Aalto University
School of Electrical
Engineering

Basic Principles in Networking

IPsec and VPN

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

Version 1.0

Aalto University
School of Electrical
Engineering

Motivation (5 min)

Most dangerous new attacks (RSA 2020)

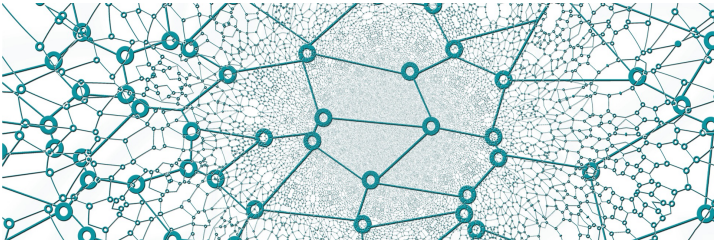
Aalto University
School of Electrical
Engineering

Part I (20 min)

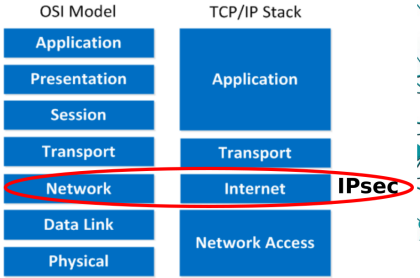
IPsec

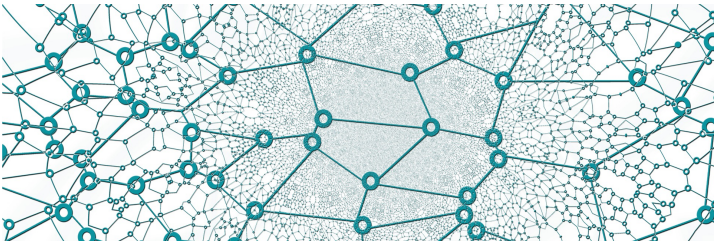
IPSec

OSI Model	TCP/IP Stack
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Network Access
Physical	

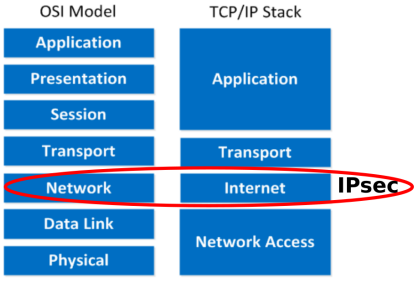


IPSec


OSI Model
TCP/IP Stack
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Transport
Internet
Network Access
IPsec

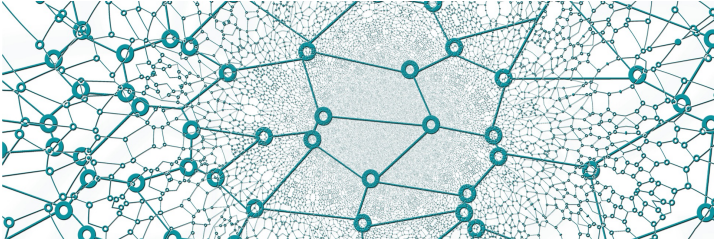


IPSec

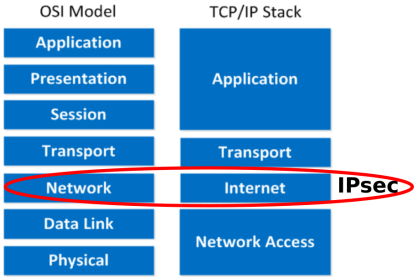


With confidentiality at network layer ...

...all protocol and type information hidden
(e.g. TCP, UDP, ICMP, SMTP, ...)

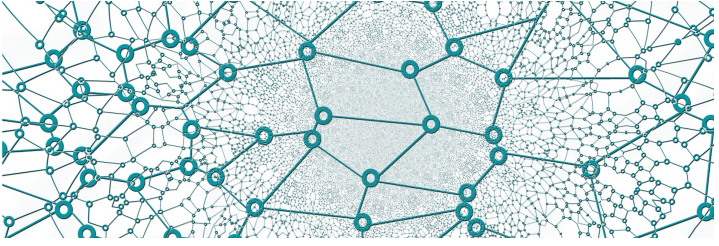


IPSec



With confidentiality at network layer ...

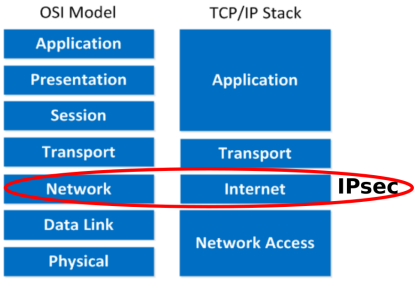
...all protocol and type information hidden (e.g. TCP, UDP, ICMP, SMTP, ...)



