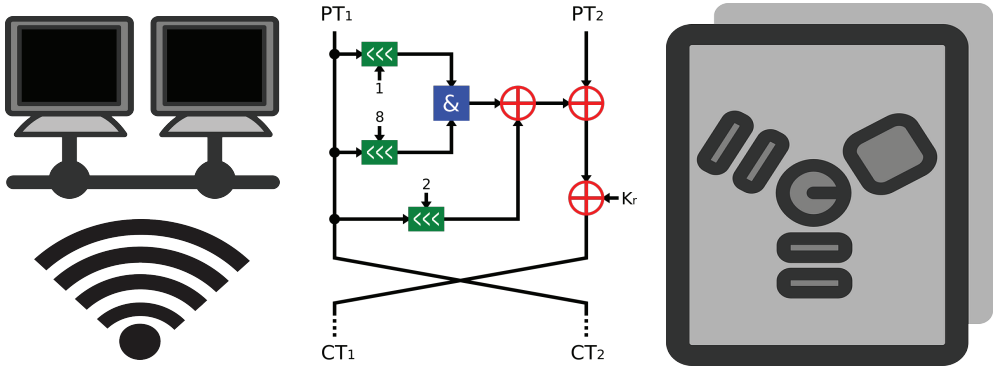
CSE 40567 / 60567: Computer Security



Network Security 2

Homework #6 has been released. It is due on 4/16 at 11:59PM (your timezone)

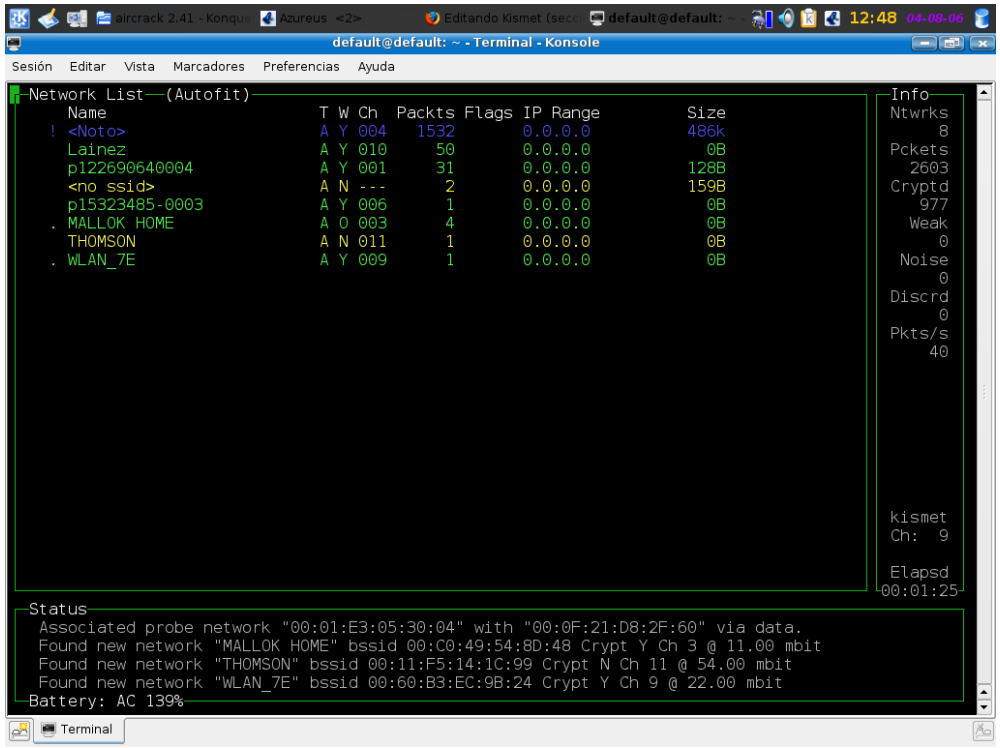
See **Assignments Page** on the course website for details

Wireless Eavesdropping

- Open access points
- WEP attacks
  - Less common these days, but occasionally WEP-enabled devices are encountered
- Known weaknesses in WPA and WPA2
  - Authenticated attacker may be able to sniff the network

Kismet (Unix)

