



Secure Communication over Untrusted Networks

Jan Vossaert

Overview

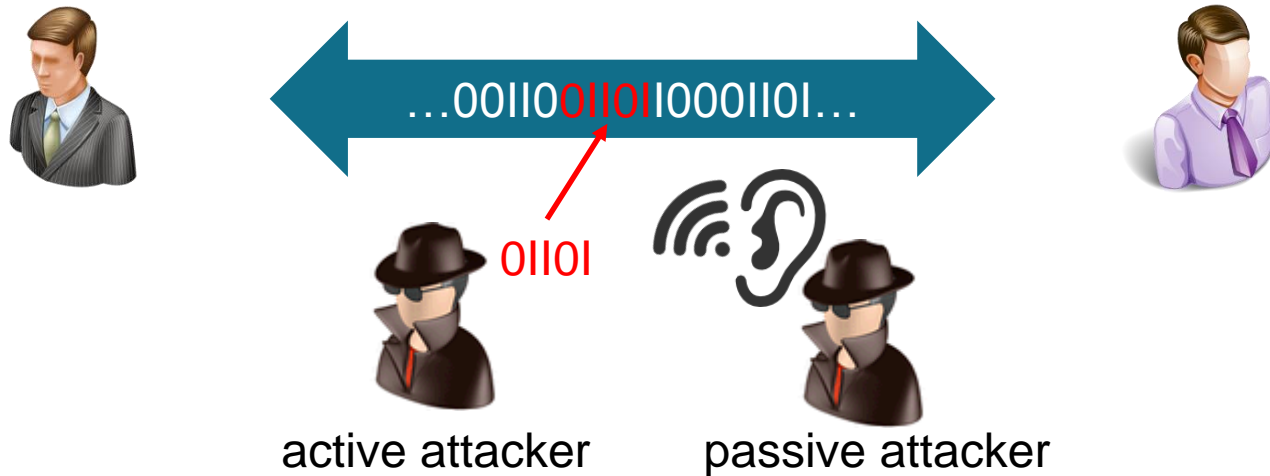
- Introduction
- Secure communication basics
- Secure communication technologies
 - Transport layer security
 - Virtual private network
- Seminar in September
- Concluding remarks