IPSec Services

1. confidentiality
2. authentication
3. data integrity
4. replay-attack prevention

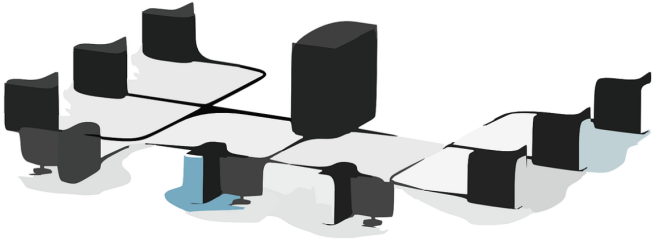
IPSec



Private Network (PN)

Stand-alone physical network including routers, links and DNS infrastructure

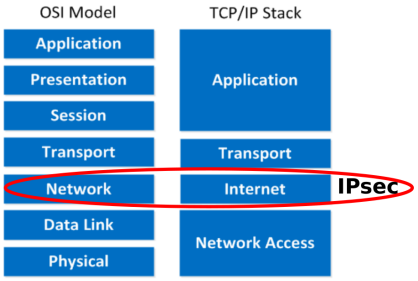
Separated from the public internet



IPSec Services

1. confidentiality
2. authentication
3. data integrity
4. replay-attack prevention

IPSec



IPSec Services

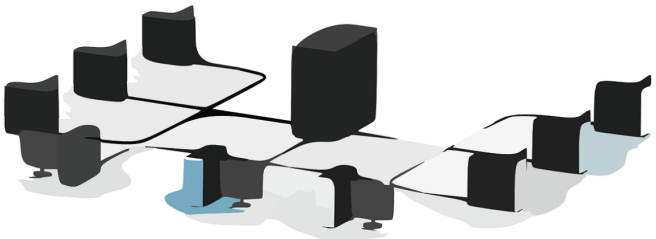
1. confidentiality
2. authentication
3. data integrity
4. replay-attack prevention

Private Network (PN)

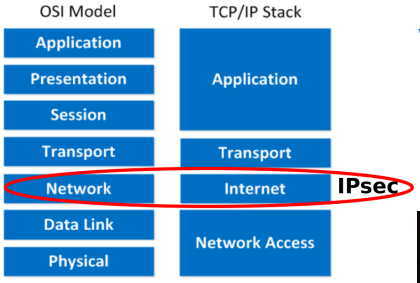
Stand-alone physical network including routers, links and DNS infrastructure

Separated from the public internet

High maintenance cost



IPSec



IPSec Services

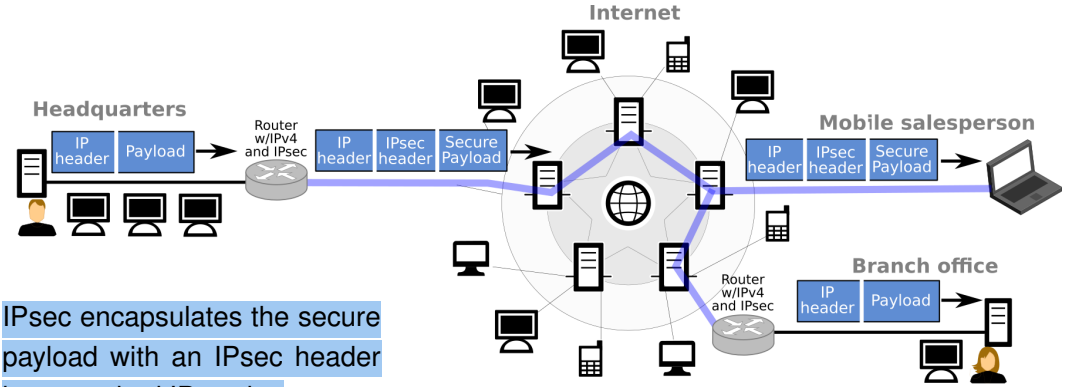
1. confidentiality
2. authentication
3. data integrity
4. replay-attack prevention

Virtual Private Network (VPN)

institution's inter-office traffic is sent over the public internet rather than over a physical independent network.

IPsec

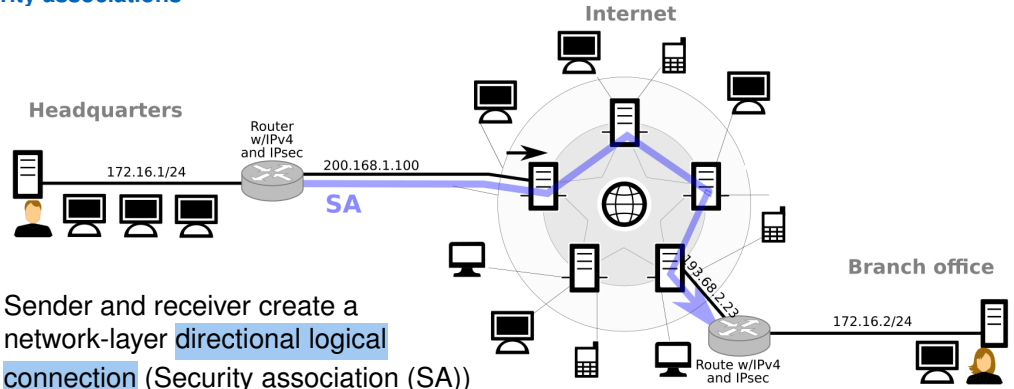
IPsec and VPNs



IPsec encapsulates the secure payload with an IPsec header in a standard IP packet

IPsec

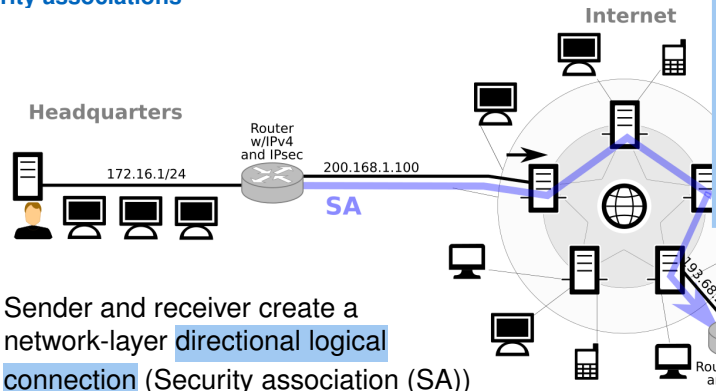
Security associations



Init: Sender and receiver create a network-layer directional logical connection (Security association (SA))