https://www.kismetwireless.net/

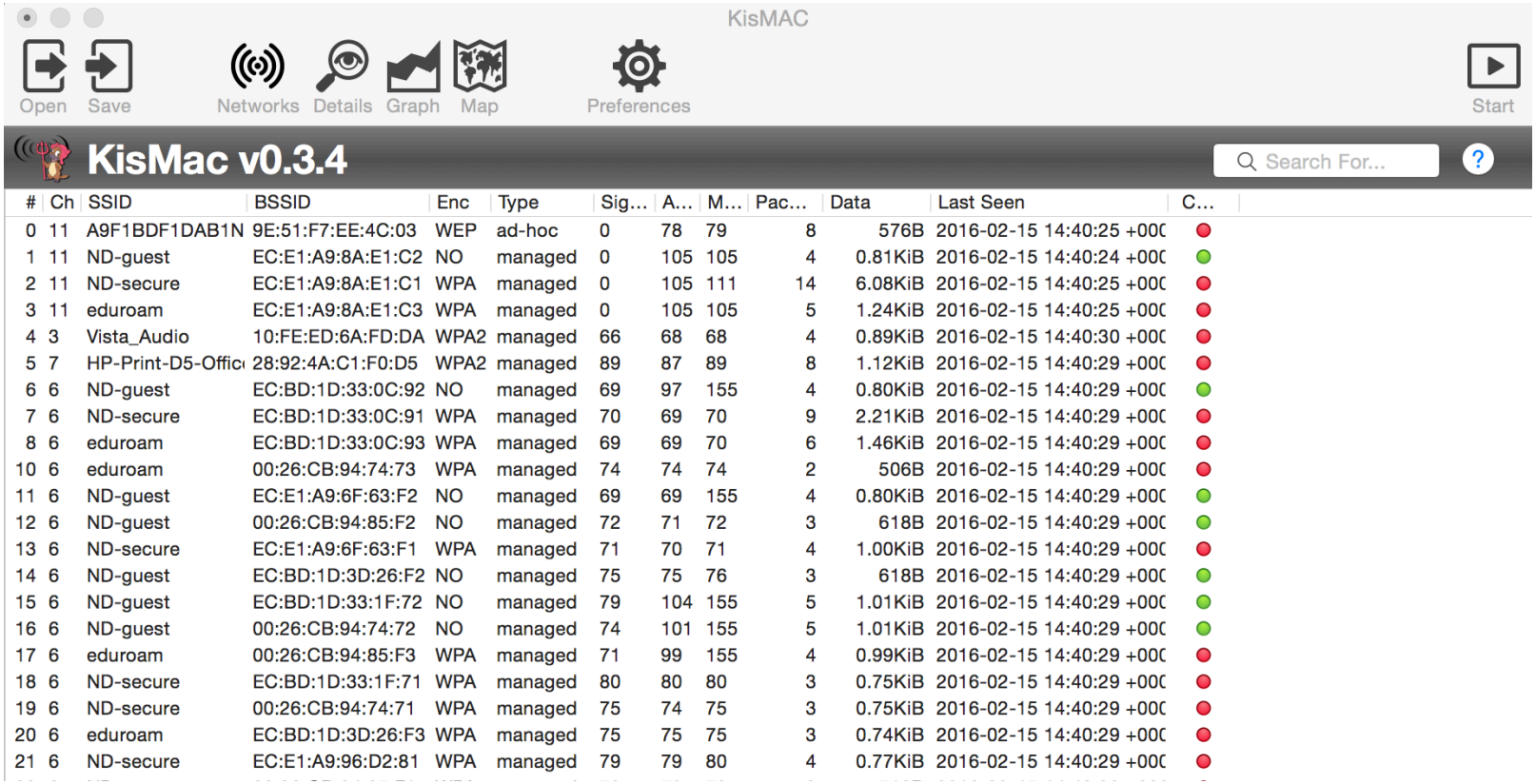


- 802.11 sniffing
- Standard PCAP logging
- Client/Server modular architecture
- Plug-in architecture to expand core features
- Multiple capture source support
- Live export of packets to other tools via tun/tap virtual interfaces
- Distributed remote sniffing via light-weight remote capture
- XML output for integration with other tools

KisMac2 (OS X)

https://github.com/IGRSoft/KisMac2

Mac version of Kismet, with a friendlier UI



#	Ch	SSID	BSSID	Enc	Type	Sig…	A…	M…	Pac…	Data	Last Seen	C…
0	11	A9F1BDF1DAB1N	9E:51:F7:EE:4C:03	WEP	ad-hoc	0	78	79	8	576B	2016-02-15 14:40:25 +00(	
1	11	ND-guest	EC:E1:A9:8A:E1:C2	NO	managed	0	105	105	4	0.81KiB	2016-02-15 14:40:24 +00(	
2	11	ND-secure	EC:E1:A9:8A:E1:C1	WPA	managed	0	105	111	14	6.08KiB	2016-02-15 14:40:25 +00(	
3	11	eduroam	EC:E1:A9:8A:E1:C3	WPA	managed	0	105	105	5	1.24KiB	2016-02-15 14:40:25 +00(	
4	3	Vista_Audio	10:FE:ED:6A:FD:DA	WPA2	managed	66	68	68	4	0.89KiB	2016-02-15 14:40:30 +00(	
5	7	HP-Print-D5-Offic	28:92:4A:C1:F0:D5	WPA2	managed	89	87	89	8	1.12KiB	2016-02-15 14:40:29 +00(	
6	6	ND-guest	EC:BD:1D:33:0C:92	NO	managed	69	97	155	4	0.80KiB	2016-02-15 14:40:29 +00(	
7	6	ND-secure	EC:BD:1D:33:0C:91	WPA	managed	70	69	70	9	2.21KiB	2016-02-15 14:40:29 +00(	
8	6	eduroam	EC:BD:1D:33:0C:93	WPA	managed	69	69	70	6	1.46KiB	2016-02-15 14:40:29 +00(	
10	6	eduroam	00:26:CB:94:74:73	WPA	managed	74	74	74	2	506B	2016-02-15 14:40:29 +00(	
11	6	ND-guest	EC:E1:A9:6F:63:F2	NO	managed	69	69	155	4	0.80KiB	2016-02-15 14:40:29 +00(	
12	6	ND-guest	00:26:CB:94:85:F2	NO	managed	72	71	72	3	618B	2016-02-15 14:40:29 +00(	
13	6	ND-secure	EC:E1:A9:6F:63:F1	WPA	managed	71	70	71	4	1.00KiB	2016-02-15 14:40:29 +00(	
14	6	ND-guest	EC:BD:1D:3D:26:F2	NO	managed	75	75	76	3	618B	2016-02-15 14:40:29 +00(	
15	6	ND-guest	EC:BD:1D:33:1F:72	NO	managed	79	104	155	5	1.01KiB	2016-02-15 14:40:29 +00(	
16	6	ND-guest	00:26:CB:94:74:72	NO	managed	74	101	155	5	1.01KiB	2016-02-15 14:40:29 +00(	
17	6	eduroam	00:26:CB:94:85:F3	WPA	managed	71	99	155	4	0.99KiB	2016-02-15 14:40:29 +00(	
18	6	ND-secure	EC:BD:1D:33:1F:71	WPA	managed	80	80	80	3	0.75KiB	2016-02-15 14:40:29 +00(	
19	6	ND-secure	00:26:CB:94:74:71	WPA	managed	75	74	75	3	0.75KiB	2016-02-15 14:40:29 +00(	
20	6	eduroam	EC:BD:1D:3D:26:F3	WPA	managed	75	75	75	3	0.74KiB	2016-02-15 14:40:29 +00(	
21	6	ND-secure	EC:E1:A9:96:D2:81	WPA	managed	79	79	80	4	0.77KiB	2016-02-15 14:40:29 +00(	

