Welcome to

Network Security Basics

Learn to defend your organisation

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

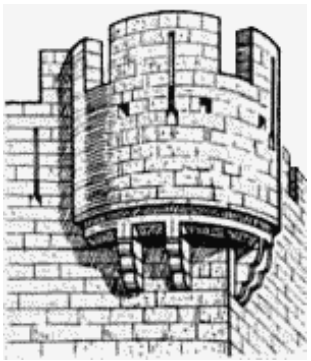
network-security-basics.tex in the repo security-courses

Contact information

- Henrik Kramselund Jereminsen, internet samurai mostly networks and infosec
- Independent network and security consultant
- Master from the Computer Science Department at the University of Copenhagen, DIKU
- Email: hkj@zencurity.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Goals: Network Security Basics



My overall goal

- Introduce networking and related security issues
- Introduce resources, programs, people, authors, documents, sites that further your exploration into network security

Plan for today

A blue-team introduction to Communication and Network Security

- Challenges in network security
- The basic tools for countering threats
- Introduce the encryption protocols in use in networks
  Virtual Private Network (VPN) and Transport Layer Services (TLS).
- Network segmentation will be discussed
- How tools like Firewalls, Access Control Lists (ACL) and VLANs can help reduce risk for the network.
- Examples from Zeek Security Monitor for getting information about flows

Duration: 4 hours - with breaks

Keywords: Encryption, TLS, VPN, VLAN IEEE 802.1q, Wifi security, IEEE 802.1x, IKE version 2, IPsec

Time schedule

- 17:00 - 18:15
  Introduction and basics
- 30min break
- 18:45 - 19:30 45min
- 15min break
- 19:45 - 21:00
  break somewhere

About equipment and exercises

- Bringing a laptop is not required, but welcome.
- Exercises booklet will be referenced, but it is expected that participants will do exercises on their own later or at the scheduled hacker days
- The hacker days will be announced in the event calendar and also take place during BornHack in the network warrior village

Next Hacker day October 31st, at HK 10:00 - 17:00!

Course Materials

This material is in multiple parts:

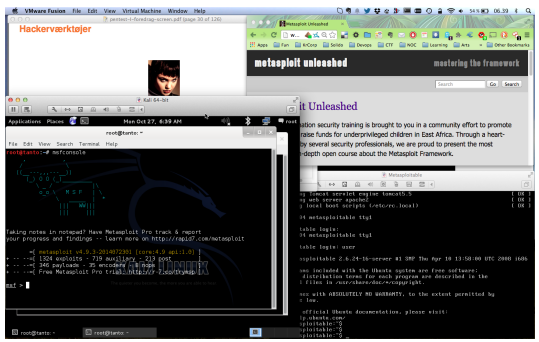
- Slide shows - presentation - this file
- Exercises - PDF which is updated along the way

Links

- All materials will be released as open source at:
  https://github.com/kramse/security-courses/
- Additional resources from the internet linked from lecture plans:
  `https://zencurity.gitbook.io/kea-it-sikkerhed/`
- Note: the presentation slides are not a substitute for reading the books, papers and doing exercises, many details are not shown

Note: slides and materials will be in english, but presentation language will be danish

Hackerlab Setup



- Hardware: modern laptop CPU with virtualisation
  Dont forget to enable hardware virtualisation in the BIOS
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine `https://www.kali.org/`

Networking Hardware

If you want to do exercises, sniffing data it
will be an advantage to have a wireless USB network card.

- The following are two recommended models:
- TP-link TL-WN722N hardware version 2.0 cheap
- Alfa AWUS036ACH 2.4GHz + 5GHz Dual-Band and high performing
- Often you need to compile drivers yourself, and research a bit
- Get an USB 3.0 1Gbit Ethernet too

Getting an USB card allows you to use the regular one for the main OS, and insert the USB into the virtual machine

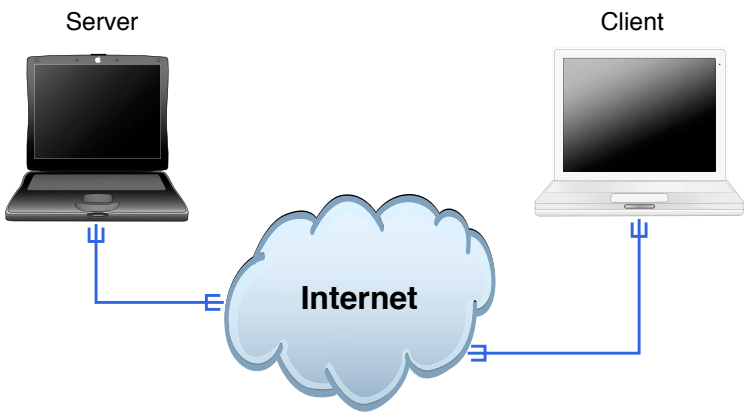
Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: `http://www.stophacking.dk` lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!

Internet Today



Clients and servers, roots in the academic world

Protocols are old, some more than 20 years

Very little is encrypted, mostly HTTPS

Internet is Open Standards!

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

RFC, BCP, FYI, informational
de første stammer tilbage fra 1969

Ændres ikke, men får status Obsoleted når der udkommer en nyere version af en standard

Standards track:
Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

Hvad er Internet

Kommunikation mellem mennesker!

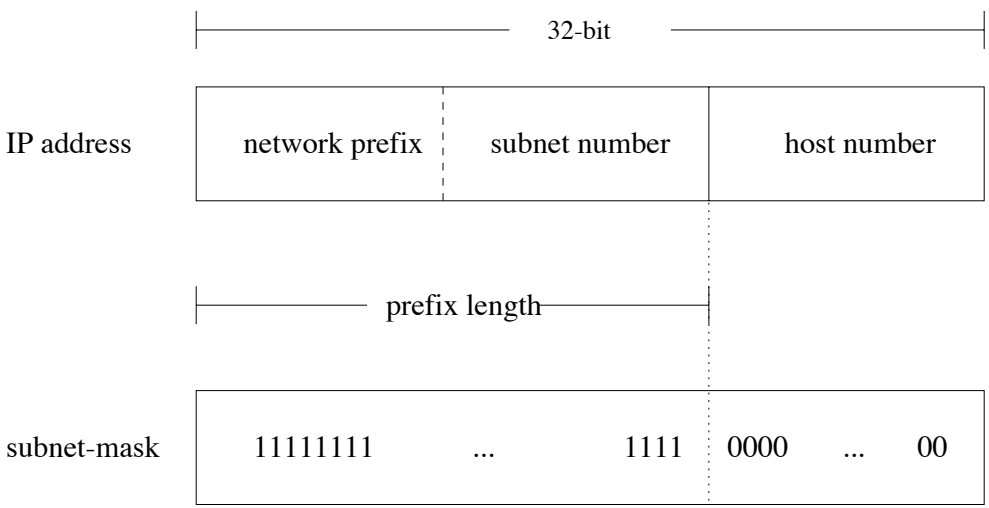
Baseret på TCP/IP

- best effort
- packet switching (IPv6 kalder det packets, ikke datagram)
- forbindelsesorienteret, *connection-oriented*
- forbindelsesløs, *connection-less*

RFC-1958:

> A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set"of rules that generates a large, varied and evolving space of technology.

Fælles adresserum



Hvad kendetegner internet idag

Der er et fælles adresserum baseret på 32-bit adresser, example 10.0.0.1

CIDR Classless Inter-Domain Routing

Classful routing		Classless routing CIDR	
4 class C networks	Inherent subnet mask	Supernet	Subnet mask
192.0.8.0	255.255.255.0	192.0.8.0	255.255.252.0
192.0.9.0	255.255.255.0		252d=11111100b
192.0.10.0	255.255.255.0		
192.0.11.0	255.255.255.0	Base network/prefix	
		192.10.8.0/22	

Fælles adresserum

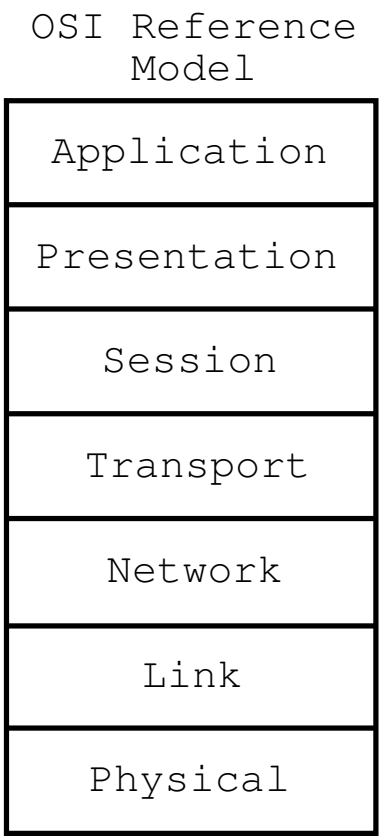
Best effort - kommer en pakke fra er det fint, hvis ikke må højere lag klare det

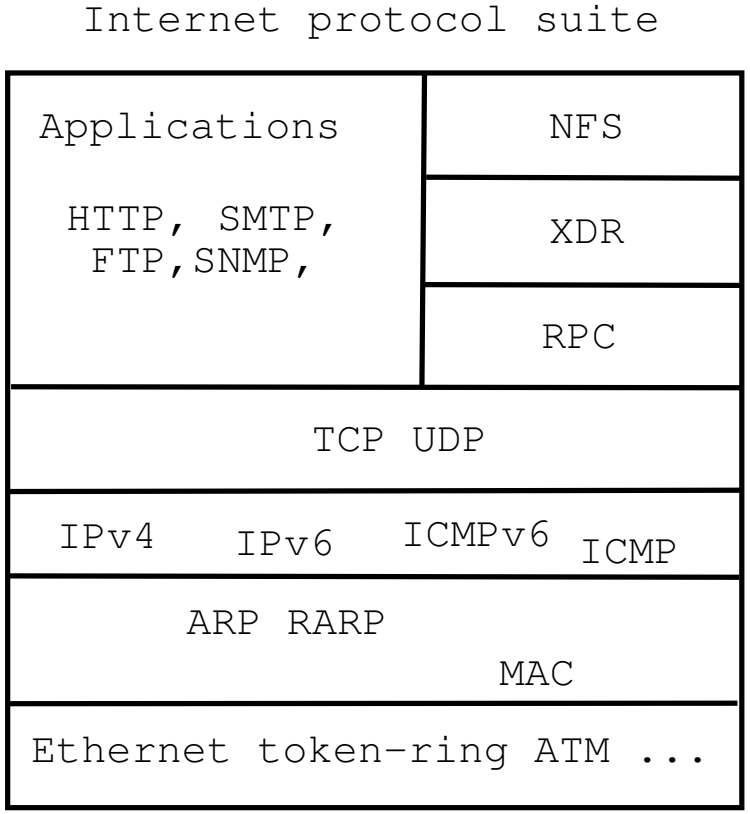
Kræver ikke mange services fra underliggende teknologi *dumt netværk*

Idag er subnetmaske en sammenhængende række 1-bit der angiver størrelse på nettet

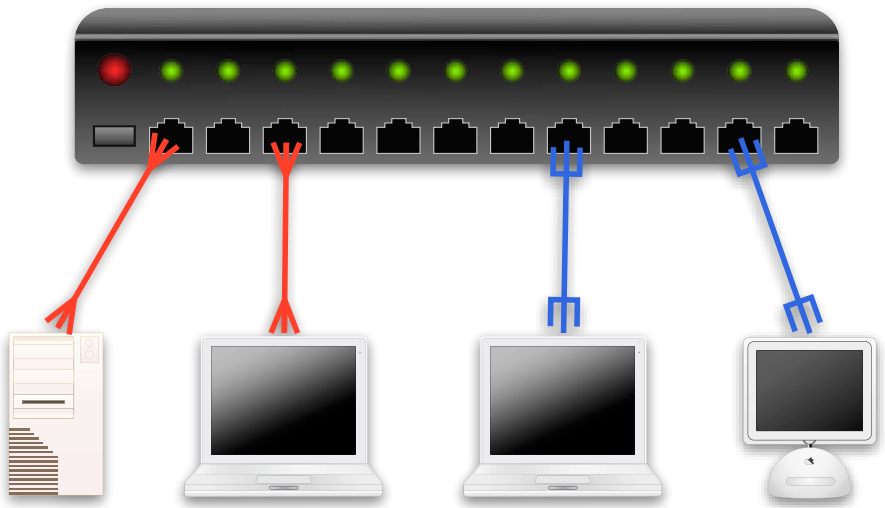
10.0.0.0/24 betyder netværket 10.0.0.0 med subnetmaske 255.255.255.0

OSI og Internet modellerne





En switch



Ved at fortsætte udviklingen kunne man samle broer til en switch

En switch idag kan sende og modtage på flere porte samtidig, og med full-duplex

Bemærk performance begrænses af backplane i switchen

MAC adresser

```
00-03-93    (hex)        Apple Computer, Inc.
000393      (base 16)    Apple Computer, Inc.
                         20650 Valley Green Dr.
                         Cupertino CA 95014
                         UNITED STATES
```

Netværksteknologierne benytter adresser på lag 2

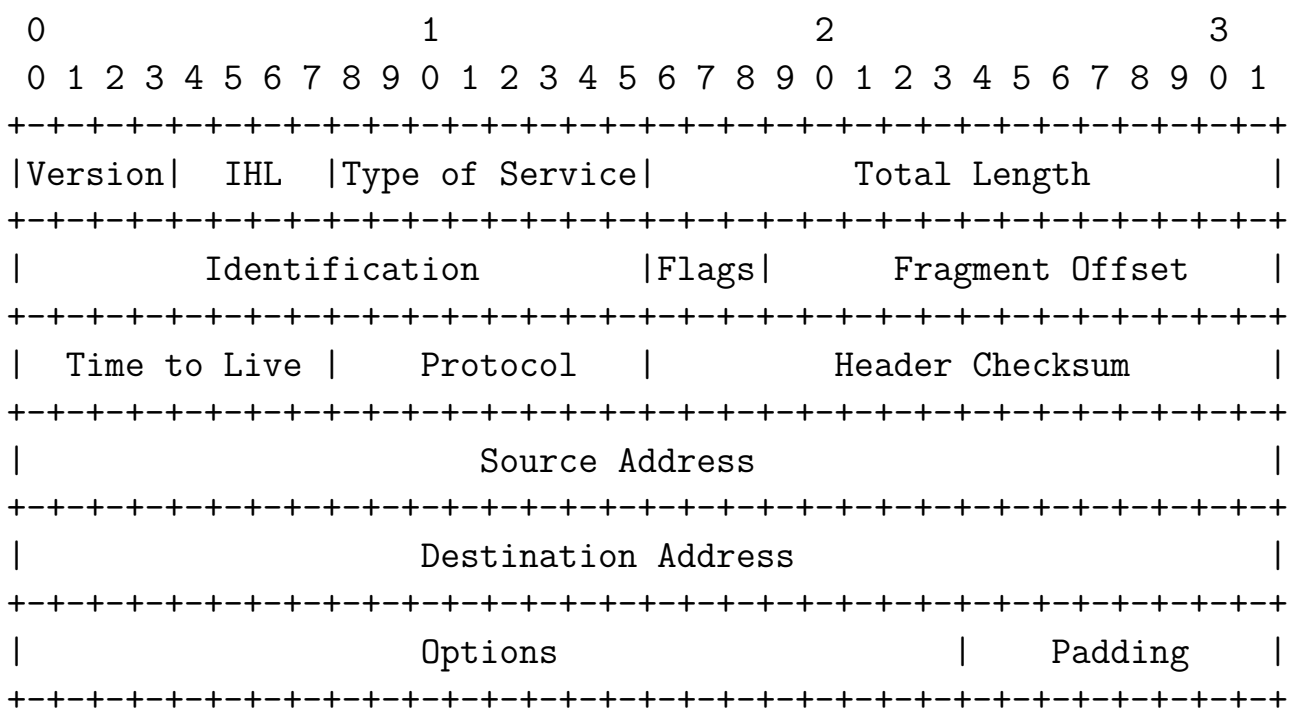
Typisk svarende til 48-bit MAC adresser som kendes fra Ethernet MAC-48/EUI-48

Første halvdel af adresserne er Organizationally Unique Identifier (OUI)

Ved hjælp af OUI kan man udlede hvilken producent der har produceret netkortet

`http://standards.ieee.org/regauth/oui/index.shtml`

IPv4 pakken - header - RFC-791



Example Internet Datagram Header

Basale testværktøjer TCP - Telnet og OpenSSL

Telnet blev brugt til login (cleartext) over TCP, brug Netcat til test nu

Telnet kan bruges til at teste forbindelsen til mange ældre serverprotokoller som benytter ASCII kommandoer

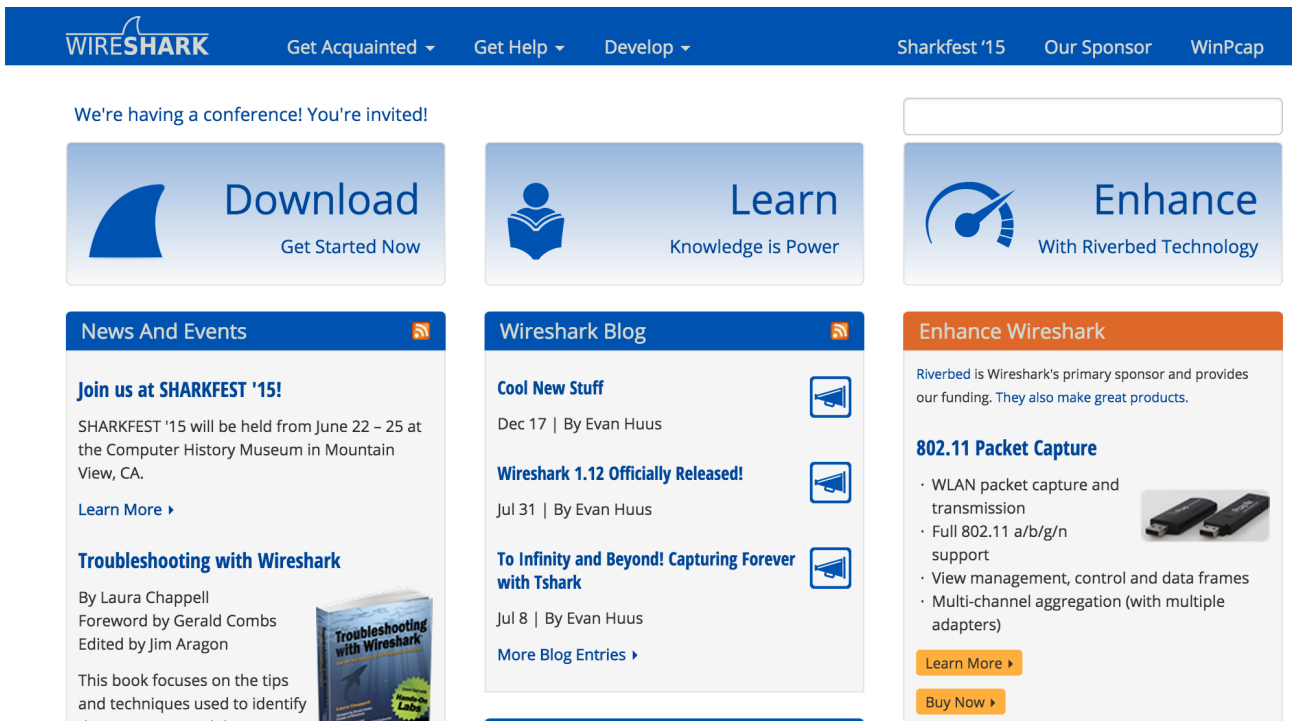
- `telnet mail.kramse.dk 25` laver en forbindelse til port 25/tcp
- `telnet www.kramse.dk 80` laver en forbindelse til port 80/tcp

