Network Security Protocols

Prof. Bart Preneel
COSIC
Bart.Preneel(at)esatDOTkuleuven.be
http://homes.esat.kuleuven.be/~preneel

February 2015

With thanks to Joris Claessens and Walter Fumy

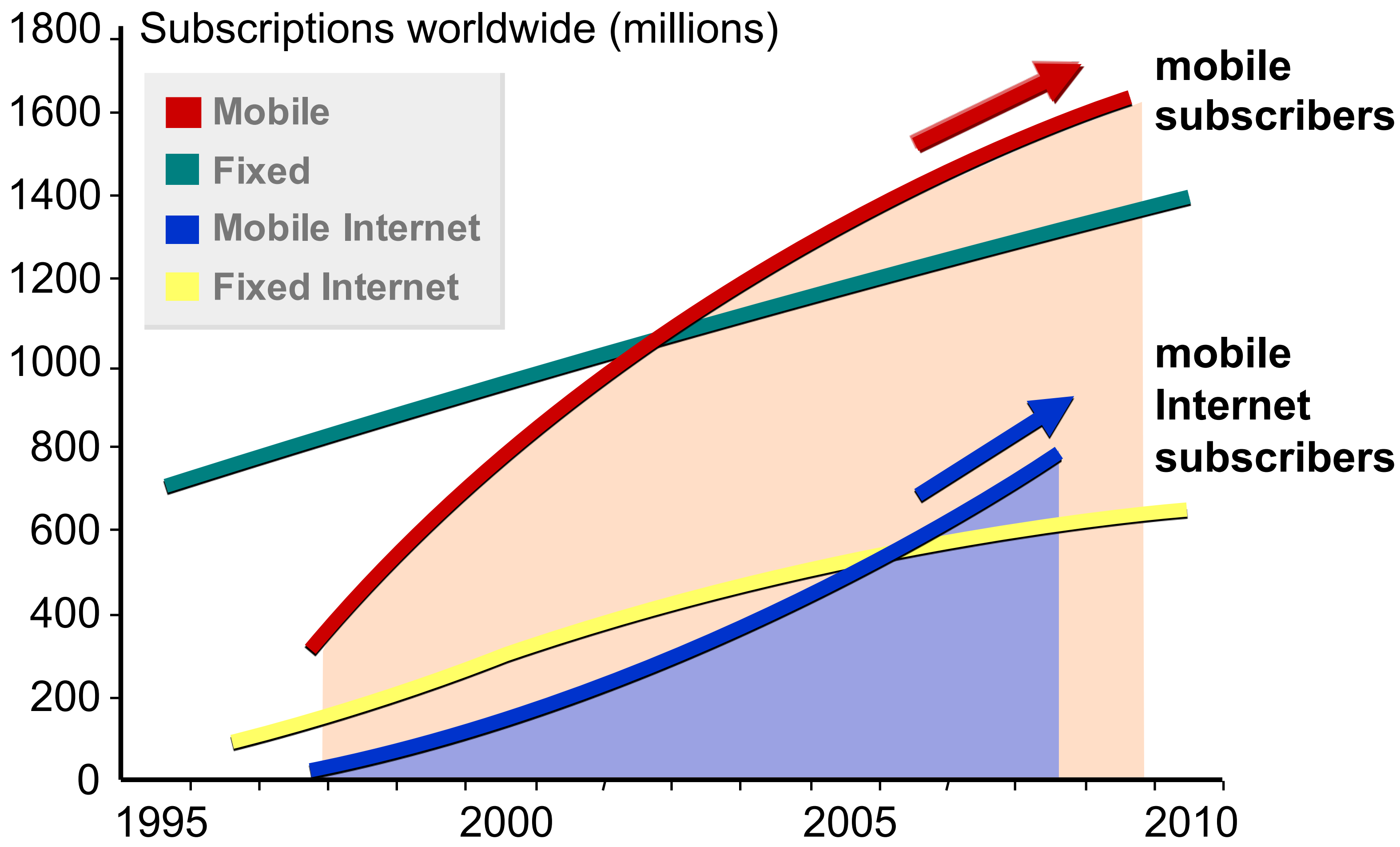
Goals

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

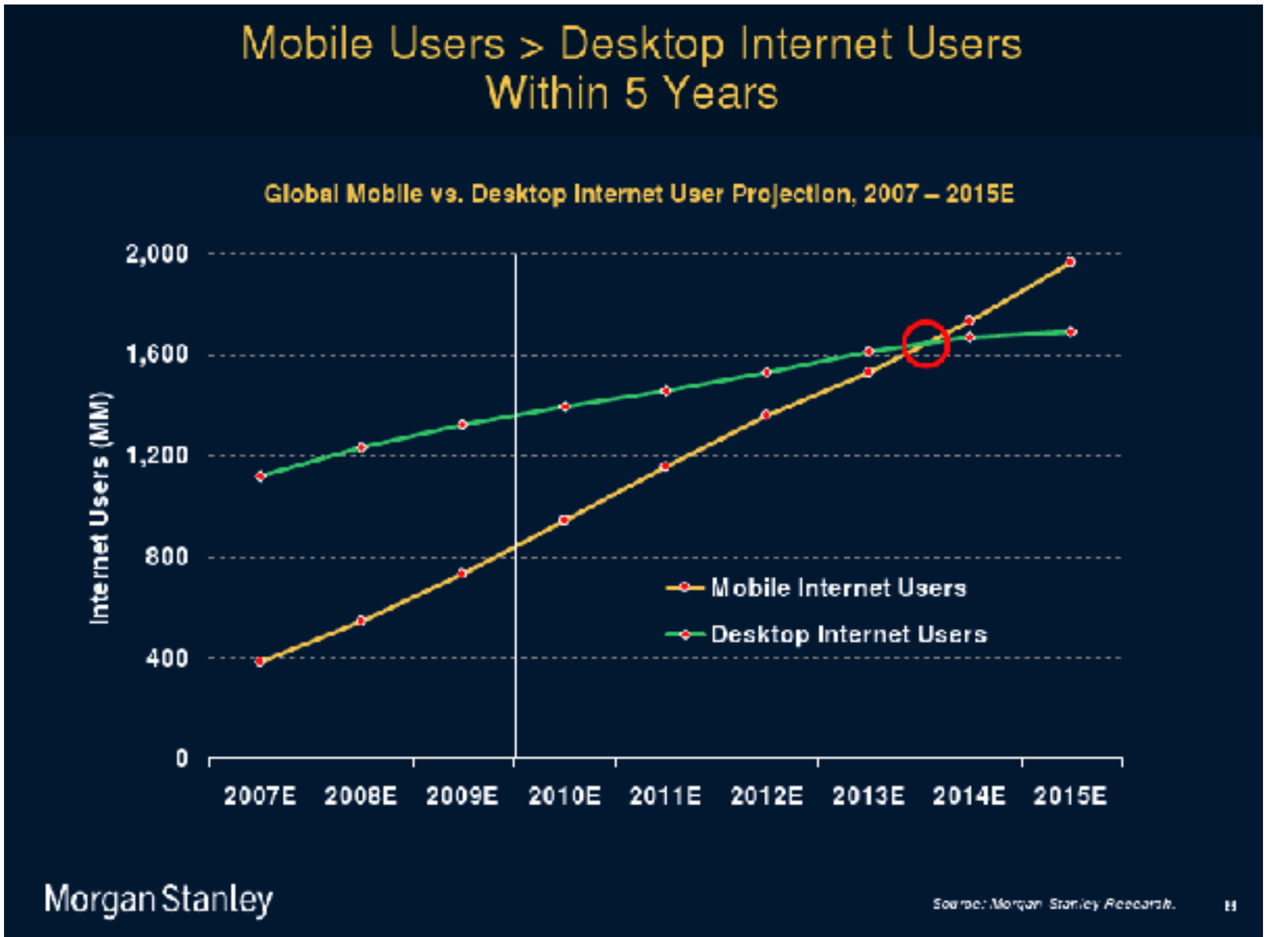
Outline

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

Internet Evolution
(prediction from 2000)



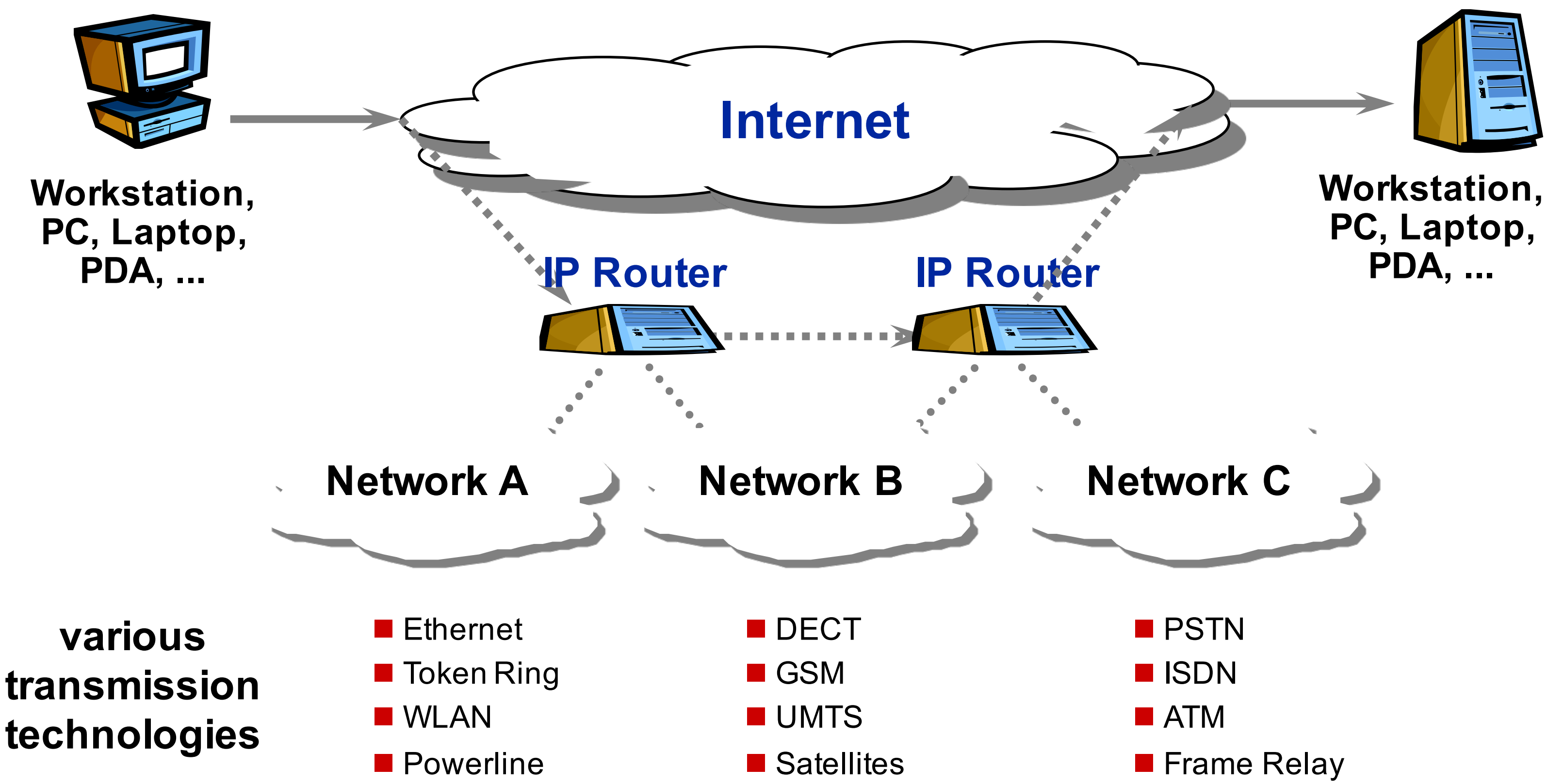
Internet Evolution
(prediction from April 2010)