IPsec

Security associations



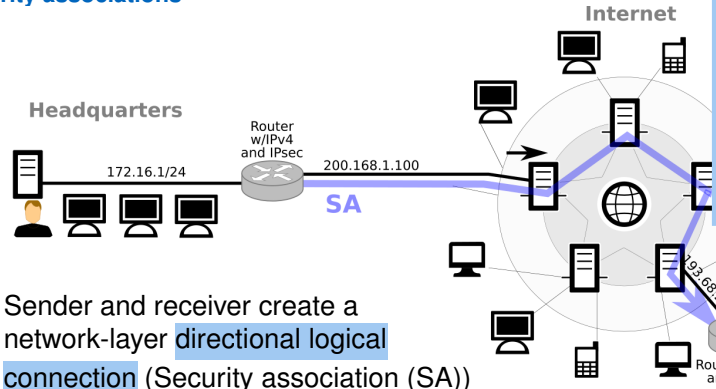
Security Association

- 32-bit identifier for SA
  (Security Parameter Index (SPI))
- Origin (200.168.1.100) & destination
  (193.58.2.23)
- Encryption type (e.g. 3DES with CBC)
- Encryption & authentication keys
- Integrity check type
  (e.g. HMAC with MD5)

Init: Sender and receiver create a network-layer directional logical connection (Security association (SA))

IPsec

Security associations



Security Association

- 32-bit identifier for SA
  (Security Parameter Index (SPI))
- Origin (200.168.1.100) & destination
  (193.58.2.23)
- Encryption type (e.g. 3DES with CBC)
- Encryption & authentication keys
- Integrity check type
  (e.g. HMAC with MD5)

Init: Sender and receiver create a network-layer directional logical connection (Security association (SA))

SA state maintained at origin and destination for session management

IPsec

IPsec datagram

Construct IPsec datagram

1. Original IPv4 datagram attached with 'Esp trailer'

ESP = 'Encapsulation Security Payload' (protocol)

IPsec

IPsec datagram

Construct IPsec datagram

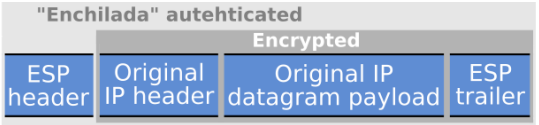
1. Original IPv4 datagram attached with 'Esp trailer'
2. Encrypt using the algorithm and key specified by SA

IPsec

IPsec datagram

Construct IPsec datagram

1. Original IPv4 datagram attached with 'Esp trailer'
2. Encrypt using the algorithm and key specified by SA
3. Append ESP header and create MAC over whole enchilada using algorithm and key specified in SA

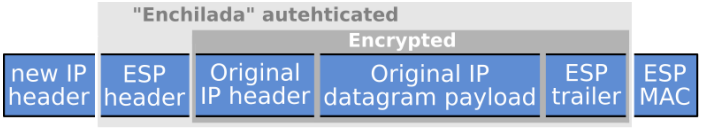


IPsec

IPsec datagram

Construct IPsec datagram

1. Original IPv4 datagram attached with 'Esp trailer'
2. Encrypt using the algorithm and key specified by SA
3. Append ESP header and create MAC over whole enchilada using algorithm and key specified in SA
4. create new IP header

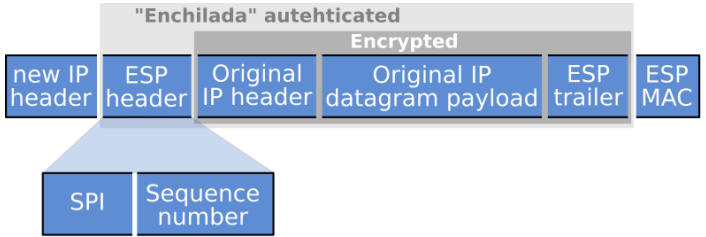


IPsec

IPsec datagram

Construct IPsec datagram

1. Original IPv4 datagram attached with 'Esp trailer'
2. Encrypt using the algorithm and key specified by SA
3. Append ESP header and create MAC over whole enchilada using algorithm and key specified in SA
4. create new IP header

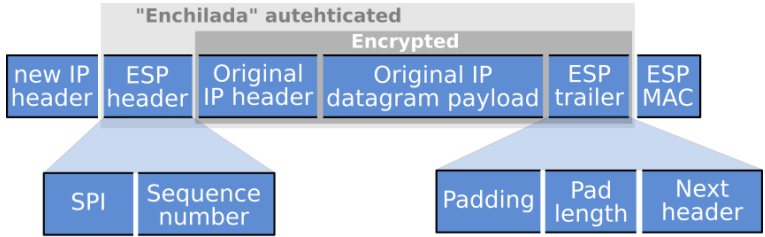


IPsec

IPsec datagram

Construct IPsec datagram

1. Original IPv4 datagram attached with 'Esp trailer'
2. Encrypt using the algorithm and key specified by SA
3. Append ESP header and create MAC over whole enchilada using algorithm and key specified in SA
4. create new IP header

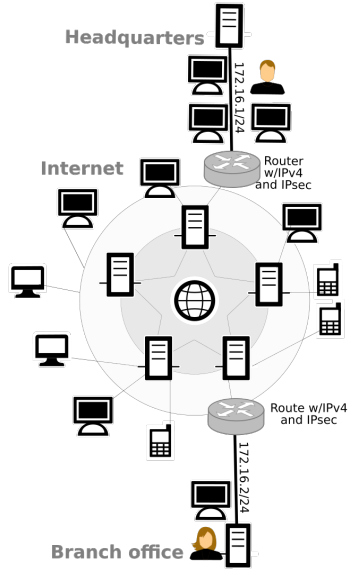


Padding of blockcipher
Pad length of padding
Next header: type of data in payload