Til krypterede forbindelser anbefales det at teste med openssl

- `openssl s_client -host www.kramse.dk -port 443`
  laver en forbindelse til port 443/tcp med SSL
- `openssl s_client -host mail.kramse.dk -port 993`
  laver en forbindelse til port 993/tcp med SSL

Med OpenSSL i client-mode kan services tilgås med samme tekstkommandoer som med telnet

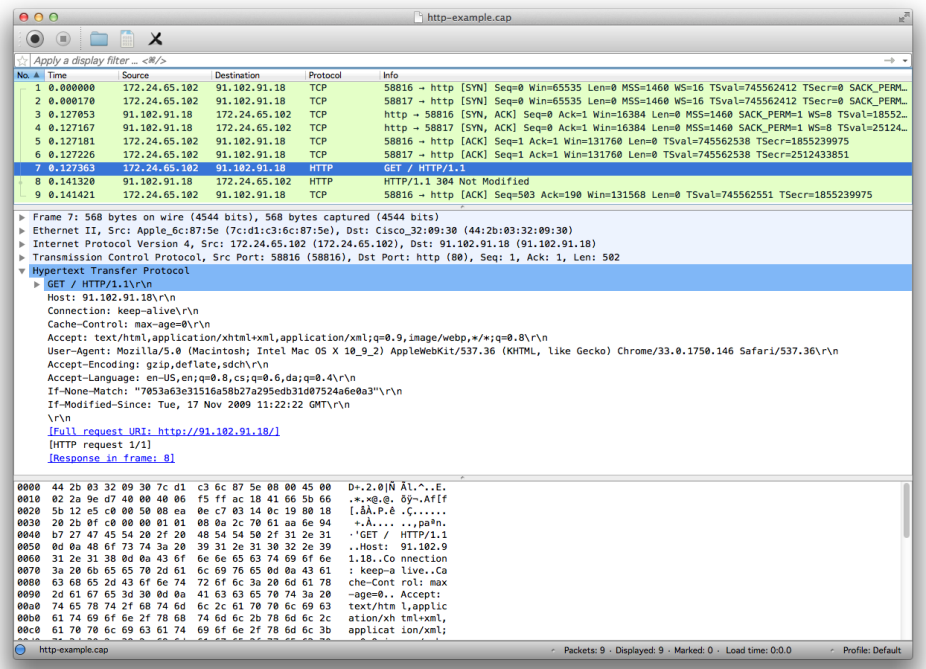
Wireshark - grafisk pakkesniffer



`http://www.wireshark.org`

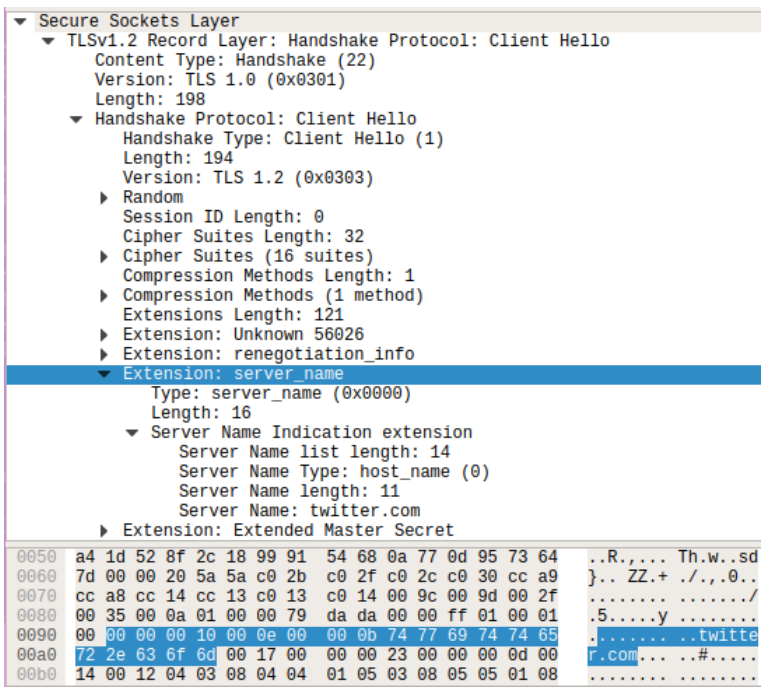
både til Windows og UNIX

Brug af Wireshark



Man starter med Capture - Options

Brug af Wireshark



Læg også mærke til filtermulighederne

Hardware IPv4 checksum offloading

IPv4 checksum skal beregnes hvergang man modtager en pakke

IPv4 checksum skal beregnes hvergang man sender en pakke

Lad en ASIC gøre arbejdet!

De fleste servernetkort tilbyder at foretage denne beregning på IPv4

IPv6 benytter ikke header checksum, det er unødvendigt

NB: kan resultere i at værktøjer siger checksum er forkert!

Vigtigste protokoller

ARP Address Resolution Protocol

IP og ICMP Internet Control Message Protocol

UDP User Datagram Protocol

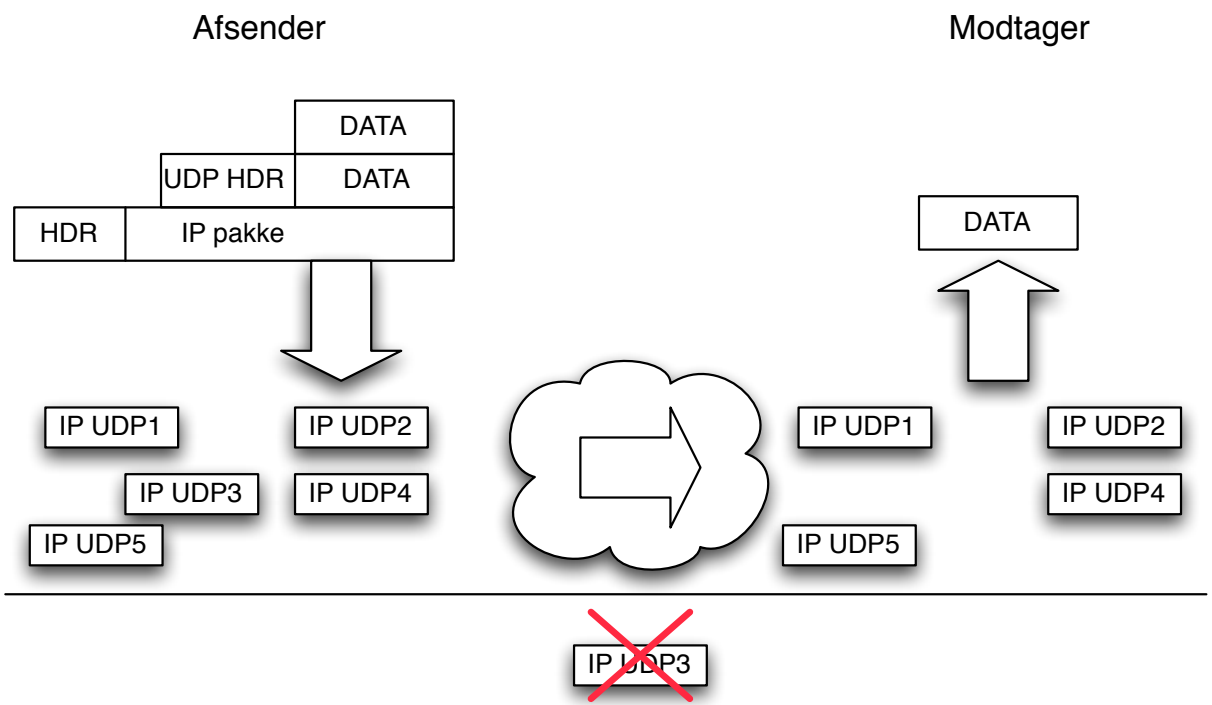
TCP Transmission Control Protocol

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

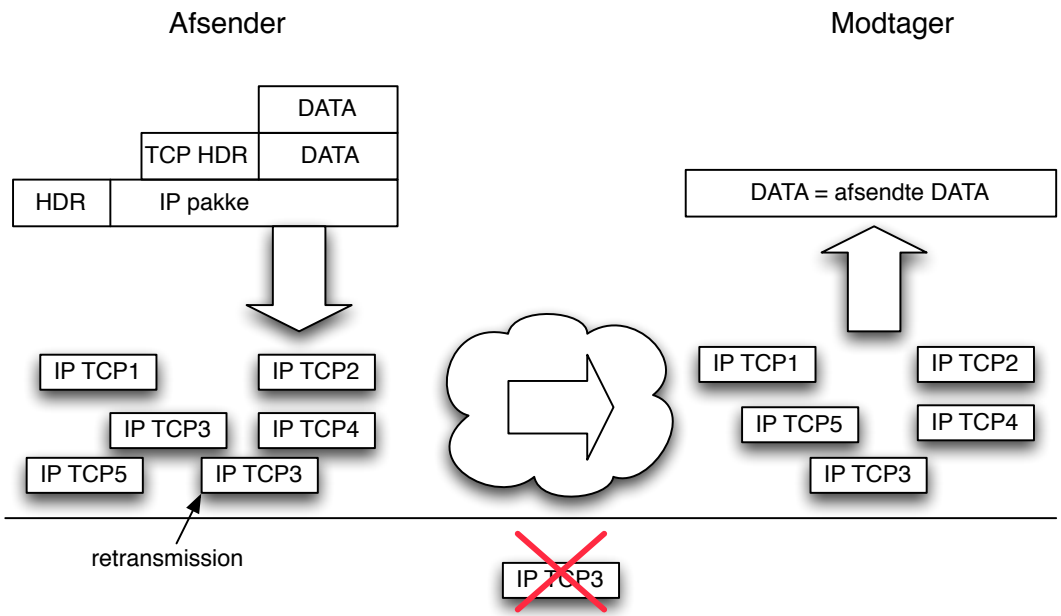
Ovenstående er omtrent minimumskrav for at komme på internet

UDP User Datagram Protocol



Forbindelsesløs RFC-768, *connection-less*

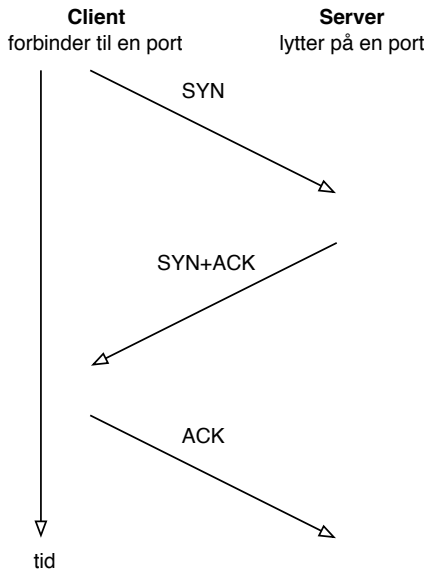
TCP Transmission Control Protocol



Forbindelsesorienteret RFC-791 September 1981, *connection-oriented*

Enten overføres data eller man får fejlmeddelelse

TCP three way handshake



- **TCP SYN half-open** scans
- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse
  - dette kan/kunne udnyttes til *stealth*-scans

Well-known port numbers

IANA vedligeholder en liste over magiske konstanter i IP

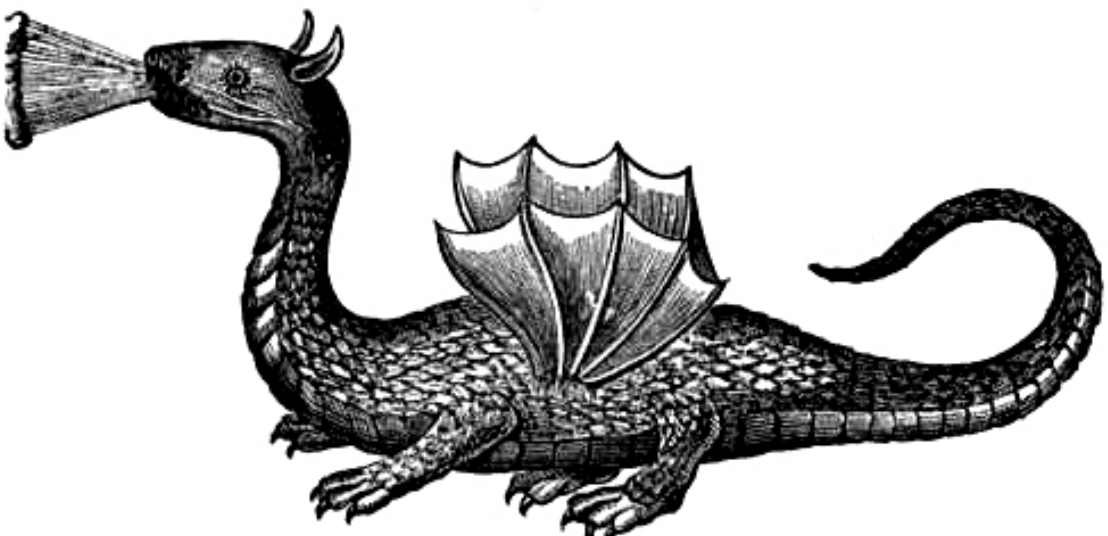
De har lister med hvilke protokoller har hvilke protokol ID m.v.

En liste af interesse er port numre, hvor et par eksempler er:

- Port 25 SMTP Simple Mail Transfer Protocol
- Port 53 DNS Domain Name System
- Port 80 HTTP Hyper Text Transfer Protocol over TLS/SSL
- Port 443 HTTP over TLS/SSL

Se flere på `http://www.iana.org`

Challenges in network security



Internet here be dragons

Security problems in the TCP/IP Suite

The paper "Security Problems in the TCP/IP Protocol Suite" was originally pub- lished in Computer Communication Review, Vol. 19, No. 2, in April, 1989

Problems described in the original:

- sequence number spoofing
- routing attacks,
- source address spoofing
- authentication attacks

Should have been fixed by now!

TCP sequence number prediction

> TCP SEQUENCE NUMBER PREDICTION One of the more fascinating security holes was first described by Morris [7] . Briefly, he used TCP sequence number prediction to construct a TCP packet sequence without ever receiving any responses from the server. This allowed him to spoof a trusted host on a local network.

tidligere baserede man login/adgange på source IP adresser, address based authentication

Er ikke en pålidelig autentifikationsmekanisme

Mest kendt er nok Shimomura der blev hacket på den måde,
måske af Kevin D Mitnick eller en kompagnon

I praksis vil det være svært at udføre på moderne operativsystemer

Se evt. `http://www.takedown.com/` (filmen er ikke så god ;-))

Det er naturligvis fint med filtre så man kun kan tilgå services FRA bestemte IP

Routing attacks

Problems described in the original from 1989:

- IP Source routing attacks - angiv en rute for pakkerne
  Knapt så brugbar idag
- Routing Information Protocol Attacks
  The Routing Information Protocol [15] (RIP) - denne bruges ikke mere, outdated
- BGPv4 som bruges idag har kæmpe problemer, kludetæppe af kludges

Check other low level attacks from `https://github.com/tomac/yersinia`

Solutions to TCP/IP security problems

Solutions:

- Use RANDOM TCP sequence numbers, Win/Mac/Linux - DO,but IoT?
- Filtrering, ingress / egress:
  "reject external packets that claim to be from the local net"
- Routers and routing protocols must be more skeptical
  Routing filtre everywhere, auth på OSPF/BGP etc.

Has been recommended for some years, but not done in all organisations

BGP routing Resource Public Key Infrastructure RPKI

DNS problems

> The Domain Name System (DNS) [32][33] provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities.

We have a lot of the same problems in DNS today

Plus some more caused by middle-boxes, NAT, DNS size, DNS inspection

- DNS must allow both UDP and TCP port 53
- Your DNS servers must have updated software, see DNS flag days https://dnsflagday.net/ after which kludges will be REMOVED!
- Use DNSSEC, DANE etc. Presentation for another day!

SNMP problems

> 5.5 Simple Network Management Protocol The Simple Network Management Protocol (SNMP) [37] has recently been defined to aid in network management. Clearly, access to such a resource must be heavily protected. The RFC states this, but also allows for a null authentication service; this is a bad idea. Even a ‘‘read-only’’ mode is dangerous; it may expose the target host to netstat-type attacks if the particular Management Information Base (MIB) [38] used includes sequence numbers. (T

True

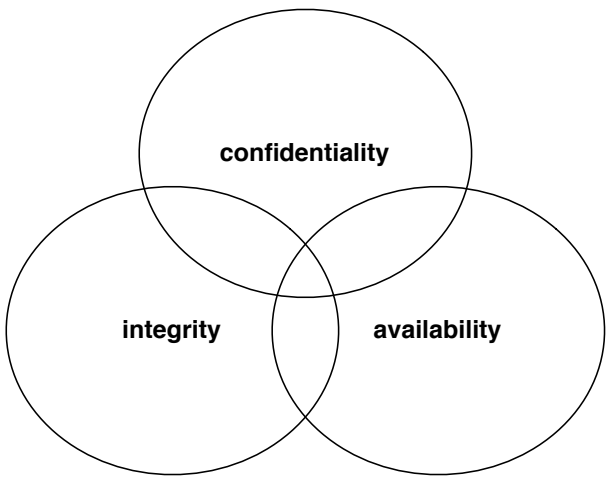
local networks

> 6.1 Vulnerability of the Local Network Some local-area networks, notably the Ethernet networks, are extremely vulnerable to eavesdropping and host-spoofing. If such networks are used, physical access must be strictly controlled. It is also unwise to trust any hosts on such networks if any machine on the network is accessible to untrusted personnel, unless authentication servers are used. If the local network uses the Address Resolution Protocol (ARP) [42] more subtle forms of host-spoofing are possible. In particular, it becomes trivial to intercept, modify, and forward packets, rather than just taking over the host's role or simply spying on all traffic.

