Computer Networks

Lecture on

Network security – selected issues

Plan of This Lecture

- Threats and security services
- Characteristic of cipher algorithms
- Public Key Infrastructure basis
- Virtual private networks

Why Is There a Security Problem?

- Why we have to pay for security?
  - to be able to use our computers and networks

- Why computers are so vulnerable?
  - in the past computer users: small communities and kind
  - mixing of data and code gives high flexibility
  - domination of homogenous systems
  - low skills and ignorance of young programmers

Why people make malicious things?	in the past	nowadays
For money ▪ hacker's services ▪ extortions	·	!!!
To take a revenge	•	!!
Ideological believes	.	!!
Cyber warfare	-	!
Smokescreen for another cybercrime	?	!
For play	!	!
To manifest their knowledge and power	!!	•
To manifest their stress	!!!	·

Attack Vectors on the OSI Layers

1	Non authorized device in a network
2, 3	Vulnerability in protocol implementations Sniffing Flooding – high volume or high rate Abuse of ICMP, ARP or IP options Manipulation of: fields in protocol headers, fragmentation
4	Vulnerability in protocol implementations Abuse of TCP options Man in the middle Port scan
5, 6, 7	Vulnerability in application implementations • Buffer overflow! • Discovery of debug entries Non authorized access Abuse of DHCP, DNS
8	Socio-techniques

Basic Terms

Threats

- Deny of Service
- Data lost
- Time lost
- Stolen data
- To be used as a hacker tool !!!

Entries for malicious code

- Viruses
- Warms
- Backdoors
- Spyware & Adware

Security tools

- AntiVirus
- Firewall
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Honey pot

Security services

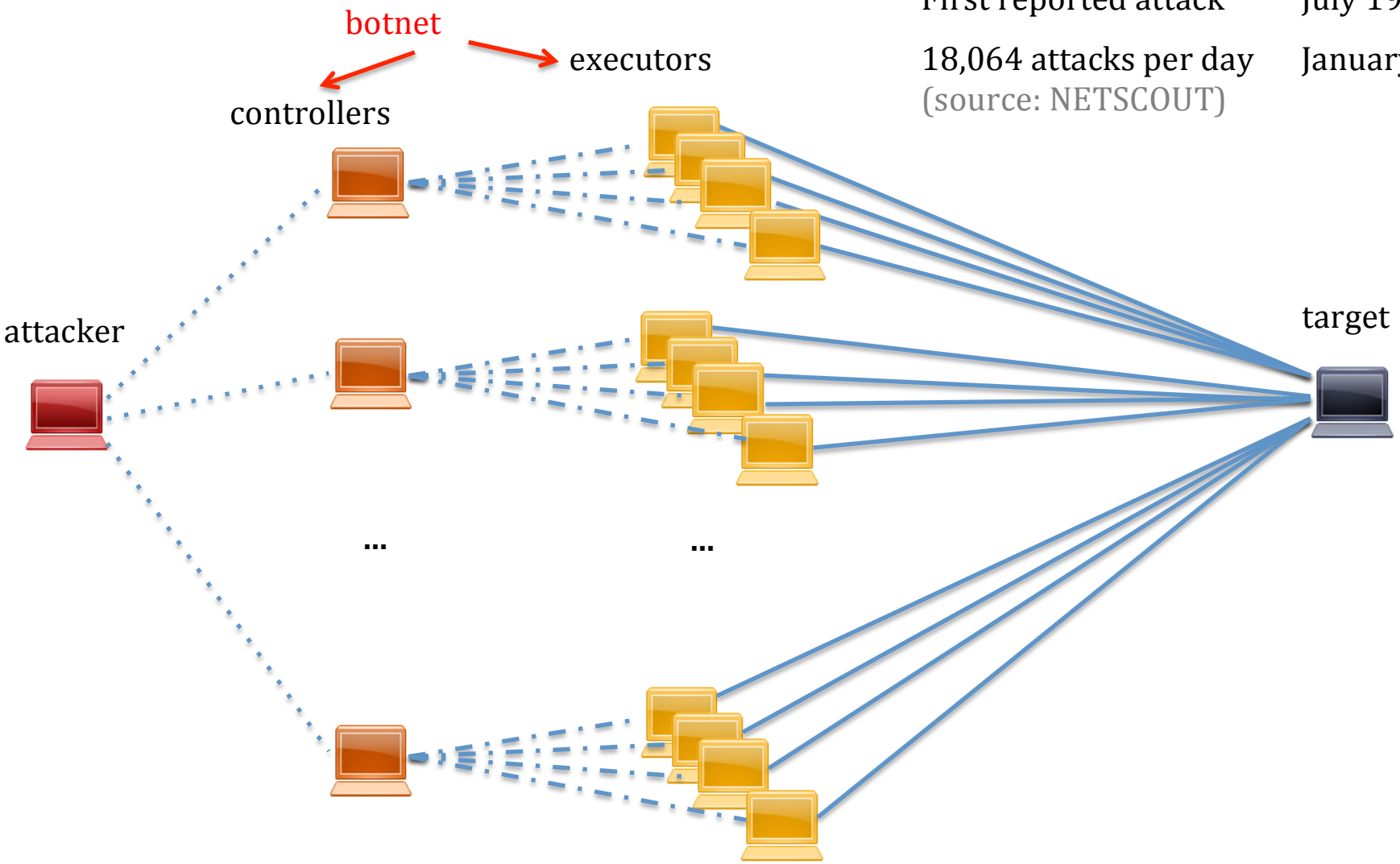
- Data confidentiality
- Data integrity
- Authentication
- Non repudiation
- Secure time reference

