Network Security Protocols

Prof. Bart Preneel
COSIC – KU Leuven - Belgium
Firstname.Lastname(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel
October 2014

With thanks to Joris Claessens and Walter Fumy

1

Goals

- Understanding how security can be added to the basic Internet protocols
- Understanding TLS and its limitations
- Understanding IPsec and its limitations

2

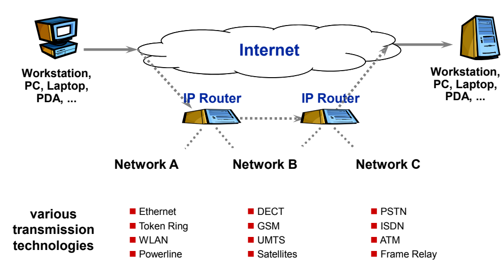
Outline

- Internet summary
- Principles
- Transport layer security
  - SSL/TLS
- Network layer security
  - IPSec, VPN, SSH

3

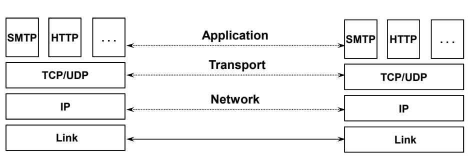
The Internet - A Network of Networks

- "IP is the protocol that integrates all infrastructures"



4

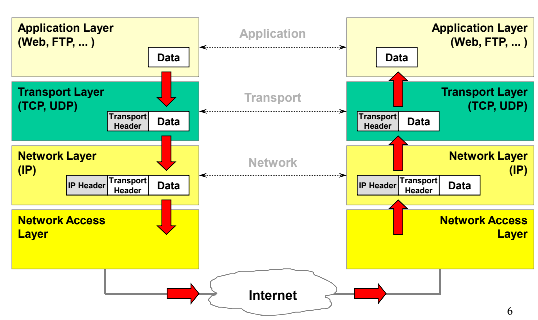
Internet Protocols



- **Network Layer**
  - Internet Protocol (IP)
- **Transport Layer**
  - Transmission Control Protocol (TCP), User Datagram Protocol (UDP)

5

Data Encapsulation



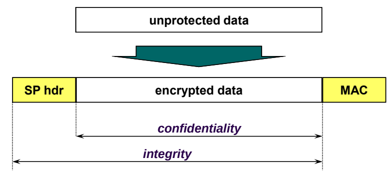
6

Security Goals (started in ISO 7498-2)

- confidentiality:
  - entities (anonimity)
  - 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

7

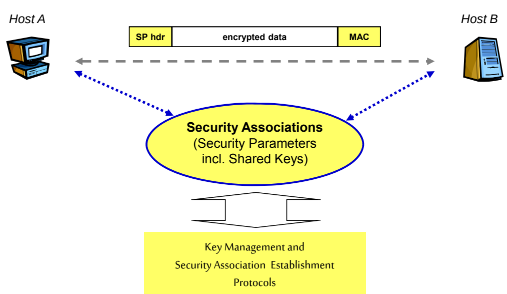
SP Architecture I: Encapsulation



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

8

SP Architecture II: Session (Association) Establishment



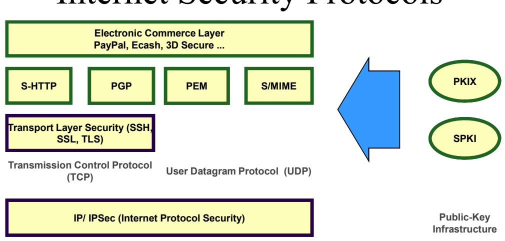
9

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?

10

Internet Security Protocols



- security services depend on the layer of integration:
  - the mechanisms can only protect the payload and/or header information available at this layer
  - header information of lower layers is not protected!!

11

COMSEC in practice

- wired
  - SSL/TLS
  - VPN: IPsec
  - VOIP
- wireless
  - GSM, 3G
  - WLAN: WPA2 (RSN)
  - PAN: Bluetooth, Zigbee

12

COMSEC

	Confidentiality	Data authentication	Entity authentication
1 G (analog)			
2 G (GSM)	weak		unilateral
3G			
WLAN			
TLS			unilateral
IPsec		optional ☹	
Skype	not open	not open	not open/meet in the middle attack

Not end to end (1 G, 2 G, 3G, WLAN)

13

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!