Today we can send VXLAN spoofed packets across the internet layer 3 and inject ARP behind firewalls, in some cloud infrastructure cases ...

A Look Back at "Security Problems in the TCP/IP Protocol Suite" about 1989 + 15 years = 2004

Confidentiality Integrity Availability



We want to protect something

Confidentiality - data holdes hemmelige

Integrity - data ændres ikke uautoriseret

Availability - data og systemet er tilgængelige når de skal bruges

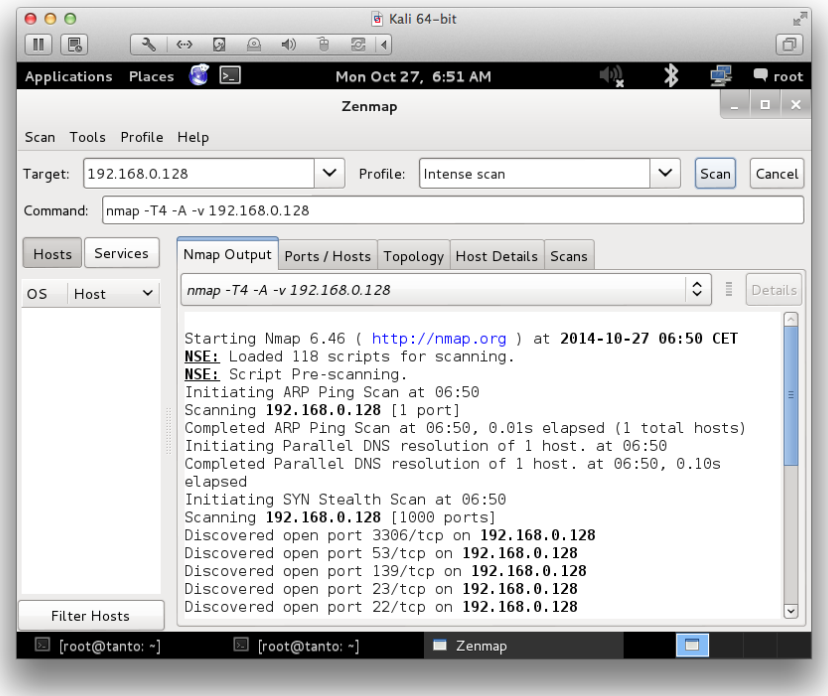
The basic tools for countering threats

- Networks have end-points and conversations on multiple layers
- Wireshark is advanced, try right-clicking different places
- Name resolution includes low level MAC addresses, and IP - names
- More than 1000 dissectors, but beware some have security issues!

- TShark and Tcpdump, I often use: `tcpdump -nei eth0`
  `tshark -z expert -r download-slow.pcapng`
- Remote packet dumps, `tcpdump -i eth0 -w packets.pcap`
- Story: tcpdump was originally written in 1988 by Van Jacobson, Sally Floyd, Vern Paxson and Steven McCanne who were, at the time, working in the Lawrence Berkeley Laboratory Network Research Group
  `https://en.wikipedia.org/wiki/Tcpdump`

Great network security comes from knowing networks!

Portscan using Zenmap GUI



Zenmap is included in the Nmap binary RPM package `https://nmap.org`

All attacks have signatures, some more noisy than others

Table 12-1: Common Passive Fingerprinting Values

Protocol header	Field	Default value	Platform
IP	Initial time to live	64	NMap, BSD, OS X, Linux
		128	Novell, Windows
		255	Cisco IOS, Palm OS, Solaris
IP	Don't fragment flag	Set	BSD, OS X, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, Cisco IOS
TCP	Maximum segment size	0	Nmap
		1440–1460	Windows, Novell
		1460	BSD, OS X, Linux, Solaris

(continued)

Systems can also be fingerprinted on various levels

Discover, filter, harden, reduce attack surfaces

Know your network!

FTP File Transfer Protocol

File Transfer Protocol - filoverførsler

Bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP

FTP sender i klartekst
USER brugernavn og
PASS hemmeligt-kodeord

Nogle varianter tillader kryptering, men brug istedet SCP/SFTP over Secure Shell protokollen

Person in the middle attacks

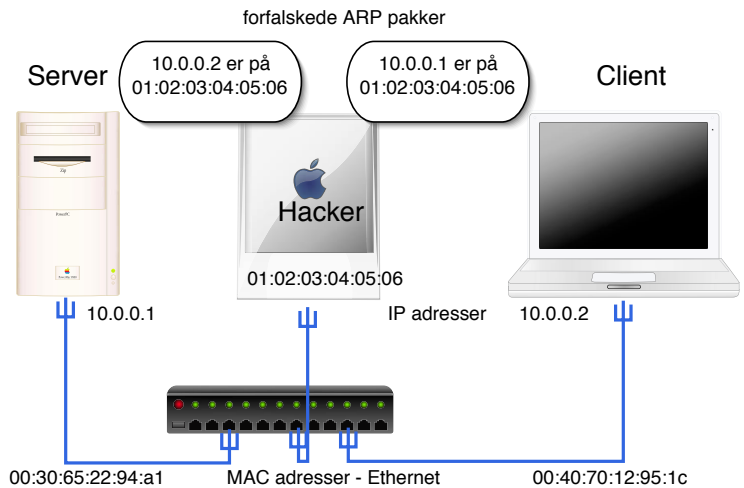
ARP spoofing, ICMP redirects, the classics

Used to be called Man in The Middle MiTM

- ICMP redirect
- ARP spoofing
- Wireless listening and spoofing higher levels like airpwn-ng `https://github.com/ICSec/airpwn-ng`

Usually aimed at unencrypted protocols

Hvordan virker ARP spoofing?



Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - som får alle pakkerne

Network Security Threats

Low level and Network Layer Attacks

- "Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems."
  evil l2 tools - STP, CDP, DTP, DHCP, HSRP, IEEE 802.1Q, IEEE 802.1X, ISL, VTP
  `https://github.com/tomac/yersinia`
- IP based creating strange fragments, overlapping, missing, SMALLL with fragroute/fragrouter
- LAND - same destination and source address
- THC-IPV6 - attacking the IPV6 protocol suite

Note: Evil repeats itself, like doing ARP poisoning across MPLS or VXLAN

Attackers are very creative!

Forsvar mod ARP spoofing

Hvad kan man gøre?

låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

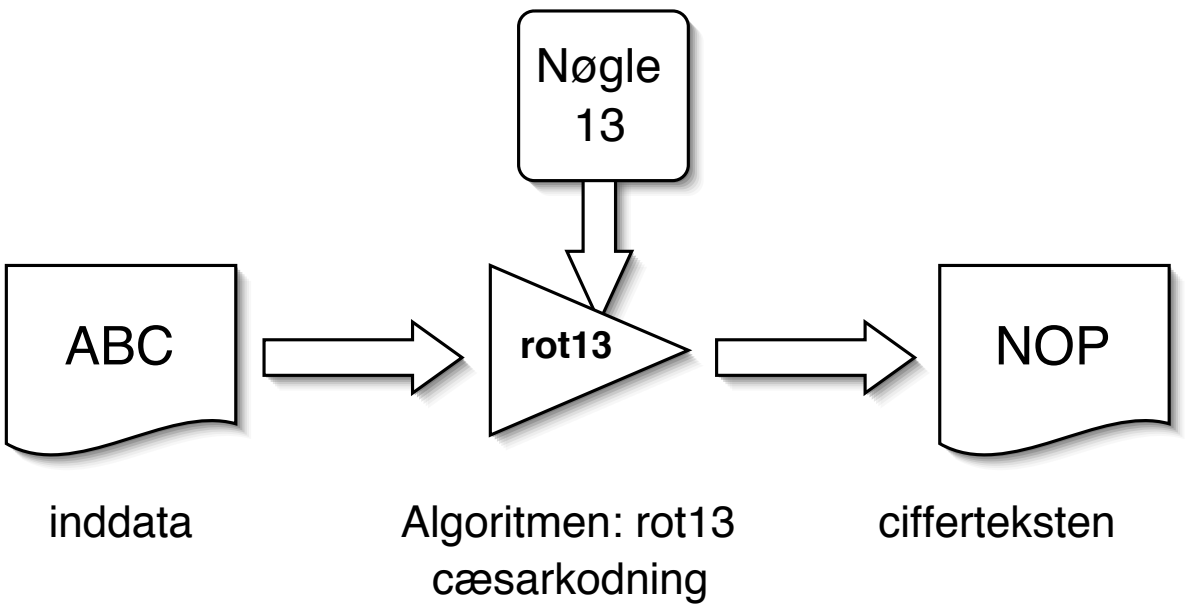
Efterfølgende administration!

Adskilte netværk - brug IEEE 802.1q VLANs

arpwatch er et godt bud - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

Introduce the encryption protocols in use in networks



Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication

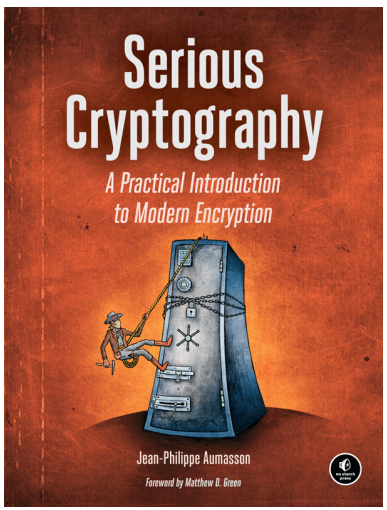
Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key, to ensure confidentiality, example algorithm AES

Public-key cryptography (like RSA) uses two related keys, a key pair of a public key and a private key. This allows for easier key exchanges, and can provide confidentiality, and methods for signatures and other services

Source: `https://en.wikipedia.org/wiki/Cryptography`

Serious Cryptography



Serious Cryptography A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson November 2017, 312 pp. ISBN-13: 978-1-59327-826-7 `https://nostarch.com/seriouscrypto`

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et successfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid
`http://www.interhack.net/people/cmcurtin/snake-oil-faq.html`

DES, Triple DES og AES

AES

Advanced Encryption Standard

DES kryptering - gammel og pensioneret!

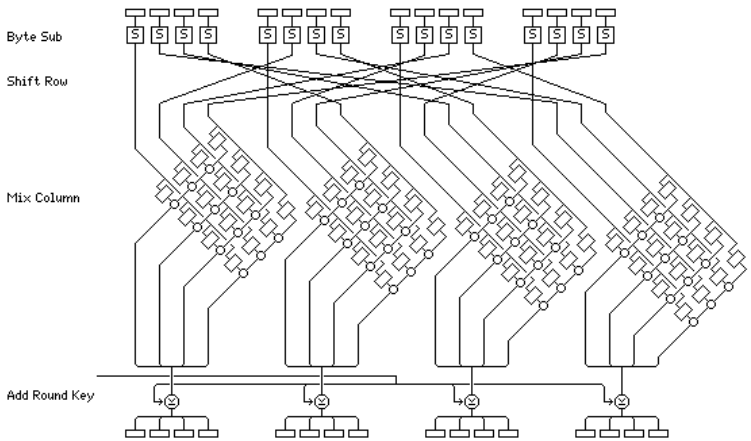
Der blev i 2001 vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

Se også `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

Findes animationer (med fejl) `https://www.youtube.com/watch?v=mlzxpkdXP58`

AES Advanced Encryption Standard



- The official Rijndael web site displays this image to promote understanding of the Rijndael round transformation [8].
- Key sizes 128,192,256 bit typical
- Some extensions in cryptosystems exist: XTS-AES-256 really is 2 instances of AES-128 and 384 is two instances of AES-192 and 512 is two instances of AES-256
- `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

RSA

> RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. ... In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978.

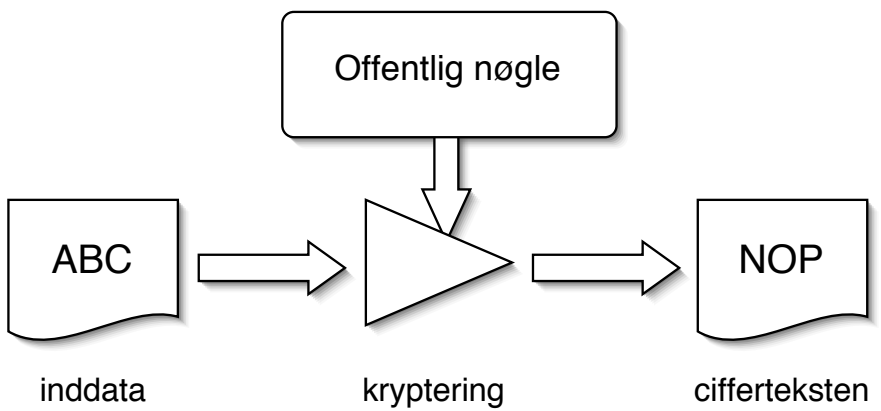
- Key sizes 1,024 to 4,096 bit typical
- Quote from: `https://en.wikipedia.org/wiki/RSA_(cryptosystem)`

Elliptic Curve

> Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.[1]

- Today we use `https://en.wikipedia.org/wiki/Elliptic-curve_cryptography`

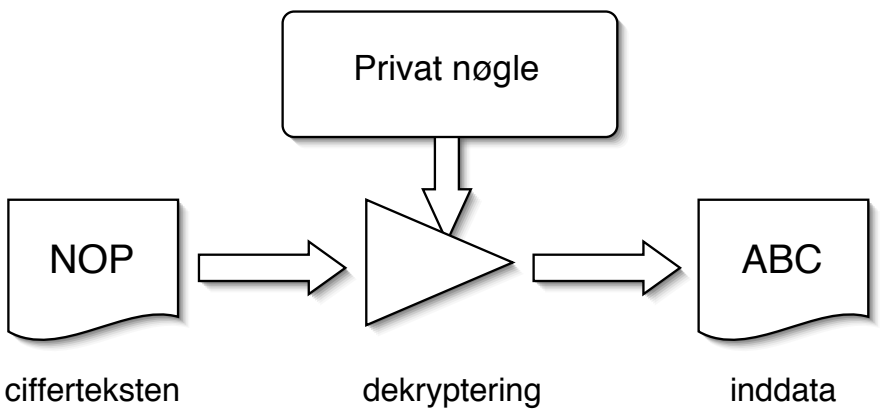
Public key kryptografi - 1



privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

offentlig-nøgle kryptografi (eksempelvis RSA) benytter to separate nøgler til kryptering og dekryptering

Public key kryptografi - 2

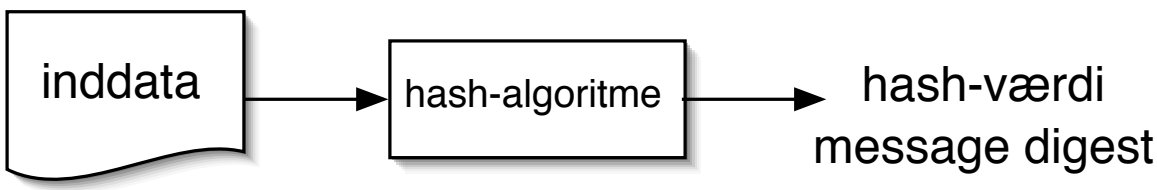


offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere

man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter
- som så verificeres med den offentlige nøgle

NB: Kryptering alene sikrer ikke anonymitet

Hashing - MD5 message digest funktion



HASH algoritmer giver en næsten unik værdi baseret på input

værdien ændres radikalt selv ved små ændringer i input

MD5 er blandt andet beskrevet i RFC-1321: The MD5 Message-Digest Algorithm

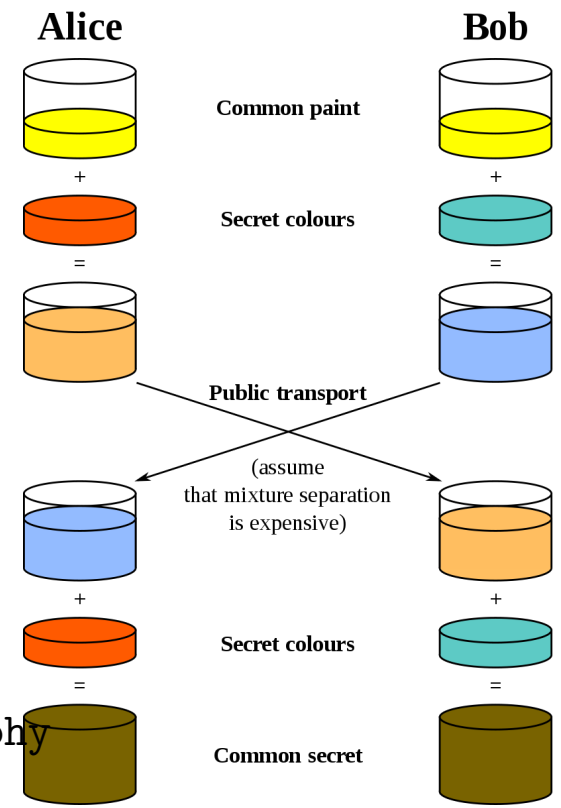
Algoritmen MD5 er baseret på MD4, begge udviklet af Ronald L. Rivest

Både MD5 og SHA-1 er idag gamle og skal generelt ikke bruges mere

Idag benyttes eksempelvis `https://en.wikipedia.org/wiki/PBKDF2`

Encryption on the web – Diffie Helman exchange

Diffie–Hellman key exchange (DH)[nb 1] is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.[1][2] DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. ... The scheme was first published by Whitfield Diffie and Martin Hellman in 1976



- Quote from: `https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange`
- Today we use `https://en.wikipedia.org/wiki/Elliptic-curve_cryptography`

Transport Layer Security (TLS)

Oprindeligt udviklet af Netscape Communications Inc.

