



Network Security

Introduction to security technologies
Gralla: chapters 44-50 and rest of part 9



- Why security?
- Basic information security concepts
- Threats in network environment
- Solutions
 - Planning
 - Firewalls
 - Intrusion detection
 - Anti-viral software
 - Cryptography



What is Information Security?

- Organizations and individuals have information, which has value
- This value must be protected against threats
 - Protection causes costs
- Computer and network threats are only one part of all threats
 - Physical threats
 - Logical threats



Terms of Data Security

- Confidentiality, luottamuksellisuus
 - We keep our secrets
- Integrity, eheys
 - Nobody changes our data
- Availability, saatavuus, käytettävyys
 - We have access to our data
- These from the CIA-model
 - Confidentiality, Integrity, Availability
 - There is a certain inherent incompatibility in these requirements, availability is often in conflict with the other requirements



Other Useful Terms

- Authentication, todentaminen (tunnistaminen)
 - We recognize another entity on the network
- Non-repudiation, kiistämättömyys
 - We can prove that something happened
- Authorization, valtuutus, oikeuttaminen
 - We control access to our data



Different Kinds of Threats

- Physical breakdowns
- Operating mistakes
- Planning mistakes
- Intentional attacks for fun and profit
- Own personnel is usually considered the largest security threat



Typical Network Threats

- Eavesdropping
 - Easy on most LANs with physical access to media
 - More difficult on backbone networks
- Break ins
 - Network is a two way medium
 - Tools make finding and exploiting known faults easier
 - Access to the computer can be used to access the data on computer or to use the computer as a base for further attacks
- Connection capture
 - TCP connections can be captured and used (software is available)
- Replay
 - The attacker re-sends an earlier message



More Network Threats

- Denial of service
 - Overloading a server
 - Faulty data packets
- Pretension
 - Fake E-mail
 - IP address forgery (IP spoofing)
- Masquerade and man in the middle
 - Attacker can pretend to be a service
- Compound attacks
 - IP traffic can be rerouted to a different path and then eavesdropped or captured



Typical Attack from Outside

- First scan the internal network addresses for hosts and services
 - Can be done in a stealthy slow and low mode
- Then attack found targets
 - Known weaknesses, exploits
 - Scripted attacks, over in less than minute
- Get the data and run or
- Prepare a base for further attacks
 - Hide tracks
 - Install Rootkit



Viruses and other Malware

- Viruses are self-replicating programs
- Trojan horses are benign-looking programs that do something harmful, too
- Worms are network viruses
- Viruses spread mostly because of user's misplaced trust and carelessness
- Modern viruses are network aware
- Currently most malware is professionally designed to target specific targets
 - E.g. to create a network of controllable hosts (bot network)
 - E.g. to modify the browser and redirect banking transactions



- Security planning
- Personnel selection and training
- Physical security
- Technical solutions
 - Host based security
 - Firewalls
 - Intrusion detection
 - Anti-viral software
 - Cryptographic solutions



- The main document for organization's security
- Defines
 - Assets
 - Threats
 - Solutions
- Contains
 - Aims
 - Resources
 - Responsibilities
 - Guidelines to personnel
- Technical implementation



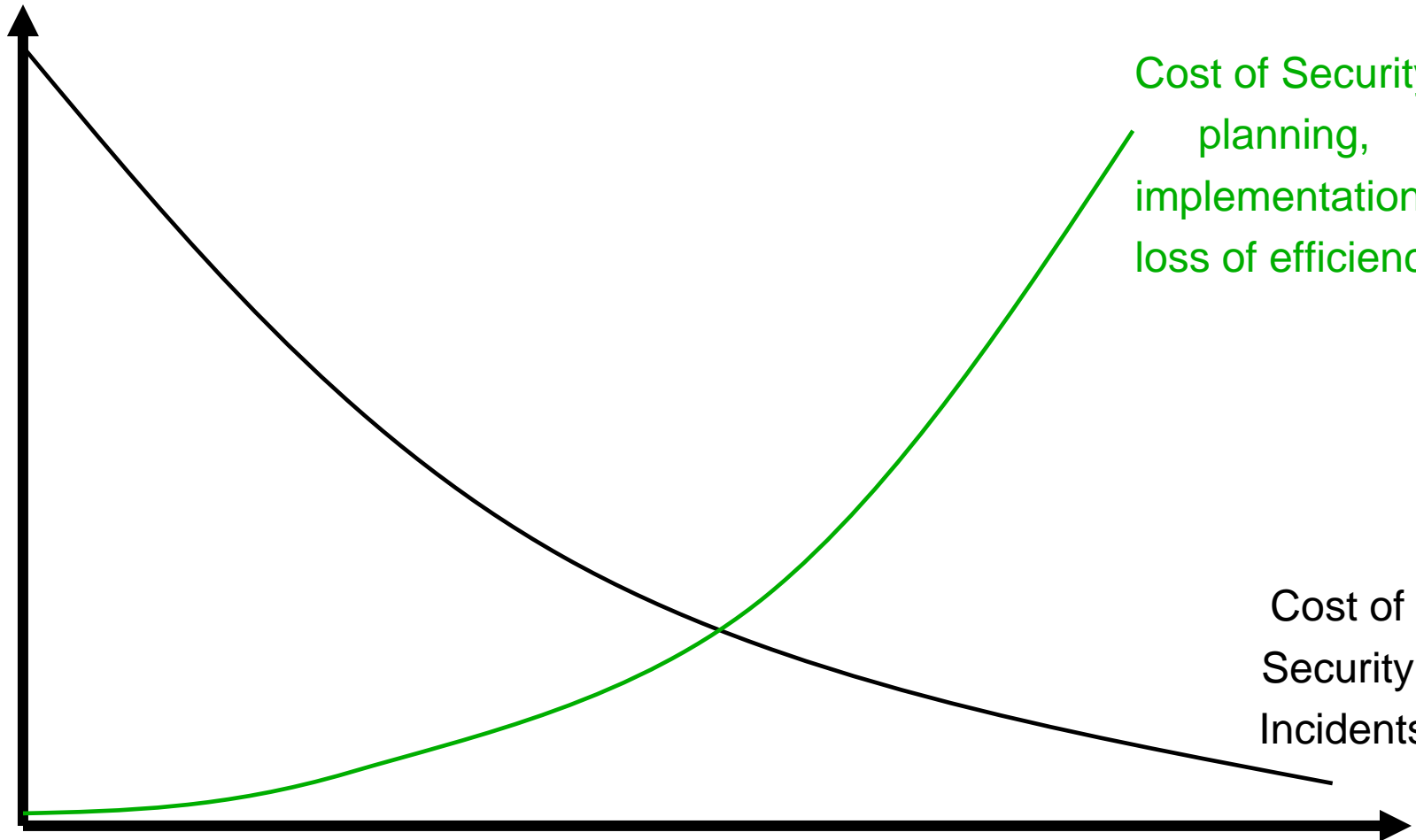
Designing an Information Security Policy