How to deal with huge data volume?

How to deal with steganography?

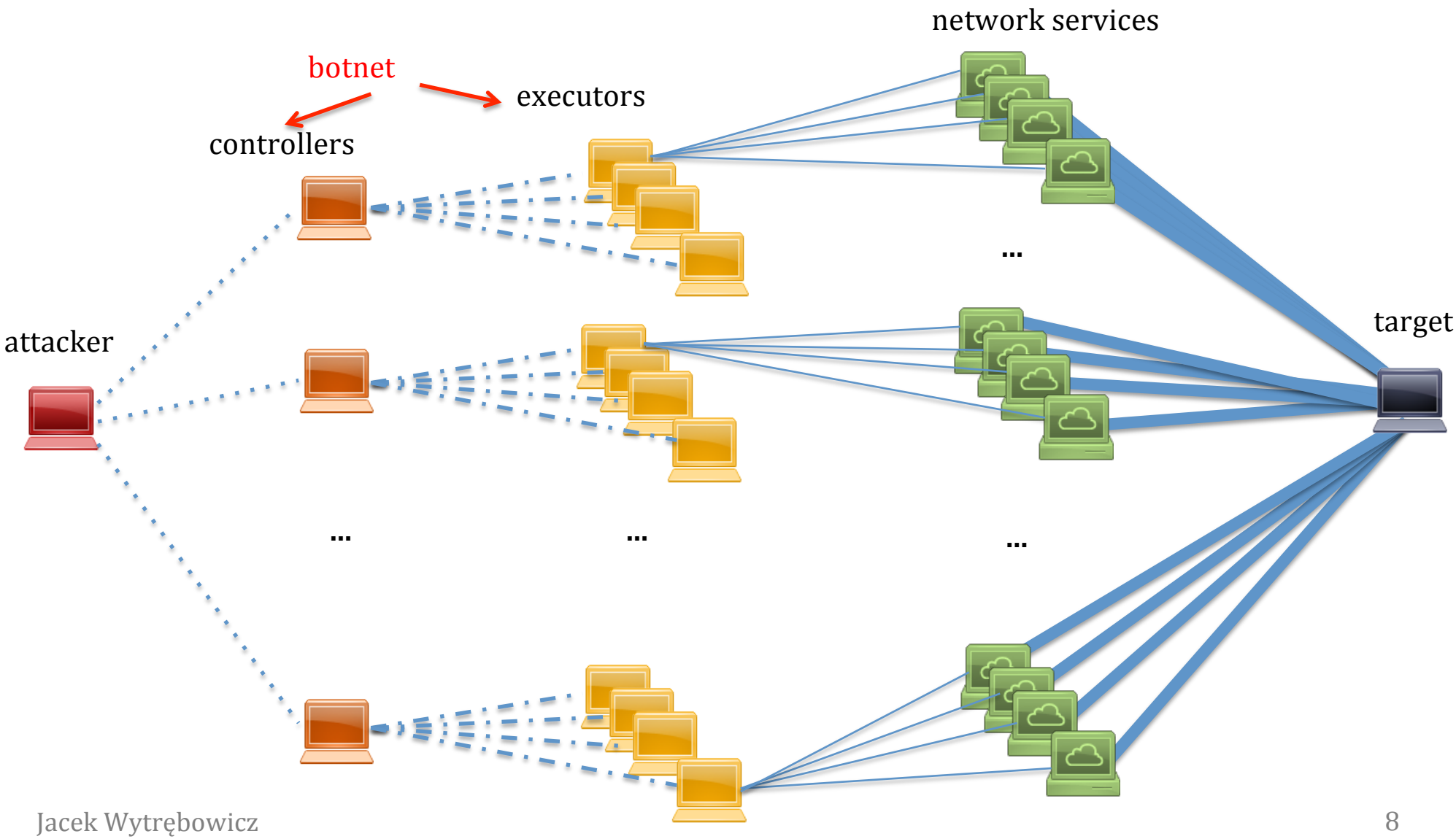
steganography – concealing a file, message, image, or video within another data