14

Network security: broader context

- fundamental protocols of the Internet do not have adequate security
- this is well understood, but there is no preventive patching
  - panic response to ever improving attacks
- changing widely used protocols is hard

- DNS attack [Kaminsky, Black Hat '08]
- BGP attack [Kapela-Pilosov, Defcon'08]

- More examples:
  - **IPV6 attacks**
  - **SNMPv3 Bug [Wes Hardakar]**
  - **Insecure SSL-VPN [Mike Zusman]**
  - **Insecure Cookies [Mike Perry]**

15

Network security: DNSSec

- long and winding road (started in 1997)
- several attacks (e.g. cache poisoning [Kaminsky08])
- several TLDs signed 2005-2009
- live in July 2010 for root
- Versign signed .com early 2011

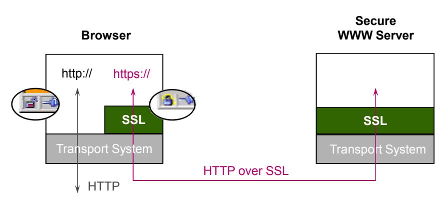
- http://www.root-dnssec.org/
- http://ispcolumn.isoc.org/2006-08/dnssec.html

16

Transport layer security

SSL / TLS

SSL/TLS Protocols

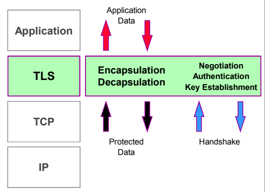


– connection-oriented data confidentiality and integrity, and optional client and server authentication.

18

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



19

SSL / TLS

- Mainly in context of WWW security, i.e., to secure the HyperText Transfer Protocol (HTTP)
- TLS: security at the transport layer
  - can be used (and is intended) for other applications too (IMAP, telnet, ftp, …)
  - end-to-end secure channel, but nothing more...
  - data is only protected during communication
  - no non-repudiation!

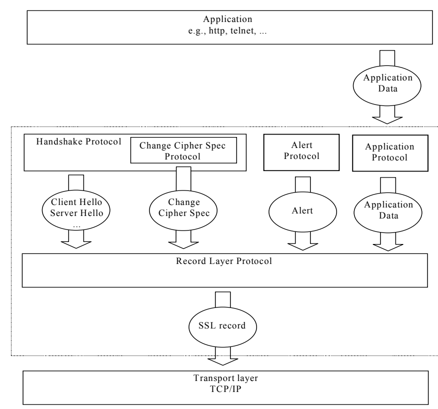
20

SSL/TLS

- "Secure Sockets Layer" (Netscape)
  - SSL 2.0 (1995): security flaws!
  - SSL 3.0 (1996): still widely used - not interoperable with TLS 1.0
- "Transport Layer Security" (IETF)
  - TLS 1.0 (01/99) adopted SSL 3.0 with minor changes - RFC 2246 - default DSA/3DES
  - TLS 1.1 (4/2006) - RFC 4346 – default: RSA/3DES; several fixes for padding oracle and timing attacks (explicit IV for CBC)
  - TLS 1.2 (8/2008) - RFC 5246
    - replaces MD5 and SHA-1 by SHA-256 (SHA-1 still in a few places)
    - add AES ciphersuites (but still supports RC4!)
    - add support for authenticated encryption: GCM and CCM
  - RFC 5176 (2/2011) removes backward compatibility with SSL 2.0
  - Currently 314 ciphersuites!

TLS 1.1 and 1.2 deployment very slow (about 25% of servers in Feb. 14); boost in Nov. 2013 (new attacks + Snowden revelations).

21



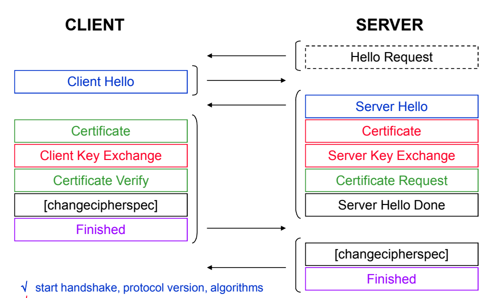
22

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
  - negotiation of cryptographic algorithms
  - client and server authentication
  - establish cryptographic keys (master key and derived key for encryption and MAC algorithm)
  - key confirmation

23

Handshake: overview



√ start handshake, protocol version, algorithms
√ authentication server + exchange (pre)master secret
√ client authentication
√ end handshake, integrity verification

24

TLS 1.2 Data Encapsulation Options

Integrity			
key size	144	160	256
algorithm options	HMAC-MD5	HMAC-SHA	HMAC-SHA256