What is floating out on the ether?

Packets captured at Eddy St. Commons (IP changed to protect the innocent):

```
17:39:25.702642 IP mediaserver-sv5-t1-2-v4.pandora.com.http >
10.10.10.1.44426: Flags [.], seq 13380:14718, ack 1, win 126,
options [nop,nop,TS val 4232024559 ecr 20810772], length 1338

17:39:25.735725 IP mediaserver-sv5-t1-2-v4.pandora.com.http >
10.10.10.1.44426: Flags [.], seq 16056:17394, ack 1, win 126,
options [nop,nop,TS val 4232024559 ecr 20810772], length 1338

17:39:25.800810 IP mediaserver-sv5-t1-2-v4.pandora.com.http >
10.10.10.1.44426: Flags [.], seq 17394:18732, ack 1, win 126,
options [nop,nop,TS val 4232024559 ecr 20810772], length 1338
```

User listening to music

What is floating out on the ether?

Packets captured at Eddy St. Commons (IP changed to protect the innocent):

```
17:40:04.618312 CF +QoS IP 10.10.10.1.53045 >
dns1.nd.edu.domain: 39098+ A? app.snapchat.com. (34)

17:40:04.629288 CF +QoS IP 10.10.10.1.53045 >
dns1.nd.edu.domain: 39098+ A? app.snapchat.com. (34)
```

User doing some messaging

What is floating out on the ether?

Packets captured at Eddy St. Commons (IP changed to protect the innocent):

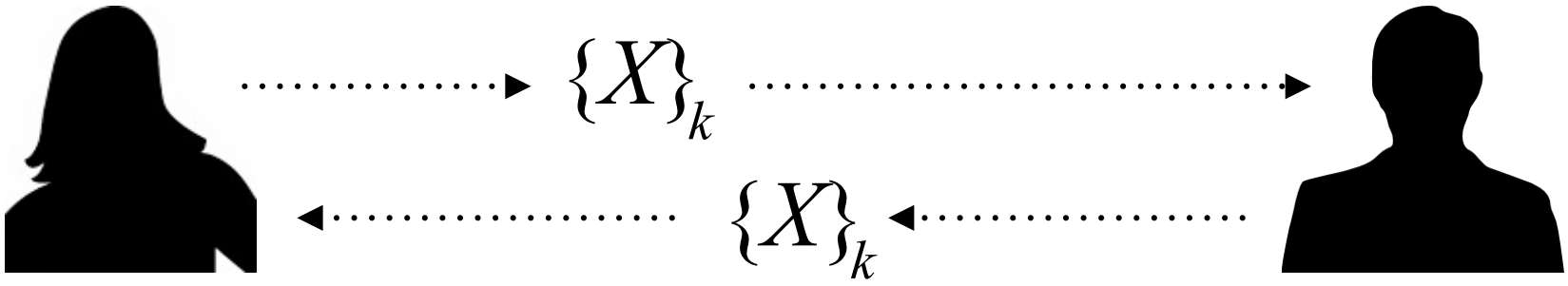
```
17:40:10.272639 CF +QoS IP 10.10.10.1.64141 > s3-1-
w.amazonaws.com.http: Flags [S], seq 2601035886, win 65535,
options [mss 1460,nop,wscale 5,nop,nop,TS val 768497473 ecr
0,sackOK,eol], length 0

17:40:10.272724 CF +QoS IP 10.10.10.1.64141 > s3-1-
w.amazonaws.com.http: Flags [S], seq 2601035886, win 65535,
options [mss 1460,nop,wscale 5,nop,nop,TS val 768497473 ecr
0,sackOK,eol], length 0

17:40:10.294845 CF +QoS IP 10.10.10.1.64141 > s3-1-
w.amazonaws.com.http: Flags [S], seq 2601035886, win 65535,
options [mss 1460,nop,wscale 5,nop,nop,TS val 768497473 ecr
0,sackOK,eol], length 0
```

