



TEKNILLINEN KORKEAKOULU

PKI-based cryptosystems



Authentication and Authorization

- Authentication, Authorization and Accounting (AAA)
 - AAA services are especially important for commercial services
- User **authentication** means verifying the identity of a user
- Based on the authentication the user may be **authorized** to perform some actions
 - Access files, run programs
 - Access cellular network, make phone calls
- The usage may be logged, creating **accounting** information
 - Which can also be used for billing
- Suomeksi: todentaminen, valtuuttaminen/oikeuttaminen



- The user connects to a Unix server

```
10$ telnet server.foo.fi
```

```
login: kiravuo
```

```
Password:
```

```
Last login: Fri Aug 7 19:03:50 2006 from jalopeno
```

```
1$ _
```

- The "telnet" program opens a TCP connection to the Telnet server
- The user replies to the login query with his username
 - This provides the **identification** of the user
- The user is prompted for the secret password shared by the user and the server
 - The password provides the **verification** for the user's identity
- The user is now **authenticated**
- Based on the authentication the starting of a shell for the user may be **authorized**
- **Accounting** information is created and also reviewed



Attacking the Telnet

- The attacker may gain the user name and password by different means
 - Overseeing the user at the keyboard
 - Eavesdropping to the connection
 - Asking the user
- Having the username and password enables the attacker to present the user's credentials to the server and thus to masquerade as the user
- The attacker may also take over the TCP connection after authentication, as its integrity is not provided
- Or the attacker may pretend to be the server and ask for the user's name and password
- Clearly plain user name and password over TCP are not good enough for networked environment
 - For secure hardware (your own computer) password is suitable
 - Or for secure connections to a known endpoint



Basis for User Authentication

- Something the user knows
 - E.g. a password
- Something the user has in his possession
 - E.g. a smart card
- Something the user embodies or is
 - Biometrics
 - E.g. user fingerprint, voice
- Sometimes also other information
 - User's location
- Usually at least two of these methods are required for the user authentication to be considered strong



Public Key Infrastructure (PKI)

- Public key cryptography is a powerful tool for verifying an entity's identity
- But managing the keys can lead to a problem of order $n(n-1)/2$
 - Especially if we are supposed to authenticate both participants of communications connections within a large group
- But if there is a trusted participant, public keys can be *certified*
 - *Certificates* bind the key to an entity (person, company)
 - A certificate is signed by encrypting its hash with the *certifier's* private key
- The whole system is called PKI
- Suomeksi: varmenne, varmentaja, julkisen avaimen infrastuktuuri



What Is a Certificate

- A document signed by a party that the system assumes is trusted
- Contains at least:
 - The subject's public key
 - The subject's identity **or** an authorization bound to the key
 - Identity of the signer
 - Signature



Setting Up a PKI

- Alice, Bob and their friends decide to set up a PKI
- They select Trent to be the certifier
- Everybody (including Trent) creates their key pair
- Everybody proves their identity to Trent
 - Trent certifies their public keys
 - Everybody gets Trent's public key
- Now everybody has their private key, certified public key and Trent's public key
- Note that even Eve and Mallory can be certified
- The only part that has to be secret is the private keys



How Is a PKI Used?

- Alice contacts Bob
 - Bob does not know who he is talking to
- Alice and Bob do an initial Diffie-Hellman key exchange
 - Eve does not know who is calling Bob
- Alice presents her certificate to Bob
 - Bob gets Alice's public key
 - Bob has Trent's public key and verifies the certificate's signature
 - Bob is still not sure he is talking to Alice
- Bob sends Alice a random number
- Alice multiplies it with another random number
- Alice encrypts the result with her private key and sends it to Bob, with the random number
- Bob decrypts the message, verifies the number by multiplying his with Alice's and comparing to the message
 - Now Bob knows he is talking to Alice



What is this Thing about Multiplying Random Numbers?