- Evaluate your current situation
 - Information assets
 - Existing security methods
- Evaluate the risks
- Decide what to protect and how
- The value of information should be defined by the owner, generally not the writer of the policy
- Actions to be implemented should be prioritized based on risk, not on the ease of technical implementation



Cost of Security

Cost



Level of Security



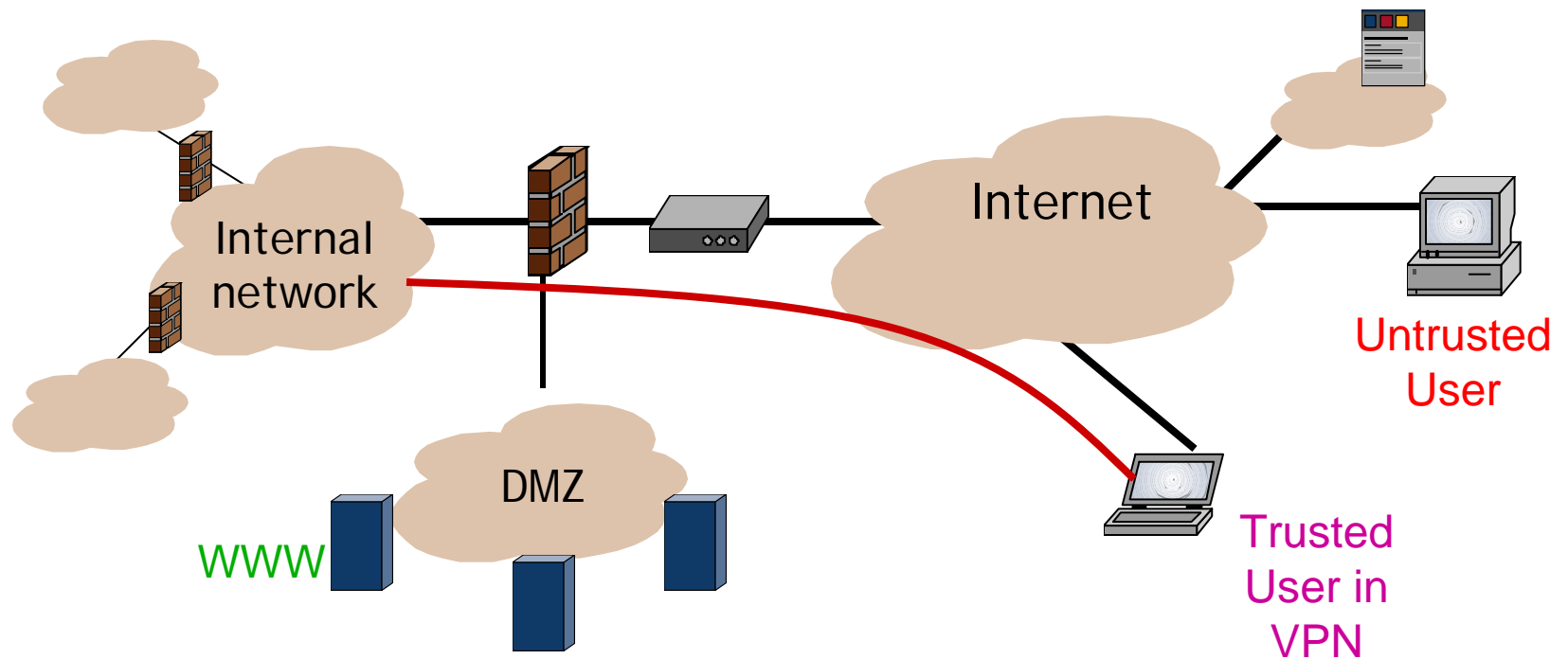
Security Is in the Processes

- Current focus on the security management area is in developing the processes of an organization in such a manner, that the organization works in a secure way
 - In the World War II allied powers could usually break most of the German Wehrmacht and Luftwaffe messages, but not Kriegsmarine messages because (besides better technology) they had good encryption discipline
 - No standard messages
 - No repeated session keys
 - No clear-text retransmissions
- This means that the security policy must be communicated to the people
 - The security policy that is delivered to the entire organization should be short, easy to understand and reasonable
 - Unreasonable security policies are usually not followed



Secure Networking

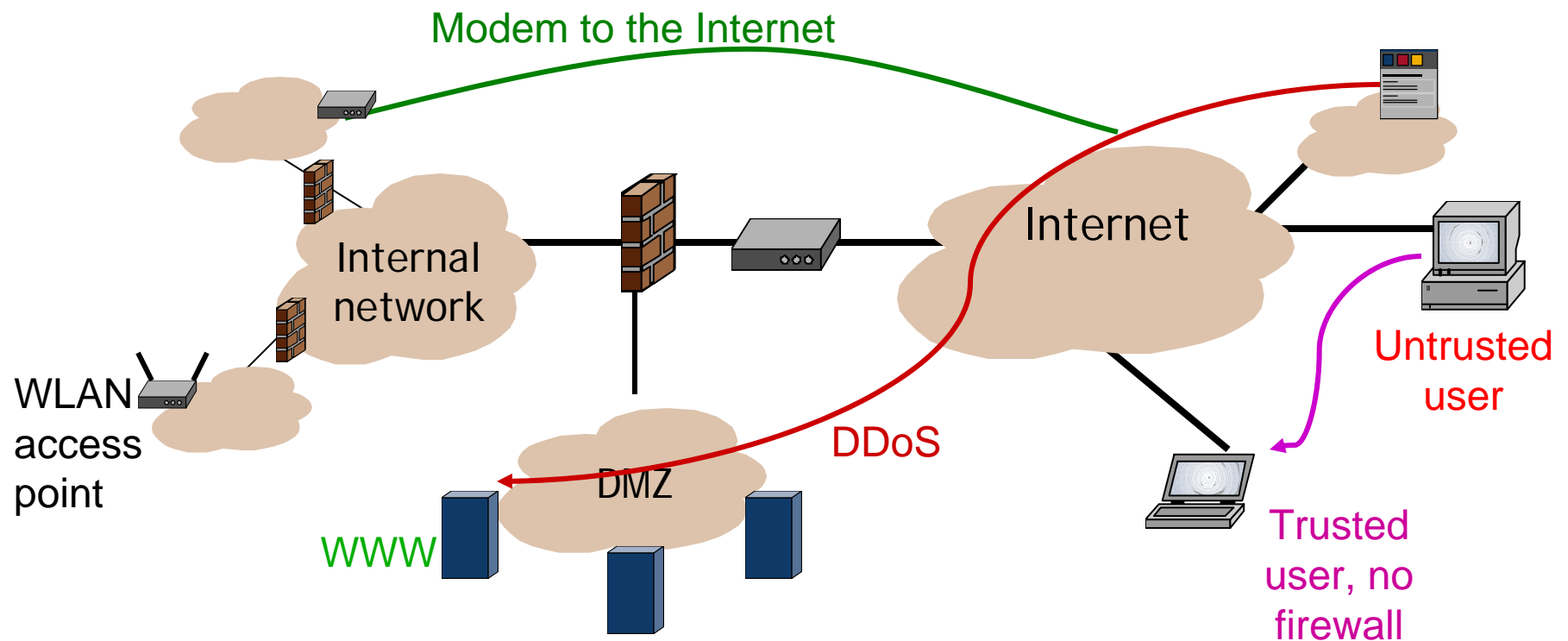
- Firewalls limit access to the network that they protect
- Encryption protects data in transit
- Cryptographic identification provides strong authentication





