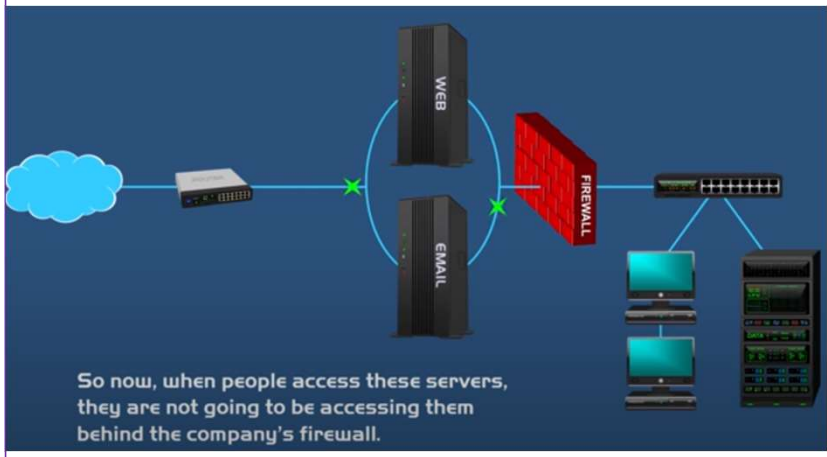
- Vi kan se, at der er forskellige Typer af Firewall som kan opsættes.
- Vi har Host-Based Firewall som egentligt skal beskytte Computeren mod Fremmede Invasioner.
- Så har vi Network-Based Firewall, hvor det kan ses at det er en kombination af Hardware og Software som egentligt ligger mellem den lokale netværk og offentlig netværk. Den beskytter det lokale Netværk.
- Det kan ses, at vi har flere typer af Firewall.
- Stand Alone Firewall er en Hardware som kan opsættes i forbindelse med beskytte Netværket.
- Routers har også indbygget feature som kan beskytte imod fremmede invasioner. PS: Mange virksomheder benytter sig af Router-Firewallen.
- Cloud Firewall er den firewall som beskytter alle dataene der beligger sig i skyen.