Introduction



passive attacker



Introduction



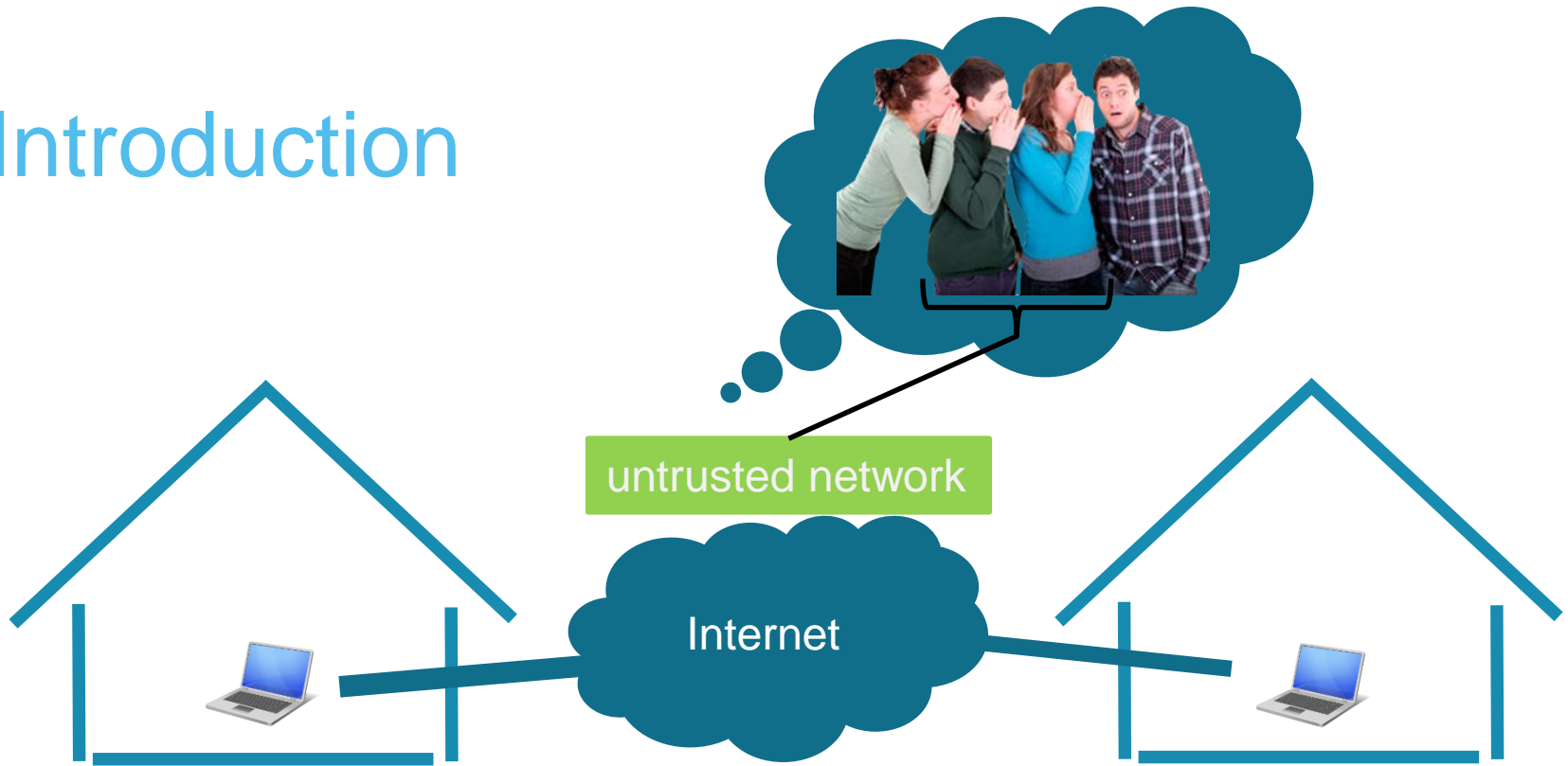
- Desired security properties:
 - Confidentiality
 - Authenticity