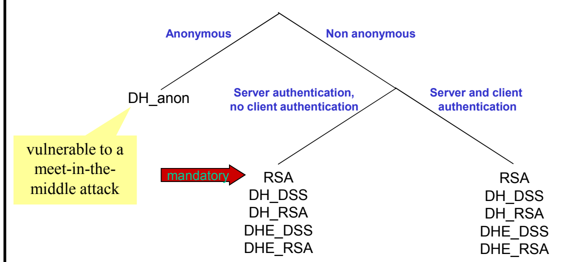
mandatory (HMAC-SHA)

Confidentiality					
key size	40	56	128	168	256
algorithm options	~~RC4_40 RC2_CBC_40 DES_CBC_40~~	~~DES_CBC~~	RC4 ~~IDEA_CBC~~ AES_CBC	3DES_EDE_CBC	AES_CBC

mandatory (AES_CBC)

25

TLS 1.2 Key Management Options



26

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!)

27 27

TLS in the future

- Reduce the number of cipher suites
- Authenticated encryption gains popularity:
  - AES-GCM
  - Chacha20 with Poly1305AES
- TLS 2.0: mandatory encryption for httpv2.0?
- Identity protection (cf. IPsec)
- Backward compatibility remains very important because of huge installed base

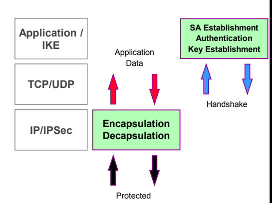
28

Network layer security

IPsec, VPN, SSH

IP Security Protocols

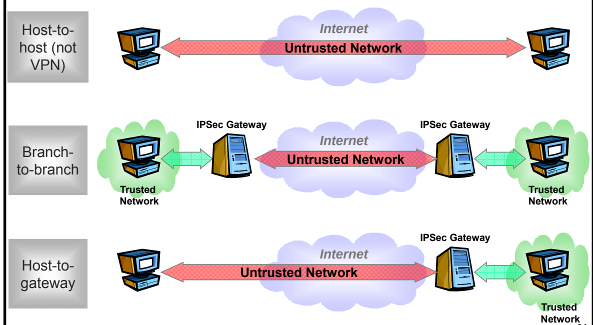
- IETF Working Group: ***IP Security Protocol (ipsec)*** ***Security Architecture for the Internet Protocol***
  - RFC 2401 (PS), 11/98
- ***IP Authentication Header (AH)***
  - RFC 2402 (PS), 11/98
- ***IP Encapsulating Security Payload (ESP)***
  - RFC 2406 (PS), 11/98
- ***Internet Key Exchange (IKE)***
  - 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**

30

IPSec VPN models: Hosts and Security Gateways



31

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

32

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)

33

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)

34

IKE Algorithm Selection Mandatory Algorithms

Algorithm Type	IKE v1	IKE v2
Payload Encryption	DES-CBC	**AES-128**-CBC
Payload Integrity	HMAC-MD5 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 [RFC2104]	PRF_HMAC_SHA1 [RFC2104]
Transfer Type 3 (Integrity)	AUTH_HMAC_SHA1_96 [RFC2404]	AUTH_HMAC_SHA1_96 [RFC2404]

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

35

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

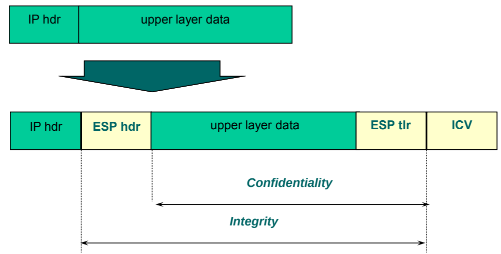
36

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

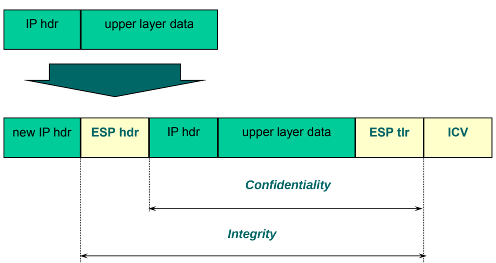
37

IPsec - ESP Transport mode



38

IPsec - ESP Tunnel mode



39

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

40

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

41

IPsec: Key management

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

42

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

43

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

44

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

45

IPsec Overview

- much better than previous alternatives
- IPsec documents hard to read
- committee 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

46

Concluding comments

- 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 but
  - many implementation issues
  - complexity creates security weaknesses
- Application and end point security: more is needed!

47

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
  - e.g., IETF-TLS Working Group http://www.ietf.org/html.charters/tls-charter.html

48

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/

49