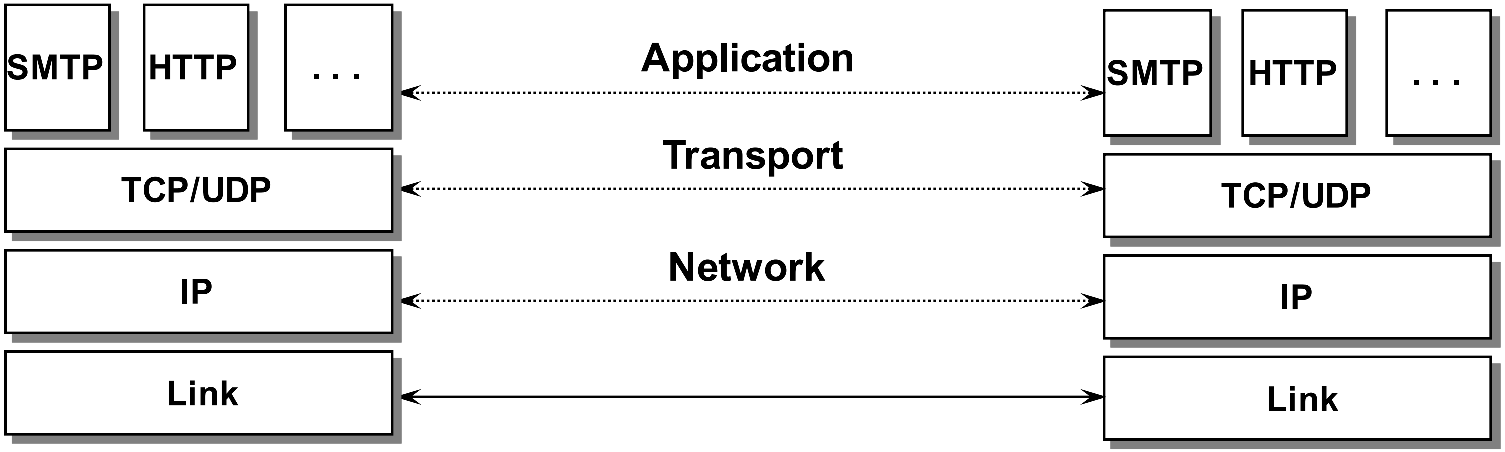
2.1 billion internet users worldwide in March 2011 (30.2%)
Source: Internet World Stats

The Internet - A Network of Networks

- “IP is the protocol that integrates all infrastructures”

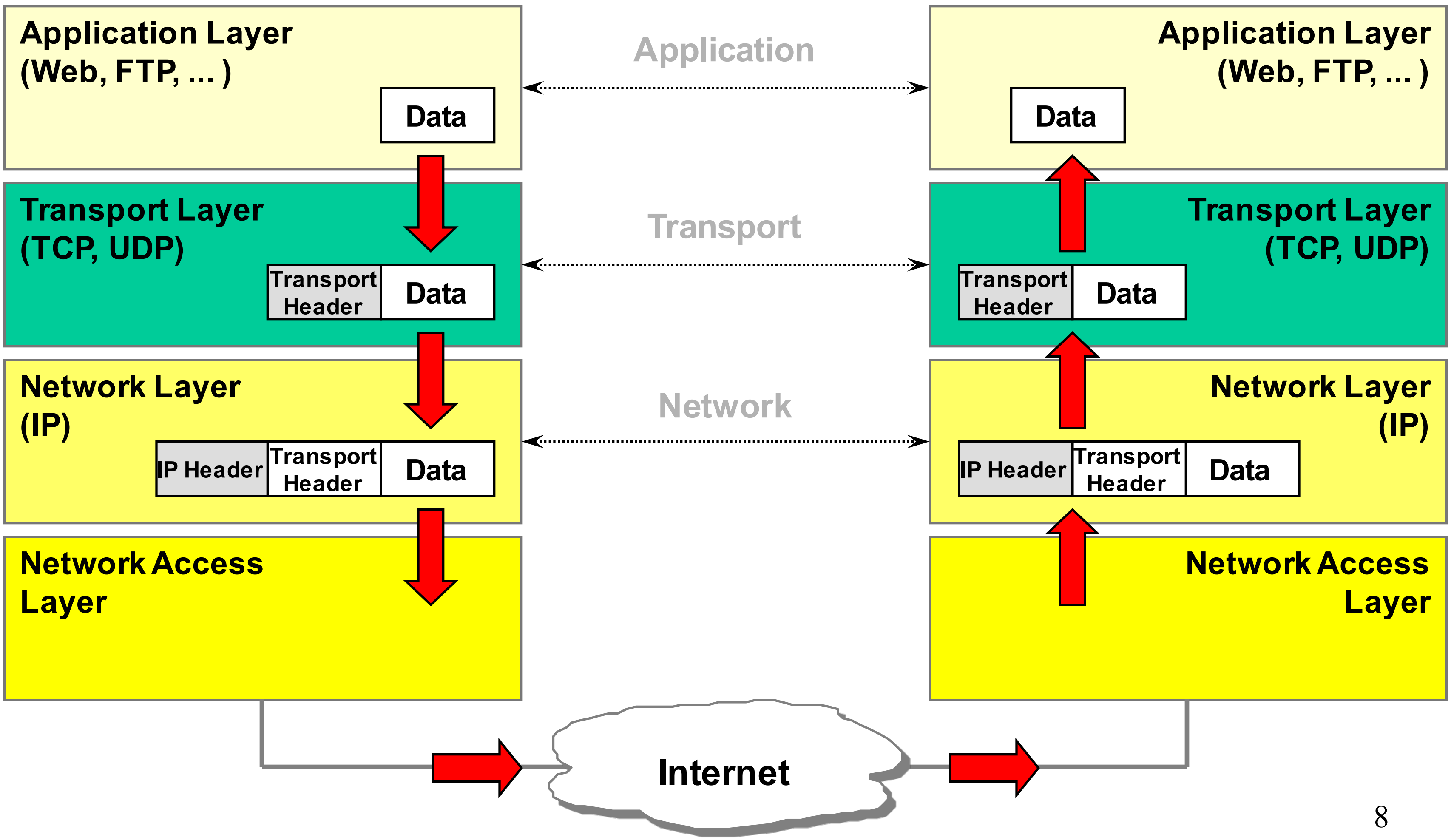


Internet Protocols



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

Data Encapsulation



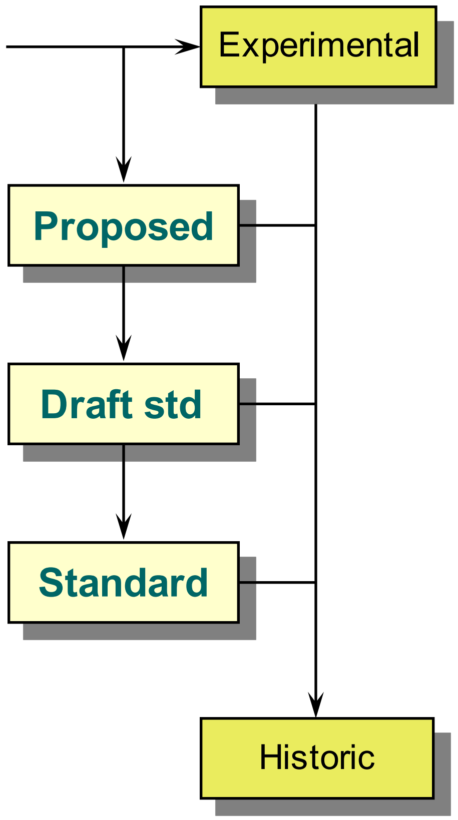
Internet Standardization

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



IETF Intermediate documents

- **Request for Comments (RFCs) with different maturity levels**
  - Experimental (E)
  - Informational (I)
  - Historic (H)
  - Best Current Practice (BCP) – does not influence bits on the wire
- **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 and Kathleen Moriarty

abfab	Application Bridging for Federated Access Beyond web
dane	DNS-based Authentication of Named Entities
dkim	Domain Keys Identified Mail
emu	EAP Method Update
ipsecme	IP Security Maintenance and Extensions
jose	Javascript Object Signing and Encryption
kitten	Common Authentication Technology Next Generation
krb-wg	Kerberos
mile	Managed Incident Lightweight Exchange
nea	Network Endpoint Assessment
oauth	Open authentication
pkix	Public-Key Infrastructure (X.509)
tls	Transport Layer Security

security work in other areas:

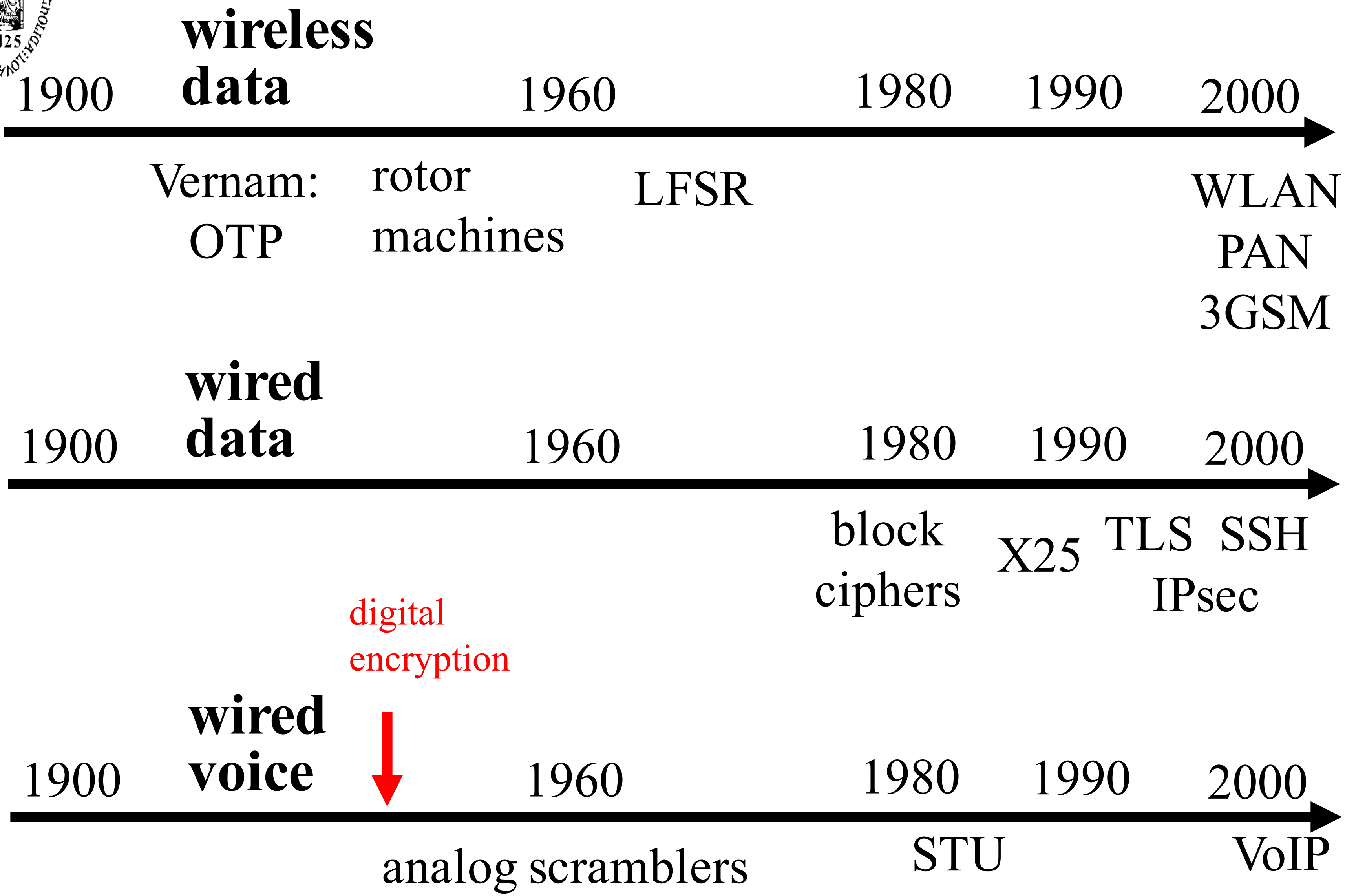
Keying and Authentication for Routing Protocols
Secure Inter-Domain Routing
DNS Extensions
Web Security

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!