Distributed Denial of Service – Attack



First reported attack	July 1999
18,064 attacks per day (source: NETSCOUT)	January 2018

Amplification Attack



Cipher types

Stream cipher – *operates on a digit: bit or byte*

- synchronous
- self-synchronous

RC4 in SSL WEP in 802.11 A5/1 in GSM

Block cipher - *operates on a fixed length block, e.g. 128 bits*

- symmetric confidential key distribution

  based on substitution / permutation networks

  - DES - *Data Encryption Standard*

    standard from 1977 56-bit key!
  - 3DES - 2 keys
  - AES - *Advanced Encryption Standard*

    standard from 2001 128, 192, 256 keys
- asymmetric public/private keys
  - Diffie-Hellman key exchange invented in 1976, RFC 2631
  - RSA algorithm in 1977
  - ElGamal algorithm in 1984
  - ECC in 1985, in use 2004

Diffie-Hellman Algorithm

1. X and Y agree on a finite cyclic group G and a generate element g in G

   e.g.: p = 23 g = 5

2. X picks a random natural number a and sends g^a to Y

   $5^6 \bmod 23 = 8$

3. Y picks a random natural number b and sends g^b to X

   $5^{15} \bmod 23 = 19$

4. X computes $(g^b)^a$

   $19^6 \bmod 23 = 2$

5. Y computes $(g^a)^b$

   $8^{15} \bmod 23 = 2$

$(g^b)^a = (g^a)^b$ shared secret key

Stream Cipher Properties

- key length: 64, 128, 256 bits
- high speed!
- low hardware complexity
- less secure than block cipher

Stream cipher algorithms are based on

- exor function
- shift registers

Implemented in transmitting and receiving hardware elements

Block Cipher Properties

Symmetric cipher

- key length: 64, 128, 256 bits
- speed
- short keys
- easy to multiply ciphering
- confidential key distribution
- many keys: N*(N-1) / 2, N users, every one to every one
- frequent change of keys

Asymmetric cipher

- key length
  - RSA: 1024, 2048 bits
  - ECC: 192, 224, 256, … bits
- only privet key has to be protected
- less key to be managed: N pairs
- non frequent change of keys
- speed, but ECC no so bad
- long keys
- lack of a formal prove of security
- risk of man in the middle attack!

Block Cipher Properties

Symmetric key bit length	Matching binary ECC bit length	Matching RSA bit length
80	163	1024
112 (3DES)	233	2048
128 (AES-128)	283	3072

Use of Asymmetric Cipher

Confidentiality

Sender → Ciphering → Deciphering → Recipient

public key *private key*

Authentication

Sender → Ciphering → Deciphering → Recipient

private key *public key*

Cryptographic Hash Functions

One-way function that maps data of arbitrary size to a bit string of a fixed size – a hash

It should be:

- deterministic
- quick to compute
- infeasible to recreate the input from the hash
- small change on input results in extensive change of the hash
- infeasible to find two different messages with the same hash