User accessing cloud-based storage

Countermeasures Against Eavesdropping

Encrypt channels

Solution we've seen before:



Getting the protocols right is another matter…

ssh session

```
$ ssh wscheirer@140.247.178.71

# tcpdump -X —n tcp port 22

11:28:41.937021 IP 140.247.178.71.22 > 140.247.178.194.48111: Flags
[P.], seq 1338:1386, ack 1458, win 247, options [nop,nop,TS val
1250596981 ecr 4256522663], length 48
    0x0000:  4500 0064 5a36 4000 4006 6165 8cf7 b247  E..dZ6@.@.ae...G
    0x0010:  8cf7 b2c2 0016 bbef bb6f c7ab a972 e152  .........o...r.R
    0x0020:  8018 00f7 1010 0000 0101 080a 4a8a 9875  ............J..u
    0x0030:  fdb5 61a7 b2e4 34da 446a 324e dfc2 d29e  ..a...4.Dj2N....
    0x0040:  b048 a3f2 b195 a741 5e0b 2550 933e f906  .H.....A^.%P.>..
    0x0050:  6902 f8f6 bc5f 9f51 86d9 8535 c284 aac8  i...._.Q...5....
    0x0060:  36e8 9ec5                                6...
```

After protocol exchanges, data packets are encrypted

`ssh` tunneling

Local port forwarding:

```
ssh -L 8080:www.server.org:80 <host>
```

Remote port forwarding:

```
ssh -R 5900:localhost:5900 guest@walter-pc
```

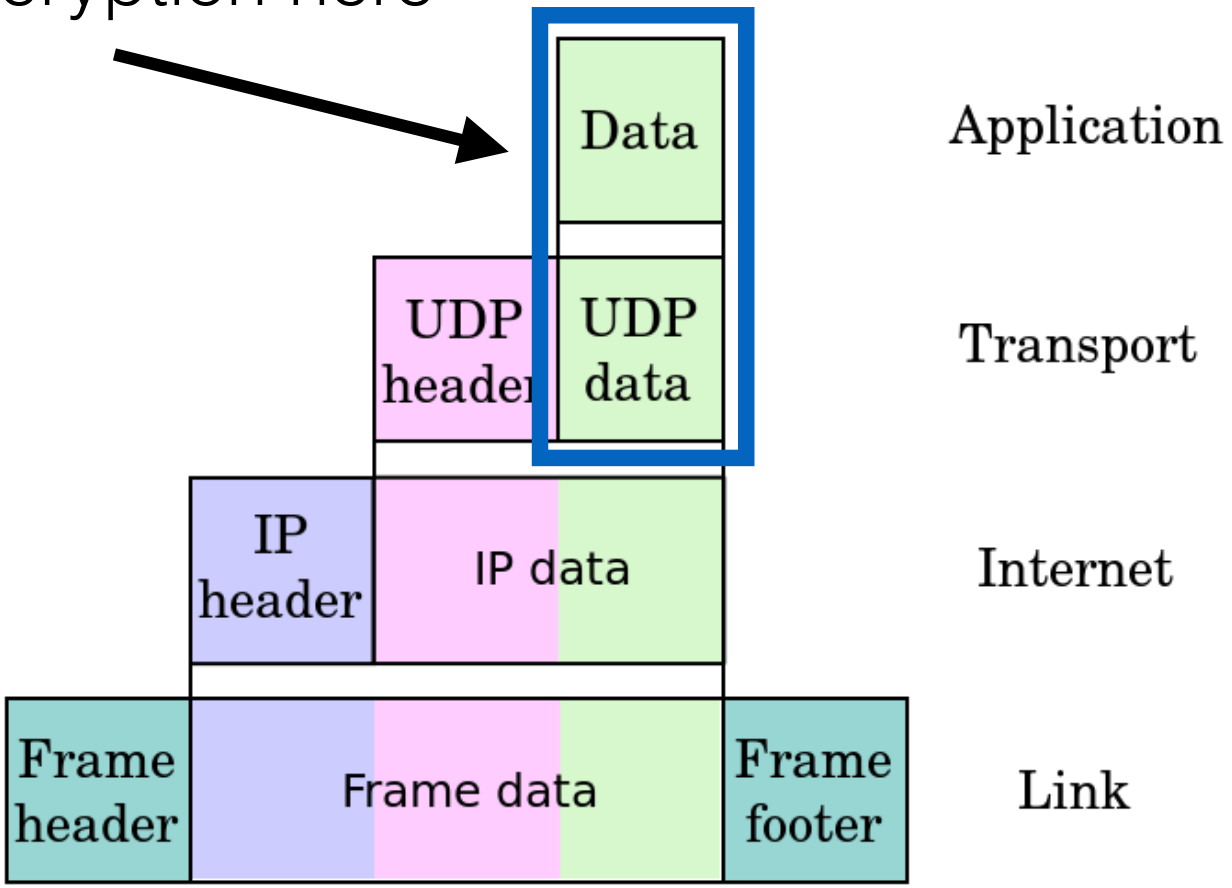
Pros: Secure connect through a firewall to use SMTP, IMAP and WWW services

