Computer Networks
Homework #11

January 18th 2018

Alessio Silvestro
Alessi.Silvestro@gmail.com

Exercise Exam + Q&A

- Exercise exam
  - Available in wiki
  - Intended for self-study; there will be no answer sheet or exercise session
- Question and Answer Session
  - **January 25th 2018**
  - Entirely for your benefit!
  - If there are no questions, there will be no answers
  - If you want a well prepared answer, please send us an email in advance

Quick Review

- https://www.youtube.com/watch?v=Rgz6Fa23gis

1 -- NetSec

- What are the security concerns network security is targeting at? What main areas of protection does network security cover?

1 -- NetSec

- Confidentiality: only sender, intended receiver should “understand” message contents
- Authentication: sender, receiver want to confirm identity of each other
- Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- Access and availability: services must be accessible and available to users

2 -- Cryptography

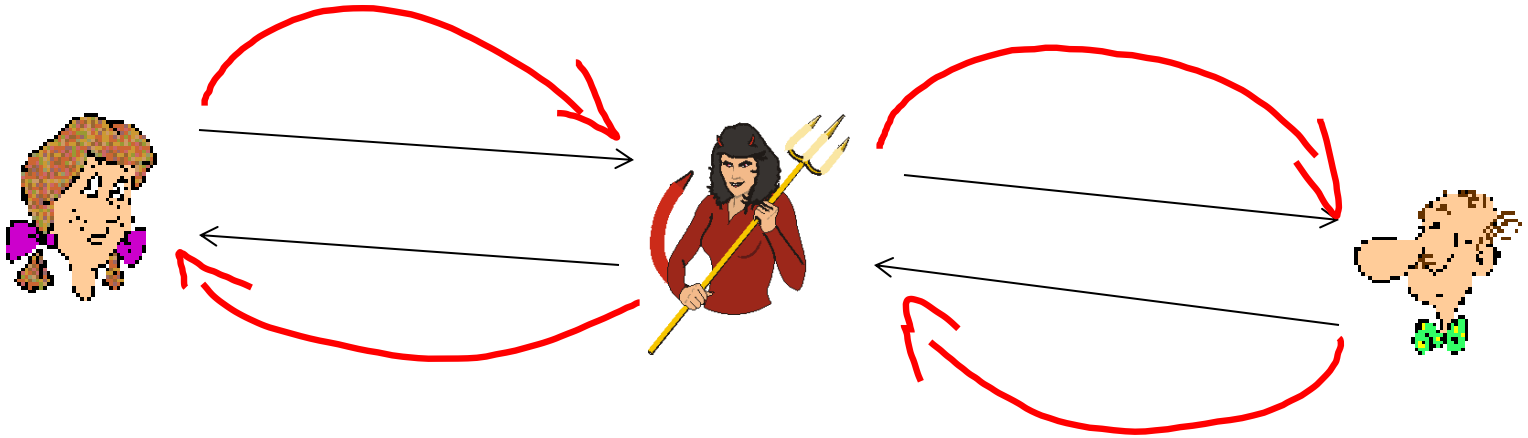
- What are the two main types of cryptography regarding Keys' type?

- Symmetric crypto (encryption + decryption with the same key): DES, 3DES, AES etc.

- Asymmetric crypto (enc and dec with different keys): RSA, Public/Private keying, Diffie-Hellman

3 -- Authentication

- What is a man-in-the-middle attack? Is public key cryptography save against that type of attack?



- Asymmetric keying only helpful if public keys are pre-known or certificate bound.

4 -- Authentication

- What other tricks does attackers use to overcome authentication protection? Please explain using the AP protocols presented in the lecture.

- AP 1.0/2.0 Just faking IDs (“I am Alice”) or spoofing an IP address
- Often record and playback attacks as in AP 3.0/3.1