IPsec

Key management in IPsec

IPsec uses Internet Key Exchange (IKE)

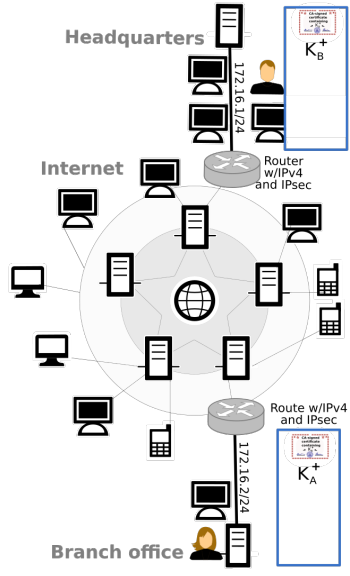


IPsec

Key management in IPsec

IPsec uses Internet Key Exchange (IKE)

init: Each IPsec entity has certificate & public key



IPsec

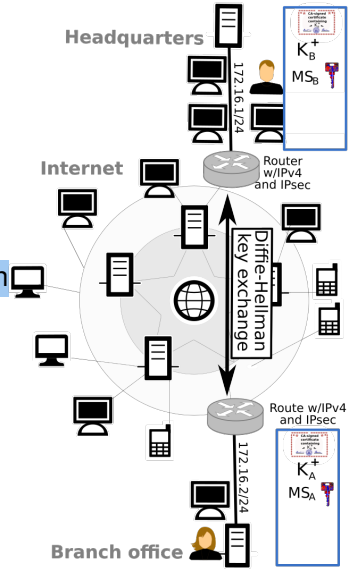
Key management in IPsec

IPsec uses Internet Key Exchange (IKE)

init: Each IPsec entity has certificate & public key

First: Bi-directional IKE SA between entities via Diffie-Hellman (no authentication)

- Establish master key



IPsec

Key management in IPsec

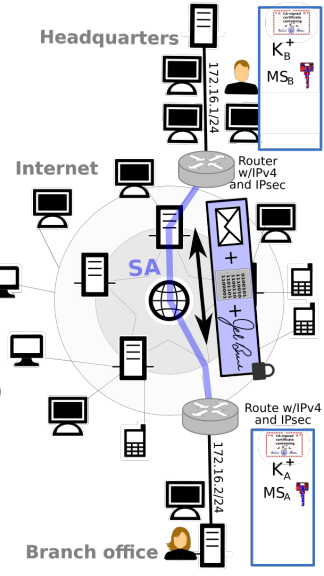
IPsec uses Internet Key Exchange (IKE)

init: Each IPsec entity has certificate & public key

First: Bi-directional IKE SA between entities via Diffie-Hellman (no authentication)

- Establish master key

Encrypted: Sign messages to authenticate (invisible to eavesdropper)



IPsec

Key management in IPsec

IPsec uses Internet Key Exchange (IKE)

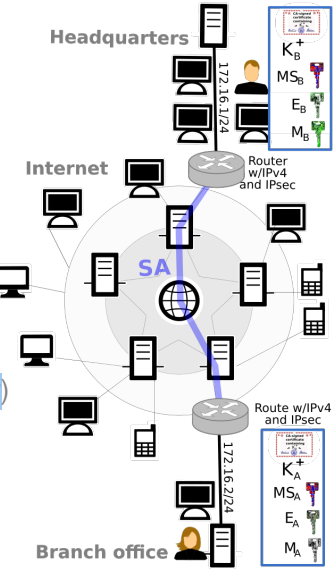
init: Each IPsec entity has certificate & public key

First: Bi-directional IKE SA between entities via Diffie-Hellman (no authentication)

- Establish master key

Encrypted: Sign messages to authenticate (invisible to eavesdropper)

Compute: IPsec SA keys from master secret



IPsec

Key management in IPsec

IPsec uses Internet Key Exchange (IKE)

init: Each IPsec entity has certificate & public key

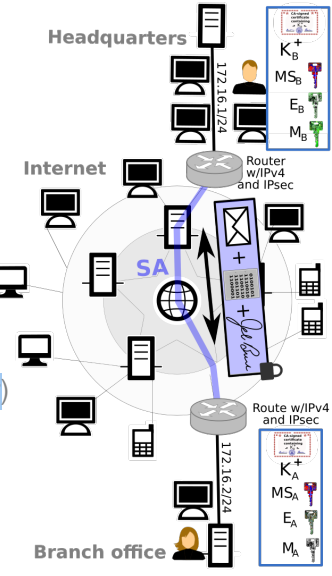
First: Bi-directional IKE SA between entities via Diffie-Hellman (no authentication)

- Establish master key

Encrypted: Sign messages to authenticate (invisible to eavesdropper)

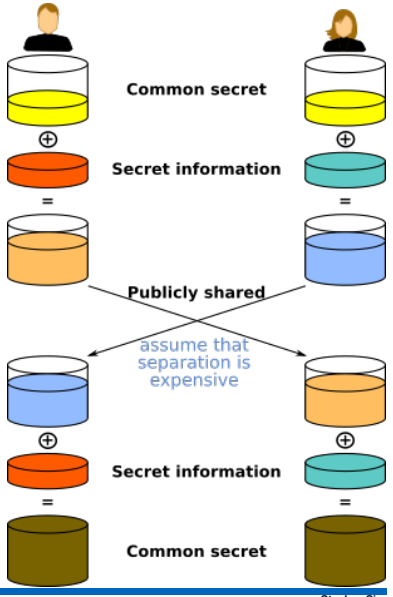
Compute: IPsec SA keys from master secret