If the inputs are longer than the hash length, then collisions can occur

collision – the same hash for two different inputs

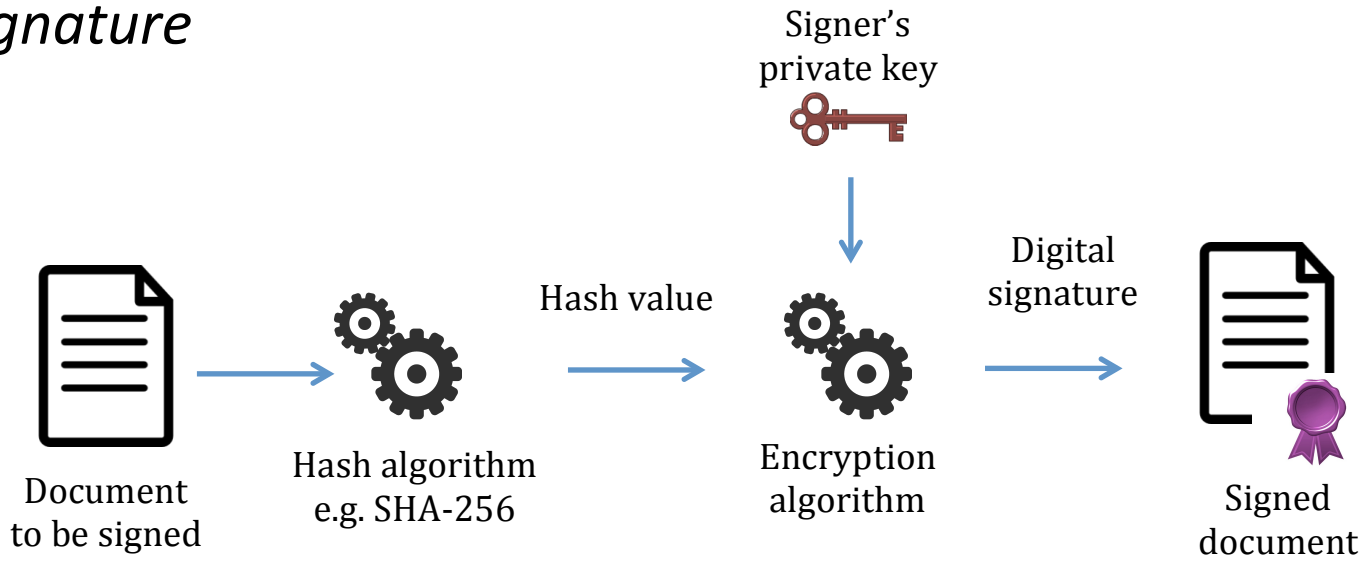
Common algorithms

- MD5 – collisions can be found in seconds, widely used in 90's
  - 160 bit length
- SHA-1, SHA-2, SHA-3 – function sets, respectively from 1993, 2001, 2015
  - SHA-1 and some SHA-2 functions have known vulnerabilities
  - suffixes of names SHA-256, SHA-384, SHA-512… say the bit length
- Whirlpool from 2000
  - 160 bit length