Introduction



- Message confidentiality 
- Message authentication 

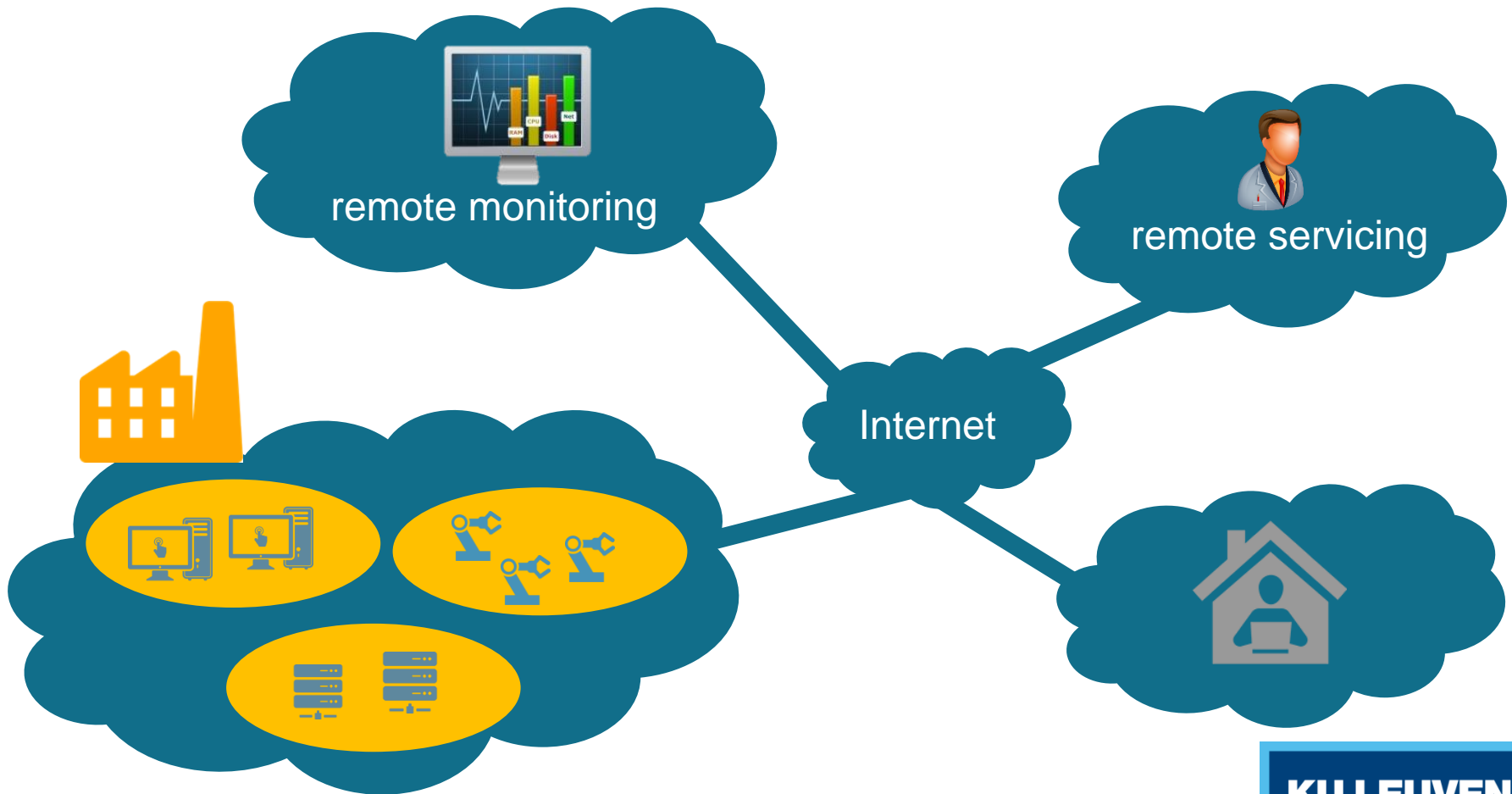
Introduction



- Message confidentiality 
- Message authentication 

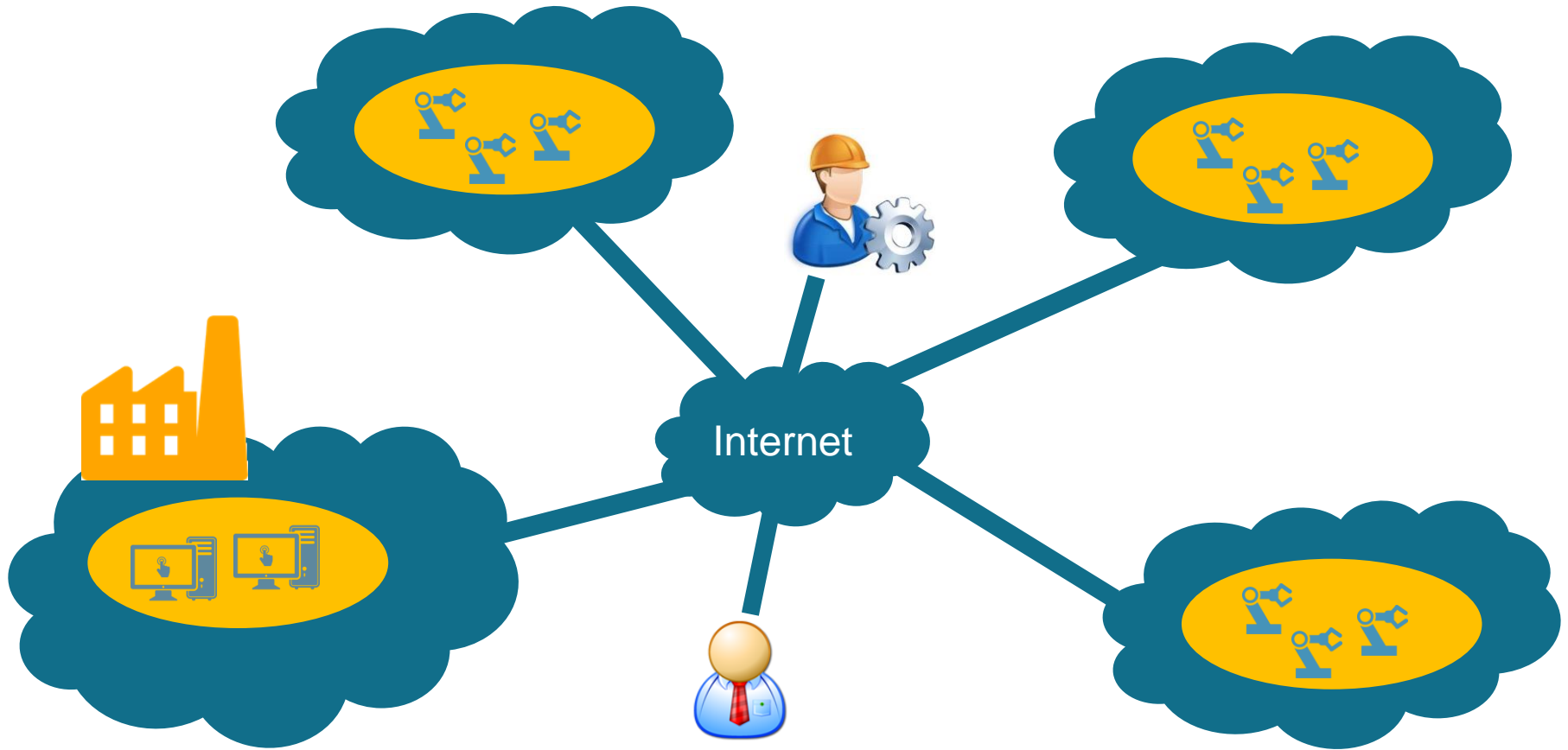
Introduction

- Remote access to local network



Introduction

- Access to devices on remote sites



Introduction

Dynamic Host Configuration Protocol (DHCP) support	Server or Relay Agent
Network Time Protocol (NTP) client	Client
Link Layer Discovery Protocol (LLDP)	As per protocol 802.2
Remote Syslog Logging	On external server
Virtual private network (VPN) throughput	max. 106 Mbps (Router mode, VPN bidirectional throughput)
	max. 66 Mbps (Stealth mode, VPN bidirectional throughput)
Number of VPN tunnels	10 (up to 250 tunnels with additional license as an option)
Encryption methods	DES, 3DES, AES-128, -192, -256
Internet Protocol Security (IPsec) mode	ESP tunnel / ESP transport
Authentication	X.509v3 certificates with RSA or PSK
Data integrity	MD5, SHA-1

Product function: Security				
Firewall configuration	Stateful inspection	Stateful Inspection	Stateful inspection	Stateful Inspection
Product function in VPN connection	–	IPSec	IPSec	IPSec
Product function				
■ Password protection	Yes	Yes	Yes	Yes
■ Restricted bandwidth	Yes	Yes	Yes	Yes
■ NAT/NAPT	Yes	Yes	Yes	Yes
Encryption algorithms	–	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Authentication procedure	–	Preshared key, X.509v3 certificates	Preshared key, X.509v3 certificates	Preshared key, X.509v3 certificates
Hashing algorithms	–	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1

VPN: True SSL/TLS VPN (Open VPN)
 Encryption: DES, 3DES, AES, 128/192/256-bit
 Authentication: Pre-shared key, X.509, Certification Authority

- Secured Management by HTTPS
- Various kind of WAN Connection Type supported: Dynamic/Static IP, PPPoE
- IP table to prevent access from unauthorized IP address
- Support VPN for secured network connection (Open VPN, PPTP, IPSEC, VPN)

