


# Internet Security Protocols

Bart Preneel  
February 2012

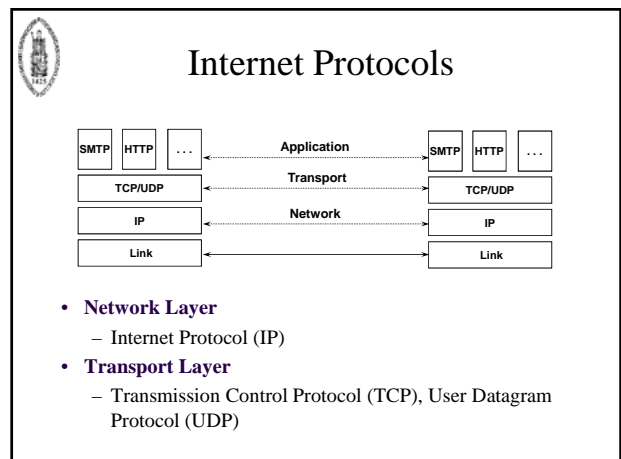
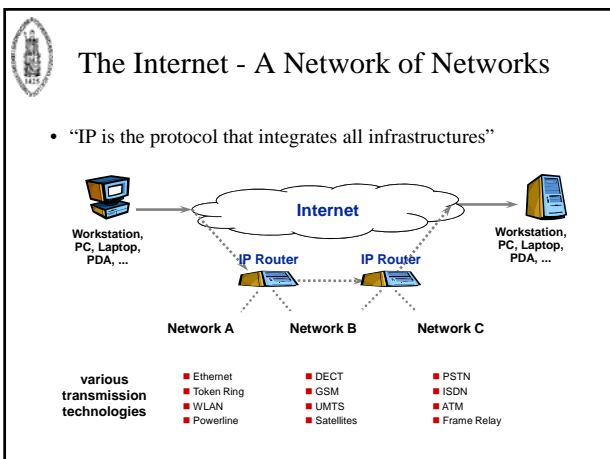
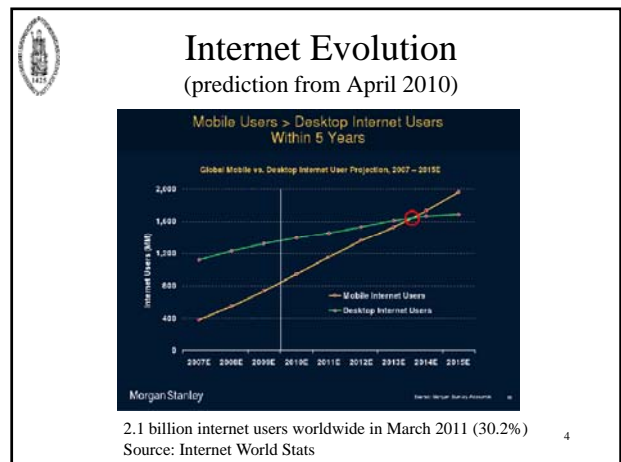
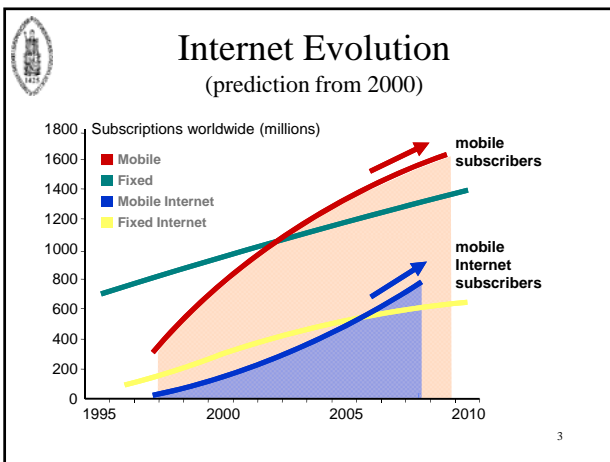
With thanks to Joris Claessens and Walter Fumy

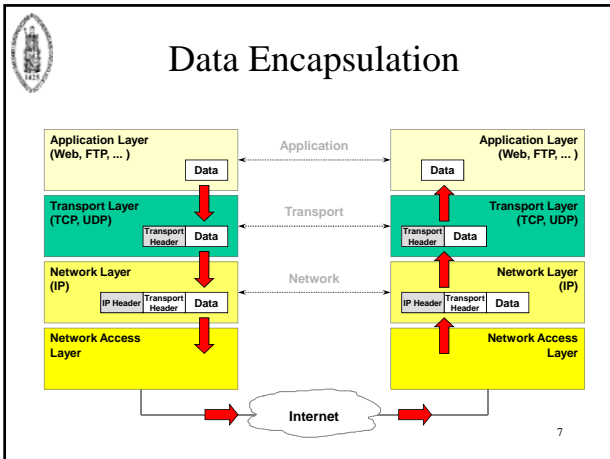


## Outline

- Internet summary
- IETF process
- Basic principles
- Transport layer security
  - SSL / TLS
- Network layer security
  - IPSec, VPN, SSH