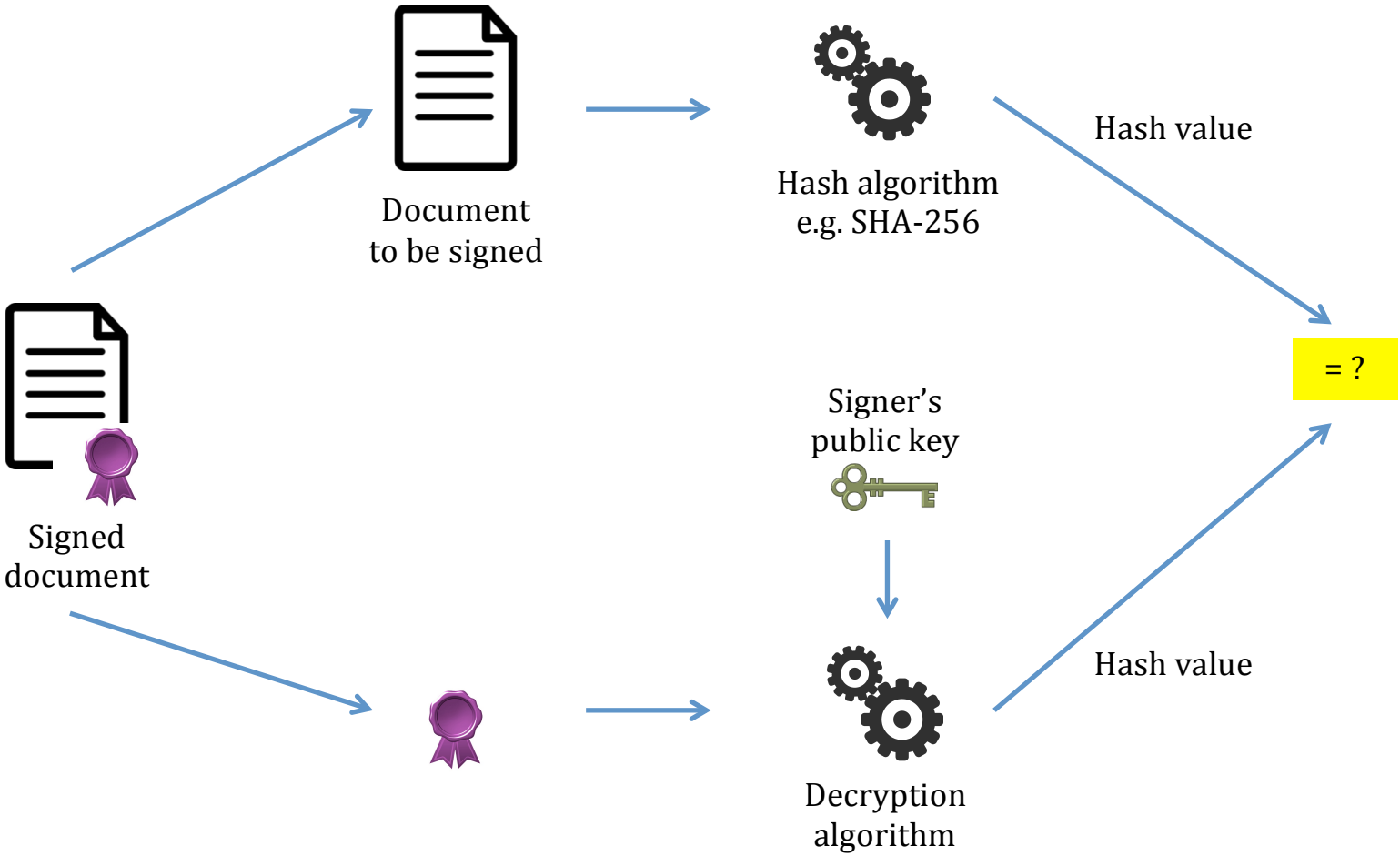
Applications

- Verifying the integrity of messages and files
- Signature generation and verification
- Password verification
- Proof-of-work
- File or data identifier

Digital Signature



Verification of Digital Signature



PKI *Public Key Infrastructure*

Provides for third-party vetting of, and vouching for, user identities

Organizational structure

- Repository
  - policies
  - CRLs - certificate revocation lists
- Certification Centre
  - certificate generation
- Registration Centre
  - personal or other subject identification

Certificates

Certificate – standard data structure for signature verification

- Qualified Certificate – issued by an approved authority
  paid
- Nonqualified Certificate – issued by any other institution
  nonpaid

Additional fields in a certificate

- **data about certificate authority**
- **certificate authority signature**
- personal biometric data
- others

Virtual Private Networks

Why do we use VPNs?

- To have access
- To save money
- To have more security

VPN is a private communications network
build over a public network

- Leased lines:
  - Dark fibres
  - SDH / SONET channels
- PSTN, X25, FR, ATM, MPLS, MetroEthernet
- Internet IP-VPN

VPN on OSI Layers

Application layer	Ciphered E-mail, DNSsec, SHTTP
Transport layer	SSL (Netscape) ← depreciated TLS (RFC 2246), SSH, SOCKS
Network layer	IPSec, GRE
	MPLS VPN
Data link layer	VPLS, L2TP, PPTP, Private ATM / FR networks built over public networks
Physical layer	Leased lines

Popular Services

- User-to-LAN
- LAN-to-LAN
- User-to-Server

RFC 2764 defines VPN types:

- VLL Virtual Leased Lines – can transport any data
- VPLS Virtual Private LAN Segments – LAN emulation
- VPRNs Virtual Private Routed Networks – separate routing domains over one infrastructure
  Virtual Routers RFC 2917, …
- VPDNs Virtual Private Dial Networks – shared Dial-Up servers in ISP network

Difficulties

- Many protocols
- Ciphering reduces throughput
- Private over public addresses
- Internet reliability

One ISP can provide SLA — *SLA – Service Level Agreement*

- VPN based on CPEs — *CPE – Customer Premises Equipment*
- ISP VPN services

Protocols Used to Build VPNs

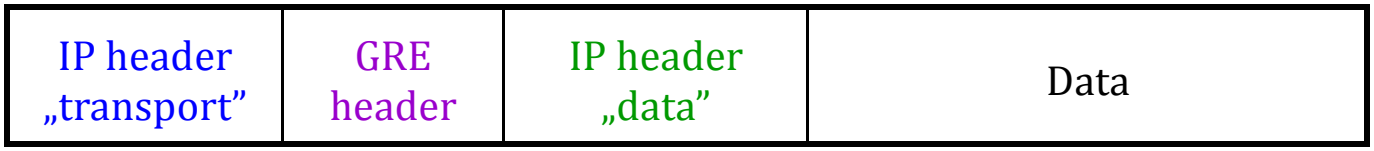
- Point-to-Point Protocol (PPP)
- Generic Routing Encapsulation (GRE)
- Point-to-Point Tunnelling Protocol (PPTP)
- Layer 2 Tunnelling Protocol (L2TP)
- IPSec