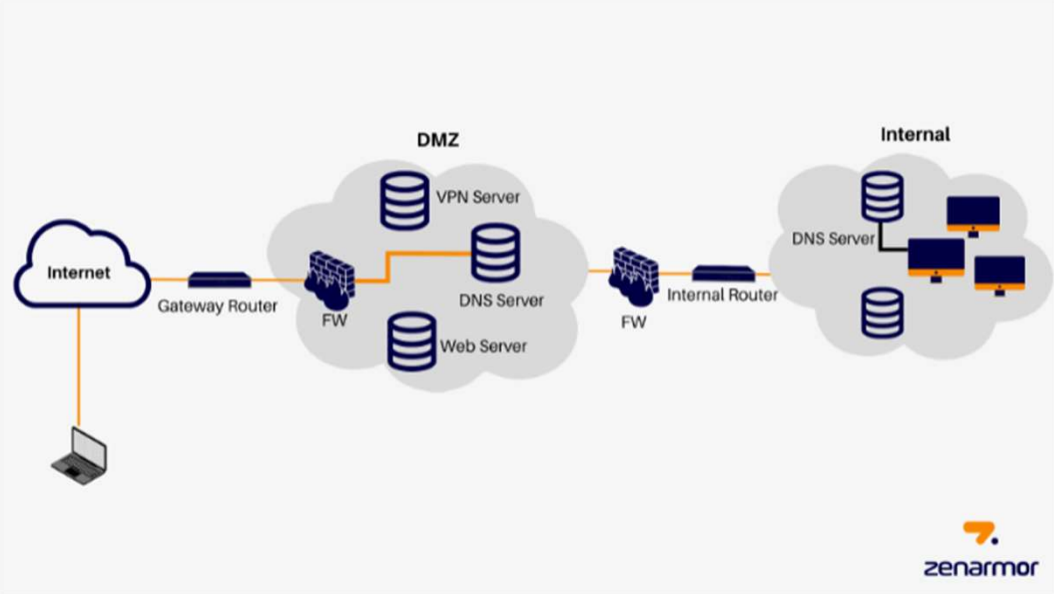


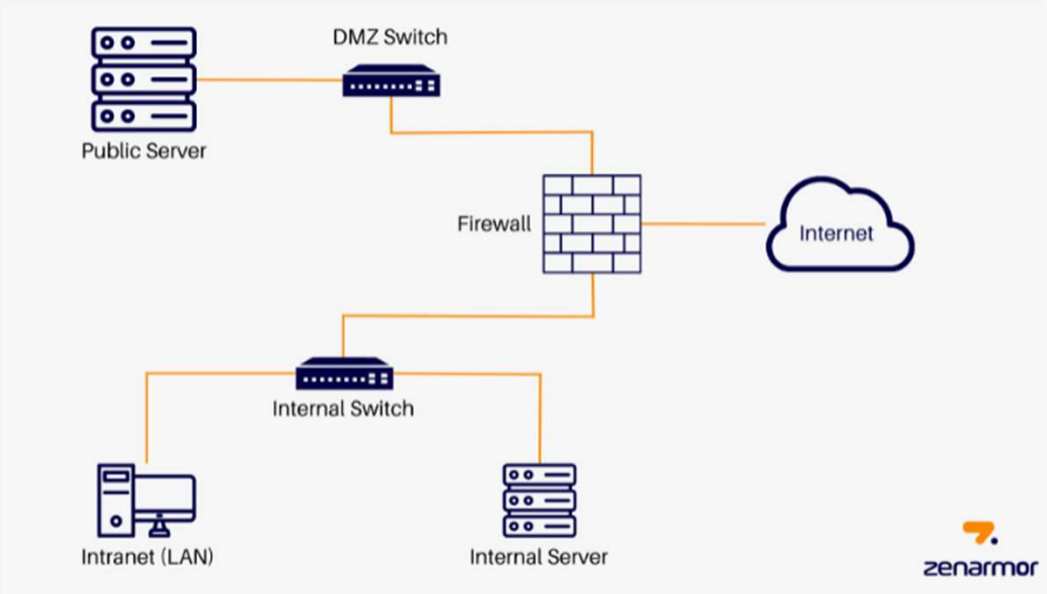
DMZ – Demilitariseret Zone

- DMZ er brugt til at forbedre sikkerheden for en Virksomheds Netværk.
- Det man forsøger, at gøre er at man opdeler Enheder således at computere og server befinder sig på hver af deres side af firewall.
- Man kan sige, at en DMZ opdeler netværket i 2 dele som er ved at tage Devices fra inden i Firewall og putte dem udenfor Firewall.
- Man kan opfatte DMZ som en grænse mellem to lande, eller ingenmandsland. Her kommer der forskellige smugler over grænsen, men bliver opfanget af Firewall (Border Security Force) og derefter taget i Custody.
- Nogengange findes Firewall på den ene side, og nogen gange på begge sider. Men når det er begge sider, så er det kun filtreret data som kører igennem det demilitariserede zone og derefter krydser igennem Firewallen.
- Man kan sige, at Demilitariseret Zone er der, hvor Firewall er ikke tilladt ligesom at militæret er ikke tilladt at befinde sig i ”ingenmandsland”.



DMZ – Demilitariseret Zone



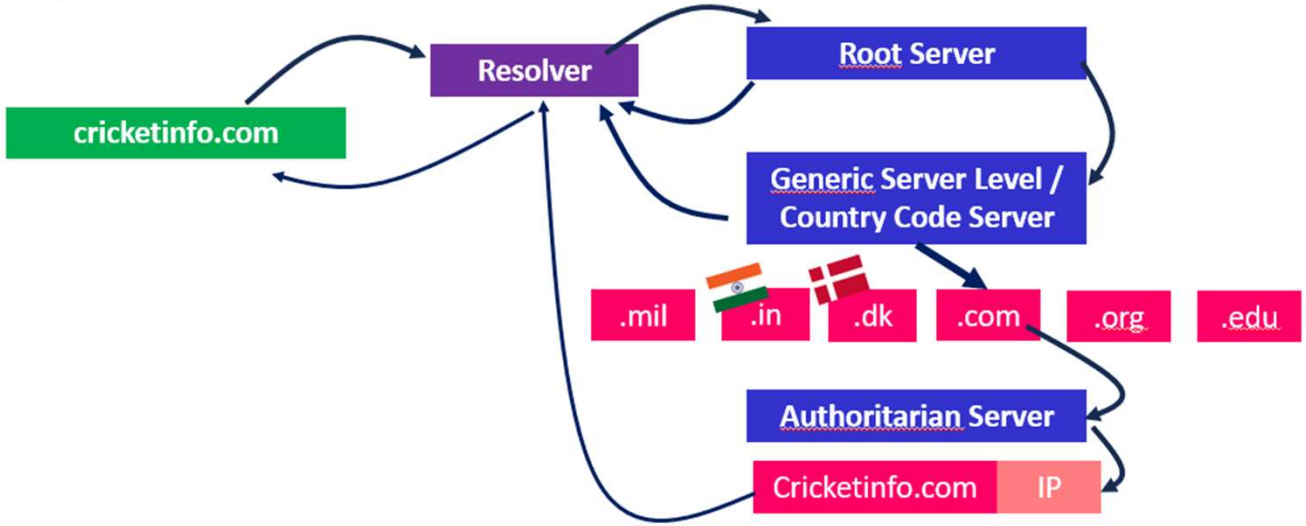


Repetition af Korte-Netværker

Vi kommer til at gennemgå kort af hvad de forskellige koncepter er. Eksempelvis DNS, HTTP(S), SSL og TLS.