Negotiate: IPsec encryption and authentication algorithms



IPsec

Diffie-Hellman Key Exchange



IPsec

Diffie-Hellman Key Exchange

Bob modulus *p* and base *g*

Alice modulus *p* and base *g*

IPsec

Diffie-Hellman Key Exchange

Bob modulus *p* and base *g* ⟷ publicly agree ⟷ Alice modulus *p* and base *g*

IPsec

Diffie-Hellman Key Exchange

Bob modulus *p* and base *g* ⟷ publicly agree ⟷ Alice modulus *p* and base *g*

Bob choose secret *b*

Alice

IPsec

Diffie-Hellman Key Exchange

Bob modulus p and base g ⟷ publicly agree ⟷ Alice modulus p and base g

Bob choose secret b ⟶ Send $B = g^b \mod p$ ⟶ Alice

IPsec

Diffie-Hellman Key Exchange

Bob modulus p and base g ⟷ publicly agree ⟶ Alice modulus p and base g

Bob choose secret b ⟶ Send $B = g^b \mod p$ ⟶ Alice

Bob

Alice choose secret a

IPsec

Diffie-Hellman Key Exchange

Bob modulus p and base g ⟷ publicly agree ⟷ Alice modulus p and base g

Bob choose secret b ⟶ Send $B = g^b \mod p$ ⟶ Alice

Bob ⟵ Send $A = g^a \mod p$ ⟵ Alice choose secret a

IPsec

Diffie-Hellman Key Exchange

Bob modulus p and base g ⟵ publicly agree ⟶ Alice modulus p and base g

Bob choose secret b ⟶ Send $B = g^b \mod p$ ⟶ Alice

Bob ⟵ Send $A = g^a \mod p$ ⟵ Alice choose secret a

Bob compute:

$$s = A^b \mod p = g^{ab} \mod p$$

Alice compute:

$$s = B^a \mod p = g^{ab} \mod p$$

IPsec

Diffie-Hellman Key Exchange

Bob modulus p and base g ⟵ publicly agree ⟶ Alice modulus p and base g

Bob choose secret b ⟶ Send $B = g^b \mod p$ ⟶ Alice

Bob ⟵ Send $A = g^a \mod p$ ⟵ Alice choose secret a

Bob compute:

$$s = A^b \mod p = g^{ab} \mod p$$

Alice compute:

$$s = B^a \mod p = g^{ab} \mod p$$

Aalto University
School of Electrical
Engineering

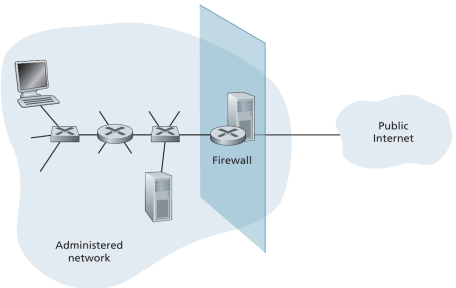
Part II (20 min)

Firewalls and Intrusion Detection Systems

Firewalls

Isolates local network from the Internet

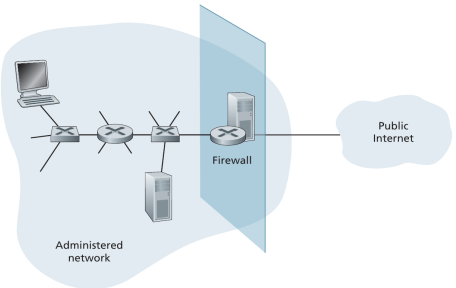
- authorized traffic passes through the firewall
- all non-authorized traffic is dropped
- firewall shall be immune to penetration



Firewalls

Isolates local network from the Internet

- authorized traffic passes through the firewall
- all non-authorized traffic is dropped
- firewall shall be immune to penetration



Three categories of firewalls:

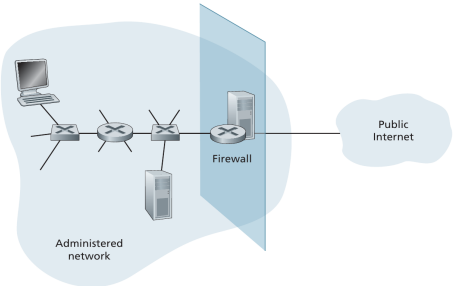
1. Packet filters
2. Stateful filters
3. Application gateways

Firewalls

Packet filters

Gateway router

- examines each datagram in isolation
- administrator-specific rules for pass or drop

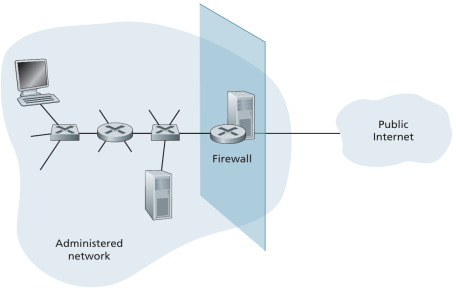


Firewalls

Packet filters

Gateway router

- examines each datagram in isolation
- administrator-specific rules for pass or drop



Filtering decisions based on (e.g.):

1. IP source or destination address
2. Protocol type in IP datagram field (TCP, UDP, ICMP, OSPF, ...)
3. TCP/UDP source and destination port
4. TCP flag bits: SYN, ACK, ...
5. ICMP message type