PPP

- PPP supports authentication and ciphering
- Can be used not only over synchronous links, but over any communication channel
- L2TP & PPTP use PPP
- Most ISPs provide PPP

GRE Generic Routing Encapsulation

- Allows encapsulation of any packets in any underlying protocol



- GRE can work on and for IP:
  - IP as a „transport”
    IP encapsulates GRE packets
  - IP as a „data”
    GRE encapsulates IP packets

PPTP Point-to-Point Tunnelling Protocol

- Developed by Microsoft, client-server
- Considered as obsolete, still in use
- Problems with firewalls

- Contains 2 packet types:
  - Control - session management for data transfer
    - Status query and signalling data
    - via TCP
  - Data
    - via PPP and GRE
    - GRE provides flexibility, IP or other protocols, e.g.: NetBEUI, IPX

L2TP Layer 2 Tunnelling Protocol

- Is based on
  - Cisco's Layer 2 Forwarding (L2F)
  - Microsoft's PPTP

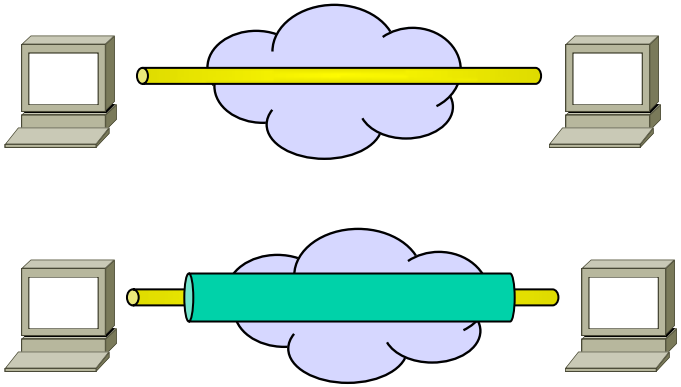
- L2TP assemble control and data channels
  - L2TP via UDP
  - Faster and thinner
  - L2TP more "Firewall Friendly" than PPTP
- LAN no ISP: addressing & authorization
- It is possible to dynamically change the end address

IPSec

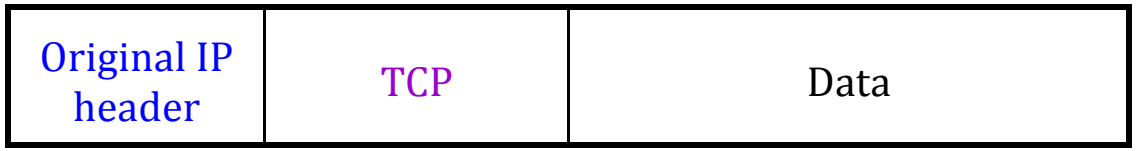
- Derived from IPv6
- Open, standard based, set of security protocols
- Aim – secure IP packets
- Strong authorization and ciphering mechanisms
- Can protect all packet or only its payload

IPSec can work in 2 modes

- Transport mode
  - Protects the next layer protocol – IP payload
  - No tunnelling – suits Intranet protection
  - Station to station communication
- Tunnelling mode
  - Protects all IP packet
  - Tunnels IP packet
  - Gateway to gateway communication