2





- ### Internet Standardization
- Rough Consensus & Running Code*
- ISOC/IAB/IESG/IETF
  - Internet Engineering Task Force (IETF)
  - IETF Working Groups
    - Mailing List Information
    - Scope of the Working Group
    - Goals and Milestones
    - Current Internet Drafts & RFCs
    - <http://www.ietf.org/html.charters/wg-dir.html>
  - RFCs
    - <http://www.rfc-editor.org>
    - <ftp://FTP.ISI.EDU/in-notes/>

- ### IETF Standards: RFC
- **Proposed Standard (PS)**
    - stable spec
    - lowest level of [standards track](#)
  - **Draft Standard (DS)**
    - at least two independent and interoperable implementations
  - **Standard (STD)**
    - widely, successfully used
- 
- ```

    graph TD
      Experimental --> Proposed
      Proposed --> Draft_std[Draft std]
      Draft_std --> Standard
      Standard --> Historic
  
```

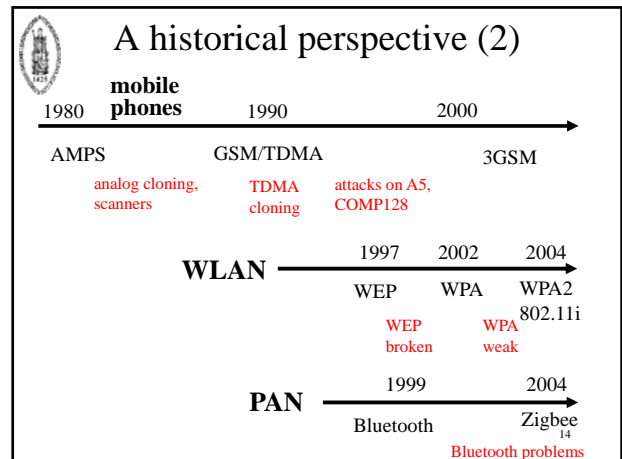
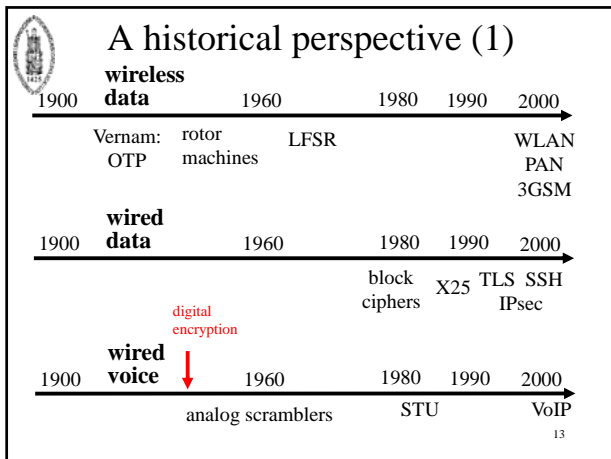
- ### IETF Intermediate documents
- **Request for Comments (RFCs) with different maturity levels**
    - Experimental (E)
    - Informational (I)
    - Historic (H)
    - Best Current Practice (BCP)
  - **Internet-Drafts (I-D)** are working documents of the working groups and have **no formal status**
  - **Protocol Status (requirement level)**
    - "required", "recommended", "elective", "limited use", or "not recommended"
    - "must" and "should"