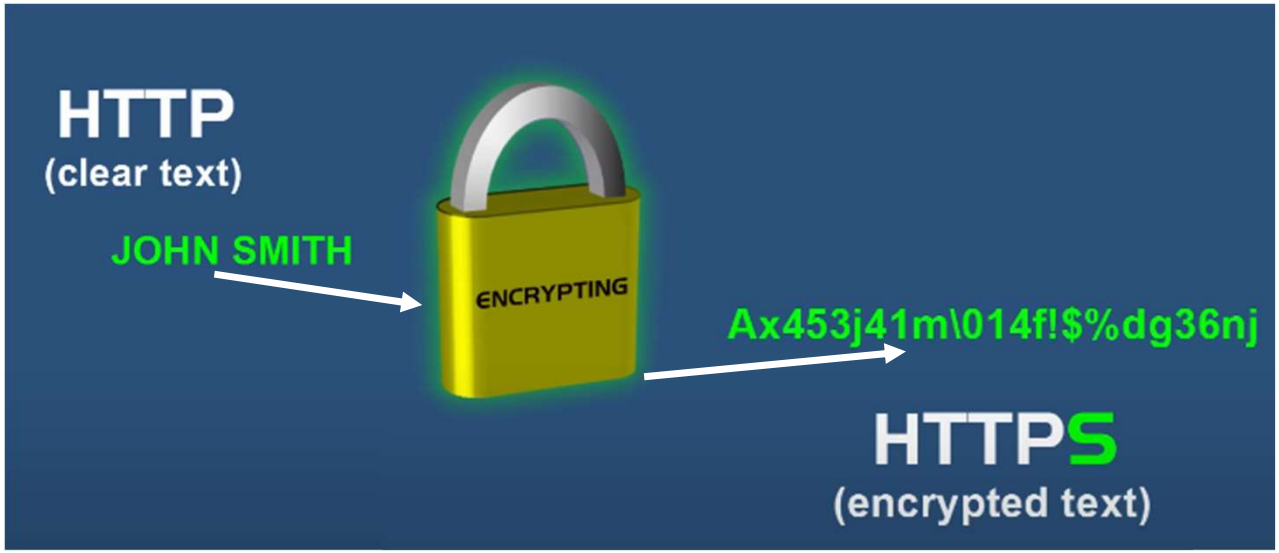
DNS – Domain Name Server

- Domain Name Server er der, hvor vi domæne navne sluttede med TLDs har allokkeret et specifik ip-adresse således at de kan findes.
- Det kan ses, at vi starter med at have en webside som sender en Request til Resolveren. Her kan det ses, at Resolveren sender en bekræftelse tilbage og siger at den sender det videre til Root Serveren.
- Når Root-Serveren modtager anmodningen, så sender den bekræftelsen igen og derefter sender den Request videre til Country Code, således at vi kan udvælge hvilket Domæne Server det tilhører under.
- Når dette er sket, bliver det sendt videre til den Autoritære Server som udgiver os en fikst ip-adresse og dermed sender det tilbage til Resolveren (Vores Advokat) og giver det videre til Webside Domæne Navnet.



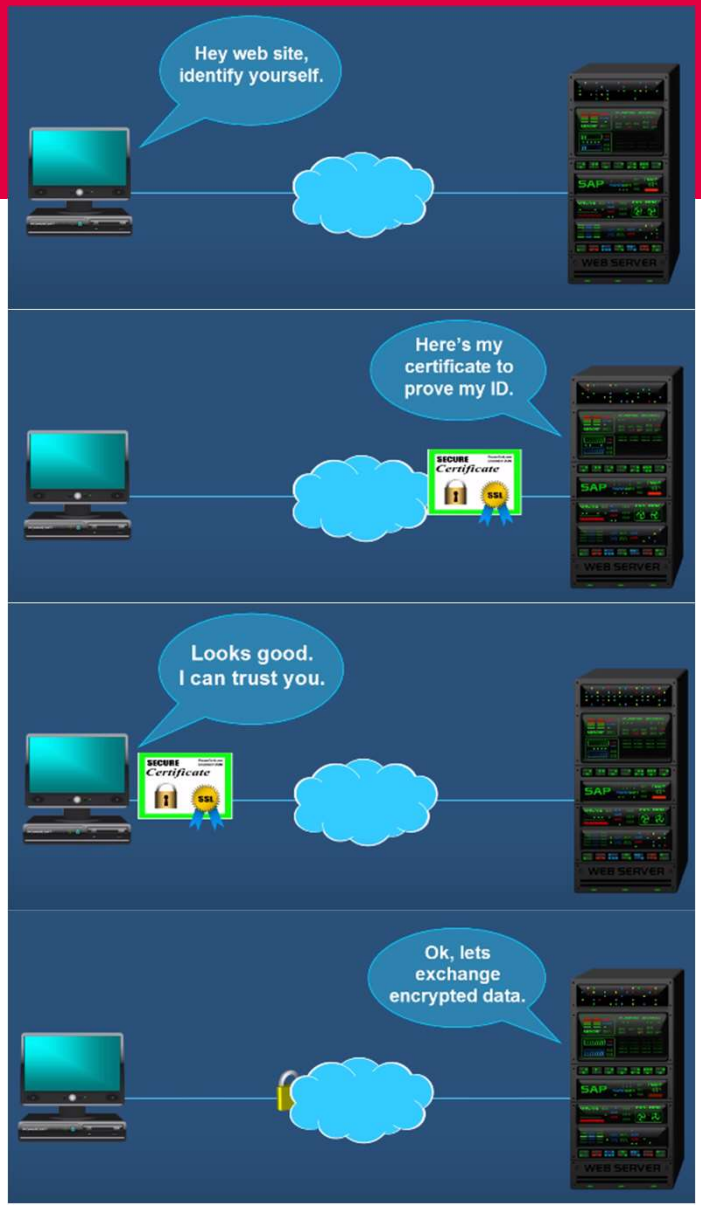
HTTPS – Secure Hypertext Transfer Protocol

