Telematics
Homework #11

Florian Tegeler

27 January 2011

Announcements

- Final exam: Thursday 10.02.2011
  - 10:00 -12:00 : GZG - MN08
- Language: English + German, answers possible in both languages

- No additional resources (calculator etc.) allowed. Just bring pens ;).

- Register with FlexNow till 3rd of February!

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
  - **3 February 2011, 10:15h**
  - 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

NetSec

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

Confidentiality

Authentication

Message integrity

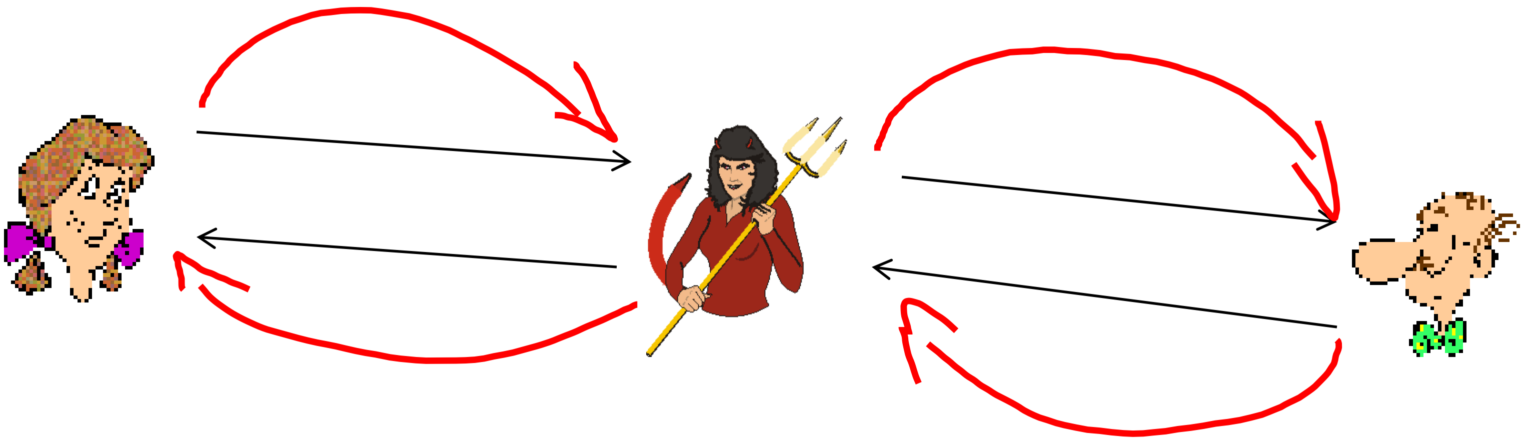
Access and availability

Cryptopgraphy

- What are the two main types of cryptography?
- 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

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.

Authentication

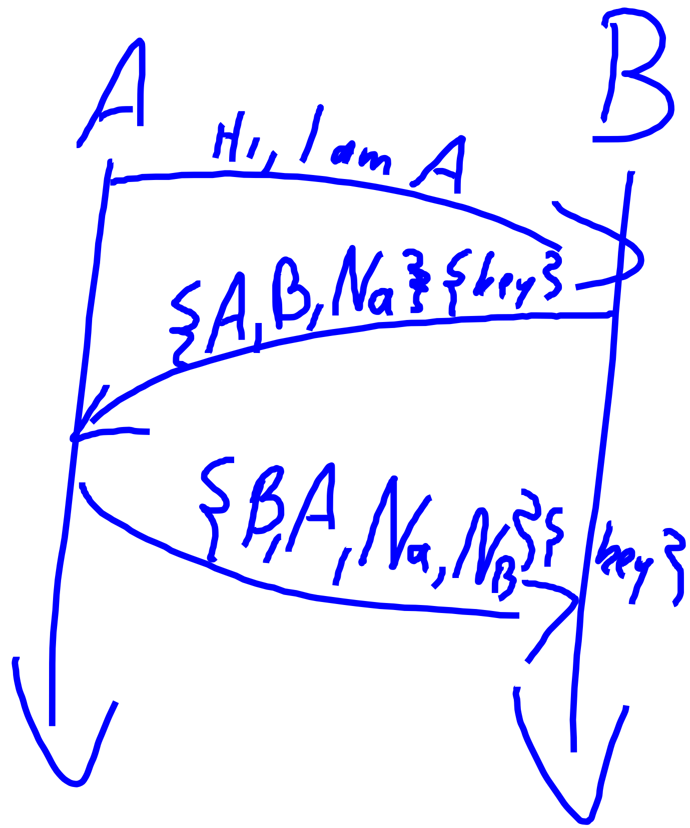
- What other tricks does attackers use to overcome authentication protection? Please explain using the AP protocols presented in the lecture.

- 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

Nonces

- What is the purpose of a nonce in an end-point authentication protocol?
  - Brings freshness
  - Prevents replay attacks
  - Example:

{X}{key}



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}

Privat SK = {d, n}

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	13444753212776963019174122373997438185440200300120230113873520991	3
d	4	16384	60		
E	5	78125	47	794708560552308362507026214655083140659880205559381016431673633560574223	5
F	6	279936	41		
G	7	823543	28		
H	8	2097152	57		
i	9	4782969	37	27081588506598106040982953896258749653831334409506086433262944331453	9
j	10	10000000	10		
k	11	19487171	11		
l	12	35831808	12	25397652694505813866070015990659936347412758528	12
m	13	62748517	62	118261299920216034323567158324881157722618355000741423528102151243191317168128	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!

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

Thank you

Any questions?