A historical perspective (1)



A historical perspective (2)

mobile phones

1980 — AMPS — analog cloning, scanners

1990 — GSM/TDMA — TDMA cloning

2000 — 3G — attacks on A5, COMP128

2010 — LTE

WLAN

1997 — WEP — WEP broken

2002 — WPA — WPA weak

2004 — WPA2/802.11i

PAN

1999 — Bluetooth

2007 — Bluetooth 2.1

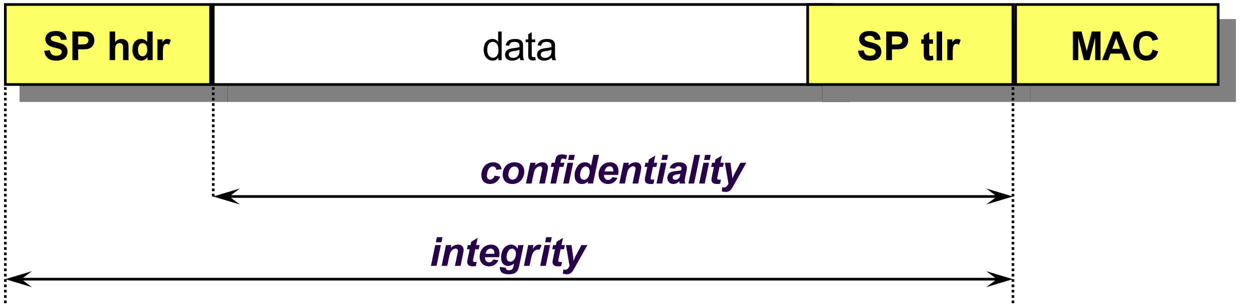
Bluetooth problems

Security Goals (started in ISO 7498-2)

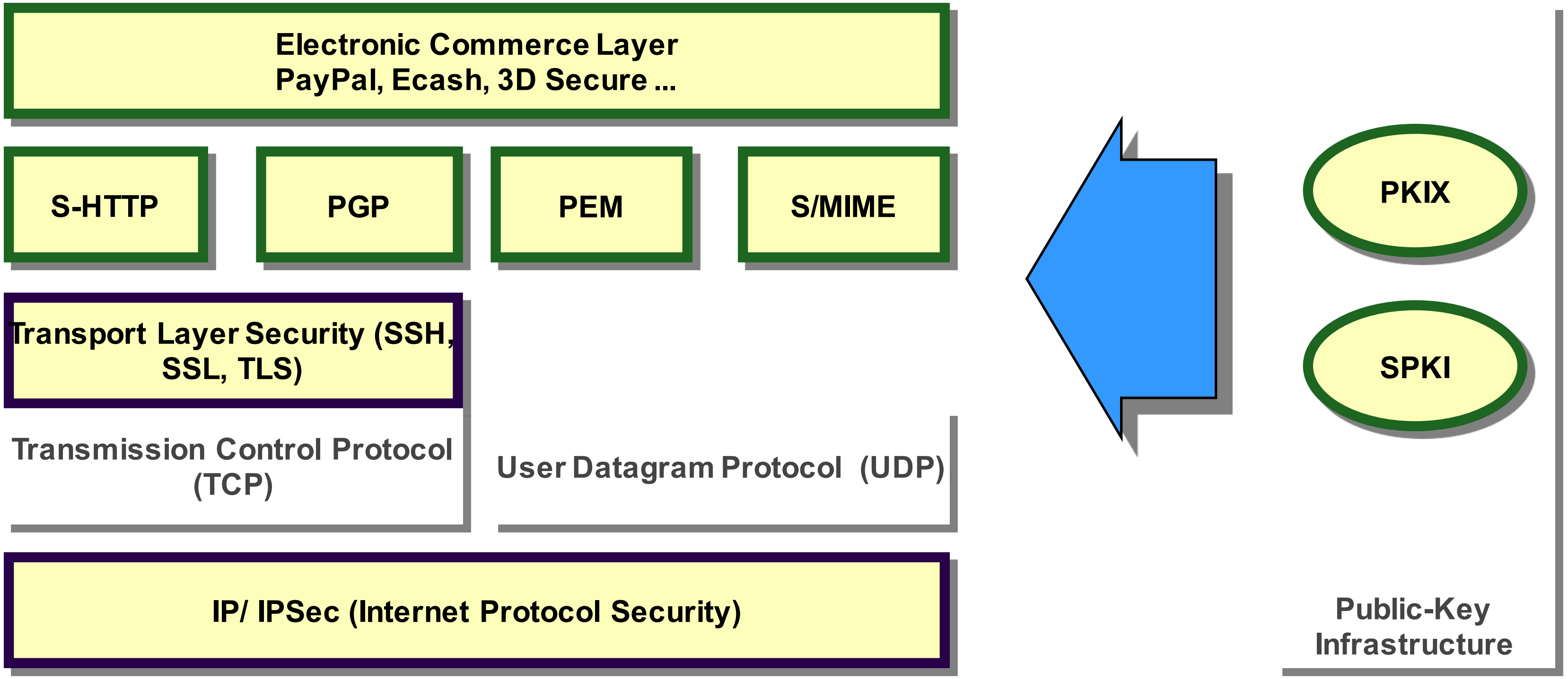
- confidentiality:
  - entities (anonimity)
  - data
  - traffic flow
- (unilateral or mutual) entity authentication
- data authentication (connection-less or connection-oriented): data origin authentication + data integrity
- access control
- non-repudiation of origin versus deniability

Security Protocols & Services

- Cryptographic techniques:
  - symmetric encipherment
  - message authentication mechanisms
  - entity authentication mechanisms
  - key establishment mechanisms (e.g., combined with entity authentication)



Internet Security Protocols

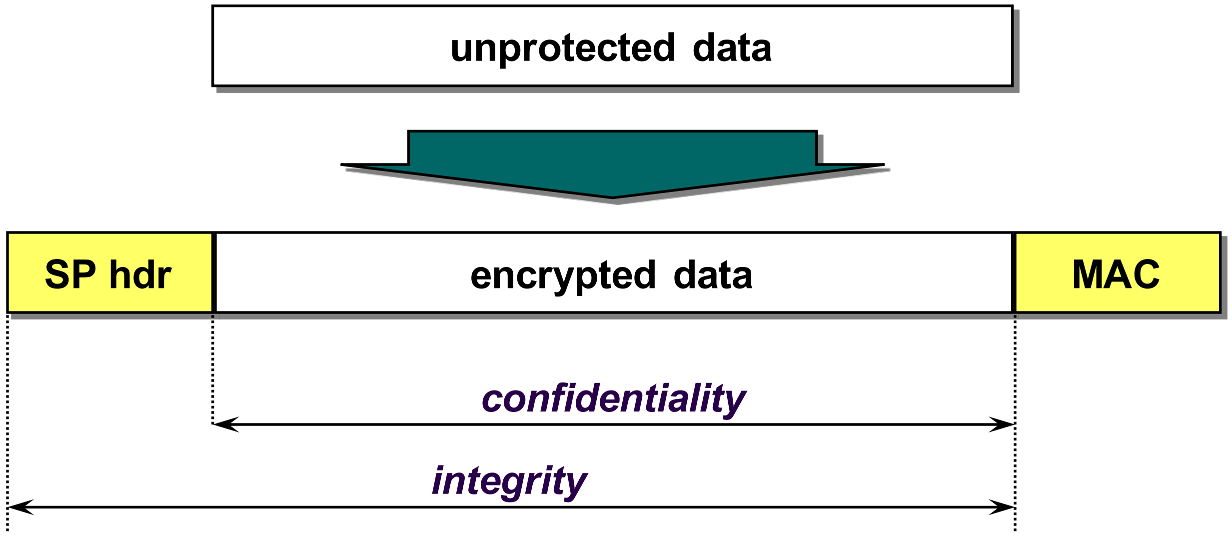


- security services depend on the layer of integration:
  - the mechanisms can only protect the payload and/or header information available at this layer
  - header information of lower layers is not protected!!

Security: at which layer?

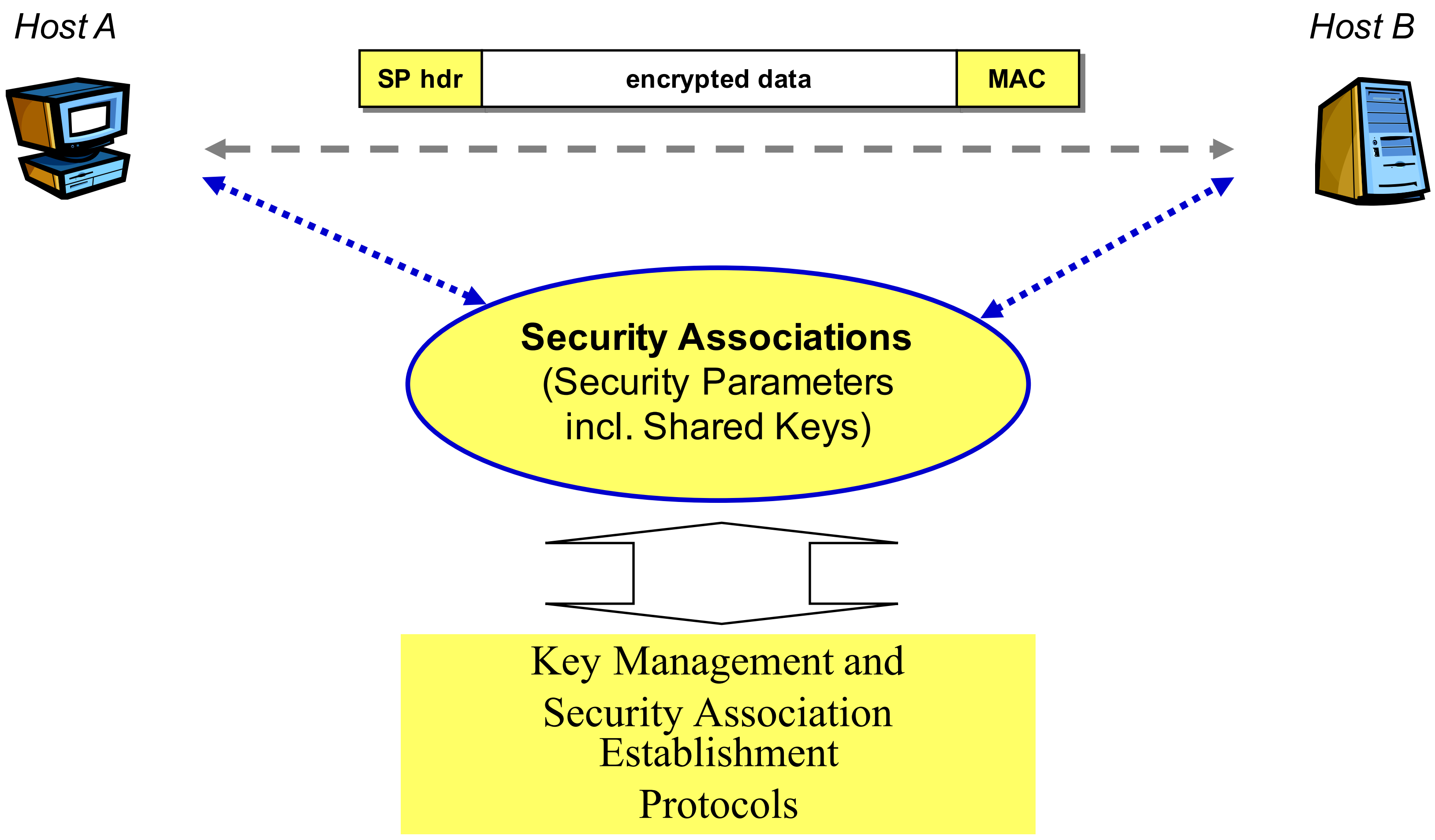
- Application layer:
  - closer to user
  - more sophisticated/granular controls
  - end-to-end
  - but what about firewalls?
- Lower layer:
  - application independent
  - hide traffic data
  - but vulnerable in middle points
- Combine?