Networking Reality

- If left unsupervised, the security is going to be broken
- Your own users can break the security intentionally or unintentionally





Host Based Security

- A host on the network is always a potential target
- Threats can be countered by:
 - Reducing the amount of available services
 - Limiting access to services
 - Software firewall
- Once the attacker is inside the host, gaining additional privileges is easier
 - From shell to root is not difficult in most common Unixen, if left unpatched for a while



- Firewalls limit access between networks
- Typically used to protect internal networks from external threats
- Two basic types
 - Filtering firewall
 - Application level firewall
- Usually both features combined to a hybrid product



Filtering Firewalls

- Each IP packet is inspected and passed on or dropped based on
 - Sender and receiver IP address
 - Protocol type (TCP, UDP, other)
 - Sender and receiver port address
 - IP or TCP options, SYN/ACK bits etc
 - Stateful knowledge of connections (TCP connections may be opened from internal to external networks)
- Many routers have most of the basic functionality of a filtering firewall
- Network address translation is an additional feature



Application Level Firewalls

- Application must connect to the firewall
 - E.g. HTTP proxy server
 - Application must be aware of the firewall
- Firewall can inspect application data
 - Prevent ActiveX
 - Search for viruses
- Firewall can also be transparent to applications and still work on application level
 - More demanding for software



Personal Or Host Firewalls

- Instead of a firewall device on the network an application in the host (work station) of the user
 - The application needs to attach to the kernel to receive the raw data
- Has the advantage of knowledge of the internal applications
 - Instead of looking at IP and TCP/UDP addresses can look at a specific application
 - Can notice if an application has changed
- Currently very popular in Windows
 - Often connected with antiviral protection to form a security suite
- When used with an external firewall adds depth to the protection



How to Defeat Viruses

- Avoid environments that actively support viruses
 - E.g. Microsoft Office tools
- Use a virus scanner that knows the signatures of different viruses
 - The virus signature database needs to be updated frequently
 - Virus scanning program manufacturers currently share new viruses efficiently and focus on keeping the scanning programs up to date
 - Heuristic scanning that would recognize “bad intentions” of a program has been proposed frequently, but it does not yet work
 - The virus scanner can remove the virus from the host file or destroy the file
 - The scanning can be done for every file when it is opened
 - The scanning can also be done to file servers or at firewalls

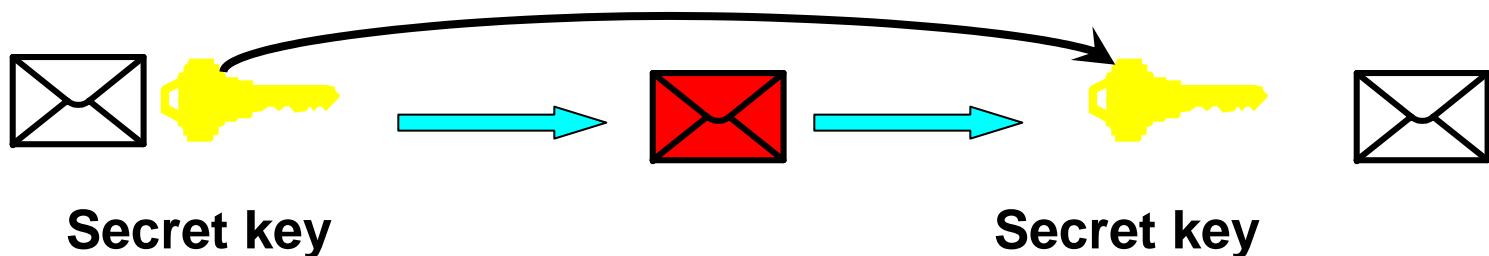


- Cryptography is a branch of mathematics that is much used in the real of information security to provide
 - Confidentiality
 - Integrity
 - Authentication
 - Non-repudiation
- These effects can only be reached when cryptography is used correctly
- Just the fact of using cryptography does not provide security in itself



Secret Key (Symmetric) Cryptography

- Encryption and decryption are based on the same key (shared secret)
- Algorithm is usually based on bit pattern transformations and bit transpositions
- Usually efficient and fast: suitable for encryption of large amounts of data
- Main problem is how to transport the secret key to both participants





How Symmetric Encryption Works?

- The main principles are
 - Confusion, bit patterns are substituted for another bit patterns
 - Diffusion, positions of bits are permuted
- Here is a sample of how the IDEA algorithm operates on a block of data, divided to four inputs, using subkeys generated from the encryption key
- This round is repeated several times to produce the encrypted data block