Cons: Internal users can open internal services up to the world

https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding

Application Layer Encryption

Apply encryption here



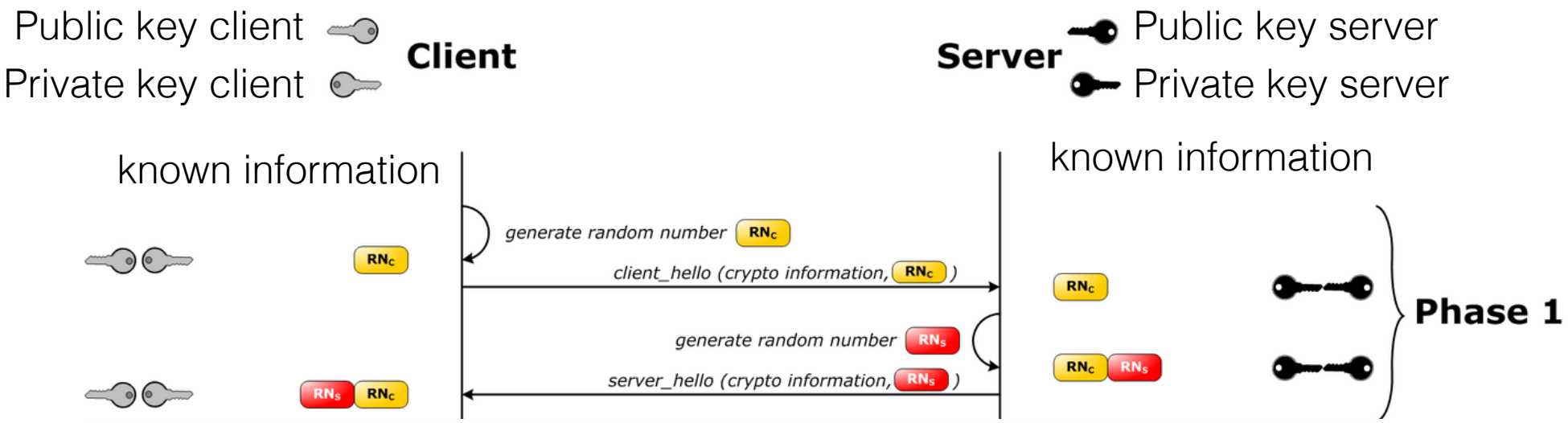
Secure Socket Layer (SSL)

Two purposes of this protocol:

1. Provide a confidentiality pipe between a browser and a web server
2. Authenticate the server, and possibly the client

Combines several cryptographic facets we discussed in Unit 2

SSL Handshake with Certs.

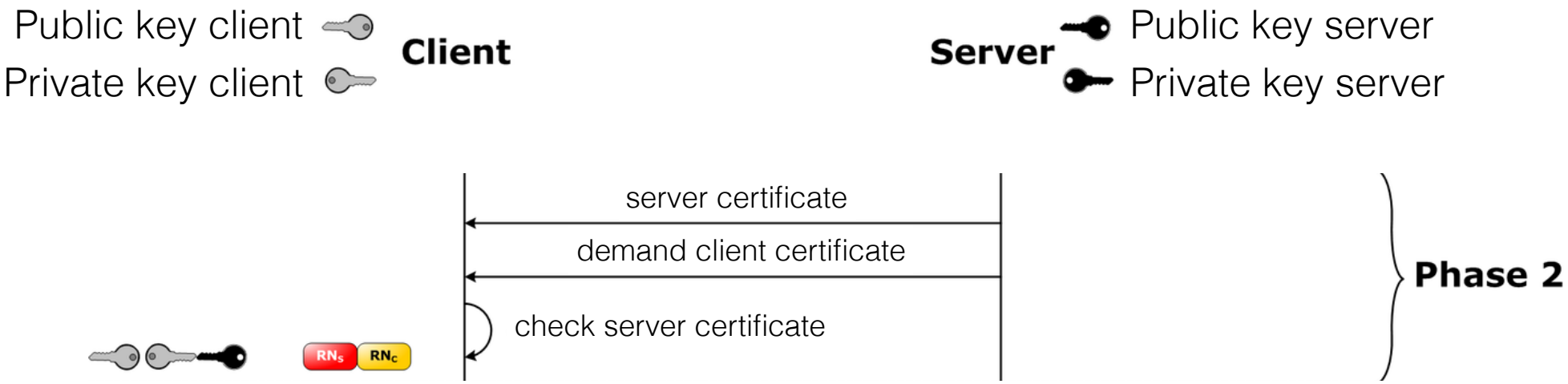


Schematic representation of the SSL handshake protocol with two way authentication with certificates.