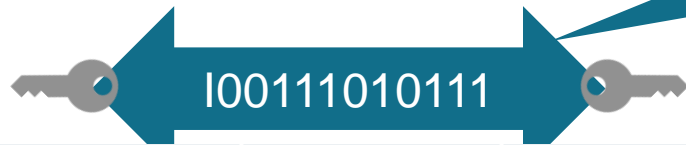
Security	
Stateful inspection firewall	Firewall rules (incoming/outgoing, management), DoS prevention, MAC filter
Encryption	Enhanced encryption (>56 Bit, up to 256Bit DES) Management access
Software	
Management	SNMPv3, SSH2/SFTP, HTTP, HTTPS, V.24 CLI, SNMPv1/2, local and central user management (RADIUS), HiDiscovery, Industrial HiVision, HiView
Multipoint VPN	IPSec VPN
Diagnostics	LEDs (Power, Linkstatus, Daten, status, ACA, RM), Meldekontakt (24 V DC / 1 A), Log-File, Syslog, Konfigurationscheck, RMON (Statistik), SFP-Diagnose (Temperatur, optische Sendeleistung), Trap für Änderungen und Konfiguration speichern, ACL Rules counter
Configuration	Command Line Interface (CLI), web interface, Auto Configuration Adapter (ACA22, ACA31), HiDiscovery, Industrial HiVision, HiView
Security	Layer 3 and Layer 2 Access Control Lists (ACL), ACL flow based limiting, Audit Trail, HTTPS, SSHv2, SFTP, SNMPv3, Management VLAN, Role based Access Control, IEEE1686 compliant configuration possible, Ingress storm protection
Routing	VLAN and port based routing, static routing, multinetting, IP masquerading, 1-to-1 NAT, port forwarding, Static and Dynamic ARP entries, OSPFv2
Redundancy functions	VRRP (Virtual Router Redundancy Protocol)
Filter	QoS 8 classes, port prioritisation IEEE 802.1D/p, VLAN IEEE 802.1Q, HTTPS, SSH, SNMP V1/V3, LLDP



Secure communication basics

- Secure channel between both parties

Confidentiality?
Authenticity?



Product function: Security				
Firewall configuration	Stateful inspection	Stateful Inspection	Stateful inspection	Stateful Inspection
Product function in VPN connection	-	IPSec	IPSec	IPSec
Product function				
■ Password protection	Yes	Yes	Yes	Yes
■ Restricted bandwidth	Yes	Yes	Yes	Yes
■ NAT/NAPT	Yes	Yes	Yes	Yes
Encryption algorithms	-	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Authentication procedure	-	Preshared key, X.509v3 certificates	Preshared key, X.509v3 certificates	Preshared key, X.509v3 certificates
Hashing algorithms	-	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1

- Confidentiality & authenticity: CBC-MAC, GCM, OCB,...

Relies on hash functions (MD5, SHA1)

Secure communication basics

- Secure channel between both parties



- Symmetric cryptography
- Session key?

Secure communication basics

- Session key establishment
 - Goal:
 - Set up a shared secret in a dynamic on-demand manner
 - Properties:
 - Both parties learn the value of the session key
 - No other parties should know the value of the session key
 - Unilateral or mutual authentication
 - Both parties are ensured the key is freshly generated

Secure communication basics

- Session key establishment
 - Types
 - Pre-shared keys (PSK)
 - Public-key infrastructure (PKI)

Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)

“is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used.”



Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)

“is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used.”



-  required to generate 
- Both parties know the identity of the other party who holds 

Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)

“is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used.”



-  required to generate 
- Both parties know the identity of the other party who holds 

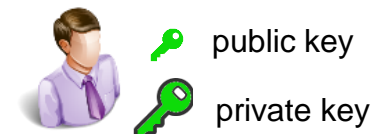
Scalability?



Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)
 - Public-key infrastructure (PKI)

“is a system to bind public keys with respective user identities by means of a certificate (e.g. X.509 certificate).”



Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)
 - Public-key infrastructure (PKI)

It's . I vouch for it.

“is a system to bind public keys with respective user identities by means of a certificate (e.g. X.509 certificate).”

public key



private key



public key



private key






Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)
 - Public-key infrastructure (PKI)

It's  . I vouch for it.