### IETF Security Area

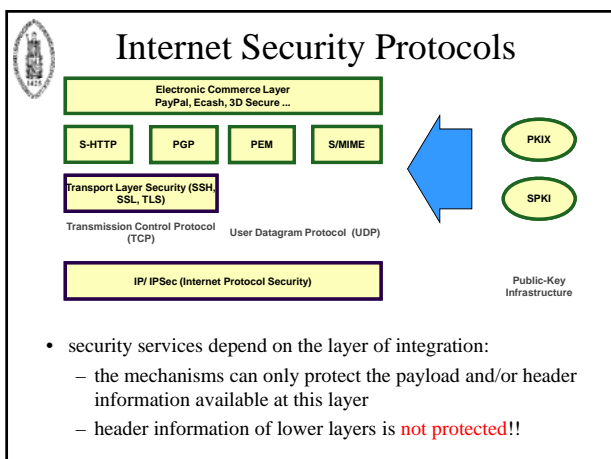
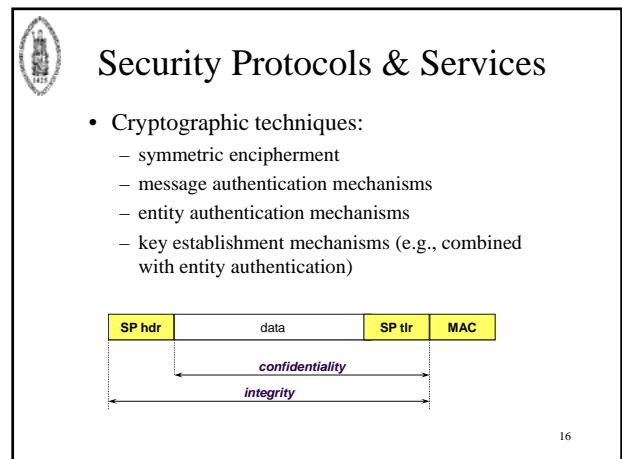
Area Directors: Stephen Farrell, Tim Polk, Sean Turner

|         |                                                      |
|---------|------------------------------------------------------|
| abfab   | Application Bridging for Federated Access Beyond web |
| dane    | DNS-based Authentication of Named Entities           |
| dkim    | Domain Keys Identified Mail                          |
| emu     | EAP Method Update                                    |
| hokey   | Handover Keying                                      |
| ipsecme | IP Security Maintenance and Extensions               |
| isms    | Integrated Security Model for SNMP                   |
| kitten  | Common Authentication Technology Next Generation     |
| krb-wg  | Kerberos                                             |
| ltans   | Long-Term Archive and Notary Services                |
| msec    | Multicast Security                                   |
| nea     | Network Endpoint Assessment                          |
| pkix    | Public-Key Infrastructure (X.509)                    |
| tls     | Transport Layer Security                             |

- ### Communications insecurity
- architectural errors
    - wrong trust assumptions
    - default = no security
  - protocol errors
    - unilateral entity authentication
    - weak entity authentication mechanism
    - downgrade attack
  - modes of operation errors
    - no authenticated encryption
    - wrong use of crypto
  - cryptographic errors
    - weak crypto
  - implementation errors
- range of wireless communication is often underestimated!*



- ### Security Goals (started in ISO 7498-2)
- confidentiality:
    - entities (anonymity)
    - data
    - traffic flow
  - (unilateral or mutual) entity authentication
  - data authentication (connection-less or connection-oriented): data origin authentication + data integrity
  - access control
  - non-repudiation of origin versus deniability



- ### Security: at which layer?
- Application layer:
    - closer to user
    - more sophisticated/granular controls
    - end-to-end
    - but what about firewalls?
  - Lower layer:
    - application independent
    - hide traffic data
    - but vulnerable in middle points
  - Combine?

### SP Architecture I: Encapsulation

- Bulk data: symmetric cryptography
- Authenticated encryption: best choice is to authenticate the ciphertext

19

### SP Architecture II: Session (Association) Establishment

20

### Algorithm Selection

"a la carte"

- each algorithm (encryption, integrity protection, pseudo-random function, Diffie-Hellman group, etc.) is negotiated independently
- less compact to encode
- more flexible
- e.g., IKEv1

"suite"

- all parameters are encoded into a single suite number; negotiation consists of offering one or more suites and having the other side choose
- simpler and more compact to encode
- potentially exponential number of suites
- less flexible
- e.g., TLS and IKEv2

21

### Transport layer security

SSL / TLS

### SSL/TLS Protocols

23

### Transport Layer Security Protocols

- IETF Working Group: **Transport Layer Security (tls)**
  - RFC 2246 (PS), 01/99
- transparent secure channels independent of the respective application.
- available protocols:
  - *Secure Shell* (SSH), SSH Ltd.
  - *Secure Sockets Layer* (SSL), Netscape
  - *Transport Layer Security* (TLS), IETF

4

### SSL / TLS

- Mainly in context of WWW security, i.e., to secure the HyperText Transfer Protocol (HTTP)
- But, in between application layer and TCP, thus can be used to secure other applications than HTTP too (IMAP, telnet, ftp, ...)