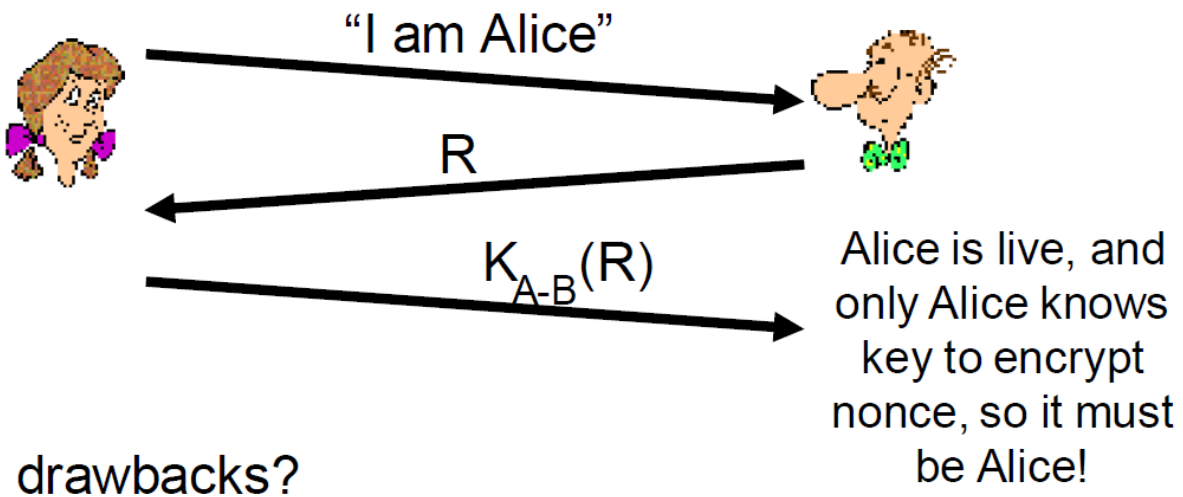
5 -- Nonces

- What is the purpose of a nonce in an end-point authentication protocol?

Goal: avoid playback attack

Nonce: number (R) used only *once –in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice a nonce, R. Alice must return R, encrypted with shared secret key



Failures, drawbacks?

6 -- Hashes

- What is the conceptual difference between a crypto-hash function and other hash functions?
  - computationally infeasible to find two different messages, x, y such that H(x) = H(y)
    - equivalently: given m = H(x), (x unknown), can not determine x.

- SHA-1, MD5 operate without a shared secret
- Additionally, key based Hash-based MACs (HMACs) HMAC-MD5 or HMAC-SHA1 available e.g. for signatures

RSA

- Perform an RSA encryption and decryption with p=7 and q=11 with the word “Telematics”.

n=7*11=77 (prime factors 7, 11)
z=(7-1)(11-1)=60 (prime factors 2, 2, 3, 5)

e needs to be chosen in a way, that it has no common prime factors with z
e=7
now we search for a d with e * d – 1 mod z = 0. With d=43 we have
e*d-1 mod 60 = 300 mod 60 = 5

RSA

m < n (m can be very large!)

$PK = \{e, n\}$

$SK = \{d, n\}$ Privat

Klartext		m^e	chiffre=m^e mod n	c^d (here: chiffre ^46)	c^d mod n
a	1	1	1	1	1
b	2	128	51		
c	3	2187	31	1344475321277696301917412237399743818544020030012023011387352099 1	3
d	4	16384	60		
E	5	78125	47	7947085605523083625070262146550831406598802055593810164316736335605742 23	5
F	6	279936	41		
G	7	823543	28		
H	8	2097152	57		
i	9	4782969	37	2708158850659810604098295389625874965383133440950608643326294433145 3	9
j	10	10000000	10		
k	11	19487171	11		
l	12	35831808	12	2539765269450581386607001599065993634741275852 8	12
m	13	62748517	62	1182612999202160343235671583248811577226183550007414235281021512431913171681 28	13
n	14	105413504	42		
o	15	170859375	71		
p	16	268435456	58		
q	17	410338673	52		
r	18	612220032	39		
s	19	893871739	68	6278895373298528368344913294912019325279912443533041880115104685557599470354432	19
t	20	1280000000	48	1965048198399560713177500537391830916254451560885426333004585474449211392	20
u	21	1801088541	21		
v	22	2494357888	22		
w	23	3404825447	23		
x	24	4586471424	73		
y	25	6103515625	53		
z	26	8031810176	5		

Telematics = 48 47 12 47 62 01 48 37 68

We are encrypting letter by letter, remember cipher algos and consider large m!

computer NETWORKS

7 – Authenticate Big Messages

1. Alice: $M_C = K^-_A(M)$ → Bob: $K^+_A(M_C)$
2. Alice: $[M_C = K^-_A(H(M))] + M$ → Bob: $K^+_A(M_C)$ and $H(M)$

8 – Secure Big Messages

1. Alice: $M_C = K^+_B(M)$ → Bob: $K^-_B(M_C)$
2. Efficient Way
   1. Share a symmetric key (K_S) using public key:

      Alice: $K^+_B(K_S)$ → Bob: $K^-_B(K_S)$
   2. Send big message using shared symmetric K_S

      Alice: $M_C = K_S(M)$ → Bob: $K_S(M_C)$

Thank you

Any questions?