- Cryptography is very hard to do right and there are many pitfalls
- If Alice would just encrypt Bob's number with her private key Bob could have a contract where Alice gives him her car and send the hash of the contract to Alice
 - Thus Alice generates the random number and modifies Bob's data with it
- These random numbers should be used only once, they are called *nonces*
- BTW, note that in the previous example Mallory could easily do a man-in-the-middle attack



The Benefits and Faults of a PKI

- **Benefits:**
 - Only N authentications needed for N participants
 - Certifier can keep his private key off-line
 - No need for online certificate creation
 - No need for anybody to reveal their private key
- **Faults:**
 - If the certified is untrustworthy, he can create false certificates
 - A complex and difficult to understand system
 - Requires online components (discussed later)
 - Selecting the certifier is not easy



- What happens if somebody's private key is revealed?
 - Anybody can masquerade as that person
- This can be solved by:
 - Time-stamping all transactions
 - Having a Certificate Revocal List (CRL) available online
 - Revoking certificates as of certain time
 - Earlier transactions are valid, latter are not
- Also certificates are usually created initially for a certain time period only
- Suomeksi: aikaleima, sulkulista



Certificate Contents

- X.509 is the most common certificate standard
- A X.509v1 certificate contains:
 - Certificate version
 - Certificate serial number
 - CA's signature algorithm
 - CA's X.500 name
 - Validity period
 - Subject's X.500 name
 - Subject's public key information
 - Signature



PKI in Applications

- How could PKI applied in applications?
 - Authentication
 - Which leads to confidentiality
 - Authorization
 - Integrity protection
 - Automatic verification of signatures
 - E.g. processing bills which require approval
- Today's practical uses
 - VPN encryption
 - Identifying web servers and encrypting the traffic
 - Encrypting and signing e-mail
 - Signing documents
- Some examples follow



Finnish Electronic Identity (FINEID, HST)

- A Finnish national project targeting at assigning a digital identity card for Finnish citizens
- Using the digital ID card, citizens should be able to authenticate themselves in the Internet in various contexts
 - Using municipal (government) services
 - Committing bank transactions
 - Sending e-mail
- Same ID card for serving several authentication purposes
- In practice this project did not receive any popularity
 - This is assumed to be due to the cost of the card (50-100 € including card and reader and due to the lack of services
- Suomeksi: Henkilön sähköinen tunnistaminen, HST



- Based on asymmetric cryptography
 - 1024-bit RSA was used in the first version
 - Every user is assigned two public/private key pairs
 - One for authentication and encryption
 - One for digital signatures
- These keys may be used in connection with SSL and S/MIME
 - Authentication of communicating ends in an SSL session
 - Verification of sender identity with S/MIME protected e-mail
- Open FINEID standards allow development of proprietary applications
 - Which could have happened



- Each user is assigned a smart card
- The smart card has a crypto processor capable of performing RSA operations, and 8 KB memory, containing
 - The user's private key for authentication and encryption
 - The user's private key for digital signatures
 - Two certificates certifying the user's public keys
 - The CA's (Finnish Population Register Centre) certificate
 - Two PIN codes, one for each private key
 - Application usage information (algorithm names, CA's name, etc.)
- The private keys are never let out of the chip
- PIN codes are used to prevent illegitimate use of the card



X.509 Certificates for FINEID

- Every user a unique digital identifier, FINUID
 - Different from the traditional national ID number used in Finland
- The FINUID code and the user name are bound to user's public keys using X.509 version 3 certificates
 - Every card has two certificates digitally signed by a Certification Authority (CA)
 - The CA's signature transmits trust between the user and the authenticator
- Finnish Population Register Centre plays the CA's role in the FINEID project



Example: Subject Field in a X.509 FINEID Certificate

```
SEQUENCE [72] {
  SET [11] {
    SEQUENCE [9] {
      OBJECT_ID [3] "2.5.4.6"      -- countryName
      PrintableString [2] "FI" } }
    SET [53] {
      SEQUENCE [15] {
        OBJECT_ID [3] "2.5.4.4"    -- surname
        T61String [8] "Törmänen" } }
      SEQUENCE [13] {
        OBJECT_ID [3] "2.5.4.45"   -- uniqueIdentifier
        BIT_STRING [12] 00 13 09 32 30 30 30 30 30 33 38 39 }
      SEQUENCE [19] {
        OBJECT_ID [3] "2.5.4.42"   -- givenName
        T61String [12] "Hilkka Leena" } } } }
```