25

### Other WWW security protocols

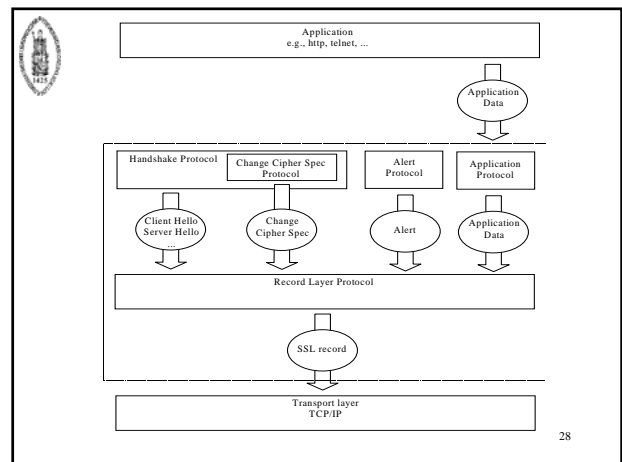
- PCT: Microsoft's alternative to SSL
- S-HTTP: S/MIME-like protocol
- SET: for credit card transactions
- XML-Signature: PKCS#7-based signature on XML documents
- ...

26

### SSL / TLS

- “Secure Sockets Layer” (Netscape)
  - SSL 2.0: security flaws!
  - SSL 3.0: still widely used - not interoperable with TLS 1.0
- “Transport Layer Security” (IETF)
  - TLS 1.0: adopted SSL 3.0 with minor changes
  - RFC 2246, 01/99 (PS)
- TLS: security at the transport layer
  - can be used (and is intended) for other applications too
  - end-to-end secure channel, but nothing more...
  - data is only protected during communication
  - no non-repudiation!

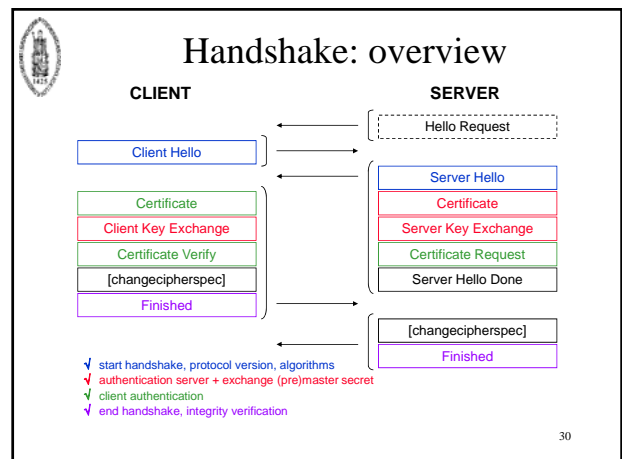
27



### SSL/TLS in more detail

- “Record layer” protocol
  - fragmentation
  - compression (not in practice)
  - cryptographic security:
    - encryption → data confidentiality
    - MAC → data authentication [no digital signatures!]
- “Handshake” protocol
  - client and server authentication
  - establish cryptographic keys (for encryption and MAC)
  - negotiation of cryptographic algorithms

29



### TLS 1.0 Data Encapsulation Options

| Integrity         |          |          |
|-------------------|----------|----------|
| key size          | 144      | 160      |
| algorithm options | HMAC-MD5 | HMAC-SHA |

**mandatory**

| Confidentiality   |                                              |         |                 |              |
|-------------------|----------------------------------------------|---------|-----------------|--------------|
| key size          | 40                                           | 56      | 128             | 168          |
| algorithm options | RC4_40<br>RC4_40<br>RC2_CBC_40<br>DES_CBC_40 | DES_CBC | RC4<br>IDEA_CBC | 3DES_EDE_CBC |

**mandatory**

### TLS 1.0 Key Management Options

```

graph TD
    Root[ ] --- Anon[Anonymous]
    Root --- NonAnon[Non anonymous]
    Anon --- DHanon[DH_anon]
    NonAnon --- ServerAuth[Server authentication, no client authentication]
    NonAnon --- ServerClientAuth[Server and client authentication]
    DHanon --- Vulnerable[vulnerable to a meet-in-the-middle attack]
    ServerAuth --- RSA1[RSA]
    ServerAuth --- DH_DSS1[DH_DSS]
    ServerAuth --- DH_RSA1[DH_RSA]
    ServerAuth --- DHE_DSS1[DHE_DSS]
    ServerAuth --- DHE_RSA1[DHE_RSA]
    ServerClientAuth --- RSA2[RSA]
    ServerClientAuth --- DH_DSS2[DH_DSS]
    ServerClientAuth --- DH_RSA2[DH_RSA]
    ServerClientAuth --- DHE_DSS2[DHE_DSS]
    ServerClientAuth --- DHE_RSA2[DHE_RSA]
    DHanon -- mandatory --> DHanon
    RSA1 -- mandatory --> RSA1
    
```