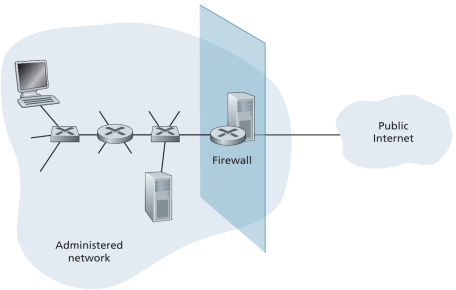
Firewalls

Packet filters

Gateway router

- examines each datagram in isolation
- administrator-specific rules for pass or drop

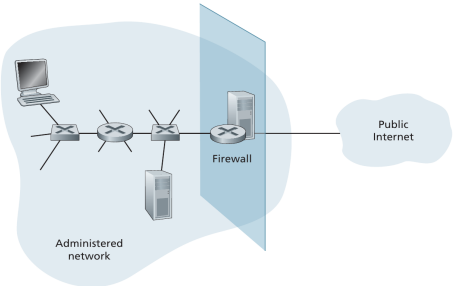
Policy	firewall setting
No outside web address	Drop outgoing packets to any IP adr, port 80
No incoming TCP	Drop TCP SYN packets
Resilience against smurf DoS attack	Drop ICMP ping pkts to broadcast adr (e.g. 130.207.255.255)
Prevent network traceroute	Drop all outgoing ICMP TTL expired traffic



Firewalls

Stateful filters

- Track all ongoing TCP traffic in a connection table

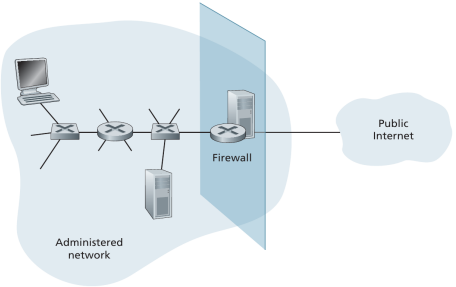


Firewalls

Stateful filters

- Track all ongoing TCP traffic in a connection table

Policy	firewall setting
No outside web address	Drop outgoing packets to any IP adr, port 80
No incoming TCP	Drop TCP SYN packets
Resilience against smurf DoS attack	Drop ICMP ping pkts to broadcast adr (e.g. 130.207.255.255)
Prevent network traceroute	Drop all outgoing ICMP TTL expired traffic

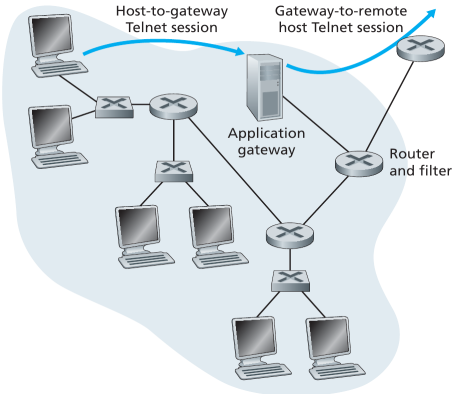


In stateless filter example, packets with ACK=1 and source port 80 get through the filter and could be used to crash local systems with malformed ACK packets

Firewalls

Application gateways

- allow application specific rules for selected users



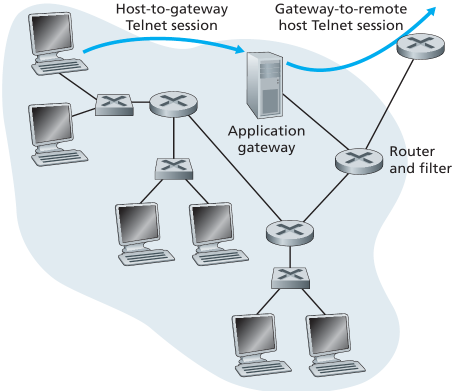
Firewalls

Application gateways

- allow application specific rules for selected users

An application gateway...

1. make policy decisions based on application data
2. take decisions beyond IP/TCP/UDP headers
3. application-specific server through which all application data must pass
4. performs user authorization



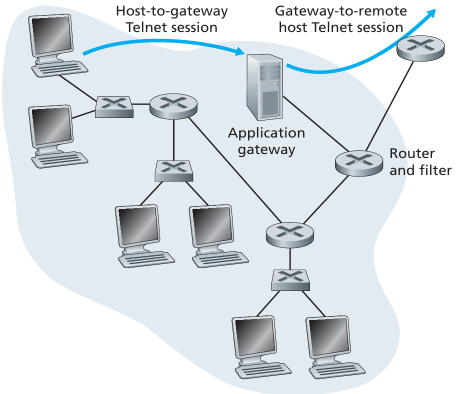
Firewalls

Application gateways

- allow application specific rules for selected users

An application gateway...