Secure Socket Layer (SSL)

- Encrypted TCP-layer connection, with server side authentication from a trusted third party
- Application independent
 - Used originally for WWW services
 - Now also for other services like protecting e-mail transport between the client and server
- Standardized as TLS, Transport Layer Security
 - <http://www.ietf.org/html.charters/tls-charter.html>



SSL in a Web Browser

- The WWW browser has public keys for several trusted third parties
- TTP:s sign certificates for WWW servers
 - They certify that a server represents an organization
- SSL server is in port 443 on the WWW server
 - The corresponding protocol in the URL is HTTPS
 - After the secure connection is created, the session proceeds using HTTP inside the secure pipe
- The browser indicates the use of SSL to the user



SSL's Simple Handshake Protocol

- Client sends server a “hello” message
- Server sends over its certificate (includes server's public key)
- Client creates a session key, sends it encrypted by the server's public key
- The rest of the session is encrypted using the session key, HTTP is spoken as usual
- Client knows who the server is, but the server does not know who the client is
 - Actually, client knows that the server's name matches its certificate, which is not quite the same thing
 - Client authentication exists, too but typically SSL is not used for it



Trusted Third Party as the Certificate Authority

- Web browser manufacturers have selected a bunch of companies that act as CAs
 - Why should I trust Microsoft/Netscape and some company called RSA when doing my banking?
 - Selling person certificates for e-mail use at \$15 without any real verification is a nice business
- In other systems caution should be exercised, too
 - If a company uses some outsider as the TTP for its internal systems, that party could break the security
- Generally in the security literature *trusted* indicates an entity, on which reliability the system is based on
 - Which does not imply that the trusted party is trustworthy
- Some countries have laws about Certificate Authorities requiring certain quality for the operation



- SSH and SSL (TSL) protect TCP only
- IPsec is designed to operate on IP level
 - Can provide authentication and/or encryption for all IP based protocols
- An integral part of IPv6, available for IPv4, too
- Independent of cryptographical algorithms used
- Independent of a key management protocol
 - This is really a way to hide a problem, as it was found out that encrypting all traffic is not really hard, but the key exchange and key management turned out to be very difficult questions



IPsec Security Services

- Access control through authentication
- Connectionless (per-packet) integrity
- Anti-replay service
- Confidentiality
- Limited traffic flow confidentiality
 - All traffic between subnets can be tunneled, thus hiding individual IP addresses
 - Also provisions for hiding data length and generating dummy traffic
- Overall IPsec provides a Virtual Private Network (VPN) by enabling IP based networks at different sites to be connected securely and transparently



How IPsec Starts?

- Two nodes want to initiate a connection
 - E.g. a software sends a packet and the *security policy database* which is part of the IPsec recognizes that this connection needs to be encrypted
- An IKE (Internet key exchange) session is initiated using ISAKMP (Internet Security Association and Key Management Protocol) to create the needed security associations
 - A security association (SA) defines an one way (simplex) connection between two nodes, the service being provided (AH/ESP), the encryption algorithms etc.
 - The keys must be available, certificates used usually
- Now all IP traffic can be encrypted



IPsec Security Mechanisms

- Two independent security mechanisms
- AH (Authentication Header) offers
 - Access control
 - Data origin authentication
 - Connectionless (per-packet) integrity
 - Rejection of replayed packets
- ESP (Encapsulating Security Payload) offers same as AH and
 - Confidentiality
 - Limited traffic flow confidentiality
- We will discuss ESP only