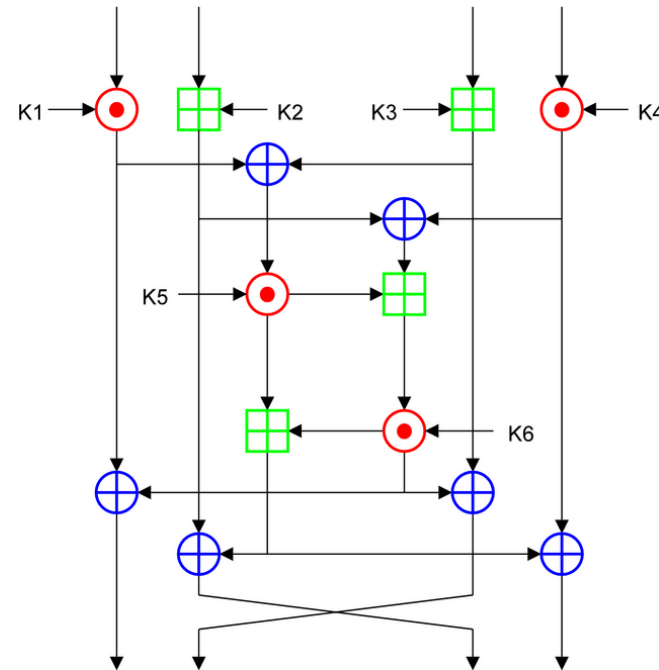


Image © Matt Crypto/Wikipedia

⊙ multiplication modulo $2^{16} + 1$

⊞ addition modulo 2^{16}

⊕ bitwise XOR



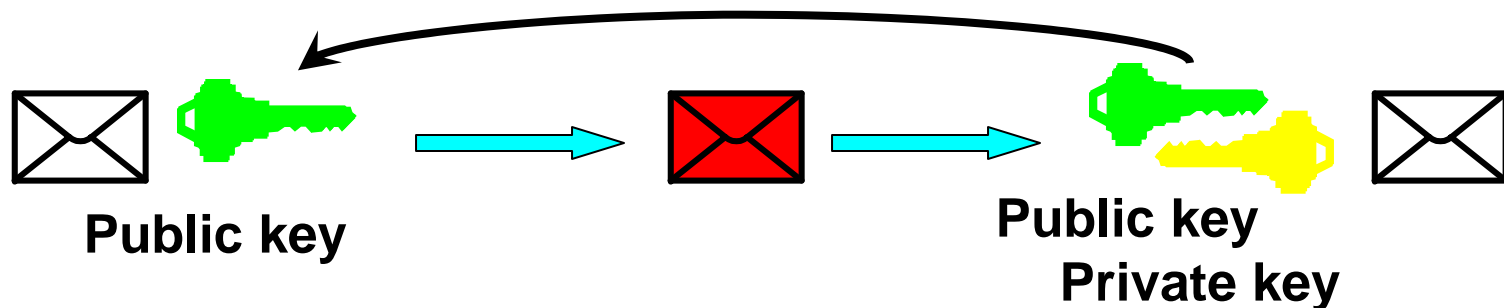
Public Key Encryption

- The public key algorithms are based on the properties of several mathematical operations
 - Very roughly: it is easy to multiply two large primes, but difficult to factor the result back to components
- An participant has two keys, related to each other
 - What is encrypted with one key can be opened with the other key
 - One key is called "public" and can be shared with other participants or even made public
 - Another key is called "private" and is kept secret
- A secret message encrypted with the public key can be opened only by applying the private key
- Public key encryption is usually not very efficient (involves multiple mathematical operations)
- Typically a random session key is created and encrypted with the recipient's public key
 - The session key is used with a symmetric algorithm to encrypt the bulk of data



Public Key (Asymmetric) Crypto

- Encryption and Decryption use separate keys
- Keys are related to each other with a mathematical relation
 - Public key can be safely published
- Whatever is encrypted with one key, can be decrypted only with the other key
- Encrypting with the private key proves the identity of the sender





Public Key Signatures

- Most public key algorithms have an interesting side effect: the keys can be reversed
- Thus anything encrypted with the private key can only be opened by the public key
 - Which means that it must have been encrypted by the holder of the private key, thus creating a signature

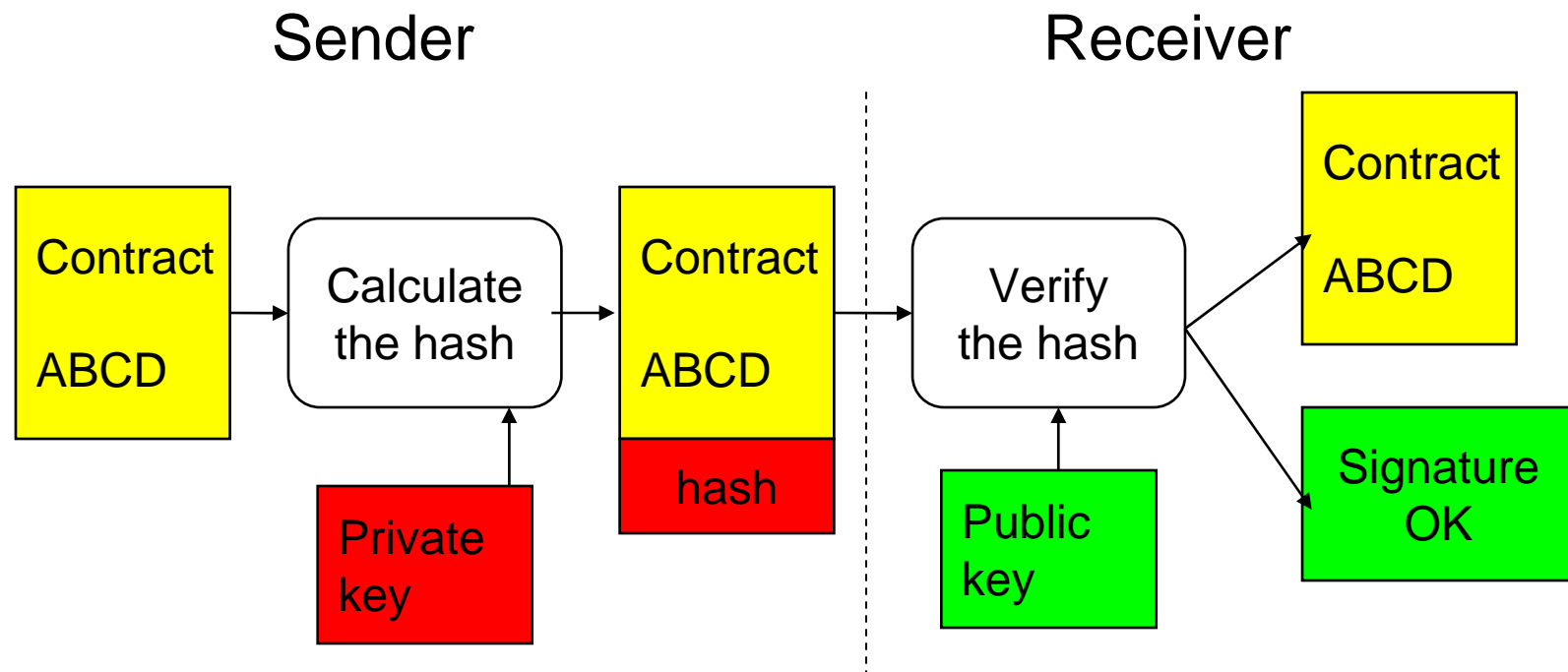


- A hash is a cryptographic one way function that produces a record smaller than the plaintext
 - Sometimes called a fingerprint
- The plaintext can not be recovered from the hash, but it is practically impossible to produce a plaintext that would produce the same hash
- Thus a hash encrypted by the document signer's private key can be used as a signature for a document
- Used to produce Message Authentication Codes (MAC) to verify the integrity of a message
- Suomeksi: tiiviste