SP Architecture I: Encapsulation



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

SP Architecture II: Session (Association) Establishment



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"

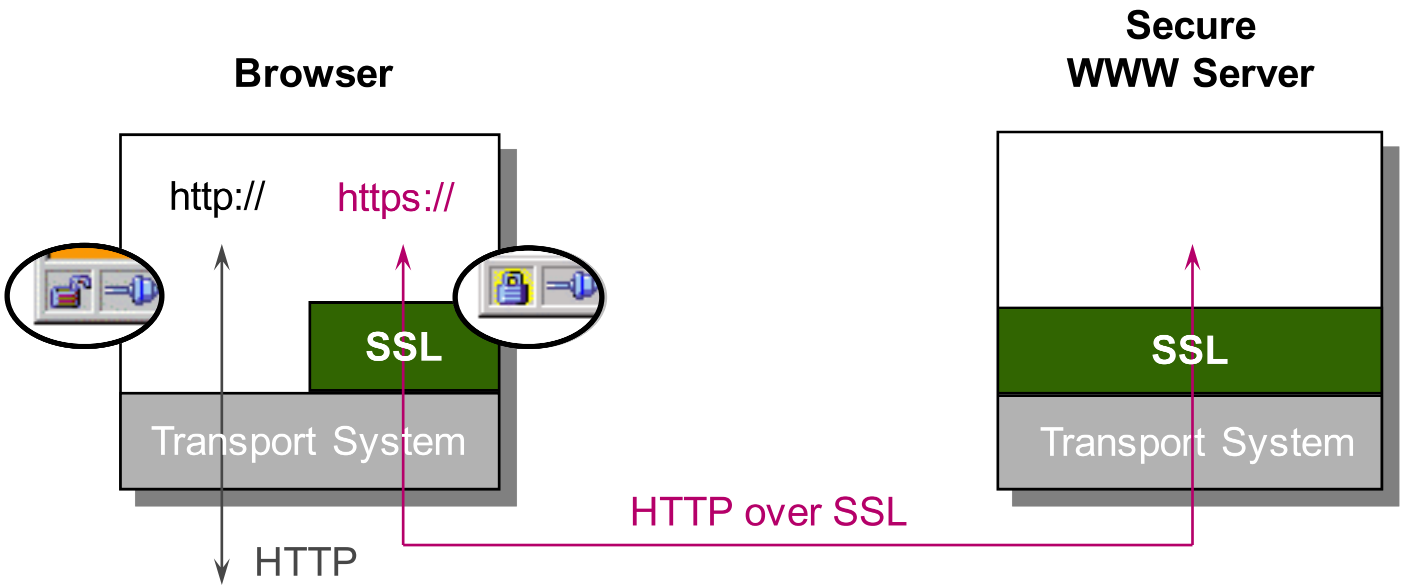
- all parameters are encoded into a single suite number; negotiation consists of offering one or more suites and having the other side choose
- simpler and more compact to encode
- potentially exponential number of suites
- less flexible

- e.g., TLS and IKEv2

Transport layer security

SSL / TLS

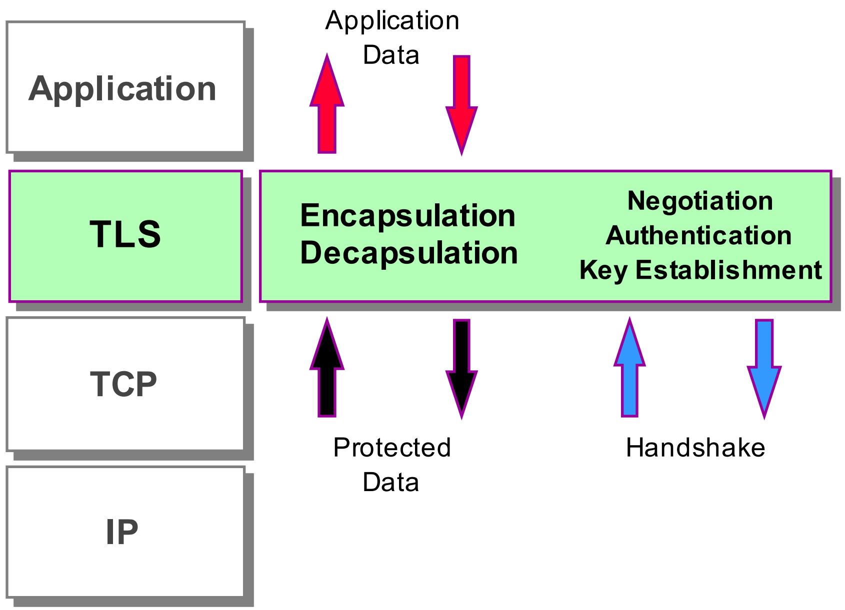
SSL/TLS Protocols



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

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



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!

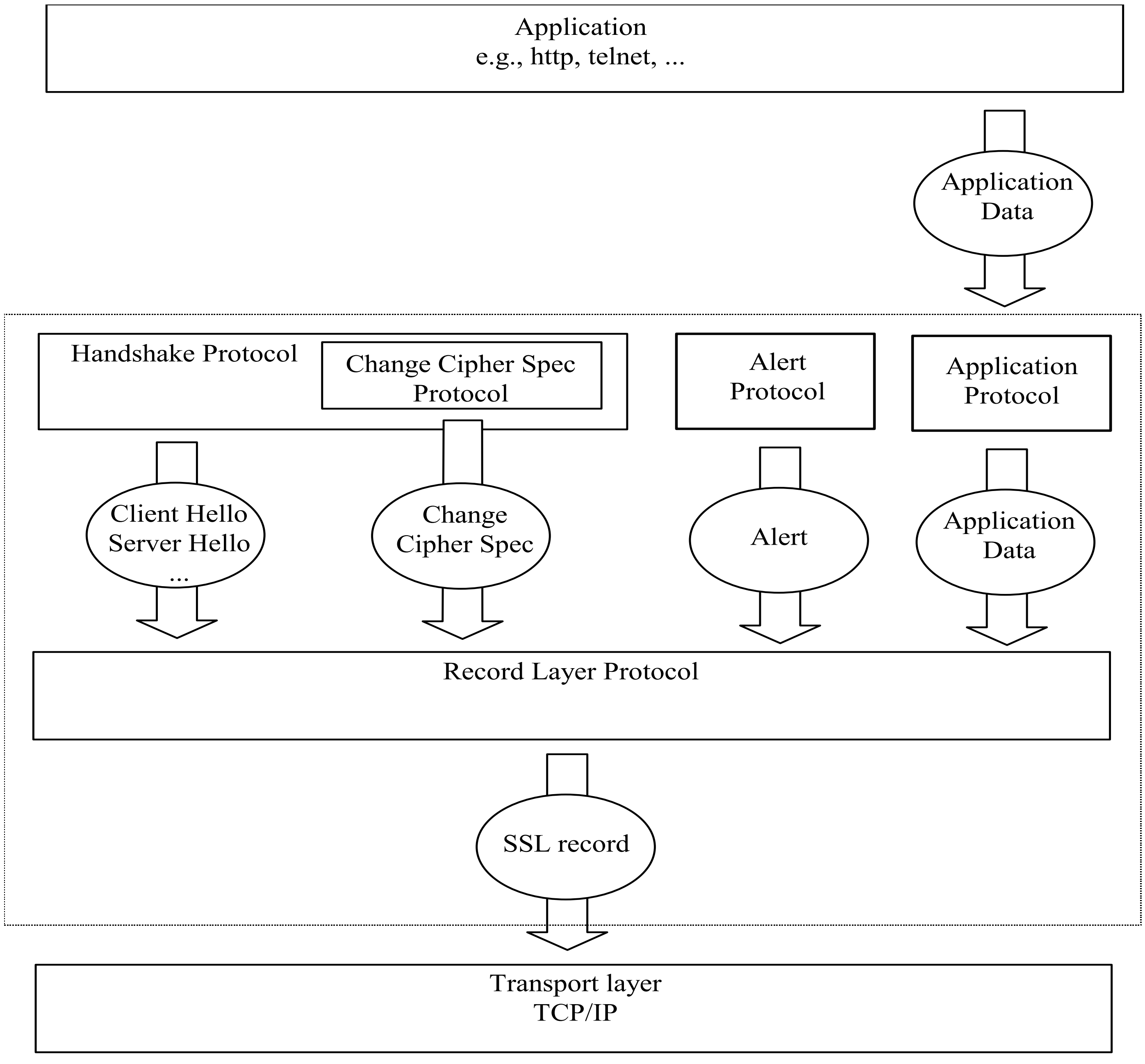
Other WWW security protocols

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

SSL/TLS

- "Secure Sockets Layer" (Netscape)
  - SSL 2.0 (1995): security flaws!
  - SSL 3.0 (1006): 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!

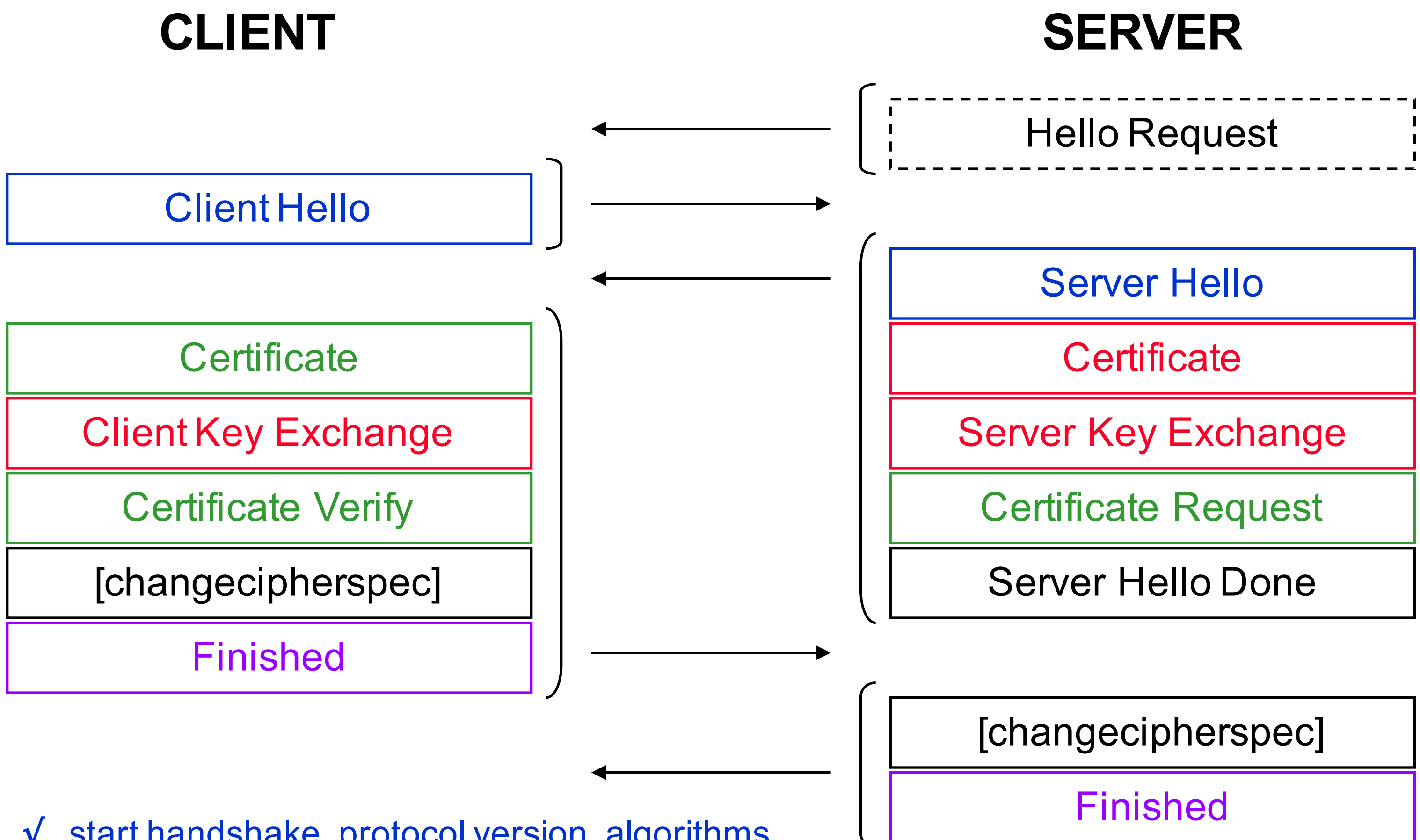
TLS 1.1 and 1.2 deployment very slow (about 25% of servers in Feb. 14); boost in Nov. 2013 (new attacks + Snowden revelations).