32

### RFC 3268: AES Ciphersuites for TLS

06/2002

| CipherSuite                      | Key Exchange | Certificate Type |
|----------------------------------|--------------|------------------|
| TLS_RSA_WITH_AES_128_CBC_SHA     | RSA          | RSA              |
| TLS_DH_DSS_WITH_AES_128_CBC_SHA  | DH_DSS       | DSS              |
| TLS_DH_RSA_WITH_AES_128_CBC_SHA  | DH_RSA       | RSA              |
| TLS_DHE_DSS_WITH_AES_128_CBC_SHA | DHE_DSS      | DSS              |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DHE_RSA      | RSA              |
| TLS_DH_anon_WITH_AES_128_CBC_SHA | DH_anon      |                  |
| TLS_RSA_WITH_AES_256_CBC_SHA     | RSA          | RSA              |
| TLS_DH_DSS_WITH_AES_256_CBC_SHA  | DH_DSS       | DSS              |
| TLS_DH_RSA_WITH_AES_256_CBC_SHA  | DH_RSA       | RSA              |
| TLS_DHE_DSS_WITH_AES_256_CBC_SHA | DHE_DSS      | DSS              |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA | DHE_RSA      | RSA              |
| TLS_DH_anon_WITH_AES_256_CBC_SHA | DH_anon      |                  |

### TLS 1.1

RFC 4346 April 2006

Limited employment in 2011

- Makes RSA with 3DES the mandatory cipher suite
  - TLS 1.1: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
  - TLS 1.0: TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- Provides several fixes, including
  - for the Rogaway and Vaudenay CBC attacks and the 2011 BEAST attack
  - for the Vaudenay, Boneh-Brumley, and Klima-Pokorny-Rosa attacks

### TLS 1.2

RFC 5246 - August 2008

- reduces dependency on MD5 and SHA-1
- add support for authenticated encryption
- add AES ciphersuites

34

### SSL/TLS: security services

**SSL/TLS only provides:**

- entity authentication
- data confidentiality
- data authentication

**SSL/TLS does not provide:**


- non-repudiation
- unobservability (identity privacy)
- protection against traffic analysis
- secure many-to-many communications (multicast)
- security of the end-points (but relies on it!)

35

### SSL/TLS: security ?

- SSL/TLS offers an adequate security level but it is a very complex protocol
- TLS 1.x is the result of a public reviewing process: several problems have been identified in earlier versions (SSL 2.0/3.0) and have been solved
- In 2012: limited deployment of 1.1 and almost none of 1.2

36



## SSL/TLS: evaluation


**Old problems**

- bad implementation; e.g., random number generation
- PKCS#1 attack is patched (use other padding scheme: OAEP; server error messages should contain less information)
- version / cipher suite roll back attempts now patched (due to backward compatibility; disable export algorithms if possible)

**Remaining problems**

- traffic analysis: e.g., length of ciphertext might reveal useful info
- PKI issues: revocation, root keys, certificate parsing,...
- web spoofing and phishing
- what if the user does not know that a particular website has to use SSL/TLS (solution HSTS)
- plenty of known plaintext (both SSL/TLS and HTTP related)

37




## TLS Renegotiation attack

[Marsh Ray 9 November 2009]

- Cipher suite can be renegotiated dynamically throughout the session
  - Negotiation and renegotiation look the same
- Person-In-The-Middle can inject (plaintext) traffic in a protected session as if it came from a client
  - establishes an unauthenticated session with a server
  - proxies another authenticated session between the client victim and the same server
  - triggers a renegotiation
  - server: last message received from attacker prior to renegotiation is attached to first message received from client after renegotiation

**TLS renegotiation indication extension**  
RFC 5746 – February 2010




## Implementation attacks

### Debian-OpenSSL incident [13 May 2008]


<https://cseweb.ucsd.edu/~hovav/dist/debiankey.pdf>

- Weak key generation: only 32K keys
  - easy to generate all private keys
  - collisions
- Between 13-17 May 2008  
280 bad keys out of 40K (0.6%)
- Revocation problematic




IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

| AFFECTED SYSTEM  | SECURITY PROBLEM                                                          |
|------------------|---------------------------------------------------------------------------|
| FEDORA CORE      | VULNERABLE TO CERTAIN DECODER RINGS                                       |
| XANDROS (SEE PC) | GIVES ROOT ACCESS IF ASKED IN DEAN VOICE                                  |
| GENTOO           | VULNERABLE TO FLATTERY                                                    |
| OLPC OS          | VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK                                   |
| SLACKWARE        | GIVES ROOT ACCESS IF USER SAYS ELISH WORD FOR FRIEND                      |
| UBUNTU           | TURNS OUT DISTR0 IS ACTUALLY 3007 MANDRIVA VISTA WITH A FEW CUSTOM THEMES |