- HTTPS betyder egentligt, at det data som vi sender i form af tydeligt tekst (HTTP) er enkrypteret til en utydeligt tekst med blandet bogstaver som ingen kan forstå.
  - Eksempelvis kan vi se, at vi sender John Smith fra HTTP, hvilket er et klart tekst.
  - Men når beskeden bliver enkrypteret, så resulterer det at vi har en mærkelig tekst som vi ikke kan forstå.
  - Denne besked siges for at være konverteret om til HTTPS, hvilket gør den sikkert.
  - Kig venligst på billedet nedenfor, så man kan få bedre overblik:



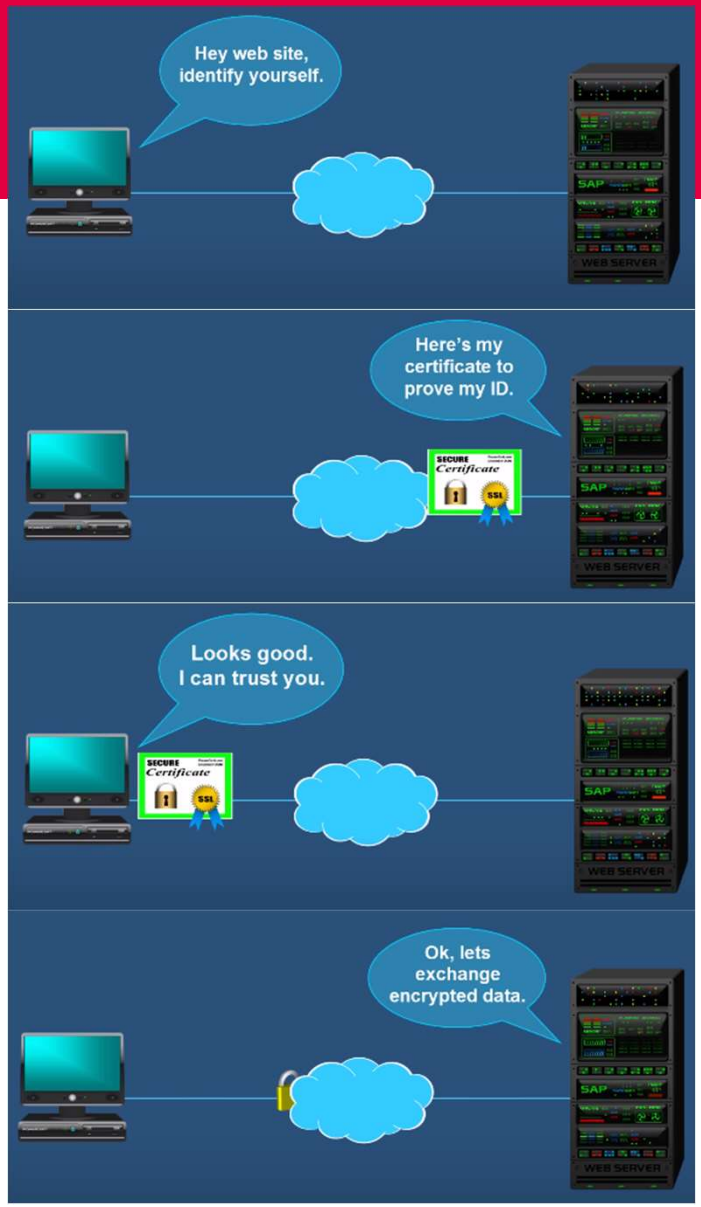
SSL – Secure Sockets Layer

- Secure Sockets Layer er en Protokol brugt af HTTP.
- SSL sørger for, at der er sikkerhed i Internettet gennem brug af Public Key Encryption, der gør det muligt at sikre data.
- Vi kan se, at når en computer forbinder sig til en webside gennem brug af SSL. Så vil computerens webbrowser spørge websiden om at identificere sig, hvor websiden sender en kopi af dens SSL-certifikat der bekræfter websidens identitet ift. Sikkerhed og Troværdighed.
- Computerens Browser vil tjekke certifikatet igennem og efterfølgende sende en besked til Webserveren. Webserveren vil sende en godkendelse tilbage, hvor kommunikation kan fortsættes.
- Dette betyder, at vores data sendes videre i form af enkrypteret data, således at der er en sikker dataoverførsel.



TLS – Transport Layer Security

- Transport Layer Security er også en Protokol brugt af HTTP.
- TLS er den seneste industri-standard og er ligesom SSL istand til at sikre dataoverførsel gennem Enkryption.