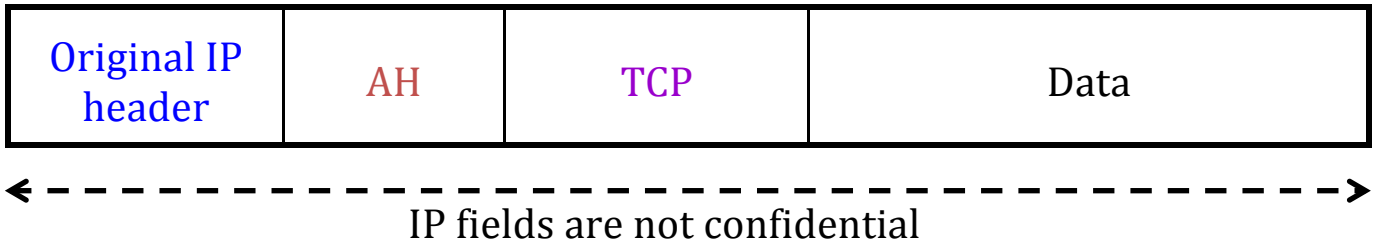


IPSec Transport Mode



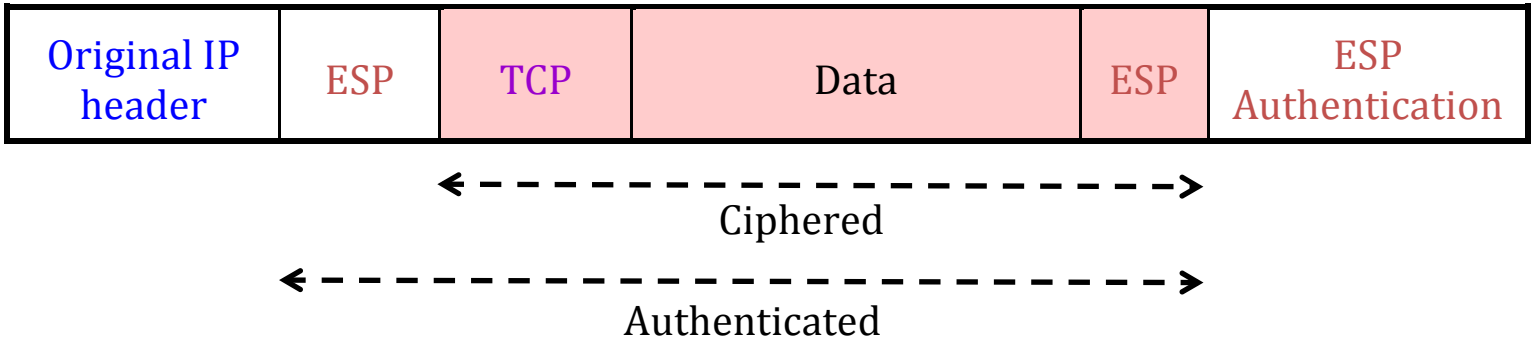
Authentication protocol

Authentication Header injection:



Security protocol

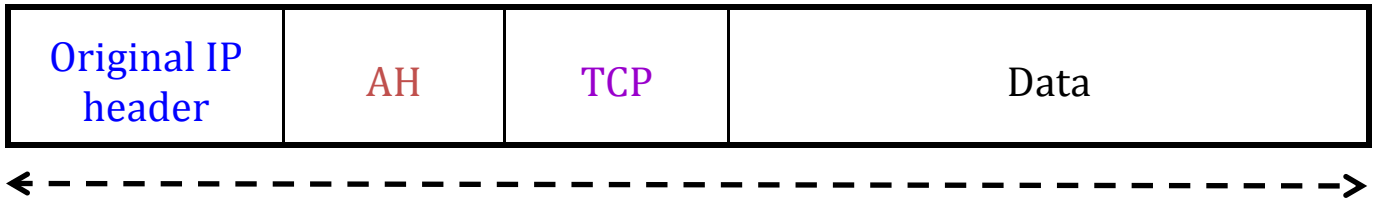
Application of Encapsulation Security Payload:



IPSec Tunnelling Mode

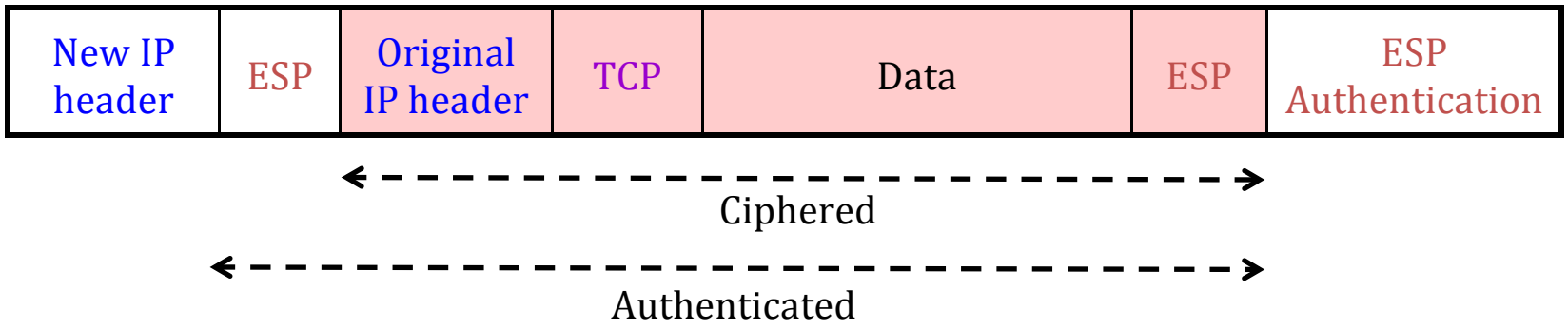
Authentication protocol

Application of Authentication Header :