1. make policy decisions based on application data
2. take decisions beyond IP/TCP/UDP headers
3. application-specific server through which all application data must pass
4. performs user authorization

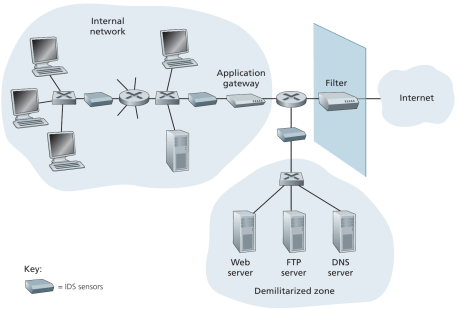


performance penalty since all traffic passes through application gateway

Intrusion detection systems

For many attack types, deep packet inspection is needed

→ Look beyond header fields and into actual application data carried by packets



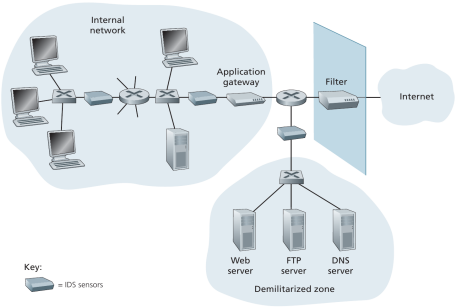
Intrusion detection systems

For many attack types, deep packet inspection is needed

→ Look beyond header fields and into actual application data carried by packets

IDSs detect wide range of attacks

- network mapping
- port scans
- TCP stack scans
- DoS bandwidth-flooding attacks
- Worms and viruses
- OS/application vulnerability attacks



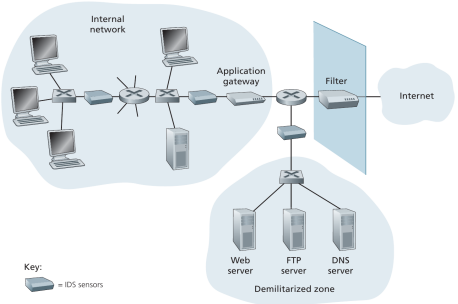
Intrusion detection systems

For many attack types, deep packet inspection is needed

→ Look beyond header fields and into actual application data carried by packets

IDSs detect wide range of attacks

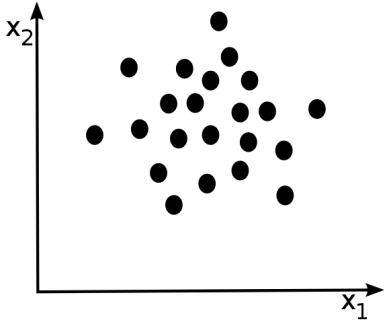
- network mapping
- port scans
- TCP stack scans
- DoS bandwidth-flooding attacks
- Worms and viruses
- OS/application vulnerability attacks