Application
e.g., http, telnet, ...
Application Data
Handshake Protocol
Change Cipher Spec Protocol
Alert Protocol
Application Protocol
Client Hello
Server Hello
...
Change Cipher Spec
Alert
Application Data
Record Layer Protocol
SSL record
Transport layer
TCP/IP

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

Handshake: overview



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

TLS 1.2 Data Encapsulation Options

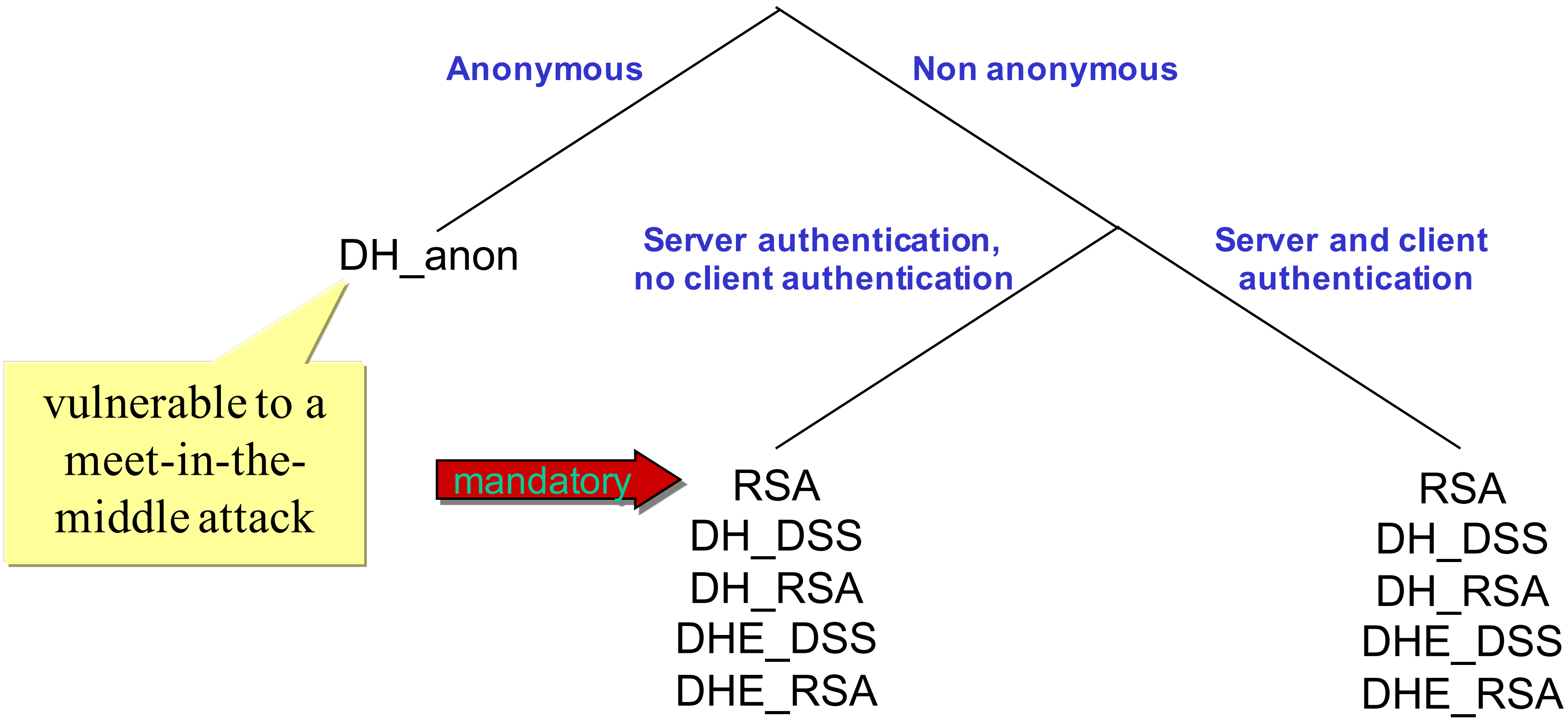
Integrity			
key size	144	160	256
algorithm options	HMAC-MD5	HMAC-SHA	HMAC-SHA256

mandatory

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

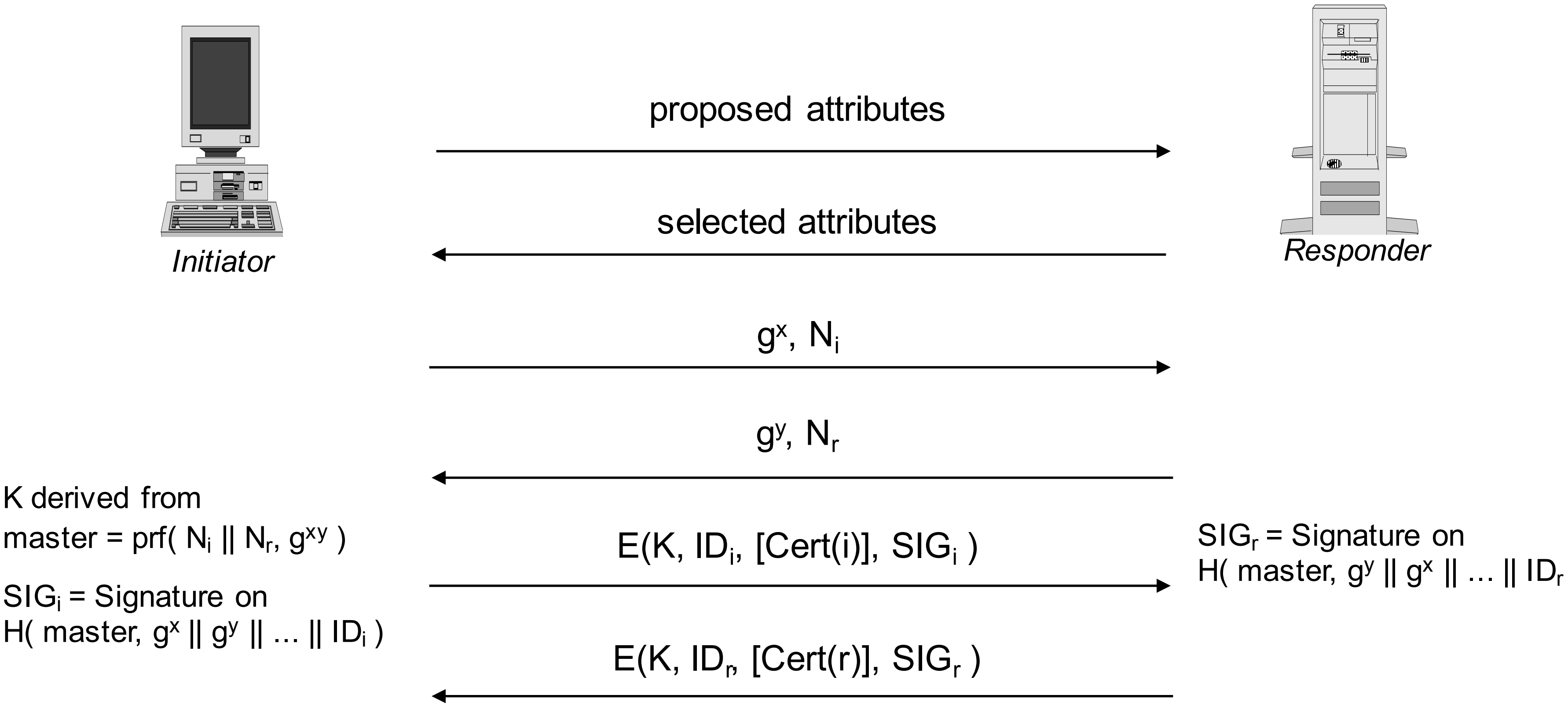
TLS 1.2 Key Management Options



Forward secrecy

- Default algorithm is RSA (better performance, at least for RSA-1024)
  - no forward secrecy: compromise of private server key results in compromise of **all past** sessions
- DH-DSS and DH-DSA: same problem
- DHE-DSS and DHE-DSA: Ephemeral Diffie-Hellman keys leads to forward secrecy
  - For performance reasons: switch to a 256-bit Elliptic Curve (e.g. Google in November 2013)

DHE_DSS (notation from IKE)



H is equal to prf or the hash function tied to the signature algorithm
(all inputs are concatenated)

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!)

36

SSL/TLS: security analysis

Detailed analysis and security reductions ("proofs"):

- Handshake protocol: most unaltered TLS ciphersuites form a secure channel (authenticated and confidential channel establishment)
- Record layer protocol: Authenticated Encryption well understood (but badly implemented)

Current analysis does not take into account the full complexity

- Cipher suites: negotiation, renegotiation, reuse of master key over multiple suites
- Cross protocol attacks
- Fragmentation
- Compression
- Timing attacks