"is a system to bind public keys with respective user identities by means of a certificate (e.g. X.509 certificate)."

public key  
private key 

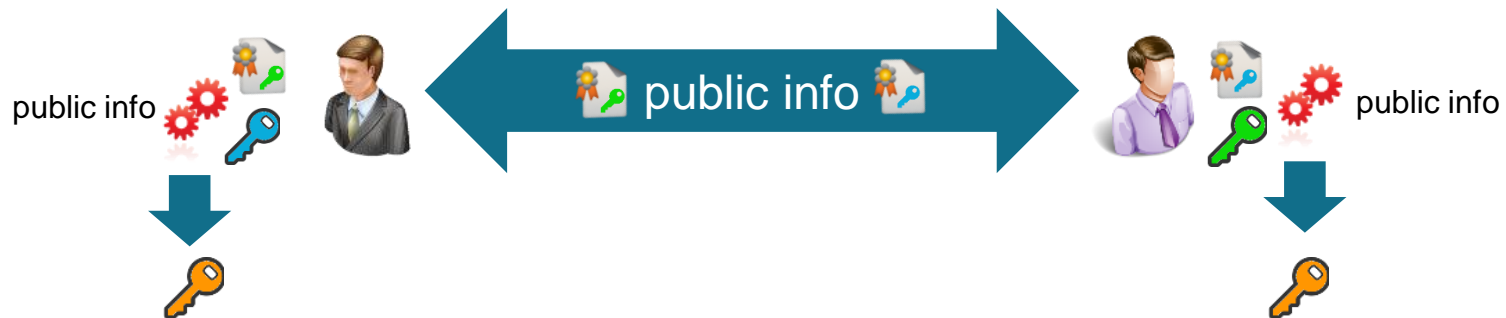
   private key



Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)
 - Public-key infrastructure (PKI)

“is a system to bind public keys with respective user identities by means of a certificate (e.g. X.509 certificate).”










Secure communication basics

- Session key establishment
 - Pre-shared keys (PSK)
 - Public-key infrastructure (PKI)

“is a system to bind public keys with respective user identities by means of a certificate (e.g. X.509 certificate).”



-  can only be generated if possession of either  or 
- Identities of the owners of  and  is certified in  
- Unilateral authentication also possible

Secure communication basics

- Summary:
 - Symmetric cryptography to protect confidentiality & authenticity of data

Dynamic Host Configuration Protocol (DHCP) support	Server or Relay Agent
Network Time Protocol (NTP) client	Client
Link Layer Discovery Protocol (LLDP)	As per protocol 802.2
Remote Syslog Logging	On external server
Virtual private network (VPN) throughput	max. 106 Mbps (Router mode, VPN bidirectional throughput)
	max. 66 Mbps (Stealth mode, VPN bidirectional throughput)
Number of VPN tunnels	10 (up to 250 tunnels with additional license as an option)
Encryption methods	DES, 3DES, AES-128, -192, -256
Internet Protocol Security (IPsec) mode	ESP tunnel / ESP transport
Authentication	X.509v3 certificates with RSA or PSK
Data integrity	MD5, SHA-1

- Public-key infrastructure: for devices that need to communicate with a large set of devices

Secure communication technologies

- System level
 - Why rely on security at application level?
 - Securing legacy applications in new environments
 - No distinction between traffic types



- Application-aware
 - More control by application
 - Feedback to user



Transport Layer Security (TLS)

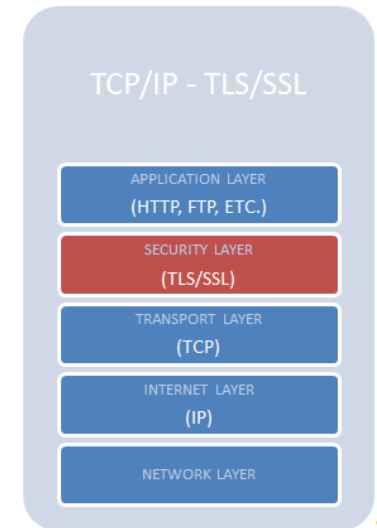
- One of the most widely deployed security protocols