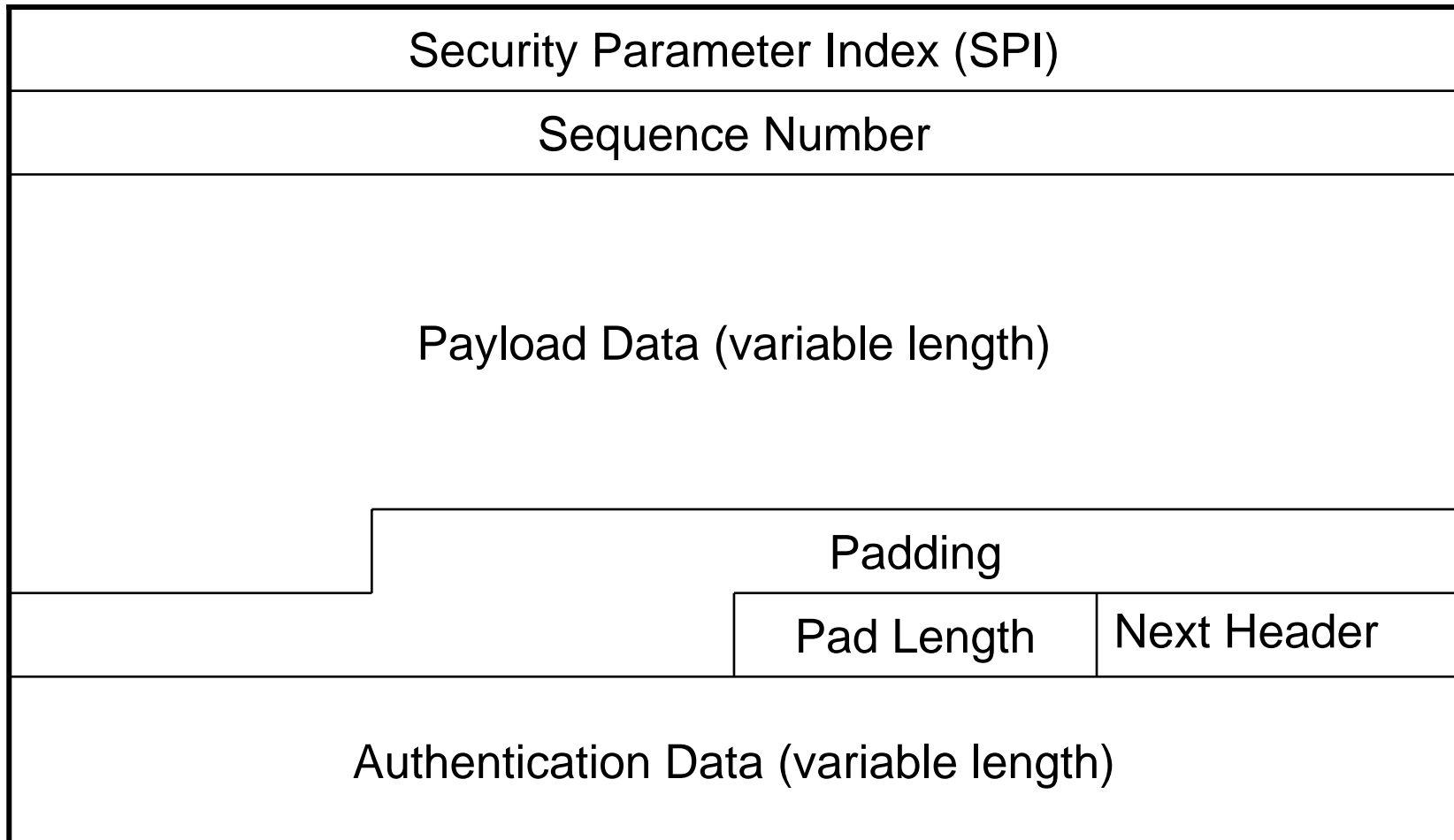


ESP (Encapsulating Security Payload)

- ESP provides confidentiality for IP traffic by encrypting the payload of a packet (TCP or UDP)
- ESP tunneling may be used
 - Encrypts the IP header, too and adds a new header
- Each packet has a Security Parameter Index, identifying the flow (SA) to which it belongs
- The monotonically increasing sequence number prevents replay
- ESP may authenticate the packet after encryption by computing a message authentication code (MAC)
 - The MAC is calculated over the IP payload data plus those IP header fields that do not change in transit, providing integrity
- ESP pads the IP payload with random bits to conceal the actual payload length and to make the length of the packet a multiple of 32 bits

