Computer Networks - Exercise 11

Stephan Sigg

Georg-August-University Goettingen, Computer Networks

23.01.2014

11.1

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

11.1

Confidentiality only sender, intended receiver should *understand* message contents

- sender encrypts message
- receiver decrypts message

Authentication sender and receiver should be able to confirm identity of each other

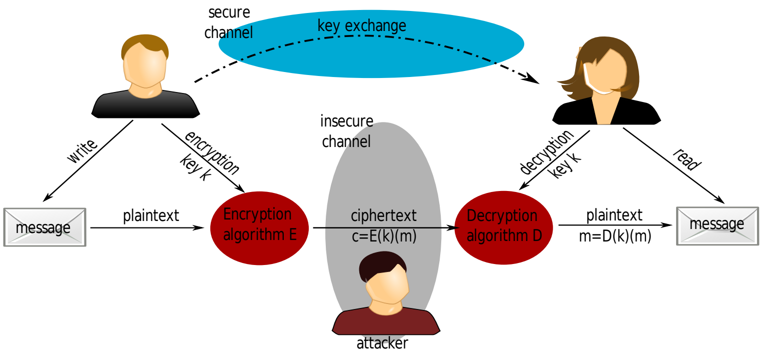
Message integrity message should not be altered (in transit, or afterwards) without detection

Access and availability services must be accessible and available to users

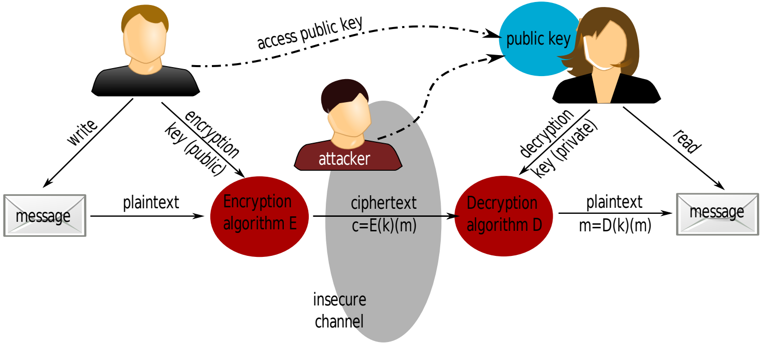
11.2

- What are pro's and con's for public vs. private key crypographic systems in computer networks?

11.2 – Symmetric encryption



11.2 – Asymmetric encryption



11.3

- RSA public key cryptography: Let p=3 and q=11. Use appropriate values for e and d and encrypt the value '3'

11.3 – RSA public key cryptography

Example

RSA key generation

1. Select two large random prime numbers p and q
2. Compute $n = p \cdot q$
3. Compute $\theta(n) = (p - 1) \cdot (q - 1)$
4. Select small odd integer e that is relatively prime to $\theta(n)$

11.3 – RSA public key cryptography

Example

RSA key generation

5. Compute d as the multiplicative inverse of $e \mod \theta(n)$
6. Publish $P = (e, n)$ as the RSA public key
7. Keep the secret pair $S = (d, n)$ as the RSA secret key

11.3 – RSA public key cryptography

Example

RSA key generation

8. Encrypt a message M
   - $C = M^e \mod n$
9. Decrypt a message C
   - $M = C^d \mod n$

11.3 – RSA public key cryptography

RSA key generation – example

- Select two prime numbers p and q
  - $p = 3; q = 11$
- Compute $n = p \cdot q$
  - $n = 33$
- Compute $\theta(n) = (p-1) \cdot (q-1)$
  - $\theta(n) = 20$

11.3 – RSA public key cryptography

RSA key generation – example

$p = 3; q = 11; n = 33; \theta(n) = 20$

- Select a small odd integer e that is relatively prime to $\theta(n)$
  - $e = 3$
- Compute d as the multiplicative inverse of $e \mod \theta(n)$
  - $d = 7$
  - Test: $3 \cdot 7 \mod 20 = 21 \mod 20 = 1$

11.3 – RSA public key cryptography

RSA key generation – example

$p = 3; q = 11; n = 33; \theta(n) = 20; e = 3; d = 7$

- Publish $P = (e, n)$ as the public key
  - Key pair: $(3, 33)$
- Keep $S = (d, n)$ as the RSA secret key
  - Secret key pair: $(7, 33)$

11.3 – RSA public key cryptography

RSA key generation – example

$p = 3; q = 11; n = 33; \theta(n) = 20; e = 3; d = 7$

$P = (3, 33)$

$S = (7, 33)$

- Encrypt the message '3':
  - $C = M^e \mod n$
  - $C = 3^3 \mod 33 = 27 \mod 33 = 27$

11.3 – RSA public key cryptography

RSA key generation – example

$p = 3; q = 11; n = 33; \theta(n) = 20; e = 3; d = 7$

$P = (3, 33)$

$S = (7, 33)$

- Decrypt the message $C = 27$:
  - $M = C^d \mod n$
  - $$\begin{aligned} M &= 27^7 \mod 33 \\ &= 10460353203 \mod 33 \\ &= 3 \end{aligned}$$

11.4

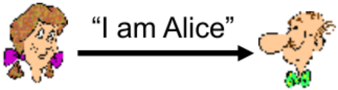
- What other tricks might attackers use to overcome authentication protection?
- Please explain using the AP protocols presented in the lecture.