Security protocol

Application of Encapsulation Security Payload:



Summary

- Threats and security services
  - Why is there a security problem?
  - Attack Vectors on the OSI Layers
  - Basic terms
  - DDoS & amplification attacks
- Characteristic of cipher algorithms
  - Cipher types
  - Diffie-Hellman Algorithm
  - Stream Cipher Properties
  - Block cipher properties
  - Use of asymmetric cipher
  - Cryptographic hash functions
    - Signature generation and verification
- Public Key Infrastructure
  - Certificates
- Virtual private networks
  - VPN types
  - VPN protocols
    - PPP
    - GRE *Generic Routing Encapsulation*
    - PPTP *Point-to-Point Tunnelling Prot.*
    - L2TP *Layer 2 Tunnelling Protocol*
    - IPSec

Questions

1. Why computers are vulnerable?
2. What are the motivations of cyber-attacks?
3. What are principal entries for malicious code?
4. Describe the principal security tools.
5. Describe the principal security services.
6. When secure time reference is needed?
7. How can we gain a secure time reference?
8. Can steganography use protocol headers, why?
9. Explain the attack called “buffer overflow”.
10. Explain the way a DDoS attack can be performed.
11. Do ciphering guarantee that a recipient discovers any malicious modification of a cipher text? Why?
12. What are popular cryptographic hash functions?
13. What are the main properties of a cryptographic hash functions?
14. What is a digital signature and what is the way to verify it?
15. How a stream cipher works?
16. Describe Diffie-Hellman key exchange.
17. Can we use symmetric cipher for authentication?

18. Can we use symmetric cipher to guarantee non repudiation?
19. Mention principal block symmetric algorithms.
20. Mention principal block asymmetric algorithms.
21. What are the advantages and disadvantages of stream ciphers?
22. What are the advantages and disadvantages of symmetric ciphers?
23. What are the advantages and disadvantages of asymmetric ciphers?
24. How authentication is performed using asymmetric ciphers?
25. What does *public key infrastructure* mean?
26. What is the difference between Qualified Certificate and Nonqualified Certificate?
27. When a certificate revocation list is updated?
28. What are Virtual Private Networks?
29. What are common disadvantages of VPNs?
30. What for a VPN can be deployed?
31. What is a common feature of VPN and VLAN?
32. Which techniques are used to build VPNs on application layer of ISO OSI model?
33. Which techniques are used to build VPNs on transport layer of ISO OSI model?
34. Which techniques are used to build VPNs on network layer of ISO OSI model?
35. Which techniques are used to build VPNs on data link layer of ISO OSI model?
36. What are the advantages of a VPN that is based on Customer Premises Equipment?
37. What are the advantages of a VPN that is an ISP service?
38. What are VPN types defined at RFC 2764?

39. What are different meanings of VPLS?
40. Why GRE (Generic Routing Encapsulation Protocol) is called generic?
41. What are the advantages of L2TP with respect to PPTP?
42. What is first (in the transmitted header chain) and why, L2TP header or IPSec header?
43. What is the difference between transport mode and tunneling mode of IPSec?
44. What are VPN's layers that can be build in MPLS networks?

Questions for curious minds

1. Give examples of socio-techniques used for attack an enterprise network.
2. What is the advantage of self-synchronous stream cipher with respect to a synchronous one?
3. What function is used in the RSA algorithm?
4. What is the web of trust?
5. What is the principal difference between X.509 and OpenPGP certificates?
6. What are the problems of public key servers? See en.wikipedia.org/wiki/Key_server_(cryptographic).
7. Can we fully trust at Qualified Certificates? See en.wikipedia.org/wiki/DigiNotar.
8. Can we tunnel ATM packets over an MPLS networks? If so, are there any limitations?
9. What is the principal function of the ssh unix command?
10. Is it possible to use the ssh unix command to set a tunnel from a home computer to given service (e.g. a local HTTP server) in a private network, having an account on a machine in the network?

11. Give an example of stunnel usage?
12. What security mechanisms are used by stunnel?
13. When is it better to lease dark fibers than to use VPN over Internet?