RN_C = Random number from client

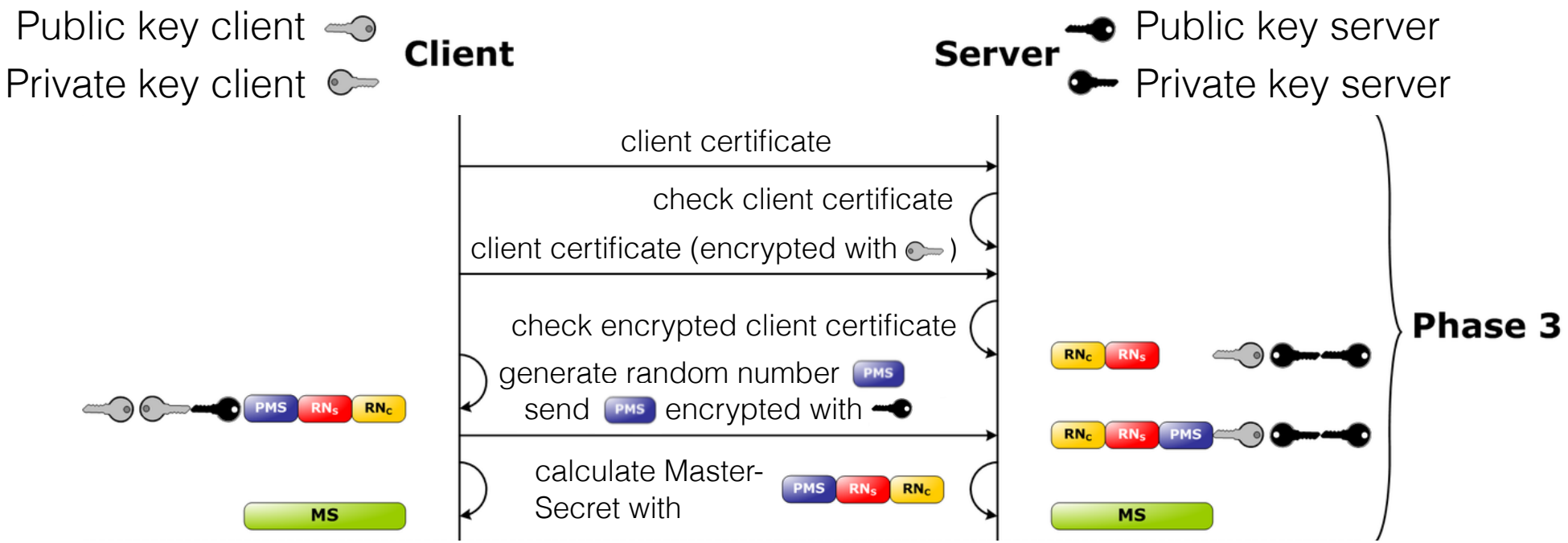
RN_S = Random number from server

SSL Handshake with Certs.



Schematic representation of the SSL handshake protocol with two way authentication with certificates.

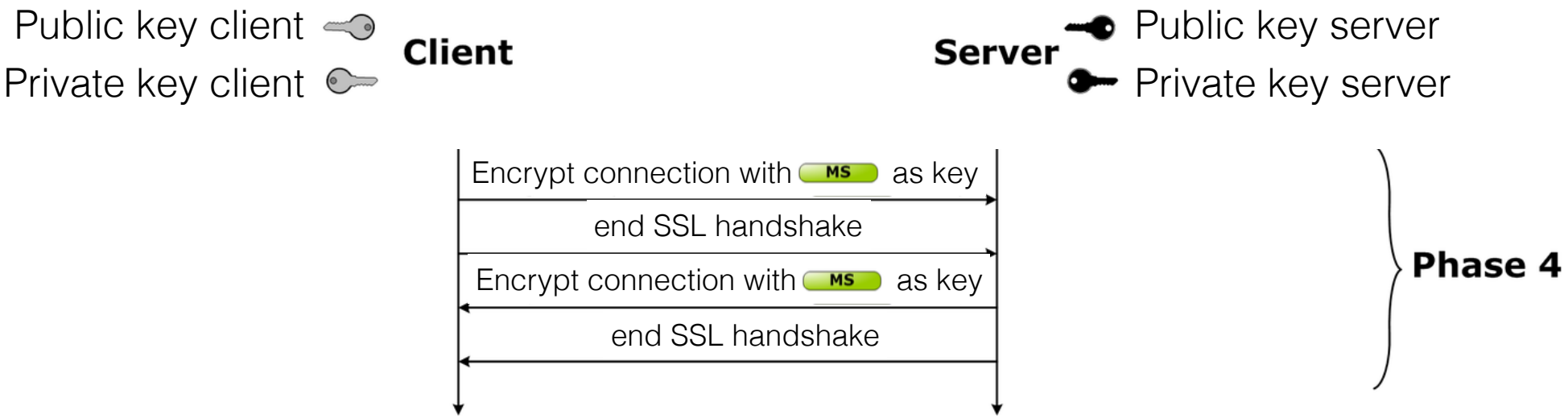
SSL Handshake with Certs.



Schematic representation of the SSL handshake protocol with two way authentication with certificates.