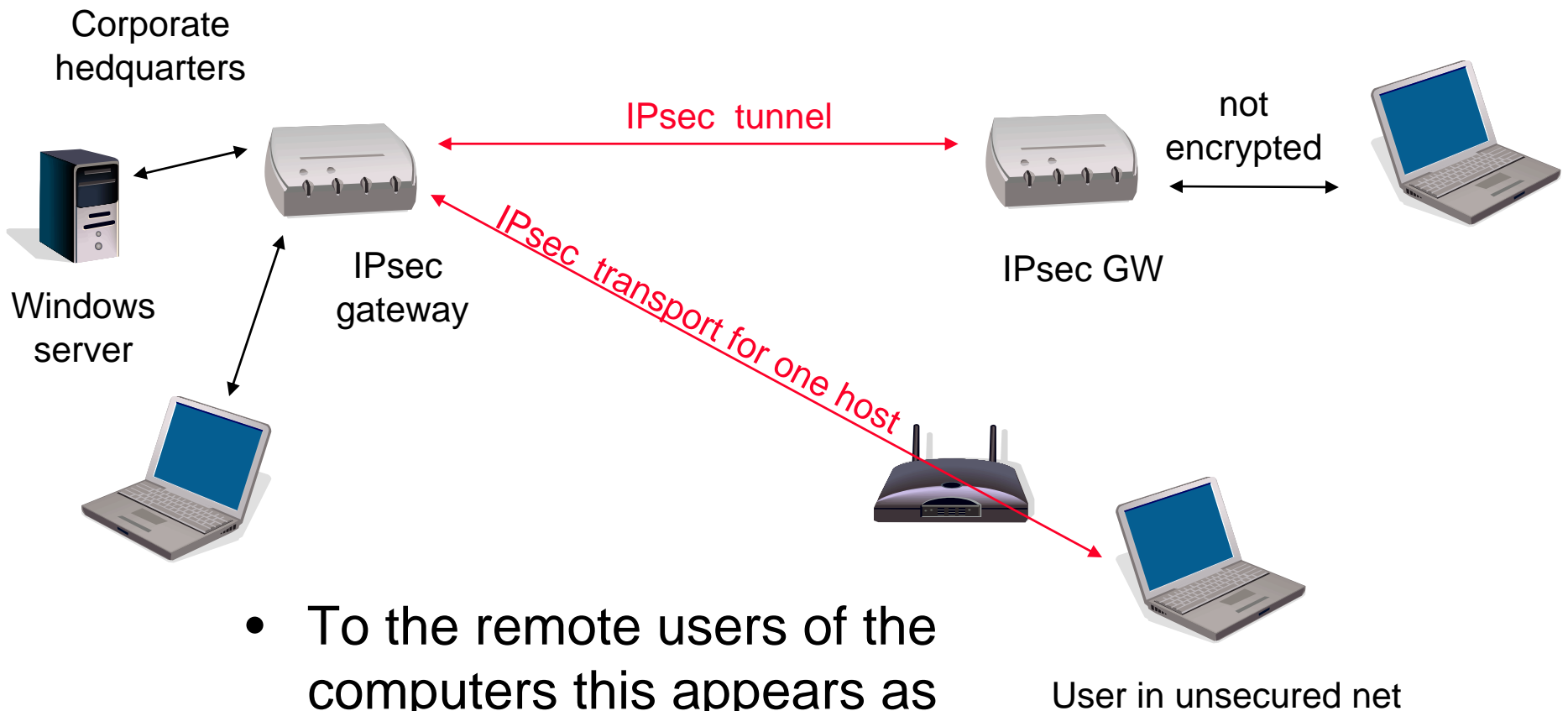


ESP Header Format





Virtual Private Network with IPsec



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



IPsec problems

- IPsec has some serious problems
- There is no standardized method for the key management
- Different vendor's IPsec implementations usually interoperate, but IKE implementations combined with the software used to create the certificates has interoperability problems
- The SAs are bound to IP addresses, which has serious problems with
 - NAT (Network Address Translation)
 - and mobility



- **Neal Stephenson: Cryptonomicon**
 - A novel (fiction) that introduces the key concepts in an easy to read form
- **Bruce Schneier: Applied Cryptography**
 - The most popular reference on how to use cryptography in different situations
- **Bruce Schneier: Secrets and Lies**
 - Why cryptography does not solve all or even most of our security problems and why his previous book was - if not useless - at least misleading