Hash Functions

- A cryptographic checksum of the data (one way function)
- Difficult (impossible) to forge
- Very useful for providing integrity and non-repudiation





- Cryptanalysis is the science and art of breaking algorithms and cipher messages
- Relies much on statistical methods and analysis of data patterns on the ciphertext
- Several attack models
 - Ciphertext only
 - Known plaintext and ciphertext
 - Chosen plaintext and ciphertext
- Brute force attack of going through the whole keyspace is utilized if keys are short enough
 - 128 meaningful bits is currently too much and 256 bits impossible
 - Note that some algorithms use keys where there is redundancy, e.g. 512 bit RSA key is not considered secure
- Current algorithms can be considered unbreakable, but cryptanalysis is also valuable as a method of evaluating algorithms



- Whole systems can be created from these primitives
- A system requires usually that several algorithms are combined with key management to do something practically useful
 - Confidentiality is usually provided by encrypting the data with a secret key algorithm and by encrypting the secret key with a public key algorithm
 - A message can be signed by encrypting the hash of the message with the private key, this can be used for non-repudiation
 - An user can be authenticated by proving the possession of the private key by encrypting a message
- Here PGP is presented as an example of a system



PGP (Pretty Good Privacy)

- Designed by Phil Zimmermann for providing cryptographic protection of e-mail and file storage
 - Uses strong cryptographic algorithms (for its own time, published 1991)
- Offers
 - Authentication using digital signatures
 - Confidentiality with the use of encryption
- Technical features
 - Byte conversion to ASCII for e-mail
 - Key management uses e-mail addresses as subject labels

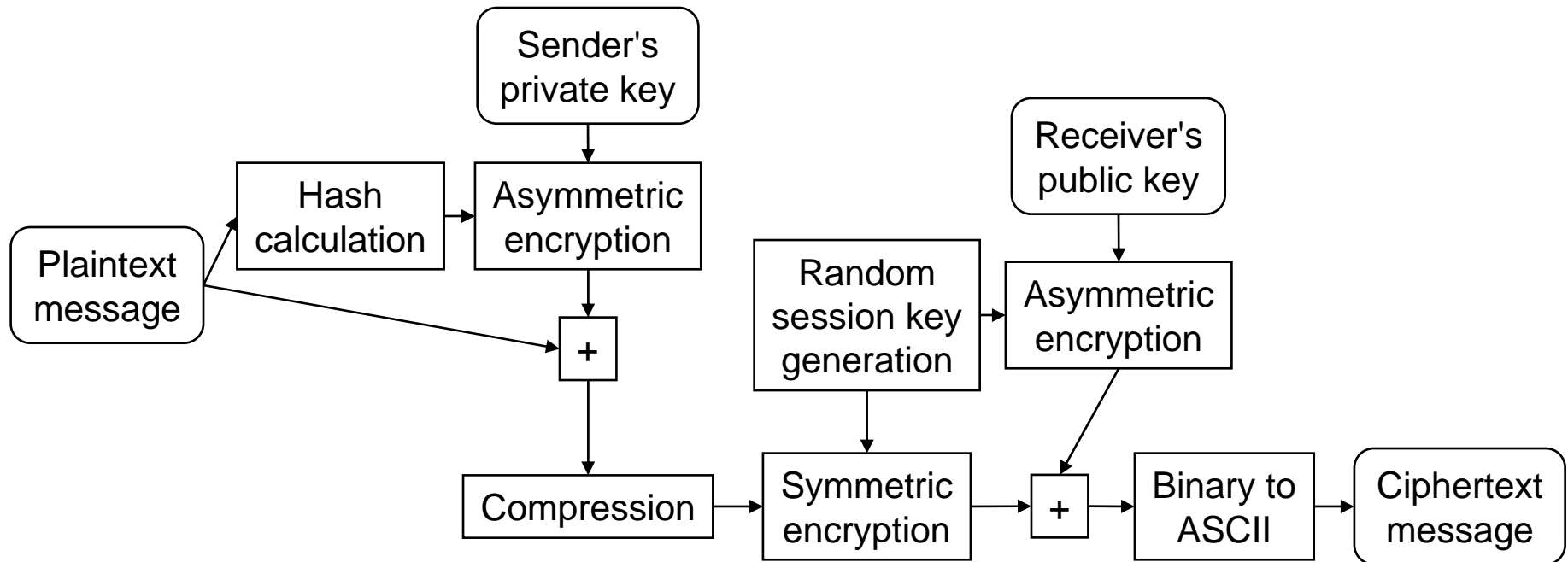


PGP Design Philosophy

- Written for individual, technically skilled end-users
 - Every user creates and manages their own keys
 - Every user has a freedom to choose, whom to trust
 - No administrative organization or governments involved in operation
 - No hierarchy in trust relationships
- Independently produced, no standardization organizations involved
 - Original versions open source, free of charge
 - Later commercialized and several incompatible versions exist