PMS = Pre-Master-Secret MS = Master-Secret

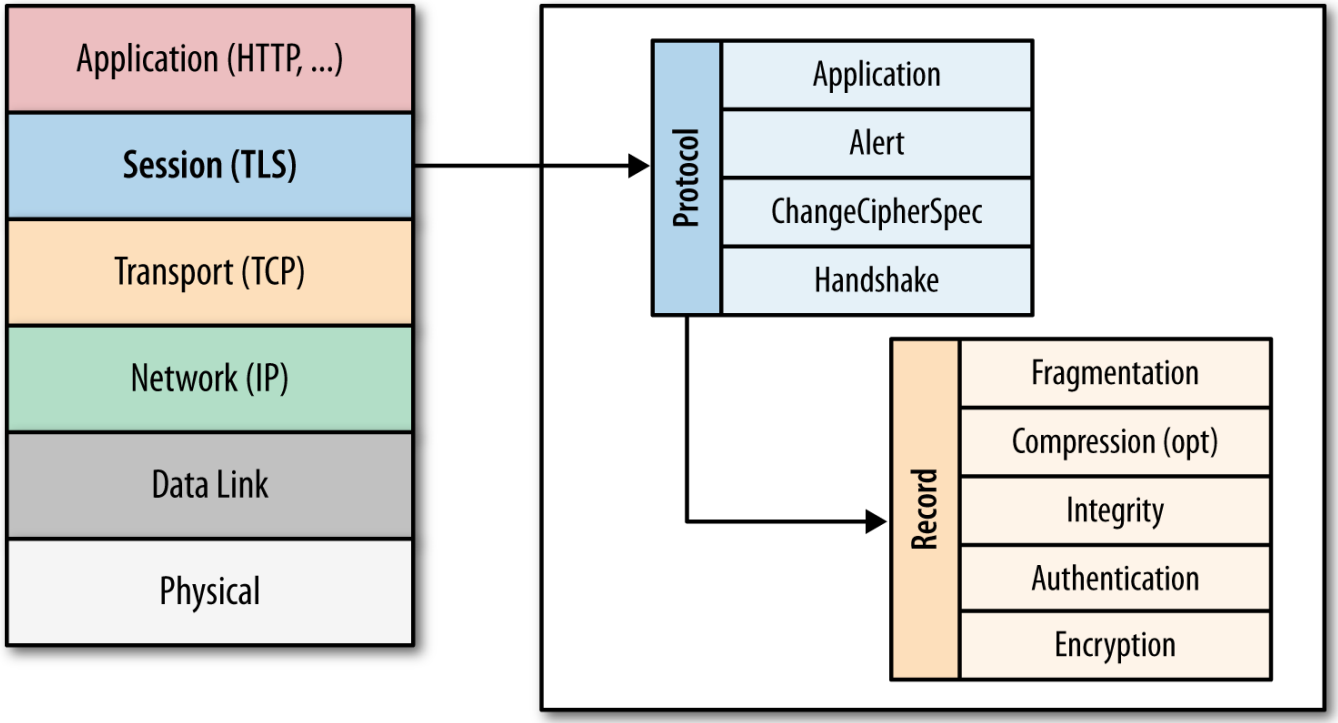
SSL Handshake with Certs.



Schematic representation of the SSL handshake protocol with two way authentication with certificates.

Transport Layer Security (TLS)

- Successor to SSL
- If you need application-specific encryption, use version 1.2 or newer