Secure Sockets Layer SSL er idag blevet adopteret af IETF og kaldes derfor også for Transport Layer Security TLS TLS er baseret på SSL Version 3.0

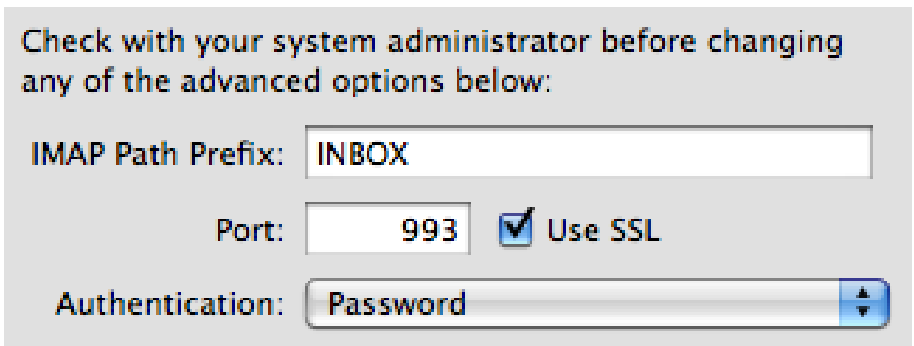
RFC-2246 The TLS Protocol Version 1.0 fra Januar 1999

RFC-3207 SMTP STARTTLS

Det er svært!

Stanford Dan Boneh udgiver en masse omkring crypto
`https://crypto.stanford.edu/~dabo/cryptobook/`

SSL/TLS udgaver af protokoller



Mange protokoller findes i udgaver hvor der benyttes SSL

HTTPS vs HTTP

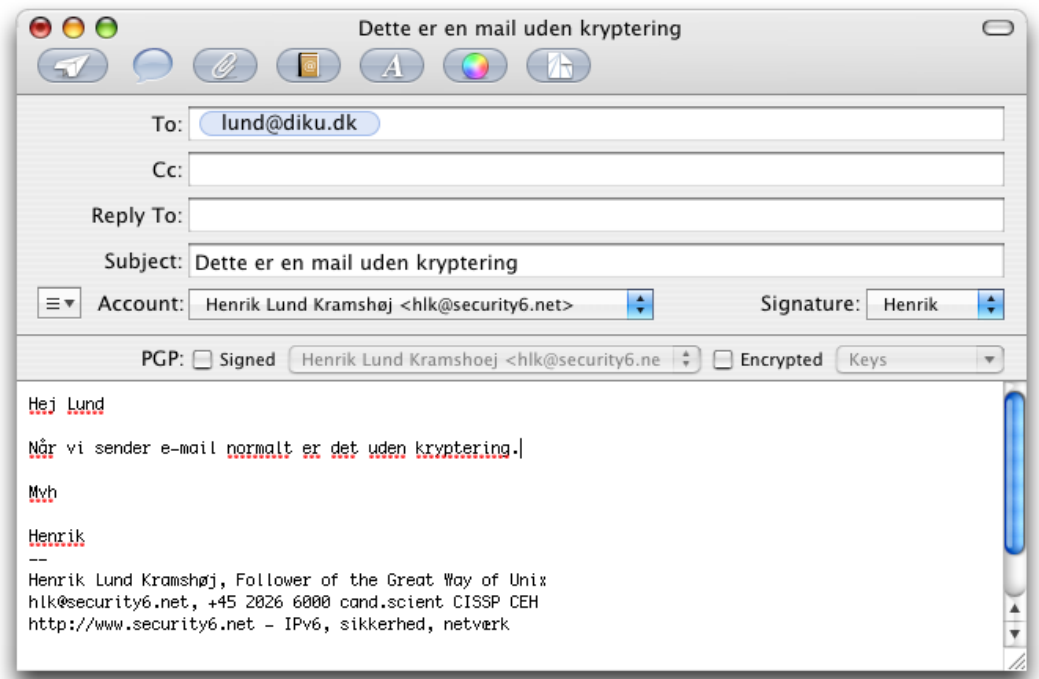
IMAPS, POP3S, osv.

Bemærk: nogle protokoller benytter to porte IMAP 143/tcp vs IMAPS 993/tcp

Andre benytter den samme port men en kommando som starter:

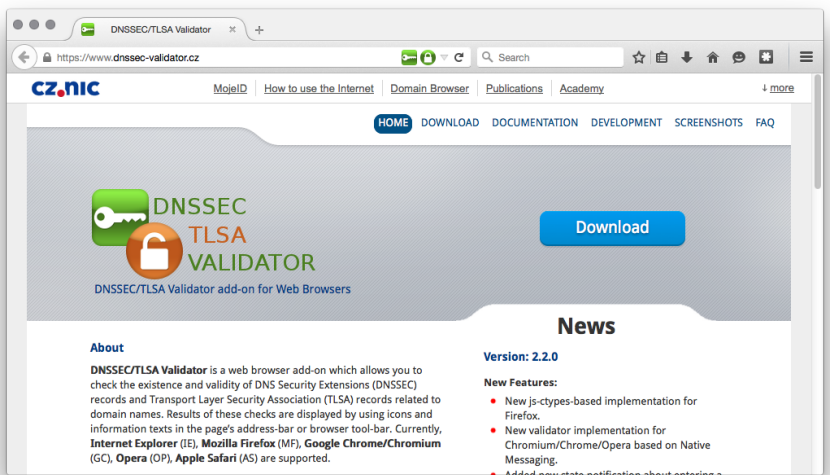
SMTP STARTTLS RFC-3207

Email er usikkert



Email uden kryptering - er som et postkort

DNSSEC get started now



"TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified by DANE protocol (RFC 6698). DNSSEC and TLSA validation results are displayer by using several icons."

DNSSEC and DANE

"Objective:

Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name."

DNS-based Authentication of Named Entities (dane)

Email security 2020 – Goals

- SPF Sender Policy Framework

  `https://en.wikipedia.org/wiki/Sender_Policy_Framework`
- DKIM DomainKeys Identified Mail

  `https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail`
- DMARC Domain-based Message Authentication, Reporting and Conformance

  `https://en.wikipedia.org/wiki/DMARC`
- DANE DNS-based Authentication of Named Entities

  `https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities`
- Brug allesammen, check efter ændringer!

SMTP TLS

> The STARTTLS command for IMAP and POP3 is defined in RFC 2595, for SMTP in RFC 3207, for XMPP in RFC 6120 and for NNTP in RFC 4642. For IRC, the IRCv3 Working Group has defined the STARTTLS extension. FTP uses the command "AUTH TLS"defined in RFC 4217 and LDAP defines a protocol extension OID in RFC 2830. HTTP uses upgrade he ader.

SMTP was extended with support for Transport Layer Security TLS

Also called **Opportunistic TLS**, where the quote is also from:
`https://en.wikipedia.org/wiki/Opportunistic_TLS`

Now we have MTA Strict Transport Security (MTA-STS) RFC 8461
so we can announce that we only accept encrypted email!

DNS over TLS vs DNS over HTTPS - DNS encryption

- Protocols exist that encrypt DNS data
- Today we have competing standards:
- *Specification for DNS over Transport Layer Security (TLS)* (DoT), RFC7858 MAY 2016
  `https://en.wikipedia.org/wiki/DNS_over_TLS`
- *DNS Queries over HTTPS (DoH)* RFC8484
- How to cofigure DoT
  `https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients`

sslscan check your web and mail server settings

```
root@kali:~# sslscan --ssl2 web.kramse.dk
Version: 1.10.5-static OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server web.kramse.dk on port 443
...
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048
Subject:  *.kramse.dk
Altnames: DNS:*.kramse.dk, DNS:kramse.dk
Issuer:   AlphaSSL CA - SHA256 - G2
```

Source: Originally sslscan from http://www.titania.co.uk but use the version on Kali Linux

SSLscan can check your own sites by IP plus SMTP and some other services!

PS From now on its TLS! Not SSL anymore, any SSLv2, SSLv3 is old and vulnerable

Virtual Private Network (VPN)

VPN are everywhere, but could be better!

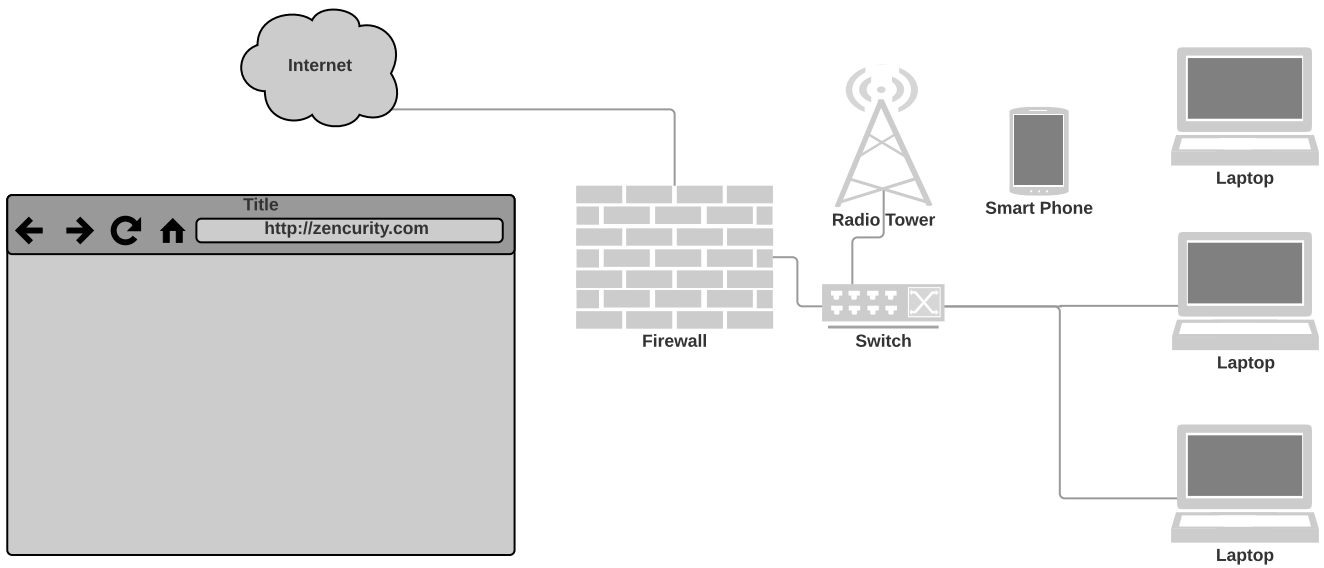
- https://en.wikipedia.org/wiki/Virtual_private_network
- https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104
- IPSec VPN between JUNOS and Cisco IOS
- Skim:
- https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
- https://en.wikipedia.org/wiki/OpenVPN
- https://en.wikipedia.org/wiki/IPsec
- https://en.wikipedia.org/wiki/DirectAccess
- https://www.wireguard.com/papers/wireguard.pdf

Example references.

Fokus 2020: VPN alle steder

- VPN er relevant for alle der har data af værdi
- Sikrer data der flyttes
- Virtual Private Network dækker over klienter der kobler op, og site-2-site

Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

Data found in Network data

Lets take an example, DNS

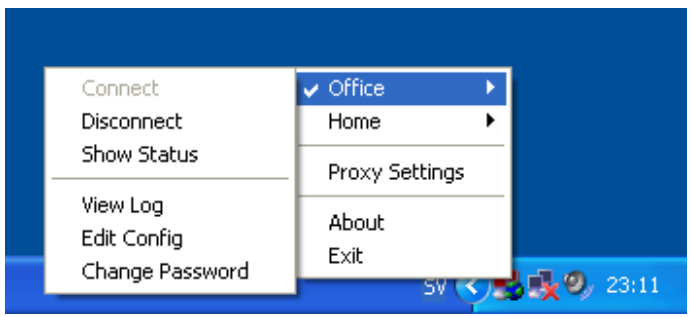
Domain Name System DNS breadcrumbs

- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit

Advice show your users,ask them to participate in a experiment

Maybe use VPN more - or always!

VPN



Virtual Private Networks are useful - or even required when travelling

VPN `http://en.wikipedia.org/wiki/Virtual_private_network`

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

IETF IPsec does work cross-vendors - sometimes, and is also increasingly becoming blocked or unusable due to NAT :-(

Recommended starting point OpenVPN - free and open, clients for "anything"

VPN without encryption

> Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.[
> ... MPLS works by prefixing packets with an MPLS header, containing one or more labels.

Source:

`https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching`

- The term VPN is also used in cases without encryption
- MPLS allows multiple customers to use the same IP prefixes, like 10/8
- MPLS is used in many provider networks
- Another example is Generic Routing Encapsulation (GRE), which is often then protected with IPsec
- People today also uses Virtual Extensible LAN (VXLAN) for cloud computing

Linux Wireguard VPN

> WireGuard is a secure network tunnel, operating at layer 3, implemented as a kernel virtual network interface for Linux, which aims to replace both IPsec for most use cases, as well as popular user space and/or TLS-based solutions like OpenVPN, while being more secure, more performant, and easier to use.

Description from `https://www.wireguard.com/papers/wireguard.pdf`

- Going to be interesting!
- single round trip key exchange, based on NoiseIK
- Short pre-shared static keys—Curve25519
- strong perfect forward secrecy
- Transport speed is accomplished using ChaCha20Poly1305 authenticated-encryption
- encapsulation of packets in UDP
- WireGuard can be simply implemented for Linux in less than 4,000 lines of code, making it easily audited and verified

IPsec

Sikkerhed i netværket

RFC-2401 Security Architecture for the Internet Protocol

RFC-2402 IP Authentication Header (AH)

RFC-2406 IP Encapsulating Security Payload (ESP)

RFC-2409 The Internet Key Exchange (IKE) - dynamisk keying

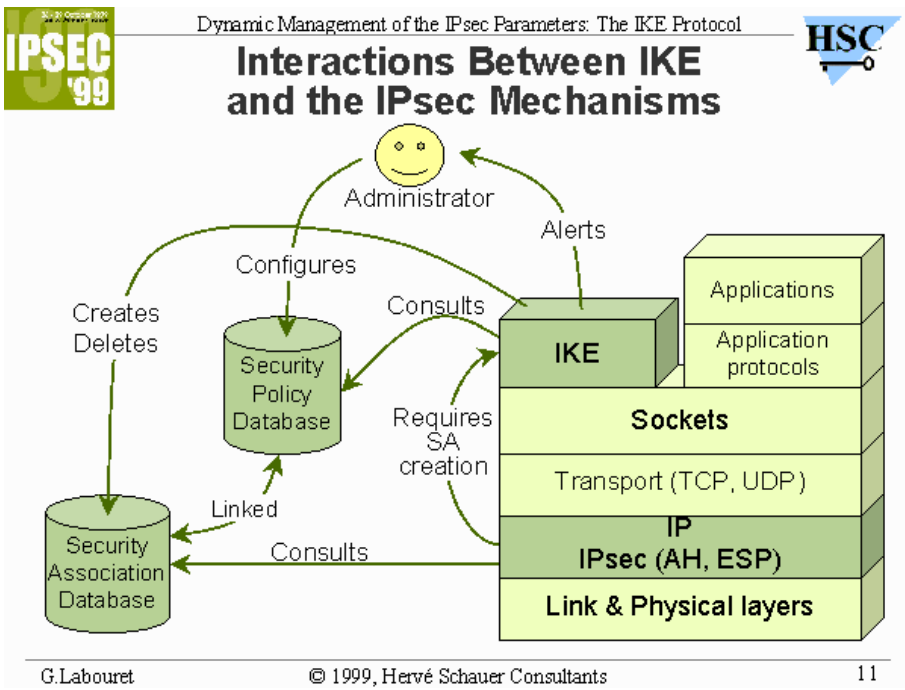
... IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap
`https://tools.ietf.org/html/rfc6071`

Både til IPv4 og IPv6

MANDATORY i IPv6! - et krav hvis man implementerer fuld IPv6 support

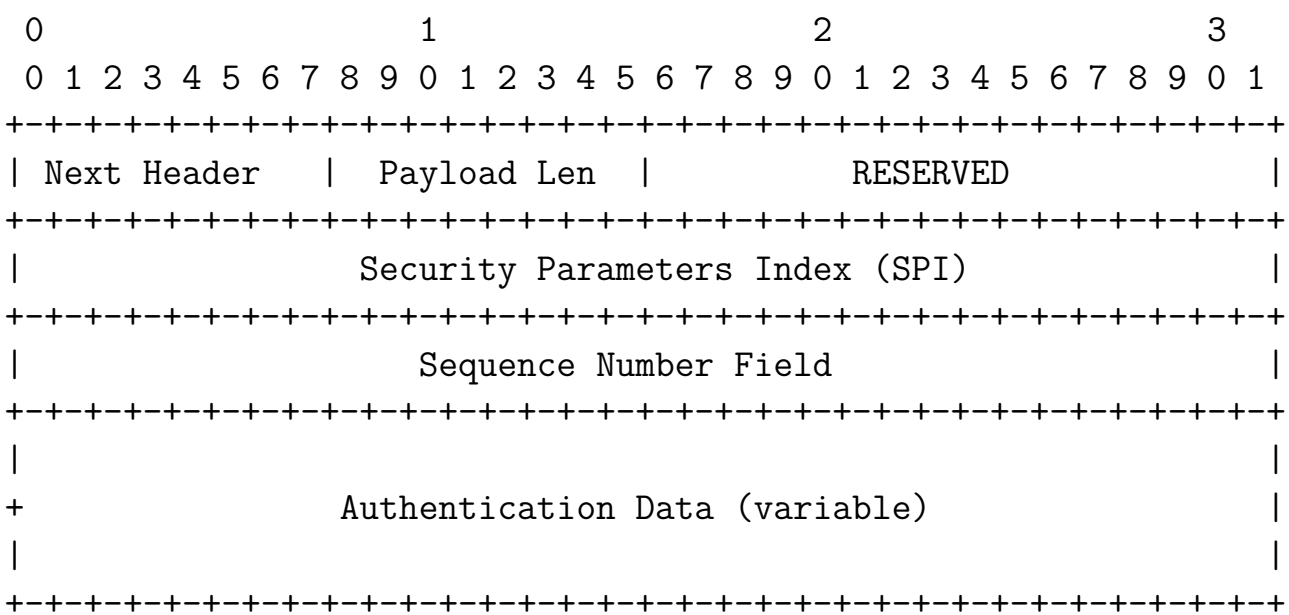
Der findes IKEscan til at scanne efter IKE porte/implementationer
`http://www.nta-monitor.com/ike-scan/index.htm`

IPsec er ikke simpelt!