## TLS certificate "NULL" issue.


- [Moxie Marlinspike'09] Black Hat
  - browsers may accept bogus SSL certs
  - CAs may sign malicious certs
- certificate for [www.paypal.com](http://www.paypal.com) [kuleuven.be](http://kuleuven.be) will be issued if the request comes from a kuleuven.be admin
- response by PayPal: suspend Moxie's account
  - [http://www.theregister.co.uk/2009/10/06/paypal\\_banishes\\_ssl\\_hacker/](http://www.theregister.co.uk/2009/10/06/paypal_banishes_ssl_hacker/)



## Security in transport layer

- Transparent for application
- Pro: can be used for all TCP-based applications, without modifying them
- Con: authentication is one, but who/what to trust, is important
- Non-repudiation?
- In practice: (partially) integrated in application

41



## Non-repudiation

- Strictly speaking only if in application, thus not provided by SSL/TLS
- SSL/TLS secures the communication channel, but not the exchanged messages
- SSL/TLS does not use digital signatures in the first place (except for client authentication)
- For electronic business, more advanced security protocols are needed...

42

### User authentication

First *authentication*, then *authorization* !

SSL/TLS client authentication:

- during handshake, client digitally signs a specific message that depends on all relevant parameters of secure session with server
- software devices, smart cards or USB tokens can be deployed through standardized cryptographic interfaces supported by browsers (Netscape: PKCS#11; MSIE: PC/SC)
- PKCS#12 key container provides software mobility

Usually another mechanism on top of SSL/TLS

43

### TLS in the future (1)

- TLS 2.0?
- Some possible TLS enhancements, discussed within the IETF TLS WG:
  - RSA-OAEP
  - identity protection [note that this is already indirectly possible by authenticating within a DH\_anon session]
  - cipher suites for compression
  - missing cipher suites (not all combinations possible)
- Backward compatibility remains very important because of huge installed base

44

### TLS in the future (2)

#### Enhancements proposed in literature

- performance improvements:
  - 'batching' [ShachamBoneh'01] and 'fast-track' [ShachamBoneh'02]
- user (identity) privacy [PersianoVisconti'00]
- client puzzles to counter denial-of-service attacks [DeanStubblefield'01]
- trust negotiation [Hess et al'02]

45

### Network layer security

IPsec, VPN, SSH

### IP Security Protocols

- IETF Working Group: **IP Security Protocol (ipsec) Security Architecture for the Internet Protocol**
  - RFC 2401 (PS), 11/98
- **IP Authentication Header (AH)**
  - RFC 2402 (PS), 11/98
- **IP Encapsulating Security Payload (ESP)**
  - RFC 2406 (PS), 11/98
- **Internet Key Exchange (IKE)**
  - RFC 2409 (PS), 11/98
  - Application layer protocol for negotiation of Security Associations (SA) and Key Establishment

- Large and complex..... (48 documents)
- Mandatory for IPv6, optional for IPv4

### IPSec VPN models: Hosts and Security Gateways



### IPsec - Security services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality
- Limited traffic flow confidentiality

49

### IPsec - Concepts

- Security features are added as extension headers that follow the main IP header
  - Authentication header (AH)
  - Encapsulating Security Payload (ESP) header
- Security Association (SA)
  - Security Parameter Index (SPI)
  - IP destination address
  - Security Protocol Identifier (AH or ESP)

50

### IPsec - Parameters

- sequence number counter
- sequence counter overflow
- anti-replay window
- AH info (algorithm, keys, lifetimes, ...)
- ESP info (algorithms, keys, IVs, lifetimes, ...)
- lifetime
- IPSec protocol mode (tunnel or transport)
- path MTU (maximum transmission unit)

51

### IKE Algorithm Selection Mandatory Algorithms

| Algorithm Type               | IKE v1                         | IKE v2                         |
|------------------------------|--------------------------------|--------------------------------|
| Payload Encryption           | DES-CBC                        | AES-128-CBC                    |
| Payload Integrity            | HMAC-MD5<br>HMAC-SHA1          | HMAC-SHA1                      |
| DH Group                     | 768 Bit                        | 1536 Bit                       |
| Transfer Type 1 (Encryption) | ENCR_DES_CBC                   | ENCR_AES_128_CBC               |
| Transfer Type 2 (PRF)        | PRF_HMAC_SHA1<br>[RFC2104]     | PRF_HMAC_SHA1<br>[RFC2104]     |
| Transfer Type 3 (Integrity)  | AUTH_HMAC_SHA1_96<br>[RFC2404] | AUTH_HMAC_SHA1_96<br>[RFC2404] |