- History
 - Netscape developed SSL protocol
 - SSL 3.0 published in 1996
 - No longer secure!
 - IETF standardization based on SSL 3.0 (RFC 5246)
 - TLS 1.0 (1999)
 - **TLS 1.2 (2008)**
 - TLS 1.3 (TBD)

Transport Layer Security (TLS)

- Intermediate layer between Transport and Application Layer
- Two phases:
 - Handshake
 - Client and/or server authentication
 - Establish cryptographic keys and parameters
 - Secure exchange of information

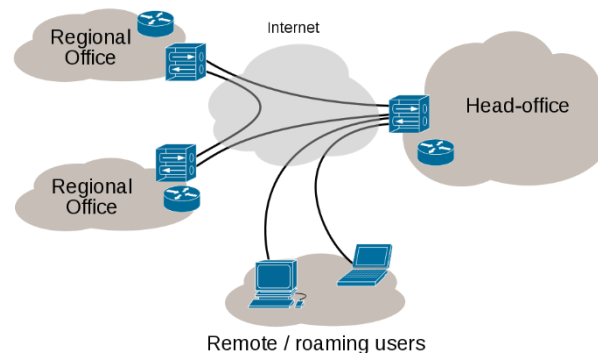


Transport Layer Security (TLS)

- Use in industrial network equipment
 - Secure management of network devices
 - Remote configuration (often via HTTPS - example)
 - User authentication over secure session
 - Secure transfer of software/firmware updates
 - Secure network communication in dedicated applications

Virtual private network

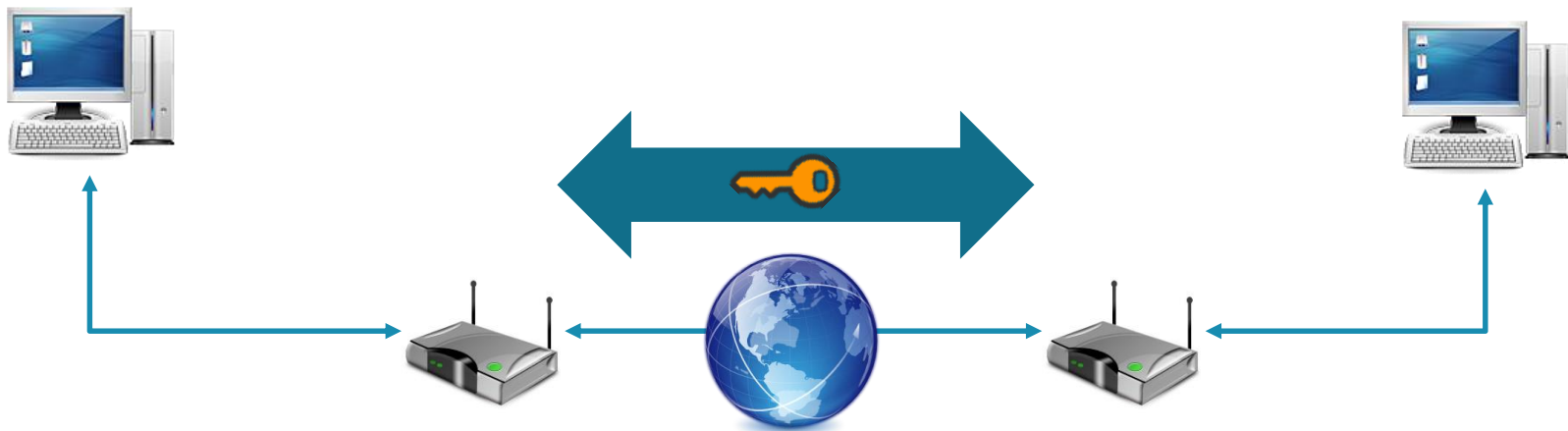
- A Virtual Private Network (VPN) extends a private network across a public network (e.g. the Internet)



- The client can access resources as if it would be directly connected to the private network
 - Traffic from device is routed over secure connection
 - Network-level component (i.e. no application support required)