Kilde: `http://www.hsc.fr/presentations/ike/`

RFC-2402 IP Authentication Header AH

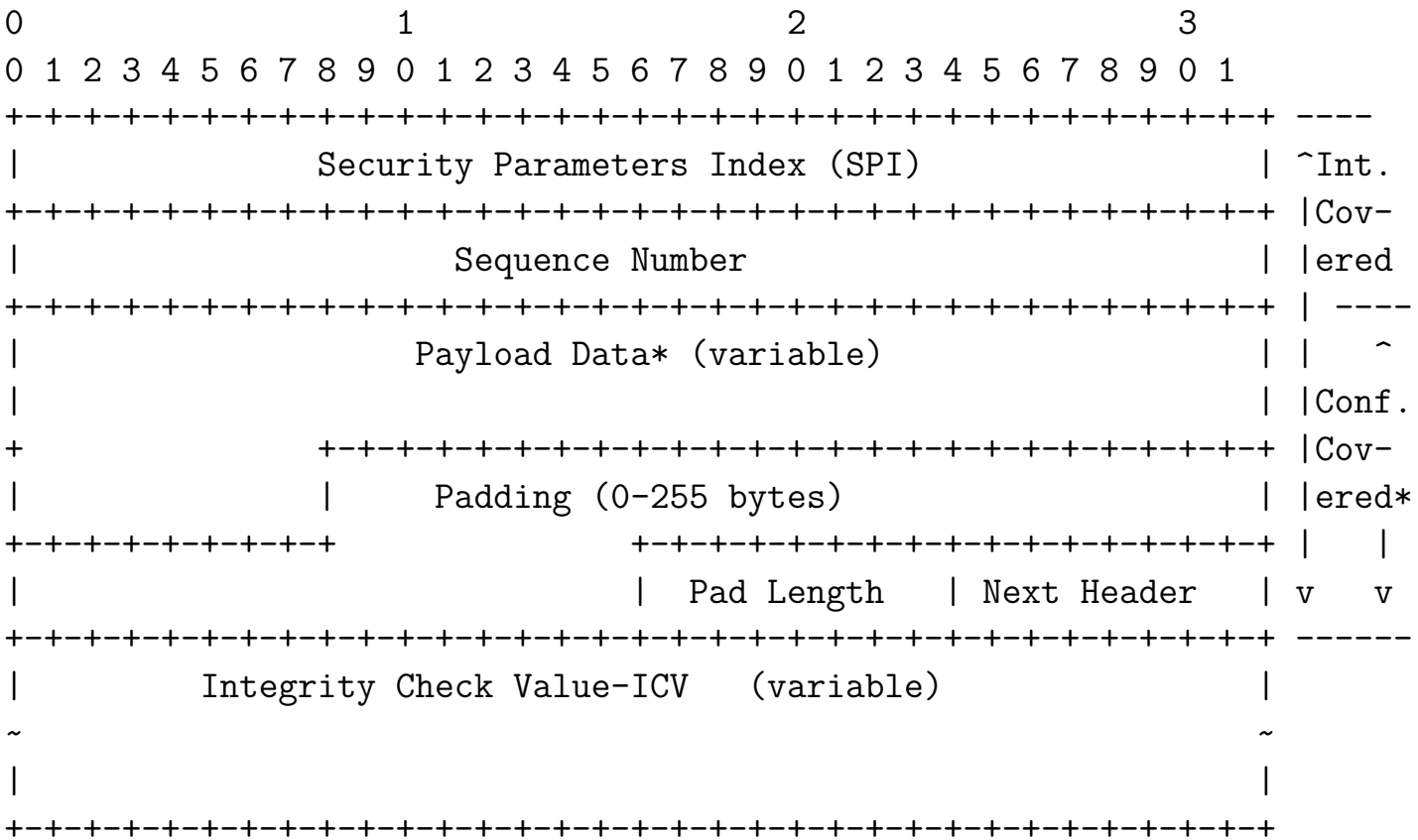


RFC-2402 IP Authentication Header AH

Indpakning - pakkerne før og efter Authentication Header:

```
            BEFORE APPLYING AH
          ----------------------------
IPv4      |orig IP hdr  |     |      |
          |(any options)| TCP | Data |
          ----------------------------

             AFTER APPLYING AH
          ---------------------------------
IPv4      |orig IP hdr  |    |     |      |
          |(any options)| AH | TCP | Data |
          ---------------------------------
          |<------- authenticated ------->|
               except for mutable fields
```

RFC-2406 IP Encapsulating Security Payload ESP

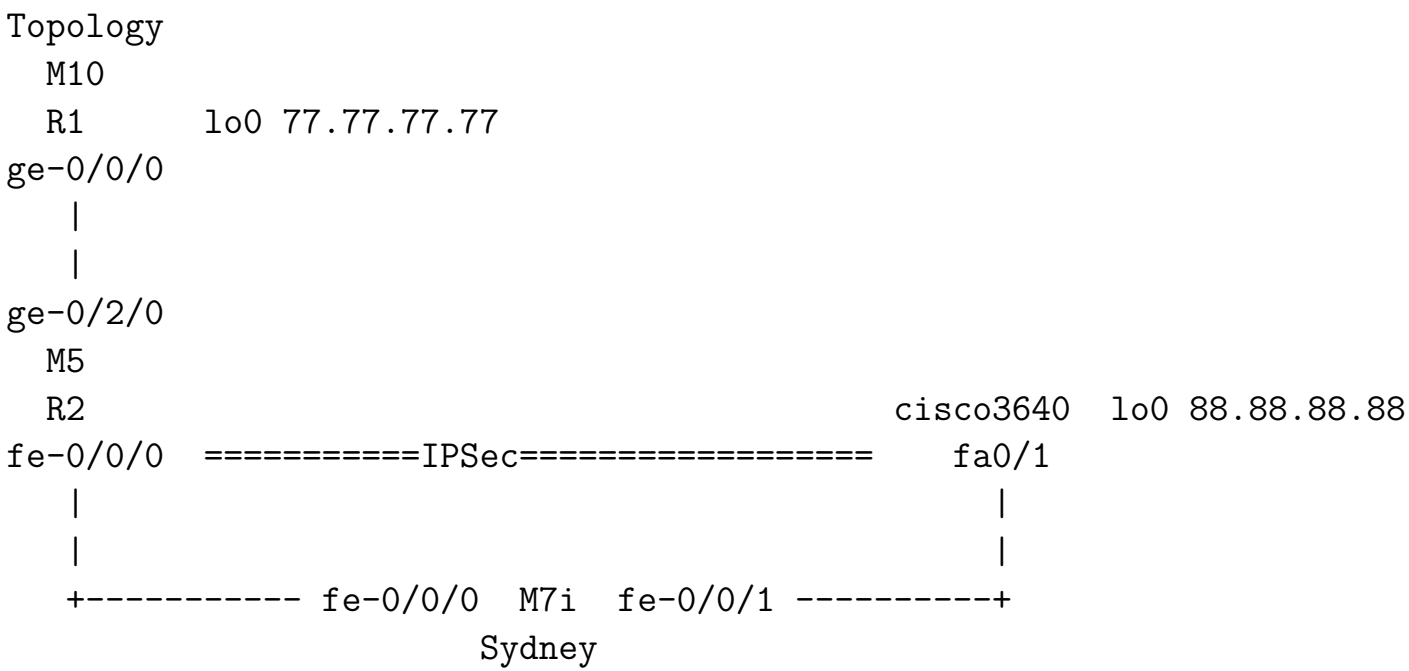


RFC-2406 IP Encapsulating Security Payload ESP

Pakkerne før og efter:

```
              BEFORE APPLYING ESP
            ----------------------------------------
      IPv6  |              | ext hdrs |     |      |
            | orig IP hdr  |if present| TCP | Data |
            ----------------------------------------


              AFTER APPLYING ESP
            ------------------------------------------------------------
      IPv6  | orig |hop-by-hop,dest*,|   |dest|   |    | ESP   | ESP|
            |IP hdr|routing,fragment.|ESP|opt*|TCP|Data|Trailer|Auth|
            ------------------------------------------------------------
                                    |<---- encrypted ---->|
                                  |<---- authenticated ---->|
```

IPSec VPN between JUNOS and Cisco IOS



Source: https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104

Cisco IOS crypto setup

```
cisco3640#sh run
crypto isakmp policy 10
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key key123 address 11.0.0.1
!
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
crypto ipsec transform-set ts-man esp-des esp-md5-hmac
!
crypto map dyn 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set ts
 match address 120
```

Not recommended settings! See later! People still use these examples!

Layer 2 Tunneling Protocol L2TP

Description from `https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol`

> The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. A virtue of transmission over UDP (rather than TCP; c.f. SSTP) is that it avoids the "TCP meltdown problem".[3][4] It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

Often used when crossing NAT, which everyone does ...

Configuration example for Cisco:

`https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14122-24.html`

OpenBSD L2TP IPsec

`https://www.exoscale.com/syslog/building-an-ipsec-gateway-with-openbsd/`

IPsec IKE-SCAN

Scan IPs for VPN endpoints with ike-scan:

```
root@kali:~# ike-scan 91.102.91.30
Starting ike-scan 1.9 with 1 hosts
(http://www.nta-monitor.com/tools/ike-scan/)
91.102.91.30 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=f0d6043badb2b7bc, msgid=f97a7508)

Ending ike-scan 1.9: 1 hosts scanned in 1.238 seconds (0.81 hosts/sec).
0 returned handshake; 1 returned notify
```

Source:

`http://www.nta-monitor.com/tools-resources/security-tools/ike-scan`

crack IKE psk?

`http://ikecrack.sourceforge.net/`

`https://www.trustwave.com/Resources/SpiderLabs-Blog/Cracking-IKE-Mission-Improbable-(Part-1)/`

Forward Secrecy

In cryptography, forward secrecy (FS), also known as perfect forward secrecy (PFS), is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if the private key of the server is compromised.[1] Forward secrecy protects past sessions against future compromises of secret keys or passwords.[2] By generating a unique session key for every session a user initiates, the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key.

Source: `https://en.wikipedia.org/wiki/Forward_secrecy`

Anbefalinger til VPN

Use the following guidelines when configuring Internet Key Exchange (IKE) in VPN technologies:
Avoid IKE Groups 1, 2, and 5.
Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively.
When possible, use IKE Group 19 or 20. They are the 256-bit and
384-bit ECDH groups, respectively.
Use AES for encryption.

Paper: `https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html`

- Certifikater/nøgler - ligesom TLS lange og rulles indimellem
- Algoritmer DES/3DES bye bye, husk både encryption og auth algoritmer
- DH-Group - +15 tak
- Check både client VPN og site-2-site
- Skift til IKEv2
- Selv disse råd er måske ikke tilstrækkelige nu!

Wi-Fi Security

Subjects

- Wifi standarder IEEE 802.11
- Authentication Protocols RADIUS, PAP, CHAP, EAP
- Port Based Network Access Control IEEE 802.1x
- Security problems in wireless protocols
- Security problems in wireless encryption
- Hacking wireless networks

Exercises you can do later:

- Wifi scanning, aka wardriving
- WPA hacking with a short password
  See for examples: `http://aircrack-ng.org/doku.php?id=cracking_wpa`

Wifi standarder IEEE 802.11

802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trådløse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen
- 802.11n endnu hurtigere
- 802.11i Security enhancements Robust Security Network RSN

New names soon:
Wi-Fi 6 to identify devices that support 802.11ax technology
Wi-Fi 5 to identify devices that support 802.11ac technology
Wi-Fi 4 to identify devices that support 802.11n technology

Kilde: `http://grouper.ieee.org/groups/802/11/index.html`

Værktøjer

- Wirelessscanner - Kali og Airodump
- Wireless Injection - aireplay-ng
- Aircrack-ng pakken generelt
- Kali `http://www.kali.org/`

Wireless networking sikkerhed i 802.11

Sikkerheden er baseret på nogle få forudsætninger

- SSID - netnavnet
- WEP *kryptering* - Wired Equivalent Privacy
- WPA kryptering - Wi-Fi Protected Access, SSID indgår i denne!
- måske MAC filtrering, kun bestemte kort må tilgå accesspoint
  Everyone can see the MAC in the air, so no security here

IEEE 802.11 Security fast forward

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by **Fluhrer, Mantin, and Shamir's** paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first **verification of the attack**. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

Source: `http://en.wikipedia.org/wiki/IEEE_802.11`

IEEE 802.11 Security fast forward

The IEEE set up a dedicated task group to create a replacement security solution, **802.11i** (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an **interim specification called Wi-Fi Protected Access (WPA)** based on a subset of the then current IEEE 802.11i draft. These started to appear in products in **mid-2003**. **IEEE 802.11i (also known as WPA2)** itself was ratified in **June 2004**, and uses government strength encryption in the **Advanced Encryption Standard AES,** instead of RC4, which was used in WEP. The modern recommended encryption for the home/consumer space is **WPA2 (AES Pre-Shared Key) and for the Enterprise space is WPA2 along with a RADIUS authentication server** (or another type of authentication server) and a strong authentication method such as EAP-TLS.

Source: `http://en.wikipedia.org/wiki/IEEE_802.11`

IEEE 802.11 Security fast forward

In January 2005, the IEEE set up yet another task group "w"to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.[24]

In **December 2011**, a security flaw was revealed that affects wireless routers with the **optional Wi-Fi Protected Setup (WPS)** feature. While WPS is not a part of 802.11, **the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours**.

WPS WTF?! - det er som om folk bevidst saboterer wireless sikkerhed!

Source: `http://en.wikipedia.org/wiki/IEEE_802.11`

airodump opsamling

BSSID	CH	MB	ENC	PWR	Packets	LAN IP / # IVs	ESSID
00:03:93:ED:DD:8D	6	11		209	**801963**	**540180**	wanlan

Når airodump kører opsamles pakkerne

Lås airodump fast til een kanal, -c eller –channel

Startes med airmon og kan skrive til capture filer:

```
airmon-ng start wlan0
airodump-ng --channel 6 --write testfil wlan0mon
```

WPA cracking med aircrack - start

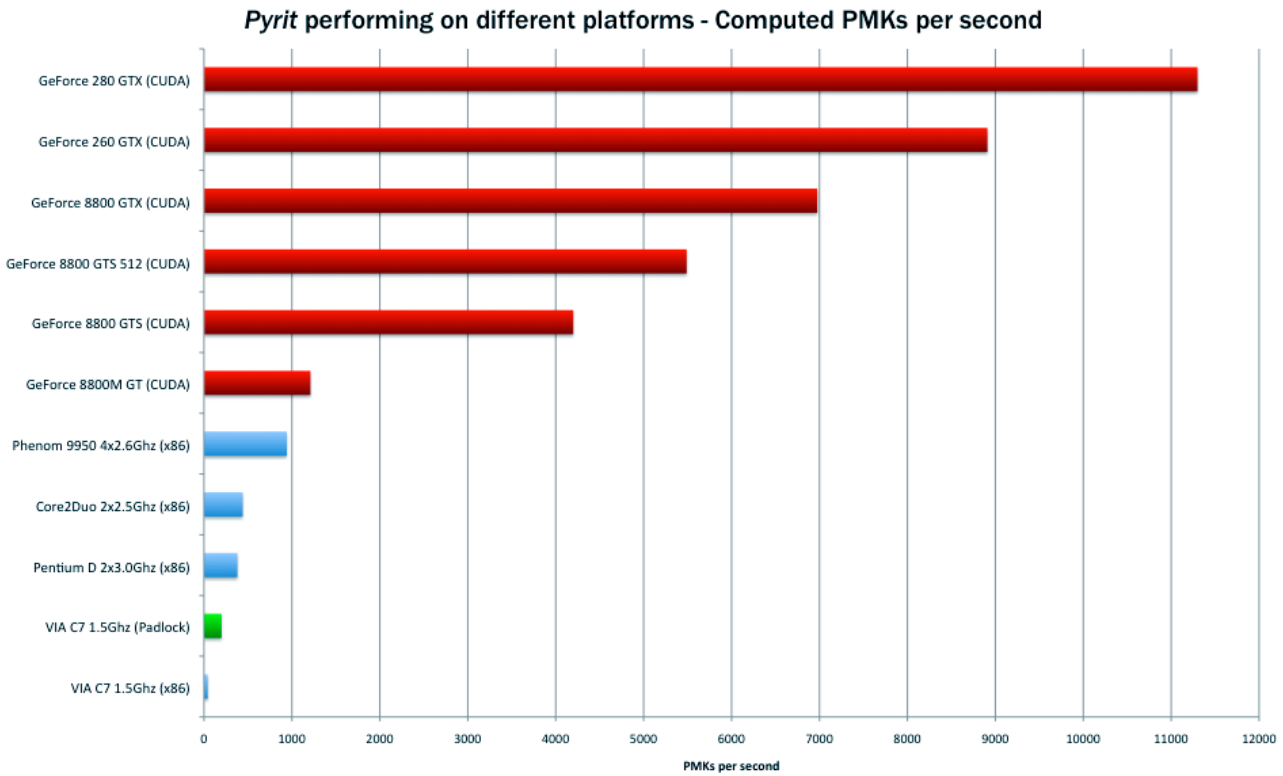
```
slax ~ # aircrack-ng -w dict wlan-test.cap
Opening wlan-test.cap
Read 1082 packets.

#  BSSID              ESSID           Encryption

1  00:11:24:0C:DF:97  wlan            WPA (1 handshake)
2  00:13:5F:26:68:D0  Noea            No data - WEP or WPA
3  00:13:5F:26:64:80  Noea            No data - WEP or WPA
4  00:00:00:00:00:00                  Unknown

Index number of target network ?  1
```

WPA cracking med aircrack - start

```
          [00:00:00] 0 keys tested (0.00 k/s)

                     KEY FOUND! [ Henrik42 ]

Master Key     : 8E 61 AB A2 C5 25 4D 3F 4B 33 E6 AD 2D 55 6F 76
                 6E 88 AC DA EF A3 DE 30 AF D8 99 DB F5 8F 4D BD
Transcient Key : C5 BB 27 DE EA 34 8F E4 81 E7 AA 52 C7 B4 F4 56
                 F2 FC 30 B4 66 99 26 35 08 52 98 26 AE 49 5E D7
                 9F 28 98 AF 02 CA 29 8A 53 11 EB 24 0C B0 1A 0D
                 64 75 72 BF 8D AA 17 8B 9D 94 A9 31 DC FB 0C ED

EAPOL HMAC     : 27 4E 6D 90 55 8F 0C EB E1 AE C8 93 E6 AC A5 1F
```

Min Thinkpad X31 med 1.6GHz Pentium M knækker ca. 150 Keys/sekund

Tired of WoW?