- Det skal bemærkes, at TLS er efterkommer af SSL.
- Dog er TLS den forbedre version af SSL, eftersom der blev opdaget nogle svage punkter ved SSL som kunne være sikkerhedstruende for computernetværket.
- Men ellers har begge Sikkerhedslager, den samme anlagte procedure at overføre data på.
- Man plejer, at kalde TLS for TLS1.0 da det er den seneste forbedre version ift. Kompatibilitet og algoritmer.



Enkryption

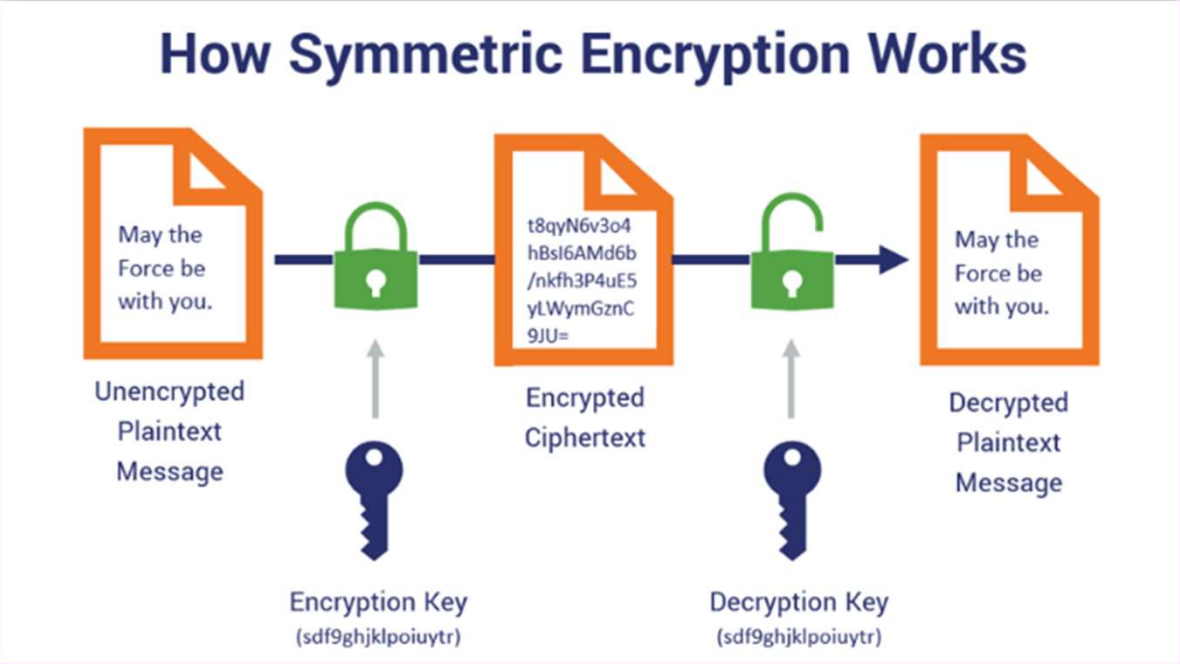
Nu kommer vi til at gennemgå Symmetrisk og Asymmetrisk Kryption.

Introduktion til Enkryption

- Inden vi går videre og snakker om begreberne Asymmetrisk Enkryption og Symmetrisk Kryption, så er det nødvendigt at kende til begrebet ”Enkryption”.
- Vi kan se, at Enkryption er der, hvor man på den anden hånd referer til den aktuelle proces af at enkryptere plænetekst data ind til uforståeligt ciphertekst.
- Enkryption er sammensat af to vigtige elementer:
  - Algoritmer: Dette er en enkryptions algoritmer som er en sæt af retninger der kan hjælpe med at løse en prolem. Mere specifikt, så er det en sæt af matematiske instruktioner og processer som udfører et specifik arbejde. Nogle algoritmer er dannet til at kunne arbejde i enten private eller offentlige kanaler.
  - Keys: Det er en kryptografisk nøgle, der kan opfattes som en lang og uforståelig lang af karakterer og tal som er brugt til at enkryptere og dekryptere data. Uanset hvad, om du snakker om asymmetrisk eller symmetrisk enkryption, så er nøglerne vigtige at beskytte for dataets sikkerhed!