TLS 1.2 enhancements

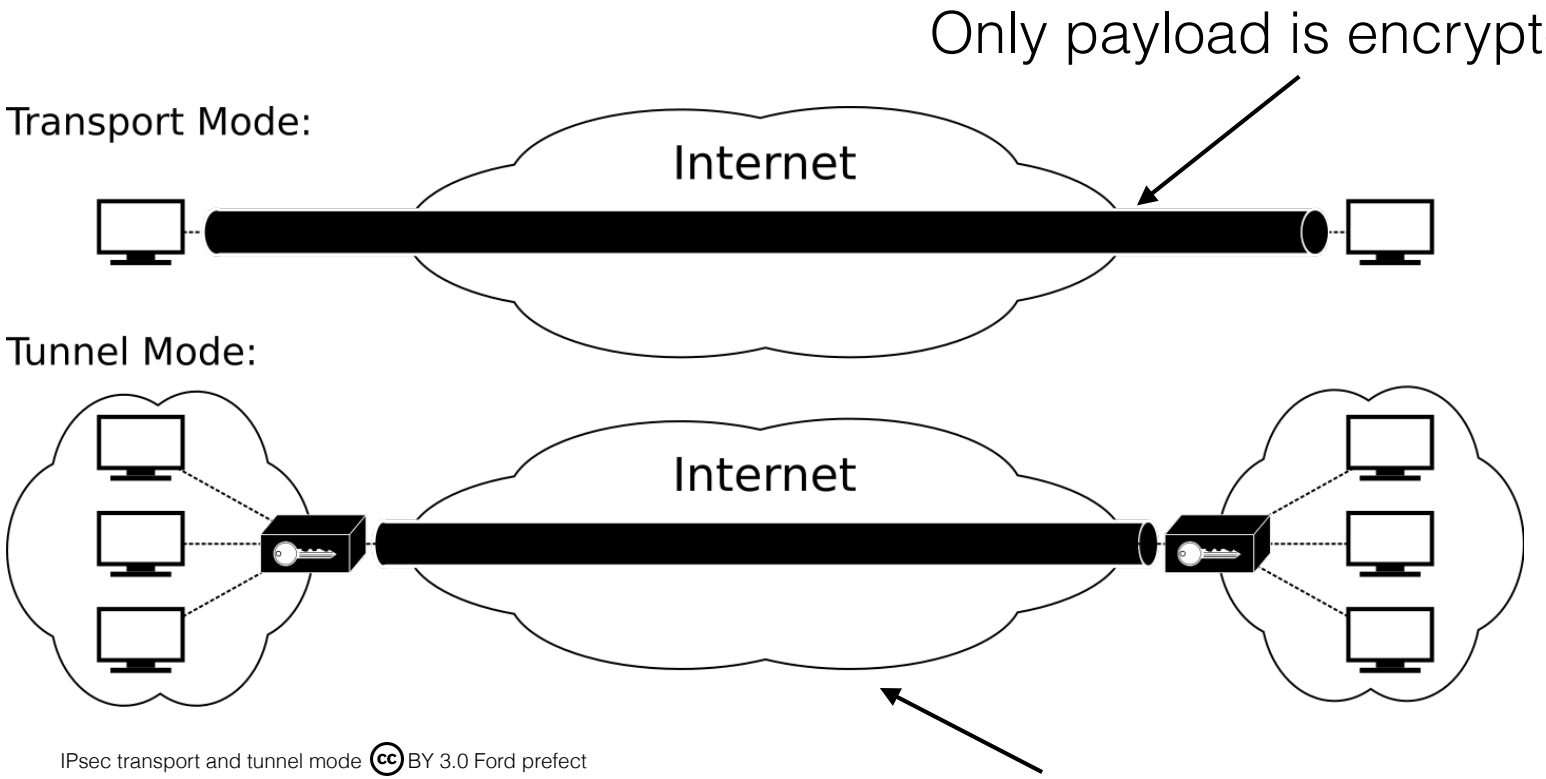
RFC 5246

- The MD5-SHA-1 combination in the pseudorandom function (PRF) replaced with SHA-256, with an option to use cipher suite specified PRFs.
- The MD5-SHA-1 combination in the finished message hash replaced with SHA-256, with an option to use cipher suite specific hash algorithms.
- The MD5-SHA-1 combination in the digitally signed element replaced with a single hash negotiated during handshake, which defaults to SHA-1.
- Enhancement in the client's and server's ability to specify which hash and signature algorithms they will accept.
- Expansion of support for authenticated encryption ciphers, used mainly for Galois/Counter Mode (GCM) and CCM mode of Advanced Encryption Standard encryption.
- TLS Extensions definition and AES cipher suites were added.

IPSEC

General network-layer encryption

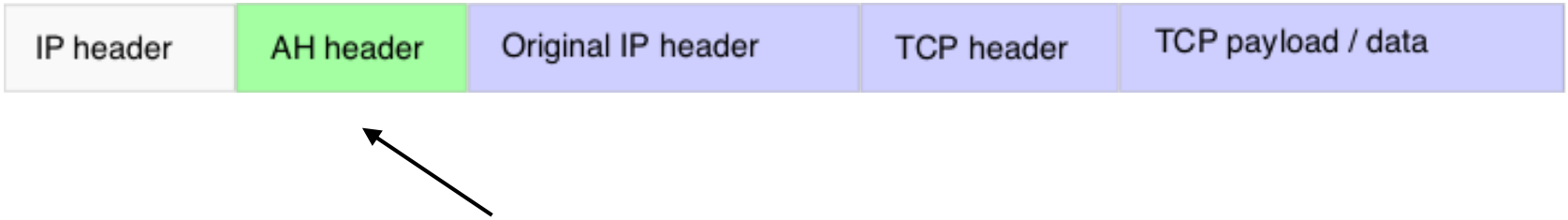
- Encrypts each IP packet of the session



IPsec transport and tunnel mode CC BY 3.0 Ford prefect

Authentication Headers

- Guarantees connectionless integrity and data origin authentication of IP packets
- Protects against replay attacks
- Operates directly on top of IP, using IP protocol 51

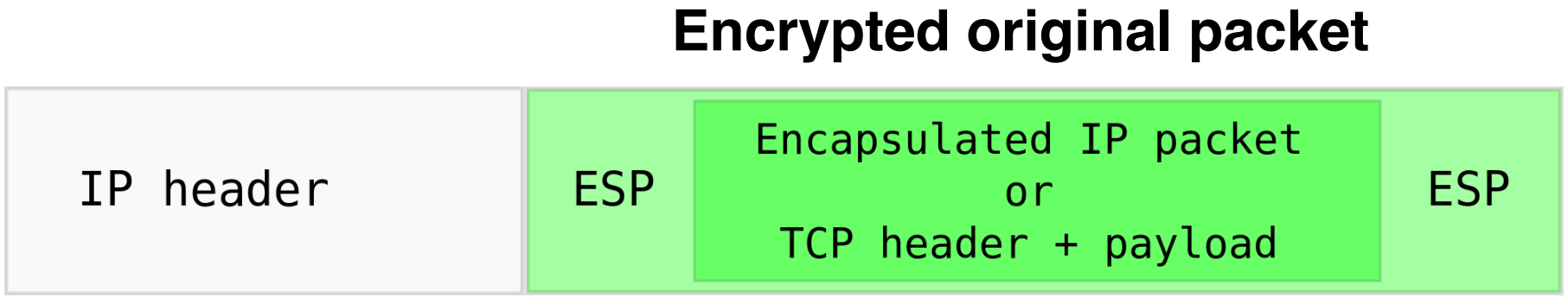


Protects payload and all non-mutable IP header fields

Encapsulating Security Payloads

Tunnel Mode: Entire IP Packet is encapsulated in a new IP packet

Should be used in conjunction with authentication header



Security Associations (SA)

Establishment of shared security attributes between two network entities