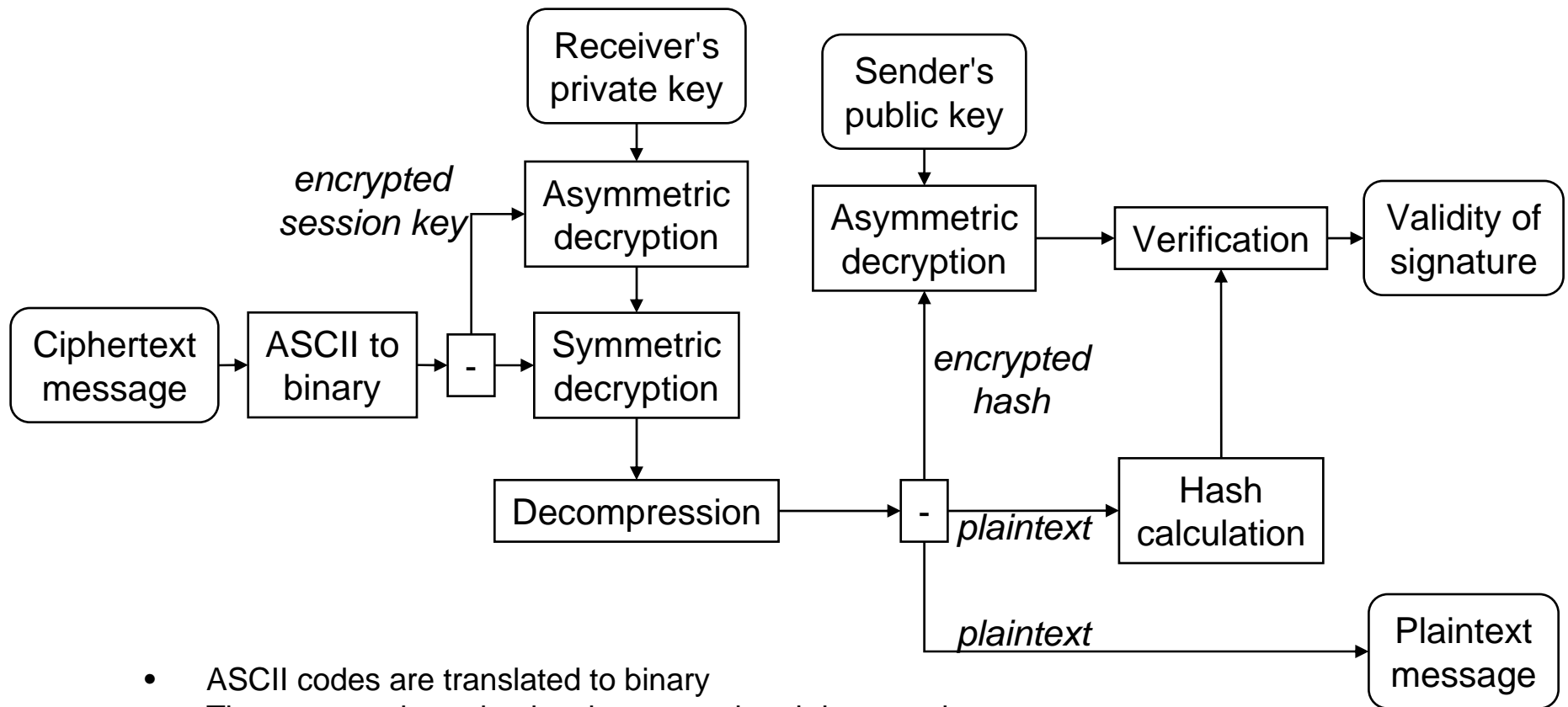
Sending a PGP Message



- The message is signed, compressed and encrypted
- The encrypted session key is added to the end of message
- Binary message is translated to characters, which pass through the e-mail system



Receiving a PGP Message



- ASCII codes are translated to binary
- The encrypted session key is removed and decrypted
- The message is decrypted and decompressed
- The encoded hash is removed and decrypted
- The hash is recalculated and compared to the hash in the message

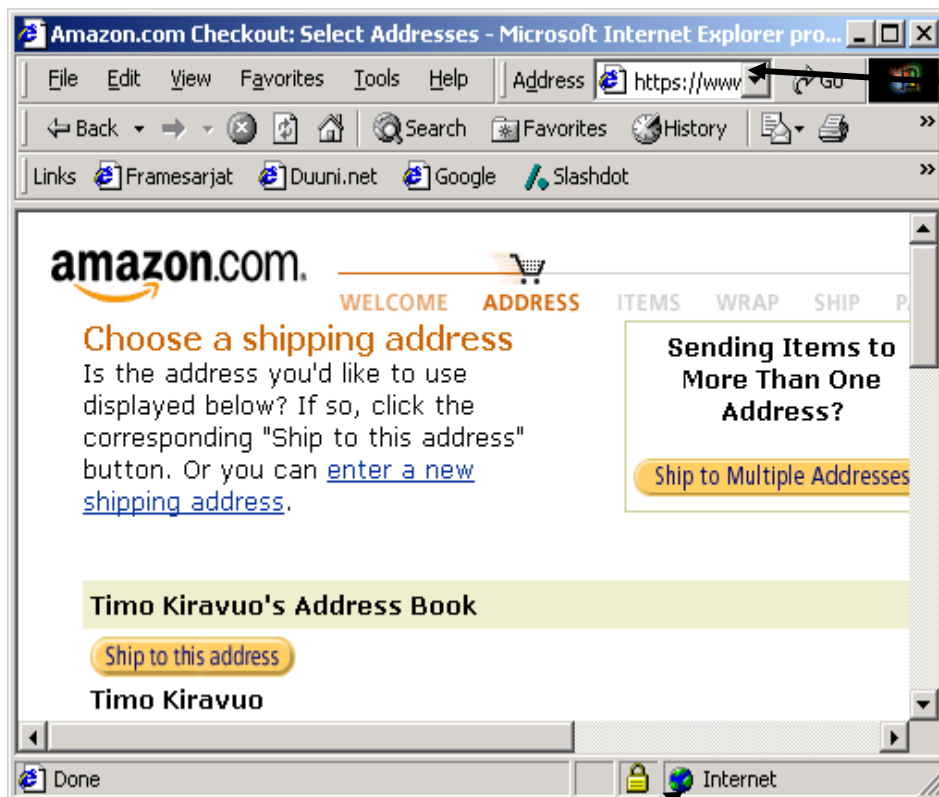


- A certificate is a cryptographically signed formal statement, which certifies a public key with some properties, like identity or access permissions
- To verify the certificate the end user must have the public key of the signer
 - Or a certificate loop must be formed, with unbroken chain of trust, starting from the verifier
- Certificates can be issued by trusted third parties
- We present SSL (Secure Socket Layer)
 - Encrypted TCP connection, with server side authentication
 - Used mostly for WWW services