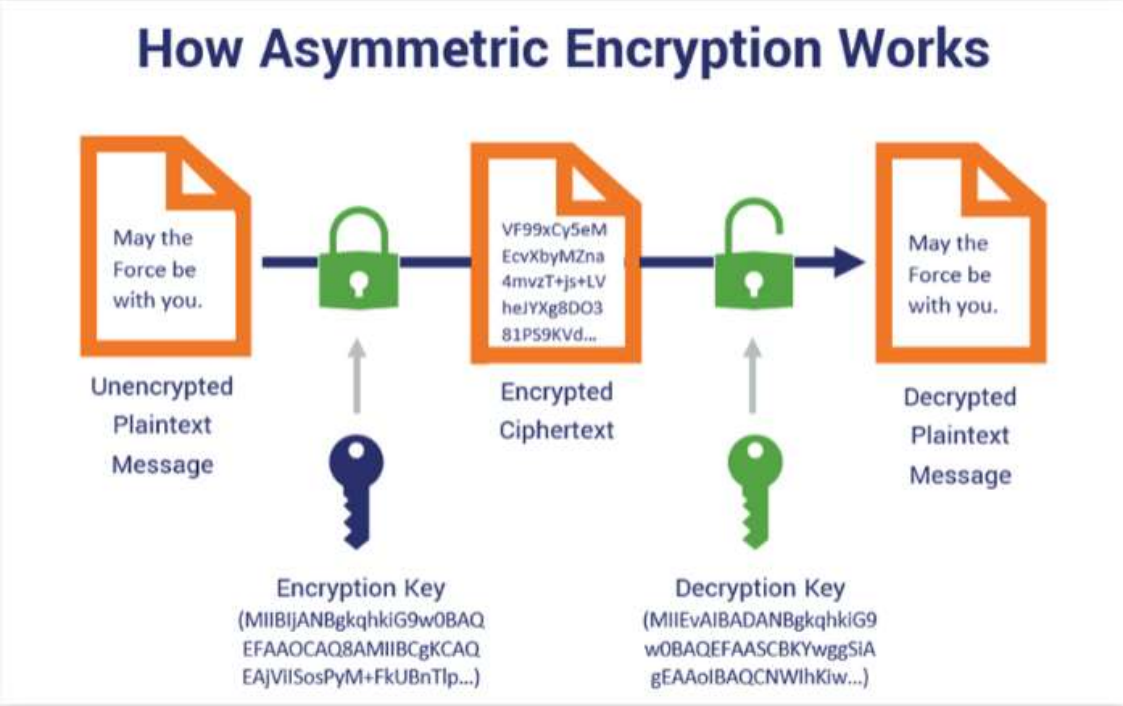
Symmetrisk Enkryption

- Set på billedet nedenfor, kan det ses at man har to parter (afsender og modtager forhold).
- Vi kan se, at i Symmetrisk Kryption er der, hvor man bruger kun en nøgler til at åbne og låse den besked som afsendes.



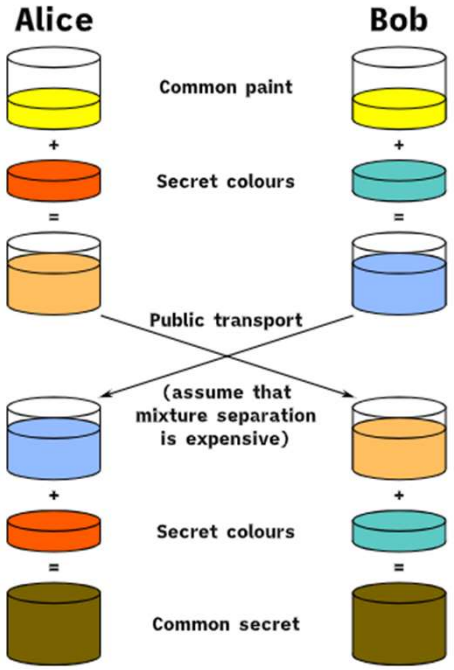
Asymmetrisk Enkryption

- Set på billedet nedenfor, kan det ses at man har to parter (afsender og modtager forhold).
- Vi kan se, at i Asymmetrisk Kryption er der, hvor det kan ses at man har to nøgler.
- Den ene nøgler er Enkryptions Nøglen som afsender har, når et besked skal enkrypteres.
- Den anden nøgle er Dekryptions Nøglen, som modtageren har, når et besked skal dekrypteres.