Kilde: `http://code.google.com/p/pyrit/`

Encrypt where?

> It is not clear that the link layer is the right one for security. In a coffeeshop, the security association is terminated by the store: is there any reason you should trust the shopkeeper? Perhaps link-layer security makes some sense in a home, where you control both the access point and the wireless machines. However, we prefer end-to-end security at the network layer or in the applications.

Source: Cheswick-chap2.pdf Firewalls and Internet Security: Repelling the Wily Hacker , Second Edition, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin

Individual Authentication

Erstatning for eet kodeord WEP – WPA

Det anbefales at bruge:

Kendte VPN teknologier eller WPA

baseret på troværdige algoritmer

implementeret i professionelt udstyr

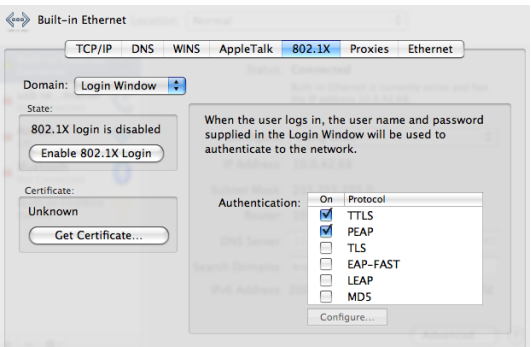
fra troværdige leverandører

udstyr der vedligeholdes og opdateres

Der findes idag andre metoder til sikring af trådløse netværk
IEEE 802.1x Port Based Network Access Control

Lav flere VLANs!

IEEE 802.1x Port Based Network Access Control



- Access points og switche tillader at man benytter IEEE 802.1x
- Denne protokol sikrer at man valideres før der gives adgang til porten
- Når systemet skal have adgang til porten afleveres brugernavn og kodeord/certifikat
- Denne protokol indgår også i WPA Enterprise
- Typisk benyttes RADIUS og IEEE 802.1x integrerer således mod både LDAP og Active Directory
- MAC filtrering kan spoofes, hvor IEEE 802.1x kræver det rigtige kodeord

Authentication Protocols RADIUS, PAP, CHAP, EAP

- Used for verifying credentials, typically username and password
- Extensible Authentication Protocol EAP
  `https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol`
- Challenge-Handshake Authentication Protocol
  `https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol`
- Password Authentication Protocol
  `https://en.wikipedia.org/wiki/Password_Authentication_Protocol`

Remote Authentication Dial-In User Service RADIUS

RADIUS er en protokol til autentificering af brugere op mod en fælles server

Remote Authentication Dial In User Service (RADIUS)

RADIUS er beskrevet i RFC-2865

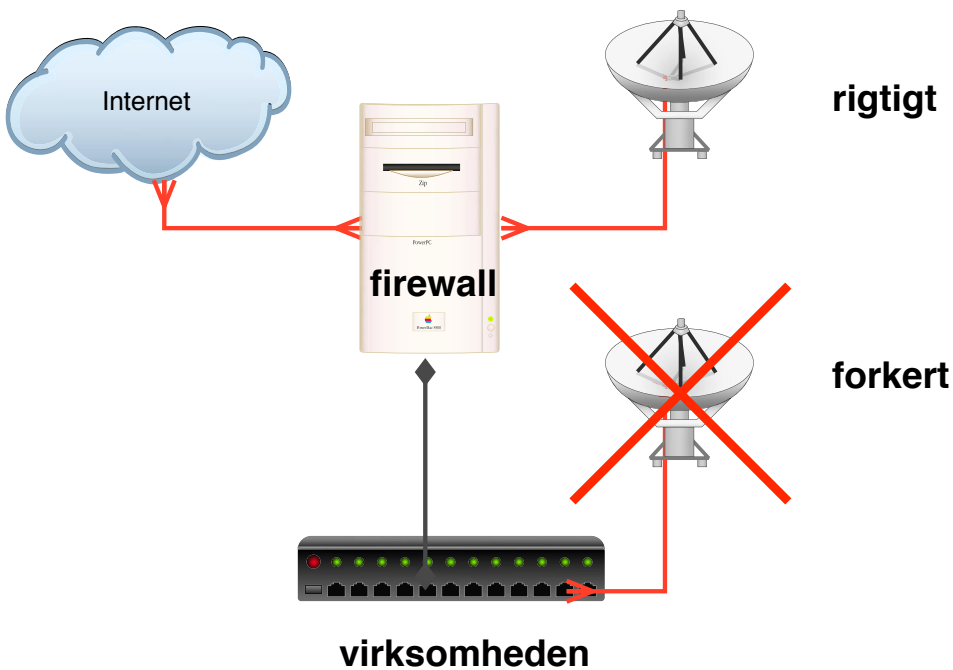
RADIUS kan være en fordel i større netværk med

- dial-in
- administration af netværksudstyr
- trådløse netværk
- andre RADIUS kompatible applikationer

`https://en.wikipedia.org/wiki/RADIUS`

Hint: Jeg har publiceret en RADIUS konfiguration der giver WPA Enterprise - med vilkårligt brugernavn og kode!
`https://github.com/kramse/conference-open-8021x`

Infrastrukturændringer



Sådan bør et access point logisk forbindes til netværket med VLAN

Network segmentation – Firewalls

`https://en.wikipedia.org/wiki/Firewall_(computing)`
`http://www.wilyhacker.com/` Cheswick chapter 2 og 3 PDF

Skim chapters from 1st edition:
`http://www.wilyhacker.com/1e/chap03.pdf`
`http://www.wilyhacker.com/1e/chap04.pdf`

The next time you are at your console, review some logs. You might think. . . "I don't know what to look for". Start with what you know, understand, and don't care about. Discard those. Everything else is of interest.
Semper Vigilans, Mike Poor

Firewalls Definition

> In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.[2]

Source: Wikipedia `https://en.wikipedia.org/wiki/Firewall_(computing)`

Cheswick chapter 2 PDF *A Security Review of Protocols: Lower Layers*
`http://www.wilyhacker.com/`

- Network layer, packet filters, application level, stateless, stateful

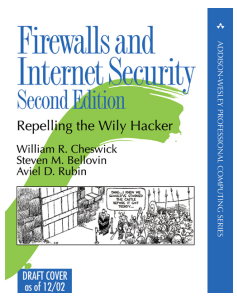
Firewalls are by design a choke point, natural place
to do network security monitoring!

Generic IP Firewalls

En firewall er noget som blokerer traffik på Internet

En firewall er noget som tillader traffik på Internet

Firewall historik



Firewalls har været kendt siden starten af 90'erne

Første bog *Firewalls and Internet Security* udkom i 1994 men kan stadig anbefales, læs den på `http://www.wilyhacker.com/`

2003 kom den i anden udgave *Firewalls and Internet Security* William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley, 2nd edition

Firewallrollen idag

Idag skal en firewall være med til at:

- Forhindre angribere i at komme ind
- Forhindre angribere i at sende traffik ud
- Forhindre virus og orme i at sprede sig i netværk
- Indgå i en samlet løsning med ISP, routere, firewalls, switchede strukturer, intrusion detection systemer samt andre dele af infrastrukturen

Det kræver overblik!

Modern Firewalls

Basalt set et netværksfilter

Indeholder typisk:

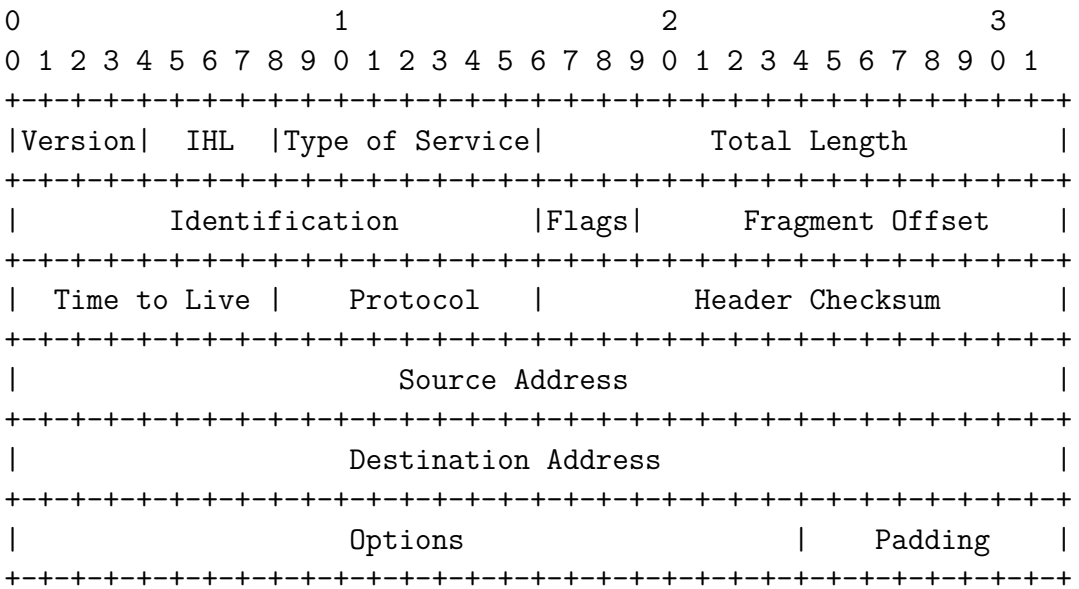
- Grafisk brugergrænseflade til konfiguration - er det en fordel?
- TCP/IP filtermuligheder - pakkernes afsender, modtager, retning ind/ud, porte, protokol, ...
- både IPv4 og IPv6
- foruddefinerede regler/eksempler - er det godt hvis det er nemt at tilføje/åbne en usikker protokol?
- typisk NAT funktionalitet indbygget
- typisk mulighed for nogle serverfunktioner: kan agere DHCP-server, DNS caching server og lignende

En router med Access Control Lists - kaldes ofte netværksfilter,
mens en dedikeret maskine kaldes firewall, ca same – same

Sample rules from OpenBSD PF

```
# hosts and networks
router="217.157.20.129"
webserver="217.157.20.131"
homenet=" 192.168.1.0/24, 1.2.3.4/24 "
wlan="10.0.42.0/24"
wireless=wi0
set skip lo0
# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "

# default block anything
block in all
# egress and ingress filtering - disallow spoofing, and drop spoofed
block in quick from $spoofed to any
block out quick from any to $spoofed

pass in on $wireless proto tcp from { $wlan $homenet } to any port = 22
pass in on $wireless proto tcp from any to $webserver port = 80

pass out
```

Packet filtering



Packet filtering er firewalls der filtrerer på IP niveau

Idag inkluderer de fleste stateful inspection

Kommercielle firewalls

- Checkpoint Firewall-1 `http://www.checkpoint.com`
- Cisco ASA `http://www.cisco.com`
- Clavister firewalls `http://www.clavister.com`
- Juniper SRX `http://www.juniper.net`
- Palo Alto `https://www.paloaltonetworks.com/`
- Fortinet `https://www.fortinet.com/`

Ovenstående er dem som jeg oftest ser ude hos mine kunder i Danmark

Open source baserede firewalls

- Linux firewalls IP tables, use command line tool ufw Uncomplicated Firewall!
- Firewall GUIs ovenpå Linux - mange! nogle er kommercielle produkter
- OpenBSD PF `http://www.openbsd.org`
- FreeBSD IPFW og IPFW2 `http://www.freebsd.org`
- Mac OS X benytter OpenBSD PF
- FreeBSD inkluderer også OpenBSD PF

NB: kun eksempler og dem jeg selv har brugt

Anbefaler UFW Uncomplicated Firewall

```
root@debian01:~# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian01:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Langt nemmere at bruge

Firewall konfiguration

Den bedste firewall konfiguration starter med:

- Papir og blyant
- En fornuftig adressestruktur

Brug dernæst en firewall med GUI første gang!

Husk dernæst:

- En firewall skal passes
- En firewall skal opdateres
- Systemerne bagved skal hærdes!

Bloker indefra og ud

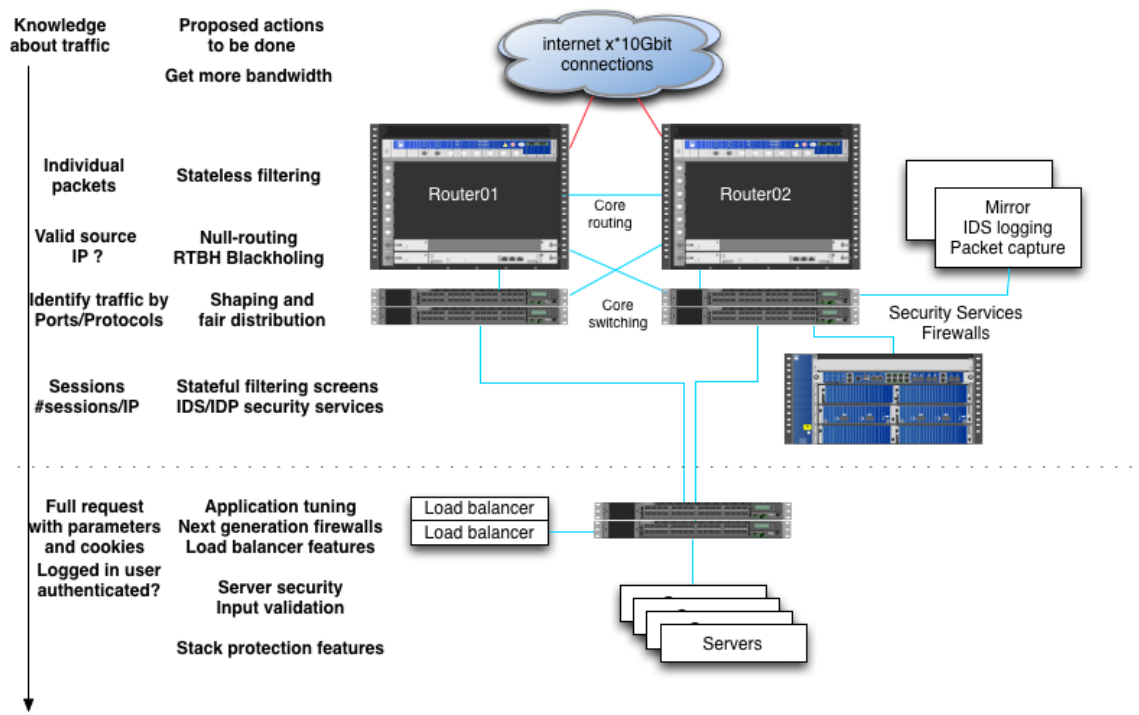
Der er porte og services som altid bør blokeres

Det kan være kendte sårbare services

- Windows SMB filesharing - ikke til brug på Internet!
- UNIX NFS - ikke til brug på Internet!

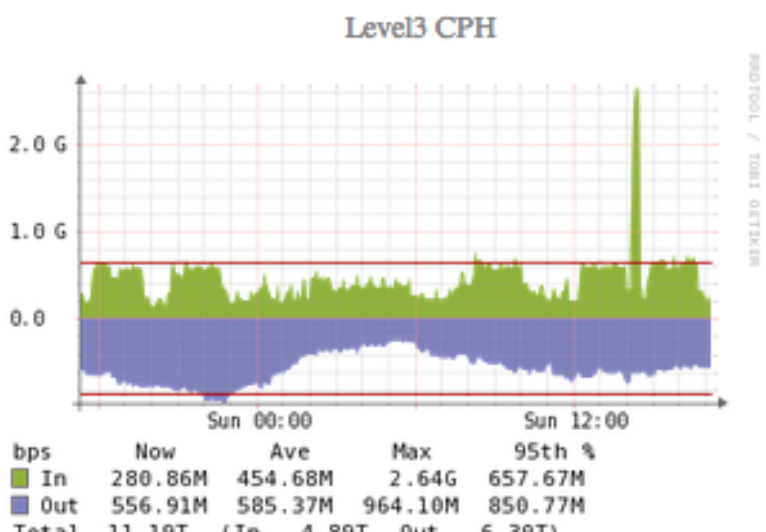
Kendte problemer som minimum

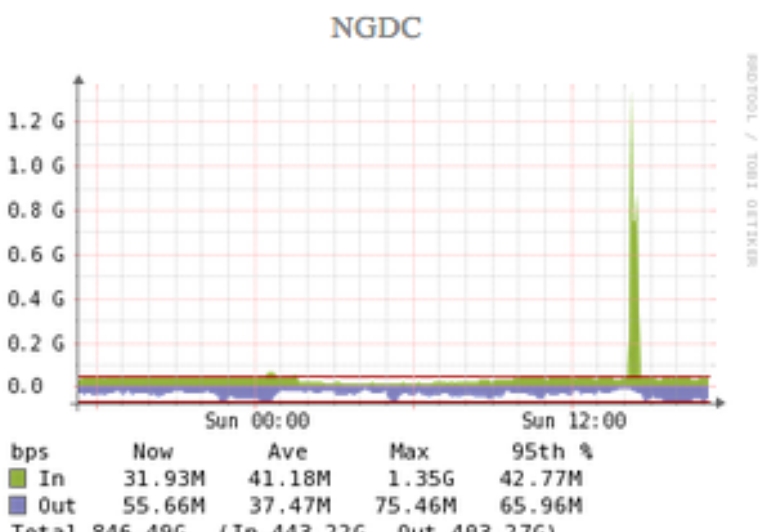
Firewall er ikke alene



Forsvaret er som altid - flere lag af sikkerhed!

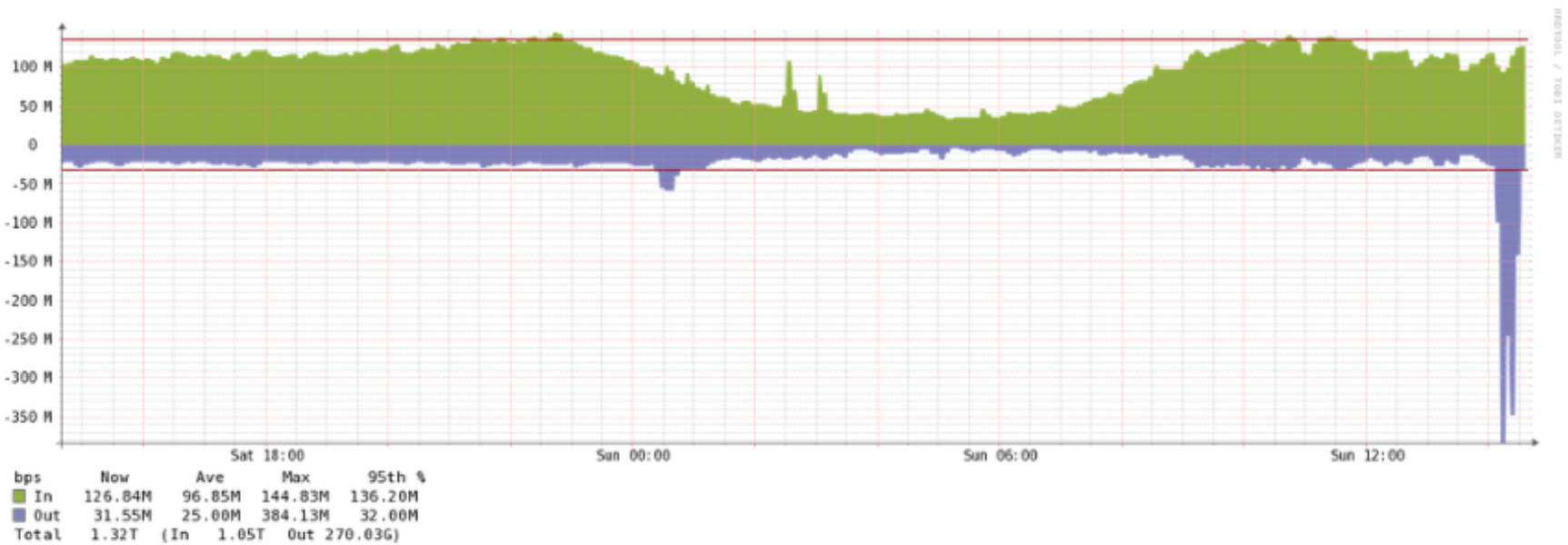
DDoS traffic before filtering





Only two links shown, at least 3Gbit incoming for this single IP

DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Better to filter stateless before traffic reaches firewall, less work!

Access Control Lists (ACL)

Stateless firewall filter throw stuff away