Source: draft-ietf-ipsec-ikev2-algorithms-00.txt, May 2003

52

### IPsec - Modes

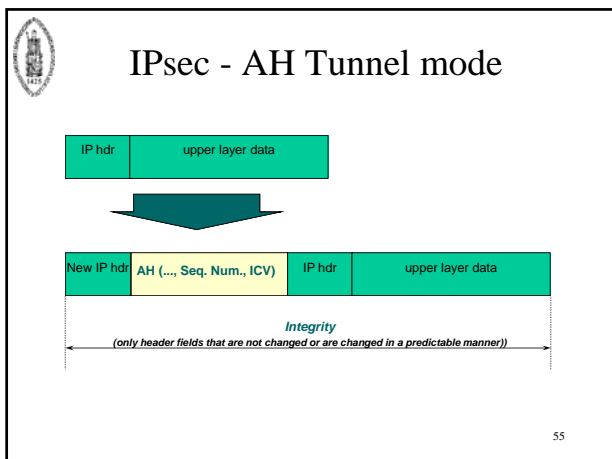
- Transport (*host-to-host*)
  - ESP: encrypts and optionally authenticates IP payload, but not IP header
  - AH: authenticates IP payload and selected portions of IP header
- Tunnel (*between security gateways*)
  - after AH or ESP fields are added, the entire packet is treated as payload of new outer IP packet with new outer header
  - used for VPN

53

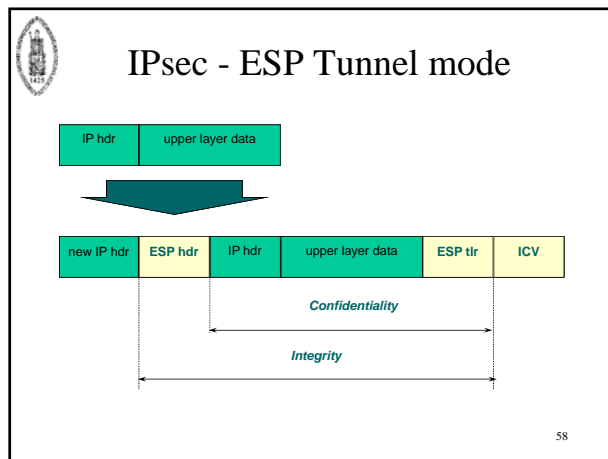
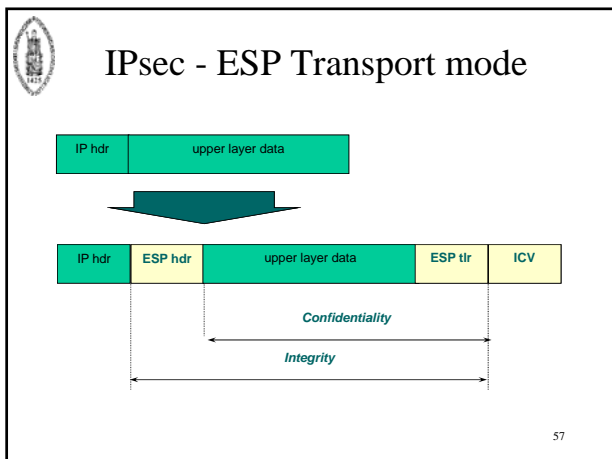
### IPsec - AH Transport mode

- Security Parameters Index: identifies SA
- Sequence number: anti-replay
- Integrity Check Value: data authentication using HMAC-SHA-1-96 or HMAC-MD5-96

54




- ### IPsec - ESP header
- Security Parameters Index: identifies SA
  - Sequence number: anti-replay
  - Encrypted payload data: data confidentiality using DES, 3DES, RC5, IDEA, CAST, Blowfish
  - Padding: required by encryption algorithm (additional padding to provide traffic flow confidentiality)
  - Integrity Check Value : data authentication using HMAC-SHA-1-96 or HMAC-MD5-96
- 56



- ### IPsec: Key management
- RFCs 2407, 2408, and 2409
  - Manual
  - Automated
    - procedure / framework
      - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408 (PS)
    - key exchange mechanism: Internet Key Exchange (IKE)
      - Oakley: DH + cookie mechanism to thwart clogging attacks
      - SKEME
- 59


- ### IPsec: Key management
- IKE defines 5 exchanges
    - Phase 1: establish a secure channel
      - Main mode
      - Aggressive mode
    - Phase 2: negotiate IPSEC security association
      - Quick mode (only hashes, PRFs)
    - Informational exchanges: status, new DH group
  - based on 5 generic exchanges defined in ISAKMP
  - cookies for anti-clogging
- 60



### IPsec: Key management


- protection suite (negotiated)
  - encryption algorithm
  - hash algorithm
  - authentication method:
    - preshared keys, DSA, RSA, encrypted nonces
  - Diffie Hellman group: 5 possibilities

61



### IKE - Main Mode with Digital Signatures


62



### IKE - Main Mode with Digital Signatures

- mutual entity authentication
- mutual implicit and explicit key authentication
- mutual key confirmation
- joint key control
- identity protection
- freshness of keying material
- perfect forward secrecy of keying material
- non-repudiation of communication
- cryptographic algorithm negotiation