TEKNILLINEN KORKEAKOULU

Encrypted WWW Connection



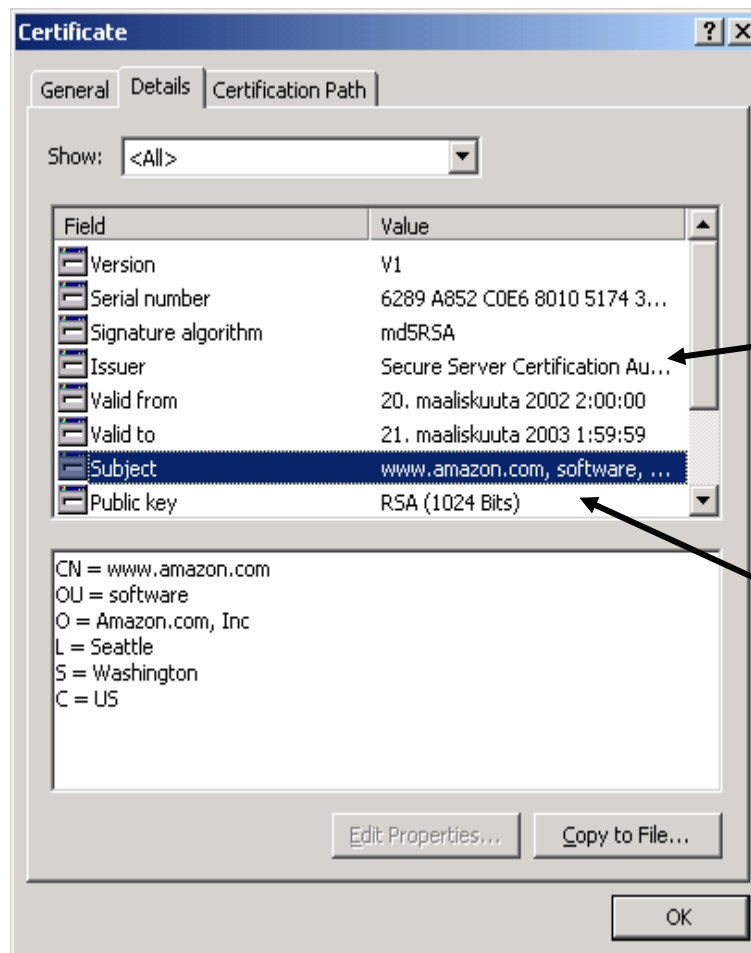
URL begins
with HTTPS

SSL encryption is in effect



TEKNILLINEN KORKEAKOULU

The Certificate from the Server



Click the lock
to read the
certificate

Certifier

Subject of
certification



Protecting Data in Transit

- Encrypting traffic is relatively easy
 - Protects confidentiality and integrity
 - SSL (Secure Socket Layer) is a standard feature in web browsers
- The real question is whom we are talking to and what they may do
 - Authentication and Authorization



- Something a person knows
 - Passwords, pass phrases
 - Difficult to remember unless used often
 - Easily revealed, read the Post-its® in your office
- Something a person has
 - Smart card, electronic token
 - Somewhat easy to lose or to be stolen
- Something a person is
 - Biometrics (generally over-hyped)
- Strong authentication usually combines two of these



Authentication Technologies

- Passwords and User Names
 - Easy to use, too easy, since users can tell them to other people
- One time passwords are better
 - Generated and stored as a list
 - Or an electronic token with a synchronized clock inside
 - Used by banks
- Or more complex systems
 - A private key on a smart card
- Authentication can be sold as a service by a third party trusted by the participants



Nothing is Perfect: Phishing

- Asking users to give their password
 - Works, but not very well
 - Users are the weak point of most security systems

Nordea's Netbank - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop Go Search Print

Nordea Netbank

In English www.nordea.fi

Take care to fill out the fields of the Form very thoroughly and to avoid possible mistakes.

Indicate the User Number and the Account Type in this area.

solo

Customer number:

Account Type: Choose

Specify 4 passwords in this area, which have never been used before. Important: Start from the FIRST non-used password and follow the sequence order. Example: If you have already used 11 passwords, indicate 4 passwords starting from the 12th (12, 13,..., 15).

= = = =

Specify your Payment Confirmation Codes in this area. A letter in the Form shall correspond to the letter in your Code Table.

A = F = L = R =

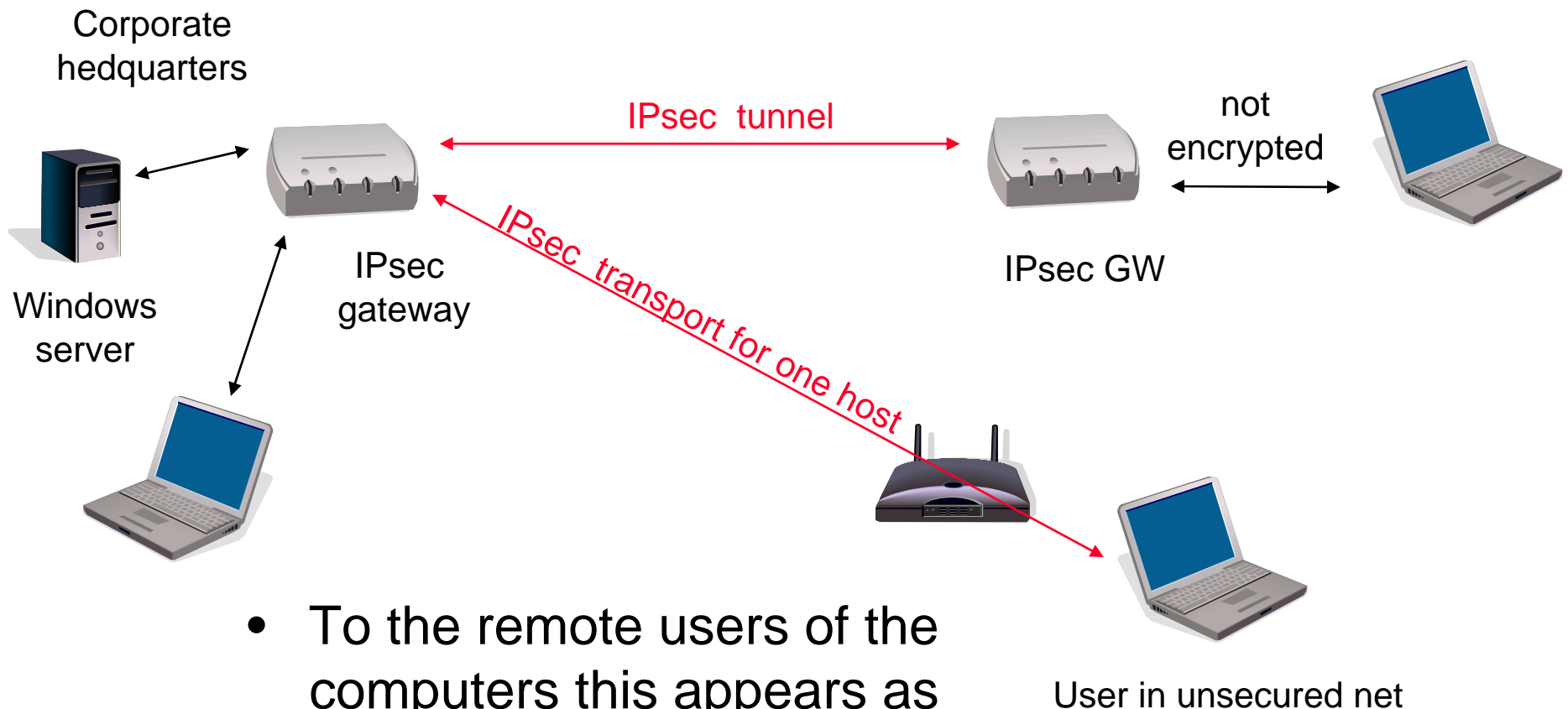
B = G = M = S =



- A protocol suite designed by the Internet Engineering Task Force (IETF)
- Describes a standard architecture for securing Internet traffic at the IP layer
 - Provides integrity and confidentiality
 - Independent of cryptographical algorithms used
- Used to build VPNs (Virtual Private Network)