```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a sample, maybe use BGP flowspec and/or RTBH */
term edgeblocker {
    from {
        source-address {
            84.180.xxx.173/32;
...
            87.245.xxx.171/32;
        }
        destination-address {
            91.102.91.16/28; }
        protocol [ tcp udp icmp ]; }
    then discard;
}
```

Hint: can also leave out protocol and then it will match all protocols

Stateless firewall filter limit protocols

```
term limit-icmp {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-100M;
        accept;
    }
}
term limit-udp {
    from {
        protocol udp;
    }
    then {
        policer UDP-1000M;
        accept;
    }
}
```

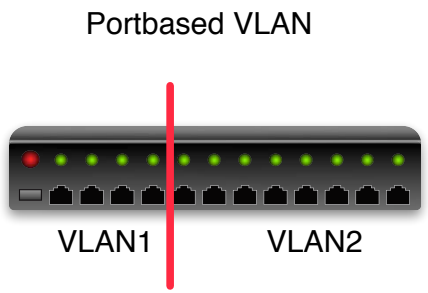
Routers also have extensive Class-of-Service (CoS) tools today

Strict filtering for some servers, still stateless!

```
term some-server-allow {
    from {
        destination-address {
            109.238.xx.0/xx;
        }
        protocol tcp;
        destination-port [ 80 443 ];
    } then accept;
}
term some-server-block-unneeded {
    from {
        destination-address {
            109.238.xx.0/xx; }
        protocol-except icmp;  }
    then { count some-server-block; discard;
    }
}
```

Wut - no UDP, yes UDP service is not used on these servers

Together with Firewalls - VLAN Virtual LAN



Nogle switche tillader at man opdeler portene

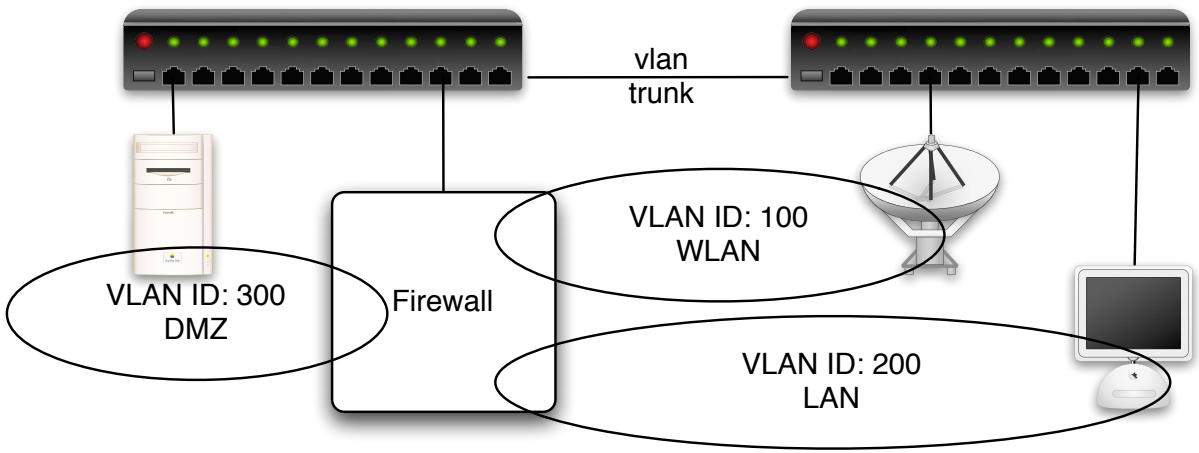
Denne opdeling kaldes VLAN og portbaseret er det mest simple

Port 1-4 er et LAN

De resterende er et andet LAN

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

IEEE 802.1q



Med IEEE 802.1q tillades VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Port Security – Rogue DHCP servers

Common problem in networks is people connecting devices with DHCPD servers

In general make sure to segment networks

Start to use port security on switches, including DHCP snooping
`https://en.wikipedia.org/wiki/DHCP_snooping`

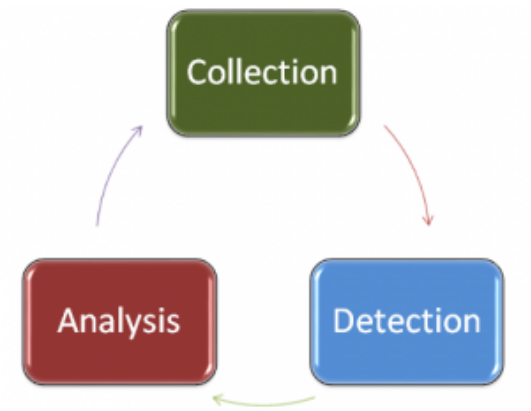
Example port security

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 4
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
set interface ge-0/0/2 mac-limit 4
set interface ge-0/0/1 persistent-learning
set interface ge-0/0/8 dhcp-trusted
set vlan employee-vlan arp-inspection
set vlan employee-vlan examine-dhcp
set vlan employee-vlan mac-move-limit 5
```

Source: Overview of Port Security, Juniper

https://www.juniper.net/documentation/en_US/junos/topics/example/overview-port-security.html

Most firewalls include some detection today



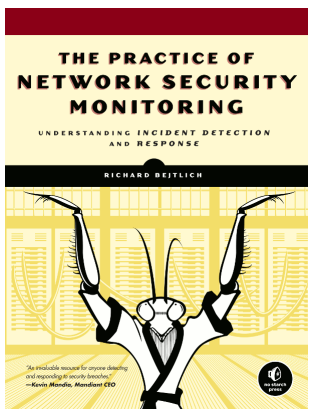
ANSM chapter 1: The Practice of Applied Network Security Monitoring

- Vulnerability-Centric vs. Threat-Centric Defense
- The NSM cycle: collection, detection, and analysis
- Full Content Data, Session Data, Statistical Data, Packet String Data, and Alert Data
- Security Onion is nice, but a bit over the top - quickly gets overloaded

Intrusion Detection

- networkbased intrusion detection systems (NIDS)
- host based intrusion detection systems (HIDS)

Network Security Monitoring



Network Security Monitoring (NSM) - monitoring networks for intrusions, and reacting to those

Recommend the book *The Practice of Network Security Monitoring Understanding Incident Detection and Response* by Richard Bejtlich July 2013

Example systems are Security Onion `https://securityonion.net/` or SELKS `https://www.stamus-networks.com/open-source/`

Indicators of Compromise and Signatures

An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.

When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Bro-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

Network Sniffing for Security

ANSM chapter 3:The Sensor Platform

- Full Packet Capture (FPC) Data
- Session Data
- Statistical Data
- Packet String (PSTR) Data
- Log Data
- Sensor Placement, designing etc.

Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders ISBN: 9780124172081 - shortened ANSM

Netflow

Netflow is getting more important, more data share the same links

Accounting is important

Detecting DoS/DDoS and problems is essential

Netflow sampling is vital information - 123Mbit, but what kind of traffic

NFSen is an old but free application `http://nfsen.sourceforge.net/`

Currently also investigating sFlow - hopefully more fine grained

sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model,
`https://en.wikipedia.org/wiki/SFlow`

Collect Network Evidence from the network

Network Flows

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share the following 7 values:

- Ingress interface (SNMP ifIndex)
- IP protocol, Source IP address and Destination IP address
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

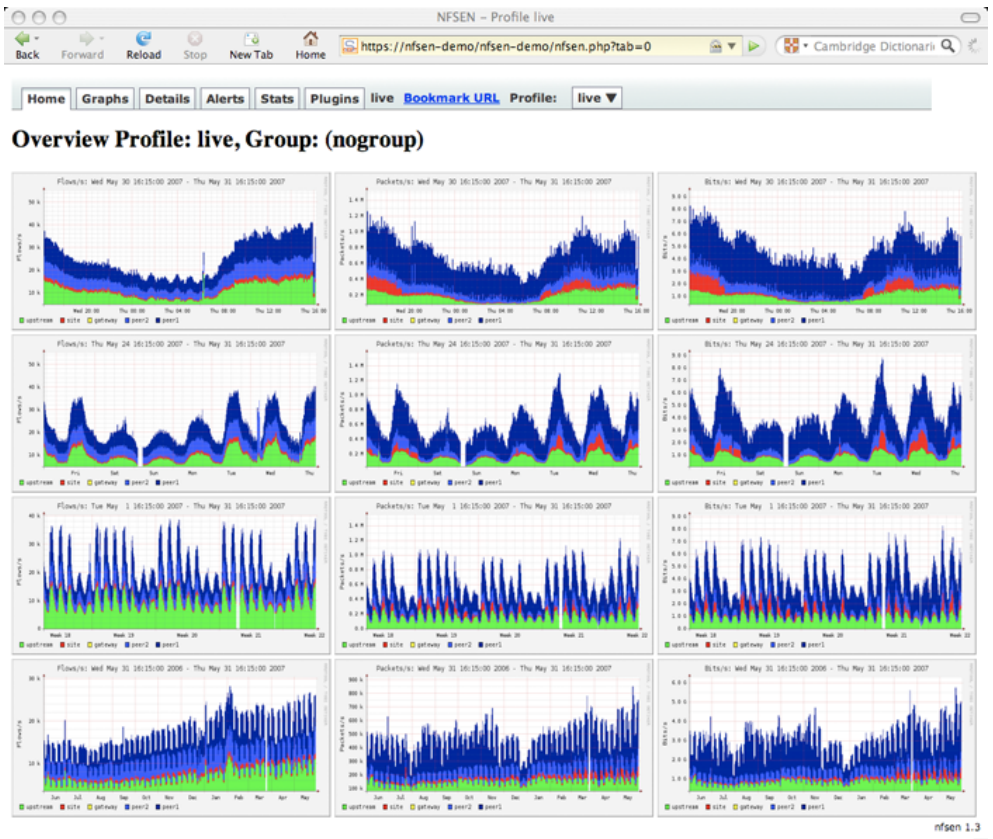
today Netflow version 9 or IPFIX

Source:

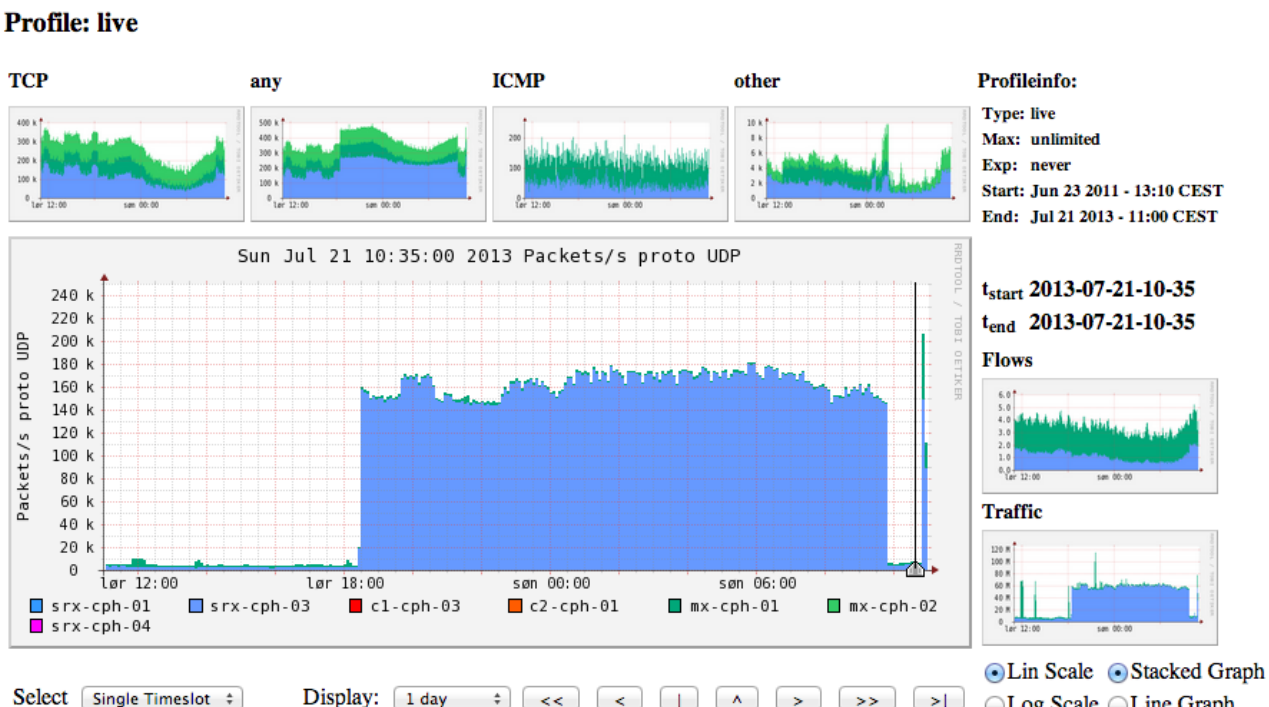
`https://en.wikipedia.org/wiki/NetFlow`

`https://en.wikipedia.org/wiki/IP_Flow_Information_Export`

Netflow using NFSen



Netflow NFSen



An extra 100k packets per second from this netflow source (source is a router)

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

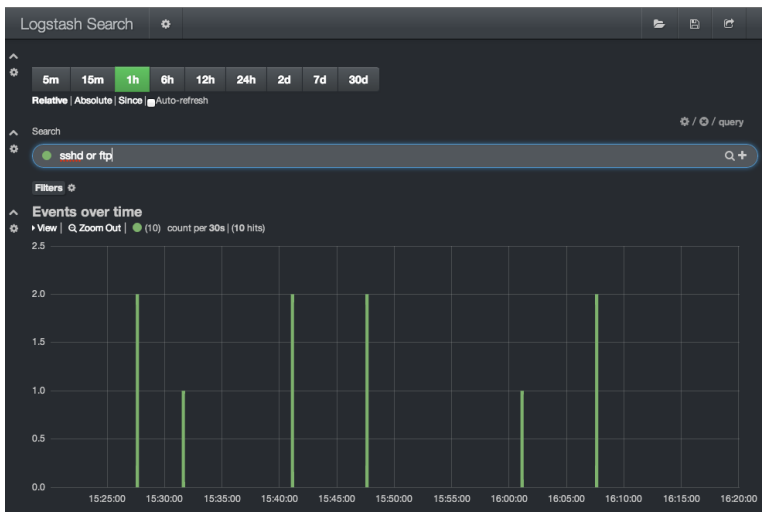
- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

View data efficiently

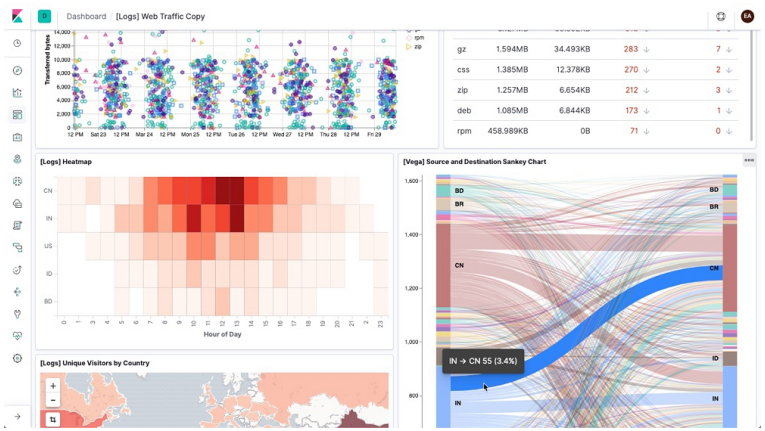


View data by digging into it easily - must be fast

Logstash and Kibana are just examples, but use indexing to make it fast!