IDS systems are either signature-based or anomaly-based

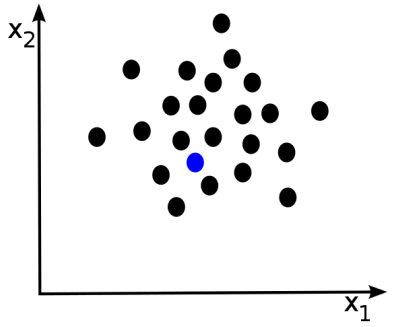
Anomaly detection

Problem statement



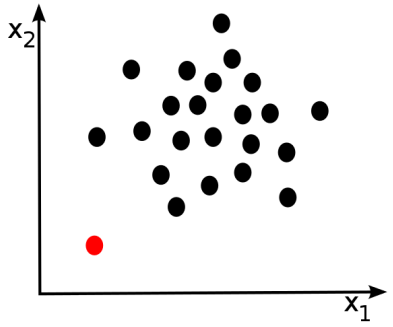
Anomaly detection

Problem statement



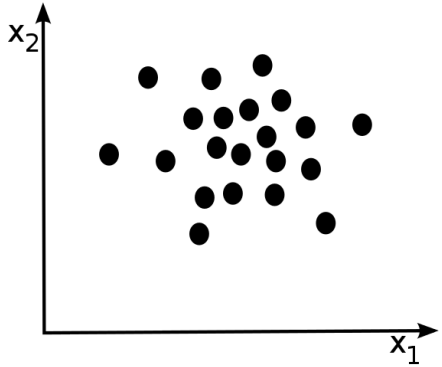
Anomaly detection

Problem statement



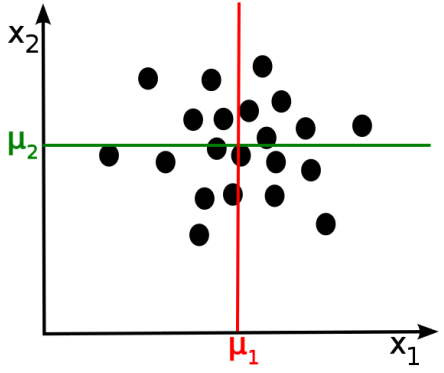
Anomaly detection

Example



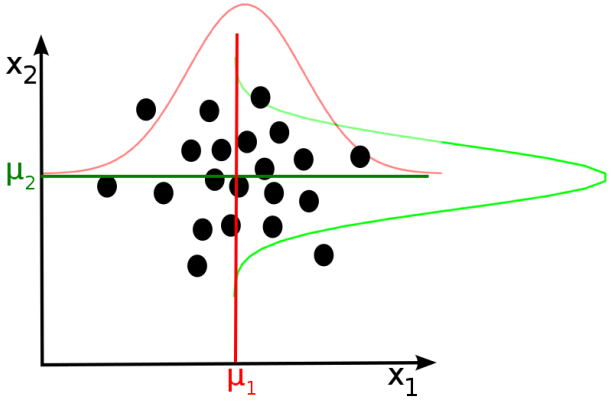
Anomaly detection

Example



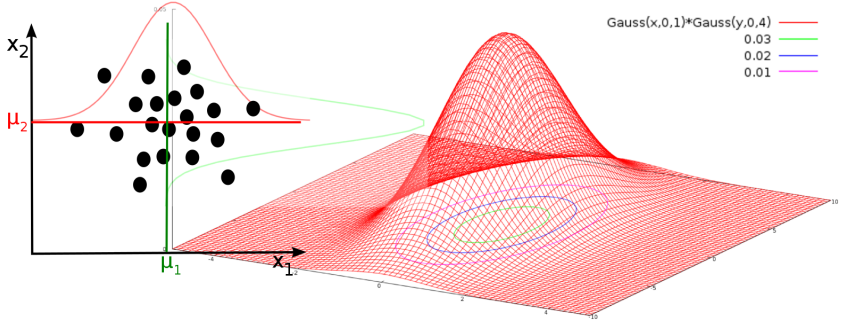
Anomaly detection

Example



Anomaly detection

Example



Anomaly detection

Problem statement

Choice of good values for ε

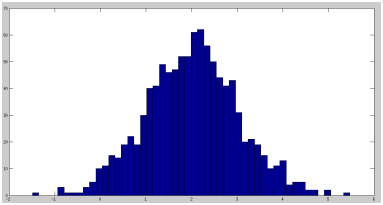
Using crossvalidation and testing sets, calculate

- Precision/Recall
- F_1-score
- ...

Anomaly detection

Non-Gaussian features

In anomaly detection, we have so far assumed Gaussian distributed features.

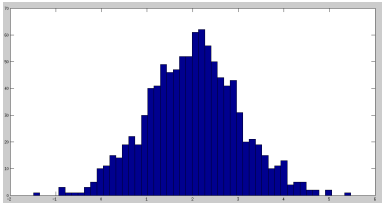


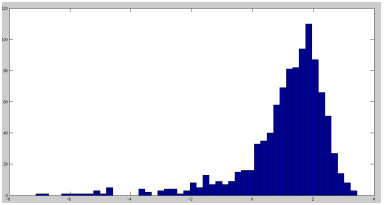
Anomaly detection

Non-Gaussian features

In anomaly detection, we have so far assumed Gaussian distributed features.

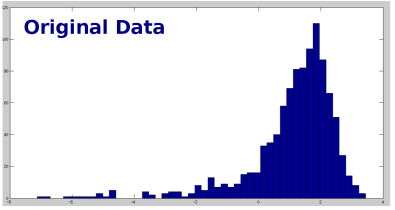
→ What if the feature distribution is not Gaussian ?

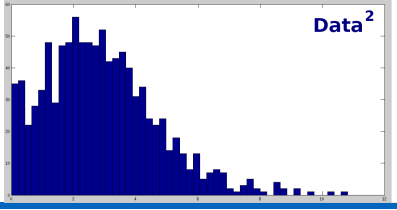


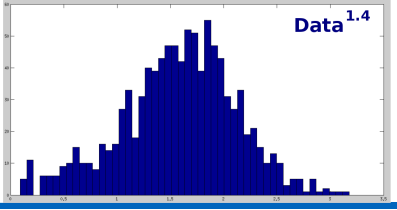


Anomaly detection

Generate new features with a more Gaussian-like distribution







Anomaly detection

Non-Gaussian features

Possible operations on features

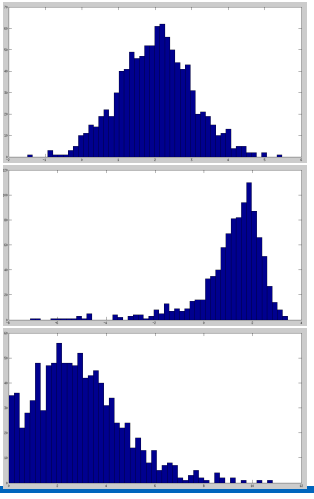
$$x_{\text{new}} = \log(x)$$

$$x_{\text{new}} = \sqrt{x}$$

$$x_{\text{new}} = x^{\frac{1}{3}}$$

$$x_{\text{new}} = \log(x + k)$$

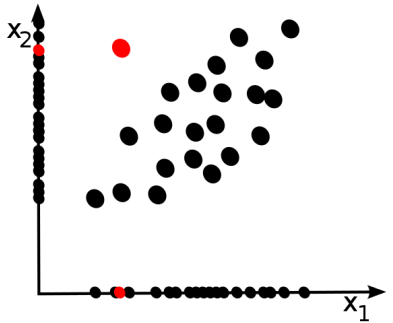
$$\vdots$$



Anomaly detection

Multivariate Gaussian Distribution

- Note that there are cases in which the anomaly looks perfectly normal when considering each dimension separately

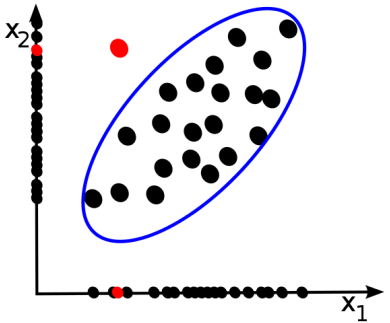


Anomaly detection

Multivariate Gaussian Distribution

- Note that there are cases in which the anomaly looks perfectly normal when considering each dimension separately

→ The consideration of multivariate Gaussian distributions might help to to detect such anomalies.



Aalto University
School of Electrical
Engineering

Video: Future perspectives (5 min)

R. Rivest, W. Diffie, A. Shamir, S. Landau

Questions?

Stephan Sigg
stephan.sigg@aalto.fi

Esa Vikberg
esa.vikberg@aalto.fi

Leo Lazar
leo.lazar@aalto.fi

Literature

- J.F. Kurose,K.W. Ross: Computer Networking: A Top-Down approach (7th edition), Pearson, 2016.
- J.F. Kurose,K.W. Ross: Computer Networking: A Top-Down approach (6th edition), Addison-Wesley, 2012.