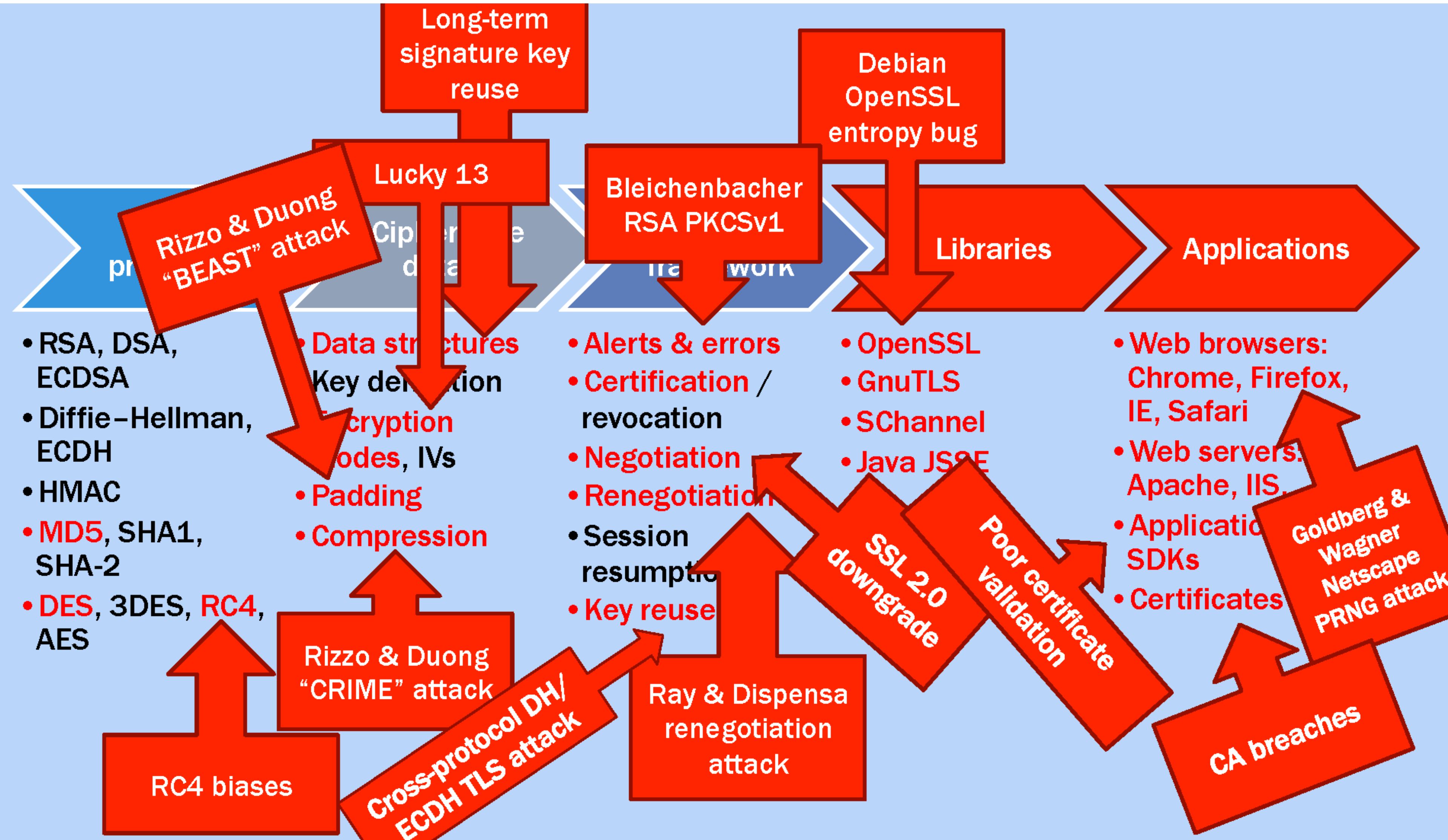
37

TLS overview [Stebila'14]

Crypto primitives	Ciphersuite details	Protocol "Framework"	Libraries	Applications
RSA, DSA, ECDSA	Data structures	Alerts and errors	OpenSSL	Web browsers
DH, EC-DH	Key derivation	Certification/re-vocation	GnuTLS	Web servers
HMAC	Encryption modes and IVs	(Re-)Negotiation	SChannel	Application SDKs
MD5, SHA-1, SHA-2	Padding	Session Resumption	Java JSSE0	Certificates
DES, 3DES, RC4, AES	Compression	Key reuse		

Theoretical analysis

TLS attack overview [Stebila'14]



TLS attacks (1)

- **Renegotiation attack (2009)**
  - allows injection of data; patched by RFC 5746
- **Version rollback attacks (2011)**
  - exploits false start feature (introduced to improve performance)
- **CRIME and BREACH attacks (2013)**
  - recovery of cookies when *data compression* is used
  - all TLS versions are vulnerable
- **Truncation attack (2013)**
  - suppress logout by injecting an unencrypted TCP FIN message
- **Heartbleed (2014)**
  - Buffer over-read in OpenSSL implemenation
- **Poodle (2014)** Padding Oracle On Downgraded Legacy Encryption
  - Man-in-the middle that exploits downgrade to SSL 3.0

TLS attacks (2)

- **Padding oracle and timing attacks**
  - RSA
    - [Bleichenbacher 98] PKCS #1v1.5 – 1 million chosen ciphertexts (in practice 200,000);
    - [Klima+ 03] 40% improvement
    - [Bardou+ 12]: reduced to about 10,000 chosen ciphertexts
    - timing attack [Kocher'95], [Boneh-Brumley'03]
  - CBC (IV and padding)
    - padding [Rogaway], [Vaudenay 02] , [Canvel+ 03]: password recovery
    - BEAST attack [Rizzo-Duon 11]: exploits IV issues - patched from TLS 1.1 onwards
    - Lucky 13 [AlFardan-Paterson'13]: timing attack on CBC padding **– no patch known**
- **Cryptographic attacks**
  - Weak random number generators: Netscape, Debian, embedded devices…
  - Exhaustive key search: 40-bit and 56-bit keys
  - Cross-protocol attack: elliptic curve parameters can be read as DH-prime
  - Biases in RC4 (re-introduced to 50% of web in Feb. 2013 to stop BEAST attack) [AlFardan+ 13] [Isobe+ 13]

TLS problems

- many PKI issues: revocation, root keys, fake certificates, certificate parsing,…
- web spoofing and phishing
- what if the user does not know that a particular website has to use SSL/TLS (solution HSTS – **HTTP Strict Transport Security** (**HSTS**): mandate that you interact with particular servers using https/TLS only)
- traffic analysis:
  - length of ciphertext might reveal useful info
  - time to retrieve a page indicates whether it has been retrieved before

TLS Renegotiation attack [Marsh Ray Nov.09]

- 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
- Fix: TLS renegotiation indication extension RFC 5746 – Feb.'10 (84% deployment in Jan.'14)

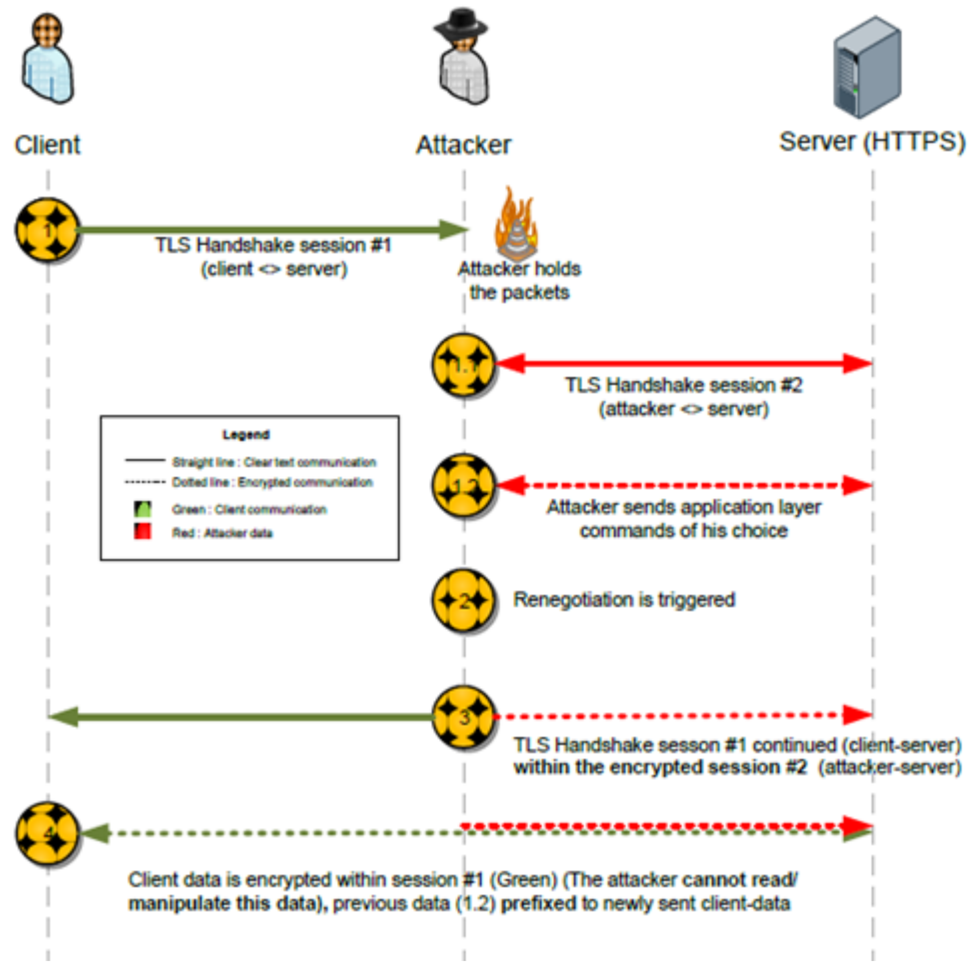


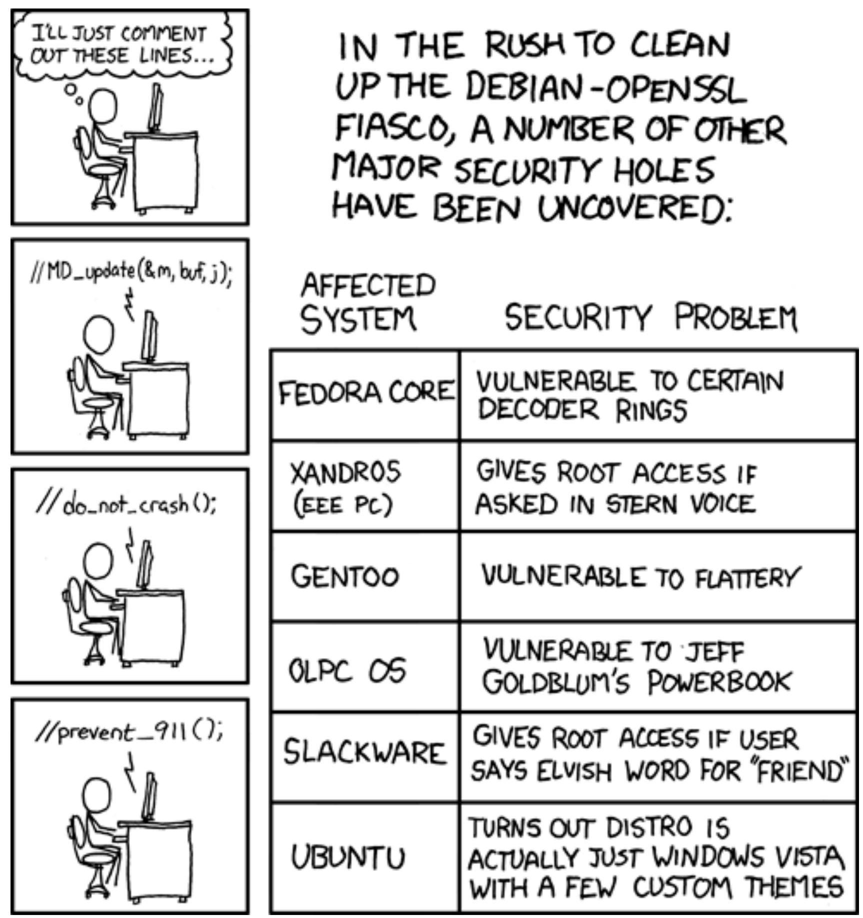
Figure: L. O'Connor

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



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\0.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/

User authentication

First *authentication*, then *authorization* !