Diffie Hellmans Princip

- Diffie Hellmans princip går ud på, at danne en kommunikation således at man kan blive undgået at blive opdaget.
- Man kan teknisk set antage det som en ”tegnesprog” princip, hvor man snakker med hinanden men den tredje part som er ”fremmede” forstår ikke hvad der egentligt foregår.
- For, at inddrage en eksempel kan det ses at vi har Alice og Bob.
  - Alice og Bob vil gerne snakker med hinanden. De ønsker, at sende orange og turkis-blå til hinanden.
  - Det som sker er, at de blander noget kemikalie og sender det offentligt over til hinanden.
  - Når de filtrer farven, eller anvender en kemikalie der kan neutralisere farverne så ender vi med at have farverne på den modsatte ende af parterne.
  - På den måde deler Alice en hemmelighed, at Bob har farven Turkis-blå. Og Bob deler en hemmelighed, som er at Alice har farven Orange.



Integrity through Signing

- Det kan ses, at når vi snakker om Integritet gennem Signing, så handler det primært og integritet og autentitet af data gennem digital signatur.
- Gennem digital signatur, accepteret vi gennem kryptografiske mekanismer at vi bekræfter en besked eller en stykke af data som ikke har været ændret og at det kommer fra den oprindelige afsender.
- Hashing af Data: Inden vi laver digital signatur, så bliver der brugt en secure-hashed algoritme som producere en længde af karakter, der repræsenterer den oprindelige data.
- Creating a Digital Signature: Når vi underskriver på data, så er den digitale signatur genereret ved brug af privat nøgle passende til public-private key. Public key kan være delt med alle, men private key afholdes ved afsenderen.
- Attaching the signature: Den digitale signatur er vedhæftet eller associeret sammen med dataet, når det bliver underskrevet. EKS: Nogle karakter af dataet kan indikere signaturen.
- Verifikation: Denne bekræfter integritet og authencitet af dataet, hvilket betyder at personen som har dekrypteringsnøglen kan åbne den digitale signatur. Vi kan hermed se den oprindelige data.