Other popular examples include Graylog and Grafana

Big Data tools: Elasticsearch



Elasticsearch is an open source distributed, RESTful search and analytics engine capable of solving a growing number of use cases.

`https://www.elastic.co`

We are all Devops now, even security people!

Kibana

Highly recommended for a lot of data visualisation

Non-programmers can create, save, and share dashboards

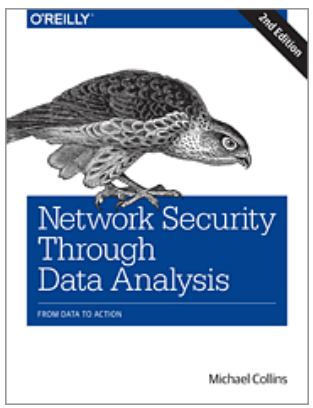
Source: `https://www.elastic.co/products/kibana`

Ansible configuration management

```
- apt: name= item  state=latest
  with_items:
        - unzip
        - elasticsearch
        - logstash
        - redis-server
        - nginx
- lineinfile: "dest=/etc/elasticsearch/elasticsearch.yml state=present
  regexp='script.disable_dynamic: true' line='script.disable_dynamic: true'"
- lineinfile: "dest=/etc/elasticsearch/elasticsearch.yml state=present
  regexp='network.host: localhost' line='network.host: localhost'"
- name: Move elasticsearch data into /data
  command: creates=/data/elasticsearch mv /var/lib/elasticsearch /data/
- name: Make link to /data/elasticsearch
  file: state=link src=/data/elasticsearch path=/var/lib/elasticsearch
```

only requires SSH+python `http://www.ansible.com`

Network Security Through Data Analysis



Low page count, but high value! Recommended.

Network Security through Data Analysis, 2nd Edition By Michael S Collins Publisher: O'Reilly Media 2015-05-01: Second release, 348 Pages

New Release Date: August 2017

Packet sniffing tools

Tcpdump for capturing packets

Wireshark for dissecting packets manually with GUI

Zeek Network Security Monitor

Snort, old timer Intrusion Detection Engine (IDS)

Suricata, modern robust capable of IDS and IPS (prevention)

ntopng High-speed web-based traffic analysis

Maltrail Malicious traffic detection system `https://github.com/stamparm/MalTrail`

Often a combination of tools and methods used in practice

Full packet capture big data tools also exist

Exercise at home – Your lab setup

- Go to GitHub, Find user Kramse, click through security-courses, courses, suricatazeek and download the PDF files for the slides and exercises:

  `https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop`

- Get the lab instructions, from

  `https://github.com/kramse/kramse-labs/tree/master/suricatazeek`

Blue Team

Think like a blue team member find hacker traffic

Get basic tools running

Improve situation

- See where the data end up
- What kind of data and metadata can we extract
- How can we collect and make use of it
- Databases and web interfaces, examples shown
- Consider what your deployment could be

Experiences gathered

Lots of information

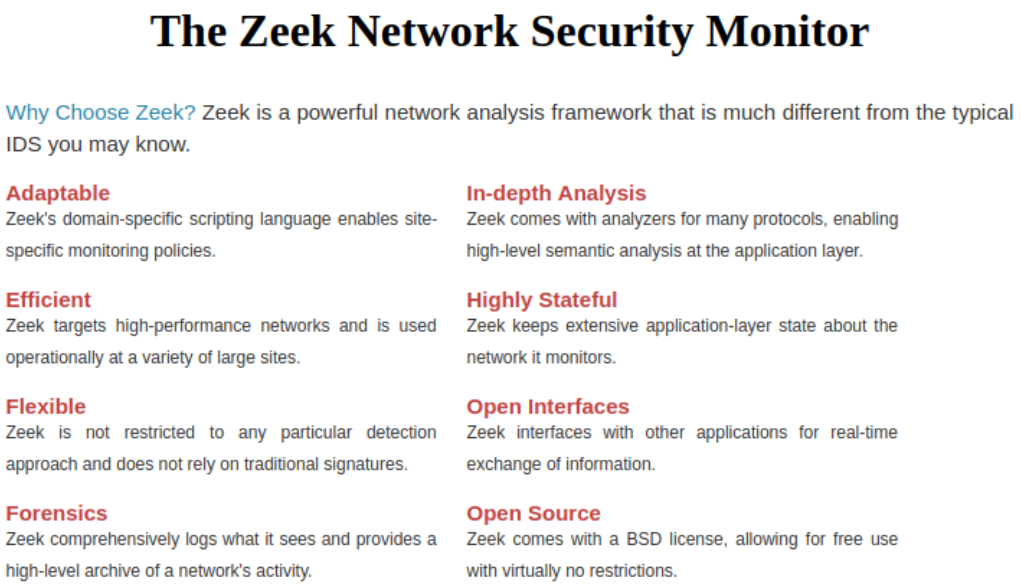
Reveals a lot about the network, operating systems, services etc.

I use a template when getting data

- Respond to ICMP: ☐ echo, ☐ mask, ☐ time
- Respond to traceroute: ☐ ICMP, ☐ UDP
- Open ports TCP og UDP:
- Operating system:
- ... (banner information)

Beware when doing scans it is possible to make routers, firewalls and devices perform badly or even crash!

The Zeek Network Security Monitor



The Zeek Network Security Monitor

Why Choose Zeek? Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Zeek's domain-specific scripting language enables site-specific monitoring policies.

In-depth Analysis
Zeek comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Efficient
Zeek targets high-performance networks and is used operationally at a variety of large sites.

Highly Stateful
Zeek keeps extensive application-layer state about the network it monitors.

Flexible
Zeek is not restricted to any particular detection approach and does not rely on traditional signatures.

Open Interfaces
Zeek interfaces with other applications for real-time exchange of information.

Forensics
Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

Open Source
Zeek comes with a BSD license, allowing for free use with virtually no restrictions.

The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework

Zeek is the tool formerly known as Bro, changed name in 2018. `https://www.zeek.org/`

Zeek IDS is

The Zeek Network Security Monitor

While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

`https://www.Zeek.org/`

Zeek scripts

```
global dns_A_reply_count=0;
global dns_AAAA_reply_count=0;
...
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
        {
        ++dns_A_reply_count;
        }

event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
        {
        ++dns_AAAA_reply_count;
        }
```

source: dns-fire-count.bro from

https://github.com/LiamRandall/bro-scripts/tree/master/fire-scripts https://www.bro.org/sphinx-git/script-refe

scripts.html

Testing Zeek

We will use a combination of your virtual servers, my switch hardware and my virtual systems.

There will be sniffing done on traffic! Don't abuse information gathered

We try to mimic what you would do in your own networks during the exercises.

Another way of running exercises might be:
`https://github.com/jonschipp/ISLET`

Recommended and used by Zeek and Suricata projects.

Get Started with Zeek

To run in "base" mode: `bro -r traffic.pcap`

To run in a "near broctl" mode: `bro -r traffic.pcap local`

To add extra scripts: `bro -r traffic.pcap myscript.bro`

Note: the project was renamed from Bro to Zeek in Oct 2018

Zeek demo: Run Zeek

```
// back to Broctl and start it
[BroControl] > start
starting bro
// and then
kunoichi:bro root# pwd
/usr/local/var/spool/bro
kunoichi:bro root# tail -f dns.log
```

More examples at:

https://www.bro.org/sphinx/script-reference/log-files.html

DNS is important

Another tool that provides a basic SQL-frontend to PCAP-files
`https://www.dns-oarc.net/tools/packetq`
`https://github.com/DNS-OARC/PacketQ`

Going back in time and finding systems that visited a specific domain can explain when and where an infection started.

Deciding on which tool to use, Zeek or PacketQ depends on the situation.

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

`http://suricata-ids.org/` `http://openinfosecfoundation.org`

Questions?

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

You are always welcome to send me questions later via email

Email: hkj@zencurity.dk Mobile: +45 2026 6000

Extras

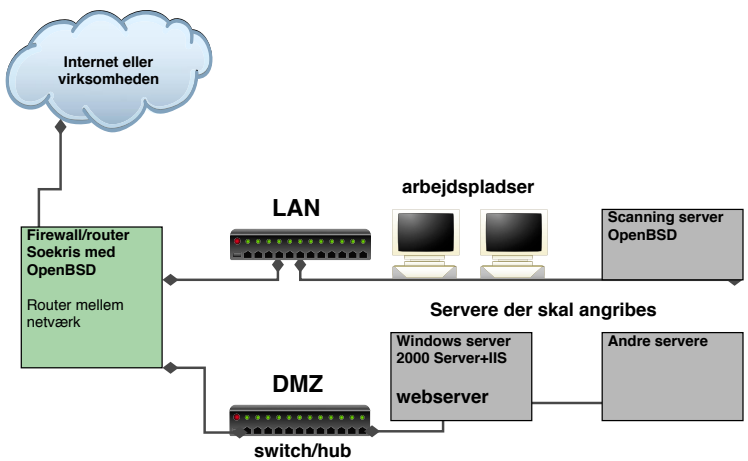
Netværksdesign og sikkerhed

Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switche - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Husk du skal også kunne opdatere dine servere

Basic Network Security Pattern Isolate in VLANs



Du bør opdele dit netværk i segmenter efter traffik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Pattern use IDS to get flow, connections and data

Use Intrusion Detection Systems - IDS

Angrebsværktøjerne efterlader spor

Det anbefales at have IDS og flow opsamling som minimum

Hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

Network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik - FØR angreb
- analyse af netværk under angreb - sender en alarm

Drift og Planlægning af sikre miljøer

Før installationen scope

- Hvad er formålet - reaktion eller "statistik"
- Hvor skal der måles - hele netværket eller specifikke dele
- Hvad skal måles og hvilke operativsystemer og servere/services

Implementationen

- Er infrastrukturen iorden som den er
- Er der gode målepunkter - monitorporte
- Et målepunkt eller flere, Hvor meget trafik skal måles

Selve idriftsættelsen

- Ændringer af infrastrukturen
- Installation af udstyret og test af udstyret udenfor drift
- Installation i driftsmiljøet
- Test af udstyret i driftsmiljøet

Eksempel Opsætning og konfiguration af IDS miljøer

Vælg en simpel installation til at starte med!

Undgå for alt i verden for meget information

- Start med en enkelt sensor
- Byg en server med database og "brugerværktøjer"
- Start med at overvåge dele af nettet
- Brug et specifikt regelsæt i starten - eksempelvis kun Windows eller kun UNIX
- Lav nogle simple rapporter til at starte med

Gør netværket mere sikkert før du lytter på hele netværket

Brug tcpdump/Ethereal til at se på trafik, lær IP pakker at kende

Brug Suricata og Zeek til at evaluere

- Husk at man kan starte med vilkårligt værktøj og senere skifte til andre produkter
- Praktisk erfaring med eget netværk er nødvendigt og værdifuldt

Honeypots

Man kan udover IDS installere en honeypot

En honeypot består typisk af:

- Et eller flere sårbare systemer
- Et eller flere systemer der logger traffik til og fra honeypot systemerne

Meningen med en honeypot er at den bliver angrebet og brudt ind i

Forslag undgå standard indstillinger

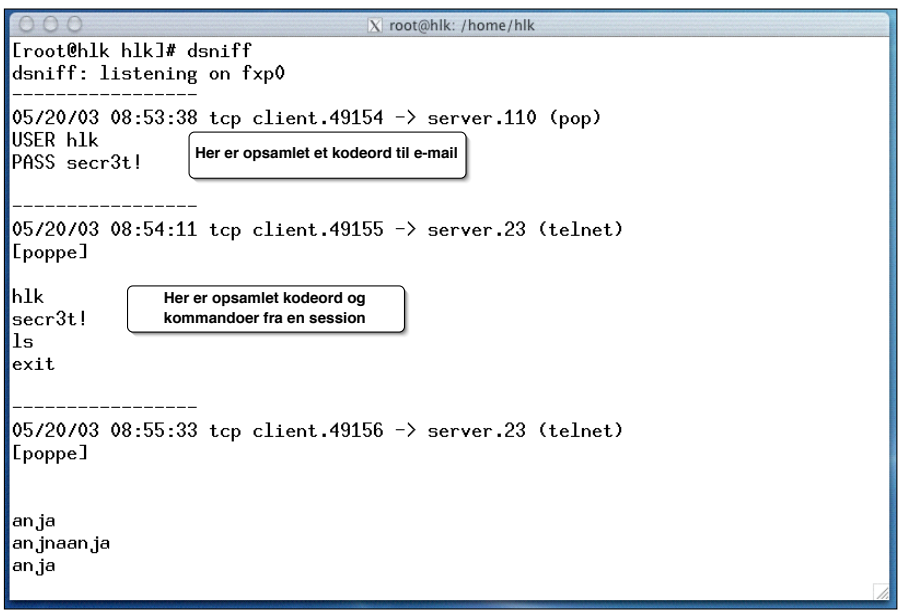
Giv jer selv mere tid til at patche og opdatere

Tiden der går fra en sårbarhed annonceres på internet til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist

NB: ingen garanti

Brug krypterede forbindelser



Især på utroværdige netværk kan det give problemer at benytte sårbare protokoller

Mission 1: Kommunikere sikkert

Du må ikke bruge ukrypterede forbindelser til at administrere netværk eller servere

Du må ikke sende kodeord i ukrypterede e-mail beskeder

Telnet daemonen - telnetd må og skal dø!
FTP daemonen - ftpd må og skal dø!
POP3 daemonen port 110 må og skal dø!
IMAPD daemonen port 143 må og skal dø!

væk med alle de ukrypterede forbindelser!

Pattern: erstat Telnet med SSH

Telnet er død!

Brug altid Secure Shell fremfor Telnet

Opgrader firmware til en der kan SSH, eller køb bedre udstyr næste gang

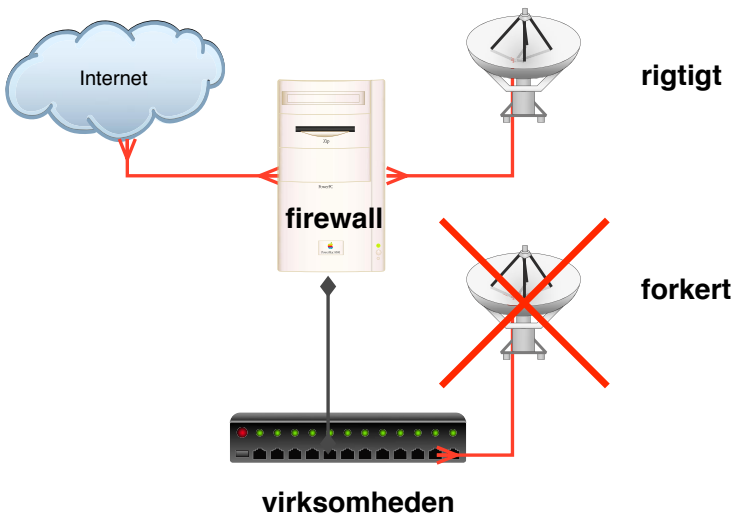
Selv mine små billige Linksys switche forstår SSH!

Pattern: erstat FTP med HTTP

Hvis der kun skal distribueres filer kan man ofte benytte HTTP istedet for FTP

Hvis der skal overføres med password er SCP/SFTP fra Secure Shell at foretrække

Anti-pattern WLAN forbundet direkte til LAN



WLAN AP'er forbundet direkte til LAN giver risiko for at sikkerheden brydes, fordi AP falder tilbage på den usikre standardkonfiguration

Ved at sætte WLAN direkte på LAN risikerer man at eksterne får direkte adgang

Pattern individuel autentificering!

ssh root@server1

Mange systemer administreres fejlagtigt ved brug af root-login eller andet delt administrator login

Undgå direkte root-login

Insister på `sudo` eller `su`

Hvorfor?

- Sporbarheden mistes hvis brugere logger direkte ind som root
- Hvis et kodeord til root gættes er der direkte adgang til alt!

At være på internet

RFC-2142 Mailbox Names for Common Services, Roles and Functions

Du BØR konfigurere dit domæne til at modtage post for følgende adresser:

- postmaster@domæne.dk
- abuse@domæne.dk
- webmaster@domæne.dk, evt. www@domæne.dk

Du gør det nemmere at rapportere problemer med dit netværk og services

E-mail best current practice

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries
...		
MAILBOX	SERVICE	SPECIFICATIONS
POSTMASTER	SMTP	[RFC821], [RFC822]
HOSTMASTER	DNS	[RFC1033-RFC1035]
USENET	NNTP	[RFC977]
NEWS	NNTP	Synonym for USENET
WEBMASTER	HTTP	[RFC 2068]
WWW	HTTP	Synonym for WEBMASTER
UUCP	UUCP	[RFC976]
FTP	FTP	[RFC959]

Kilde: RFC-2142 Mailbox Names for Common Services, Roles and Functions. D. Crocker. May 1997

RIPE NCC abuse-c

The RIPE NCC began implementing a new policy in 2013 to ensure that all resources allocated and assigned by the RIPE NCC include an "abuse-c:" attribute. The idea behind the policy is to make it easier for end users to find abuse contact information to report abuse to the appropriate resource holder, and to give resource holders a single, consistent place to include this information in the RIPE Database.

The "abuse-c:" attribute is contained within the **organisation** object, and references a **role** object containing abuse contact information in an "abuse-mailbox:" attribute. All the **organisation** objects linked by the resources you manage (both IPv4 and IPv6) must contain an "abuse-c:" attribute.

Relationship between RIPE Database objects involved in abuse-c

`https://www.ripe.net/manage-ips-and-asns/resource-management/abuse-c-information`

Hardened network device configurations

Alle services skal være konfigureret korrekt:

- Administration kun fra jump host og egne administrator netværk, SSH og HTTPS
- Alle protokoller med mulighed for *secrets* bør evalueres for om det skal benyttes
- Protokoller som BGP skal benytte route import filtre
- Protokoller som OSPF bør benytte policies OG secrets
- Brug, Router protect filter således at kun relevant adgang tillades til services på udstyret
- Brug Reverse Path Forwarding uRPF / RPF

Check you network from outside

How does your network look like from the outside?

Check your network using:

`https://stat.ripe.net/`

Consider:

- Join the NLNOG RING `https://ring.nlnog.net/`
- `https://bgpmon.net/` - commercial tool, some alternatives exist
- `https://shadowserver.org/wiki/` sign up for Shadowserver - ASN & Netblock Alerting & Reporting Service