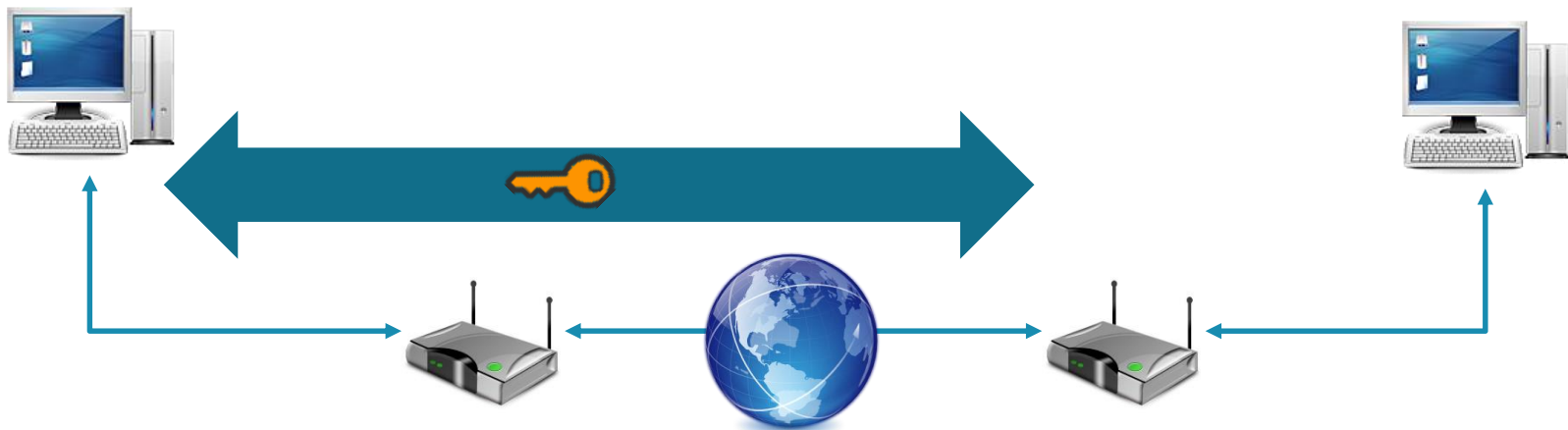
Virtual private network

- Different setups:
 - Gateway-to-gateway
 - Secure branch office connectivity over the Internet



Virtual private network

- Different setups:
 - Gateway-to-gateway
 - Host-to-gateway
 - Secure remote access to intranet services



Virtual private network

IPsec

origin

- RFC standardization

ports

- Fixed ports
 - UDP 500: key exchange
 - UDP 50: encrypted data
 - UDP 1701: initial configuration
 - UDP 4500: NAT traversal

compatibility

- Uncertain

encryption

- Standardized IPsec protocol

OpenVPN

- Open source initiative (GPL)
 - Based on SSL/TLS
- Configurable ports
 - UDP
 - TCP
 - TCP:443 to bypass restrictive firewalls
- Usually good
- OpenSSL

Virtual private network

- Use in industrial network equipment
 - Remote servicing/monitoring of equipment
 - Connecting remote sites in a secure network
 - Teleworking

Seminar in September

- Basic security concepts & algorithms
- Public-key infrastructure
 - Self-signed certificates vs commercial CAs
 - Certificate pinning/trust stores
 - Establishment & management of PKI
 - Revocation

Seminar in September

- Hands-on experience: secure communication technologies in industrial networking devices
 - Different approaches from different vendors
 - Cloud-based vs end-to-end security
 - Only compatible with devices from same vendor?
 - Vendor certificates or own PKI infrastructure?
 - Configuration
 - Encapsulation security payload (ESP) vs Authentication Header (AH)
 - Tunnel mode vs transport mode
 - Cryptographic parameters

Concluding remarks

- Certificates mainly for device authentication
- Secure session authentication often complemented with application-level authentication for **access control**
 - Username/password
 - Authentication server
 - Hardware tokens