Integrity through Signing

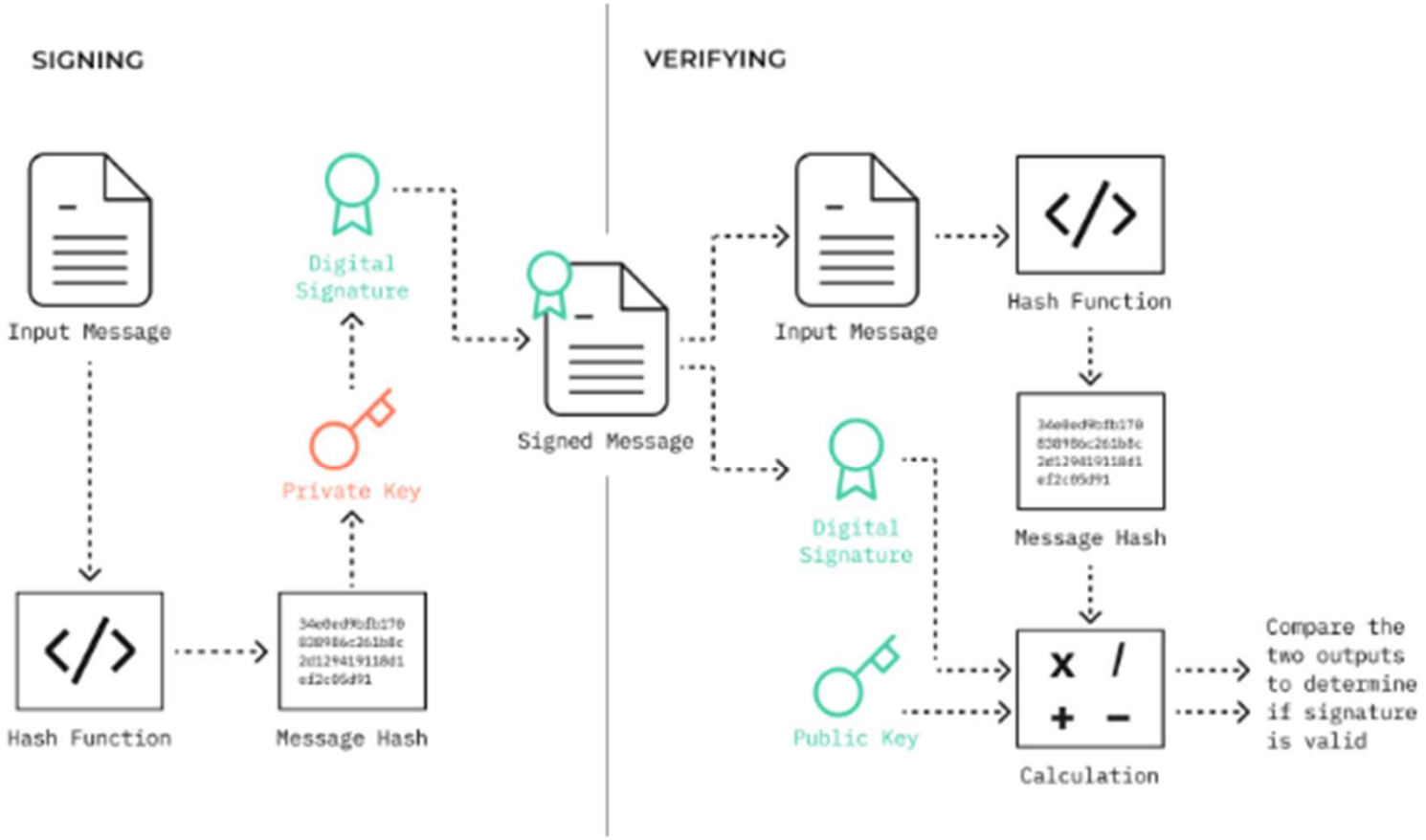


Figure: © stu

Ensure Trust

- I Operativ Systemer, så handler ”Ensure Trust” konceptet generelt om principperne som referer til øvelserne implementeret til at kunne etablere og holde styr på Sikkerheden, Reliabiliteten og Integritet af systemet.
- Autentikation og Adgangskontrol: Operativ Systemer implementere autentikations mekanismer til at verificere identitet af brugere og entiteter som forsøger at få adgang til systemet.
- Secure Boot: Det er en proces som sørger for, at kun de troværdige og verificerede software komponenter er lagret gennem systemet startup. Dette forhindrer i at lagre uautoriserede eller farlige software boot.
- Enkryption & Datasikkerhed: Operativ Systemer inkludere enkryptions mekanismer til at sikre data gemt i diske og lign. Det betyder, at hvis der nogen som får adgang til dataet uden dekryptionsnøglen, så kan de stadig ikke se dataet.
- Secure Communication: Her etableres sikker kommunikation gennem forskellige komponenter og devices, eller netværker. Protokoller som SSL og TLS er brugt her.
- Digital Signatur og Verificering: Det er her, hvor man har signaturerne som beviser at der ikke er sket ændringer ved dataet.
- Malware Protection: Det sørger fir, at danne tillid i operativ systemet således at der implementeres antivirus programmer.

Ensure Trust og Provisioning

- I Operativ Systemer, så handler ”Ensure Trust” konceptet generelt om principperne som referer til øvelserne implementeret til at kunne etablere og holde styr på Sikkerheden, Reliabiliteten og Integritet af systemet.
- Regular Updates og Patching: Det sørger for, at vi har healthcheck på. Det fortæller, om sikkerhedssystemet er up-to-date form. Hvis der er fejl, så bliver de fikset med det samme.
- Monitorering og Auditing: Her holder man styr på ligesom med en CCTV-Kamera, at der ikke sker noget unormalt i systemet således at der ikke sker problemer efterfølgende.
- **Provisioning er der, hvor man opsætter infrastrukturen af ressourcer.**
  - **Det betyder, at vi opsætter servere, netværker og brugere som kan køres automatisk og ændres ved.**

WoL og MaaS

- Vi kan se, at vi har WoL som er en protokol der vågner computerens netværk interface controlleren.
  - Det betyder, at hvis der kommer en særlig pakke, og systemet sover. Så vil systemet automatisk opvågne for at modtage den særlige pakke.
  - Et eksempel på dette kan være vores Magic Packet, hvor det kan ses at NIC signaler bliver tændte.

- MaaS står for Metal as a Service som handler egentligt håndtering af fysiske server eller computerende infrastruktur i cloud-opførende måde.
  - Hensigten er bare primært, at kunne udnytte de fysiske hardware på en mere fleksibelt måde.
  - Cloud-Like Management: Det viser, hvordan Cloud Services tillader brugere at kunne nemt håndtere og allokere virtuelle ressource gennem Software.
  - Automatisering og Provisionering: IT administratorer er tilladt at automatisere deployment af hardware servere gennem software.
  - Ressource Allocation: Det handler om bare kunne balancere arbejdsbyrden, ved at dynamisk allokkere arbejde over på en anden fysisk hardware.
  - Flexibilitet: Det tillader mere fleksible og skalerbare infrastruktur management som gør at man kan deployere hurtigere.

Terraform og Ansible

- Terraform er en værktøj som bruges til at automatisere infrasturktur ved at håndtere og provisionere forskellige typer af infrastruktur ressourcer i en deklarativ måde.
- Ansible er en open-source automatiseringsværktøj som simplificere management, konfiguration og orchestration af IT-infrastruktur. Teknisk set ligesom Kubernetes så er den i stand til at automatisere ting som deployment og lignende.

SLUT 11

Lavet af: Vivek Misra