SSL/TLS client authentication:

- During handshake, client can digitally sign a specific message that depends on all relevant parameters of secure session with server
- Support by software devices, smart cards or USB tokens
- PKCS#12 key container provides software mobility
- rarely implemented

Usually another mechanism on top of SSL/TLS

TLS 1.3

- Reduce the number of cipher suites:
  - only authenticated encryption with associated data (AEAD): AES-GCM, AES-CCM,ARIA-GCM, Camellia-GCM, ChaCha/Poly1305
  - only perfect forward secrecy (still RSA for signatures)
  - no custom DH groups
- Forbid renegotiation but keep resumption with tickets
- Improve privacy: encrypt more of the handshake
- Improve latency: target: 1-RTT handshake for naive clients but 0-RTT handshake for repeat connections

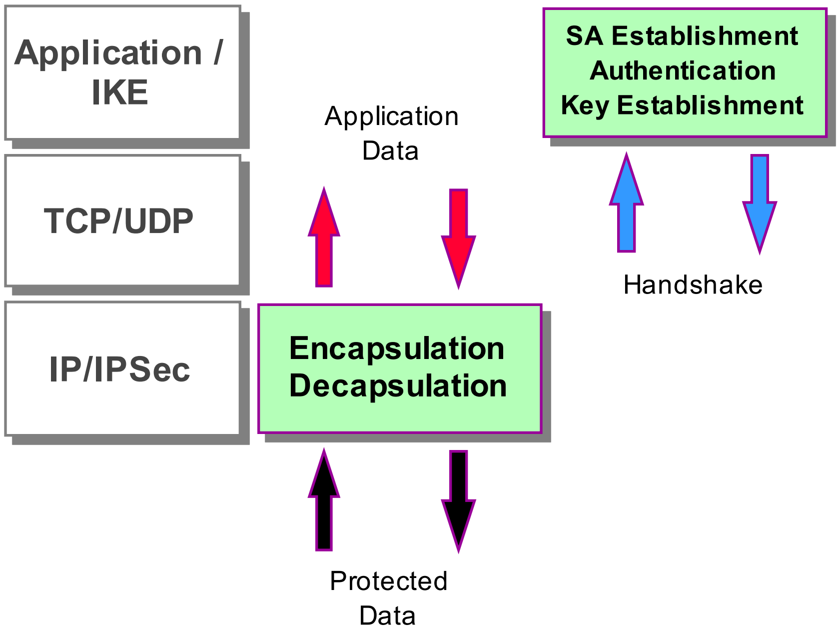
Backward compatibility remains very important because of huge installed base

Network layer security

IPsec, VPN, SSH

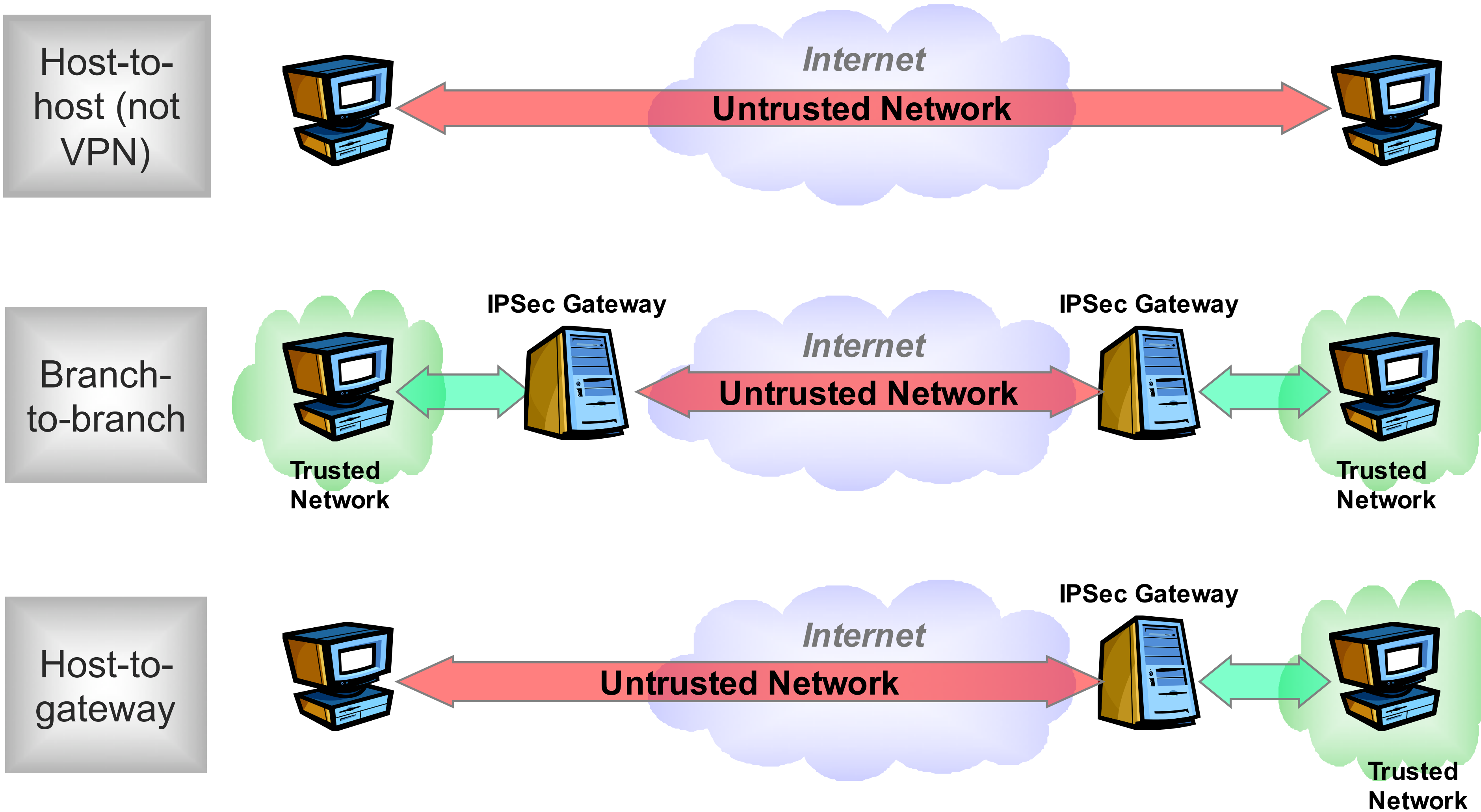
IP Security Protocols

- 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

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)

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)

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]

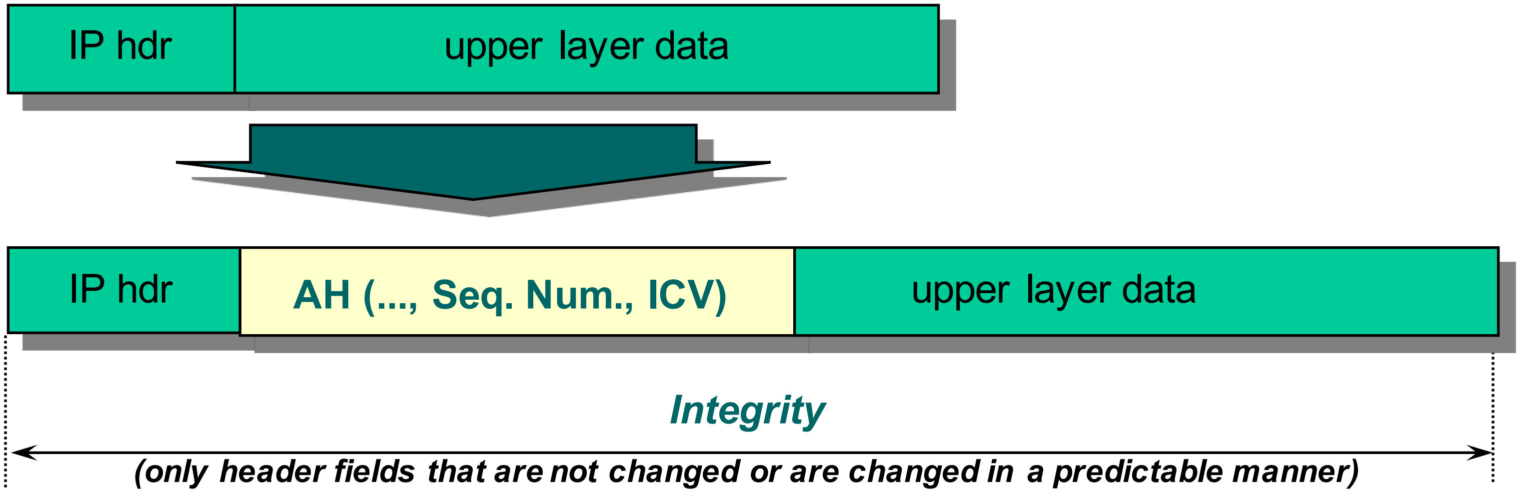
Source: draft-ietf-ipsec-ikev2-algorithms-00.txt, May 2003

IPsec - Modes

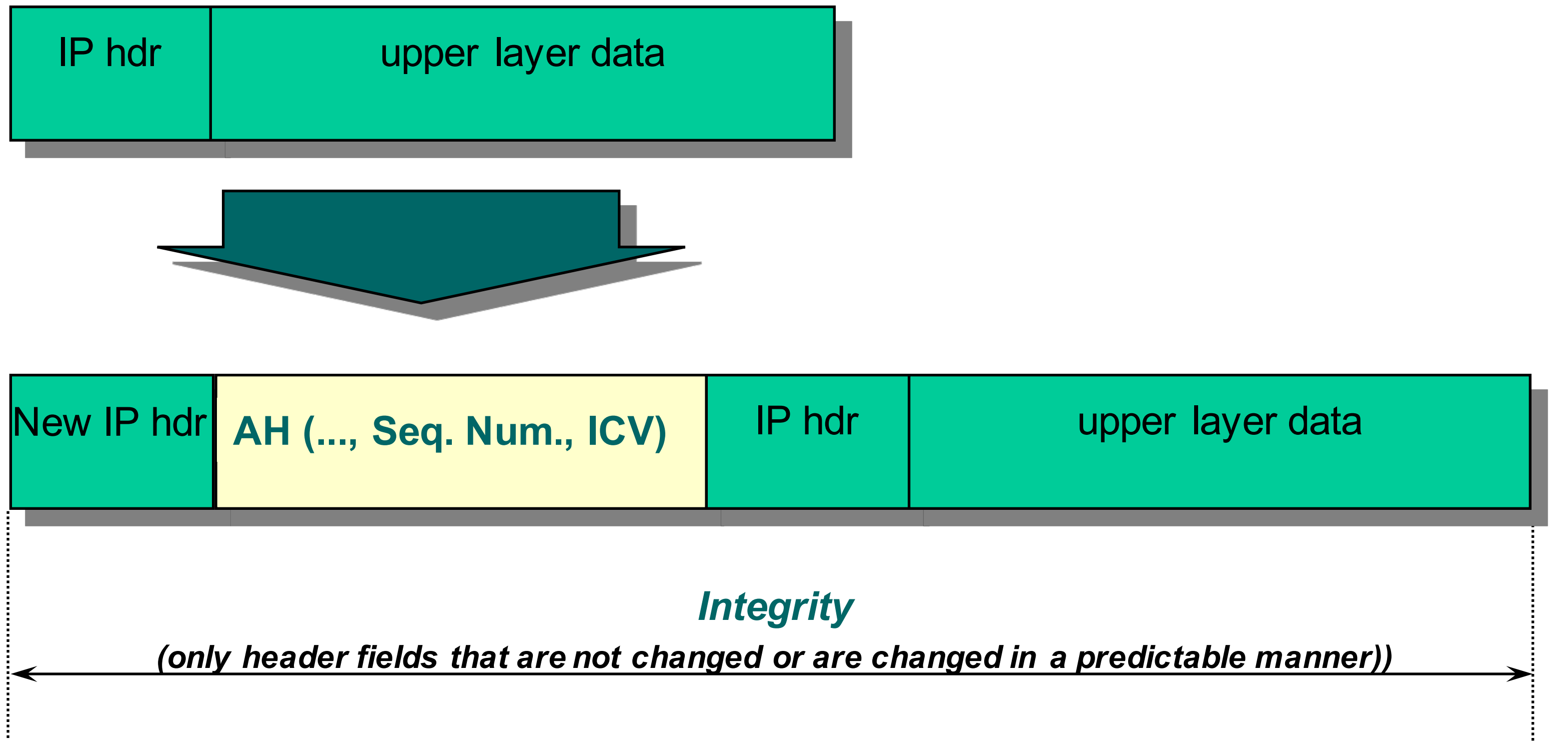
- Transport *(host-to-host)*
  - ESP: encrypts and optionally authenticates IP payload, but not IP header
  - AH: authenticates IP payload and selected portions of IP header
- Tunnel *(between security gateways)*
  - after AH or ESP fields are added, the entire packet is treated as payload of new outer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