Virtual Private Network with IPsec



- To the remote users of the computers this appears as one network



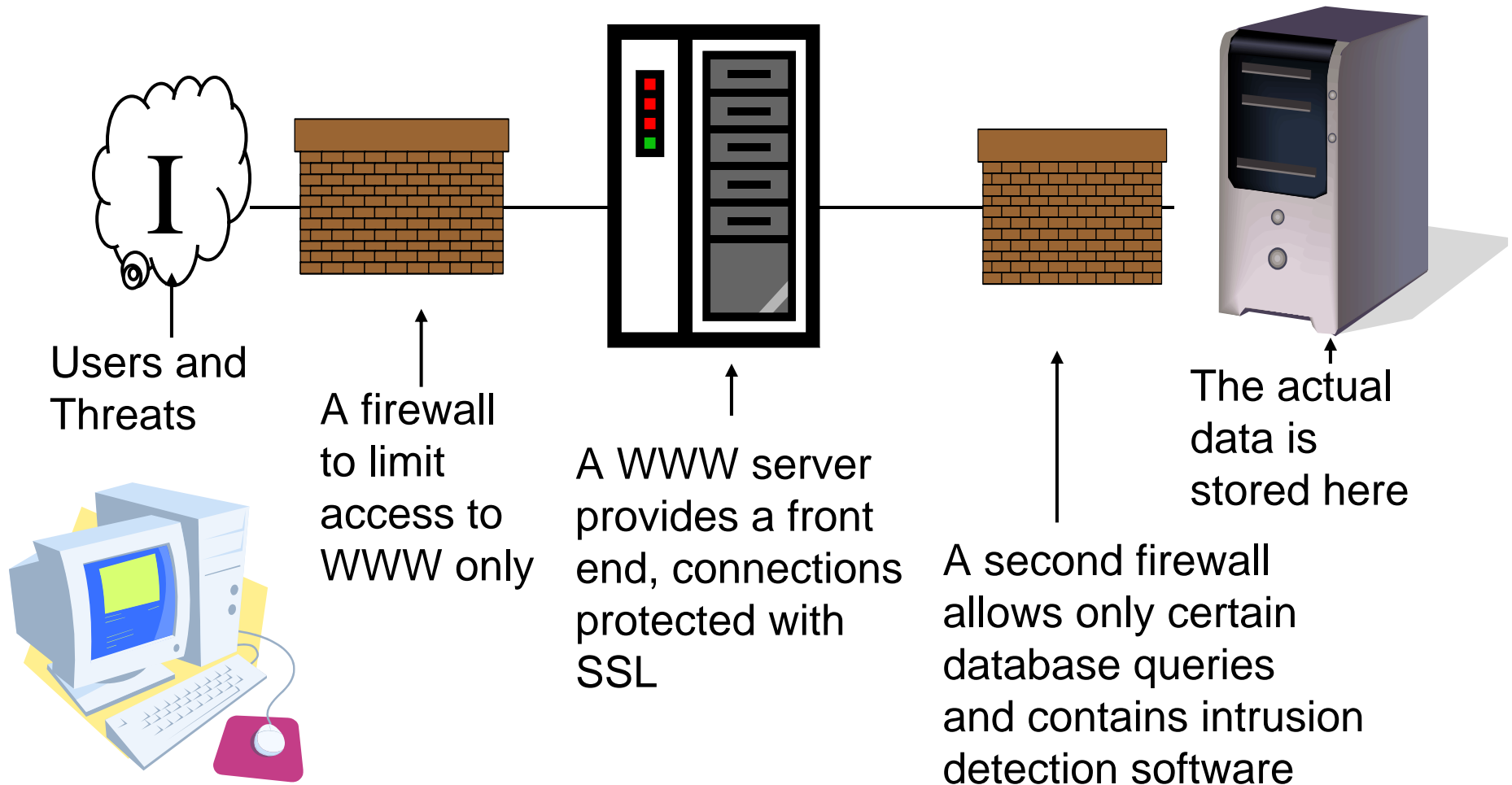
IPsec Benefits

- Cryptographical protection of Internet traffic for all protocols and applications running over IP
- IPsec security services are transparent for applications and users
- IPsec enables construction of Virtual Private Networks
- Good support for implementing and maintaining an organization's security policy
- High level of flexibility allows IPsec to be run over various types of public key infrastructure.



TEKNILLINEN KORKEAKOULU

Secure WWW Services, an Example





How to Protect a Static Web Site

- Install the system behind a firewall that allows only TCP 80 (HTTP) and 443 (HTTPS) from the Internet
- Remove all unnecessary services from the host
 - Defense in depth
- Go carefully through the configuration of the server and remove all unnecessary features
 - E.g. following symbolic links or shortcuts
- Turn on security related features
 - E.g. logging (to a separate computer) to help detect misuse
- Have a strict discipline on operations
 - To make sure that nobody weakens the security
- Etc.



More on WWW Protection

- No that the SSL does not protect the server
- Interactive sites need an analysis of the software driving the site
- Good design helps on auditing the protection
 - All interactive code in one place is easier to analyze
- Good design also helps in creating the protection
 - Modular design allows separation of tasks, like moving all customer data to a separate database host



Examination: Question formats

- Concepts and acronyms
 - Q: Firewall (1p)
 - A: A device which limits traffic between two networks
 - A: An implementation of the security policy, controls information flows
 - Q: TCP (1p)
 - A: Transmission Control Protocol, provides lossless data transmission over IP
 - A short explanation of the concept or acronym is enough
- Justify the following statements either correct or false
 - Q: IP is reliable (1p)
 - A: False, IP may lose data if e.g. router memory is overloaded
 - Q: TCP never loses data (1p)
 - A: Correct, as long as enough IP packets get through
 - A: False, if a network connection is broken, TCP may lose data
- Both the correct and false answer may be accepted for a particular question, the key is in being able to justify your position



Question formats...

- Several short questions, like "Compare UDP and TCP (3 p)"
 - A written reply, with a diagram if possible
 - Compare does **not** mean "list features", but that you really compare the technologies, like TCP provides this, UDP that
 - Also questions which require applied knowledge, like "What would happen if we tried to run TCP over Ethernet without IP?"
- Essay
 - Requires you to show that you can discuss a subject in an intelligent manner. Bullet points or diagrams are not sufficient here, you should aim to write something that looks like an article, which could be published in a magazine.



- Data security requires planning
 - Implementing technology without a security policy is useless
- Firewalls limit the effects of attacks
- Intrusion detection is a possible, but expensive solution
- Cryptography protects data in transit
 - Both integrity and confidentiality