63



### IKE v2 - RFC Dec 2005

- IKEv1 implementations incorporate additional functionality including features for NAT traversal, legacy authentication, and remote address acquisition, not documented in the base documents
- Goals of the IKEv2 specification include
  - to specify all that functionality in a single document
  - to simplify and improve the protocol, and to fix various problems in IKEv1 that had been found through deployment or analysis
- IKEv2 preserves most of the IKEv1 features while redesigning the protocol for efficiency, security, robustness, and flexibility


64



### IKE v2 Initial Handshake (1/2)

- Alice and Bob negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA
- Usually consists of two request/response pairs
  - The first pair negotiates cryptographic algorithms and does a Diffie-Hellman exchange
  - The second pair is encrypted and integrity protected with keys based on the Diffie-Hellman exchange

65



### IKE v2 Initial Handshake (2/2)

- Second exchange
  - divulge identities
  - prove identities using an integrity check based on the secret associated with their identity (private key or shared secret key) and the contents of the first pair of messages in the exchange
  - establish a first IPsec SA (“child-SA”) is during the initial IKE-SA creation

66

### IPsec Overview

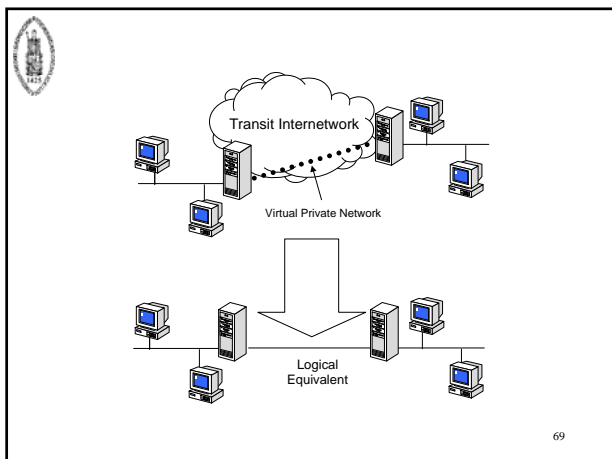
- much better than previous alternatives
- IPsec documents hard to read
- vommittee design: too complex
  - ESP in Tunnel mode with authenticated encryption probably sufficient
  - simplify key management
  - clarify cryptographic requirements
- ...and thus difficult to implement (securely)
- **avoid encryption without data authentication**

67

### VPN?

- Virtual Private Network
- Connects a private network over a public network.
- Connection is secured by tunneling protocols.
- The nature of the public network is irrelevant to the user.
- It appears as if the data is being sent over the private network.

68



### VPN - Common use

- Remote user access over the Internet
- Connecting networks over the Internet
- Connection computers over an intranet

70

### Remote user access over the Internet

- You can use existing local Internet connections.
- No need for long distance connections

71

### Connecting networks over the Internet

- You can use existing local Internet connections.
- No need for long distance connections or leased lines

72

**Connecting computers over an intranet**

- Provides easy client access to secured or hidden networks within the corporate network

73

**VPN - Basic requirements**

- User authentication and user authorization
- Data authentication and data confidentiality
- Key management
- Encapsulation
  - data of private network is encapsulated in packets suited for transmission over the public network. (tunneling protocol)
- Address management
  - assign a client's address on the private net

74

**Tunneling**

75

**Final remarks**

**Some observations**

- IPsec is really transparent, SSL/TLS only conceptually, but not really in practice
- SSH, PGP: stand-alone applications, immediately and easy to deploy and use
- Network security: solved in principle
- Electronic commerce security: more is needed!

77

**More information (1)**

- William Stallings, *Cryptography and Network Security - Principles and Practice*, Fifth Edition, 2010
- N. Doraswamy, D. Harkins, *IPSec (2nd Edition)*, Prentice Hall, 2003 (outdated)
- Erik Rescorla, *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley, 2000.
- IETF web site: [www.ietf.org](http://www.ietf.org)
  - e.g., IETF-TLS Working Group  
<http://www.ietf.org/html.charters/tls-charter.html>

78



### More information (2)

- Jon C. Snader, *VPNs Illustrated: Tunnels, VPNs, and IPsec*, Addison-Wesley, 2005
- Sheila Frankel, *Demystifying the IPsec Puzzle*, Artech House Computer Security Series, 2001
- Anup Gosh, *E-Commerce Security, Weak Links, Best Defenses*, Wiley, 1998
- Rolf Oppliger, *Security Technologies for the World Wide Web*, Artech House Computer Security Series 1999
- W3C Security (incl WWW Security FAQ)  
<http://www.w3.org/Security/>

79