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



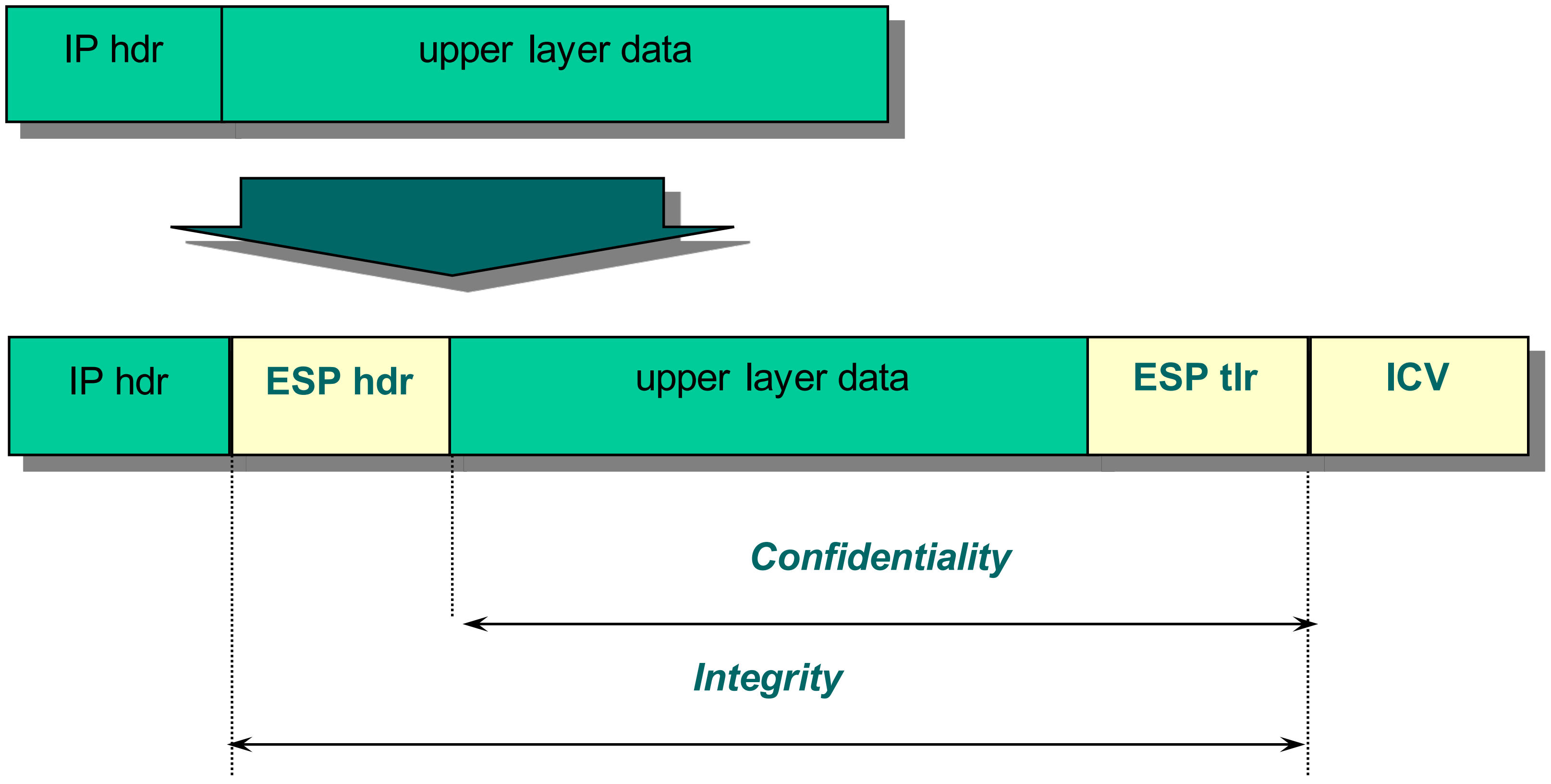
IPsec - AH Tunnel mode



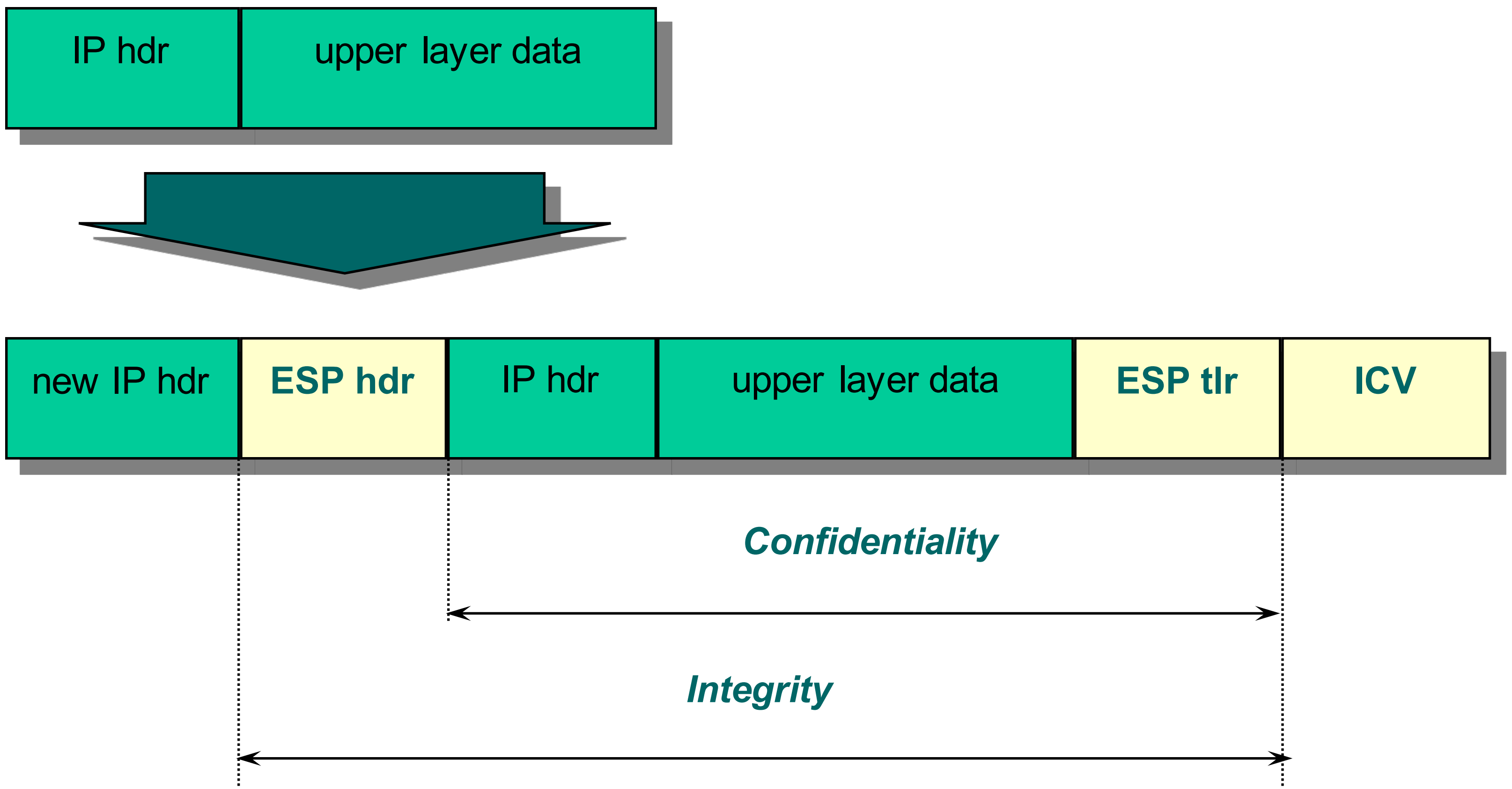
IPsec - ESP header

- 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

IPsec - ESP Transport mode



IPsec - ESP Tunnel mode



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

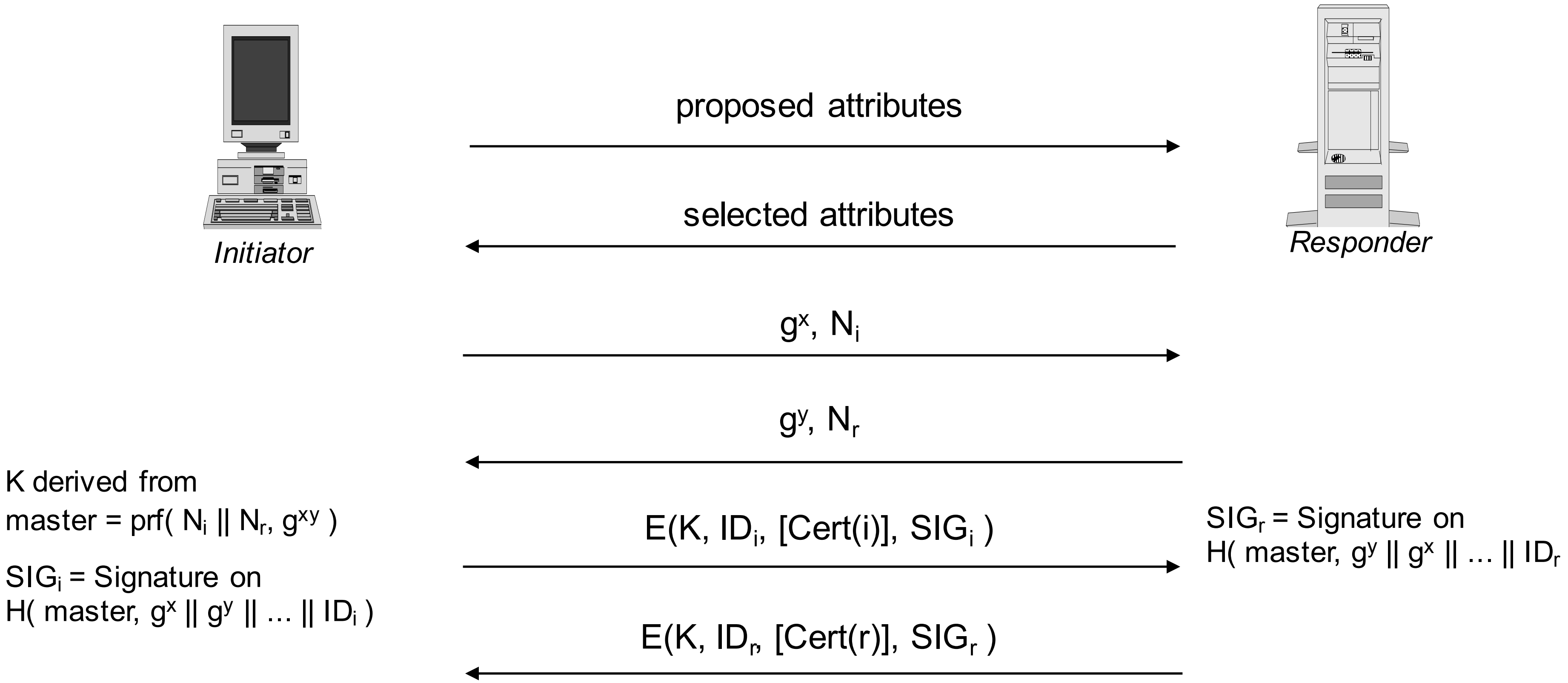
IPsec: Key management

- 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

IPsec: Key management

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

IKE - Main Mode with Digital Signatures



H is equal to prf or the hash function tied to the signature algorithm
(all inputs are concatenated)

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

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

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

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

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

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
  - remote user access over the Internet
  - connecting networks over the Internet
  - connection computers over an intranet

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!

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

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/