11.4

Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"



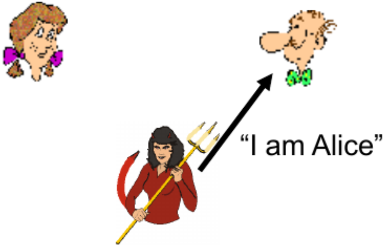
Failure scenario??

11.4

Authentication

Goal: Bob wants Alice to “prove” her identity to him

Protocol ap1.0: Alice says “I am Alice”



in a network,
Bob can not “see” Alice,
so Trudy simply
declares
herself to be Alice

11.4

Authentication: another try

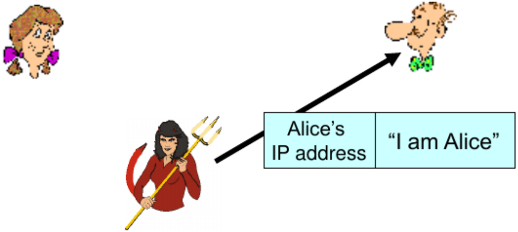
Protocol ap2.0: Alice says “I am Alice” in an IP packet containing her source IP address

Failure scenario??

11.4

Authentication: another try

Protocol ap2.0: Alice says “I am Alice” in an IP packet containing her source IP address

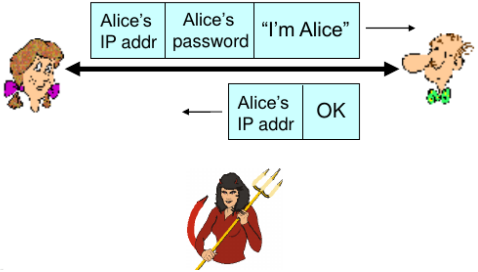


Trudy can create a packet “spoofing” Alice’s address

11.4

Authentication: another try

Protocol ap3.0: Alice says “I am Alice” and sends her secret password to “prove” it.

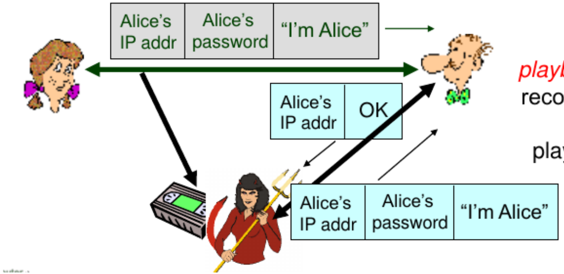


Failure scenario??

11.4

Authentication: another try

Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.

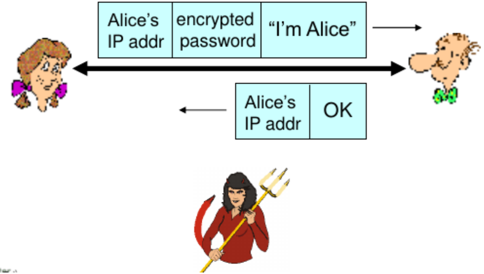


playback attack: Trudy records Alice's packet and later plays it back to Bob

11.4

Authentication: yet another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.

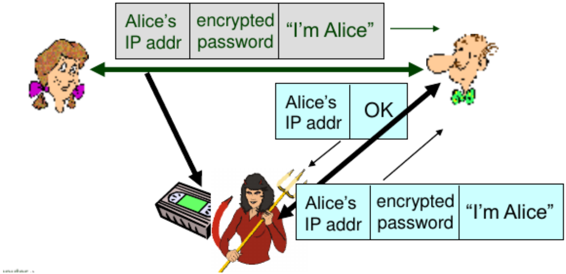


Failure scenario??

11.4

Authentication: another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



record and playback still works!

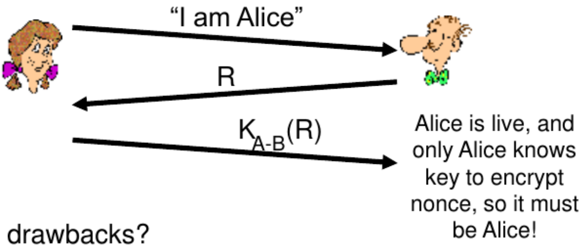
11.4

Authentication: yet another try

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?

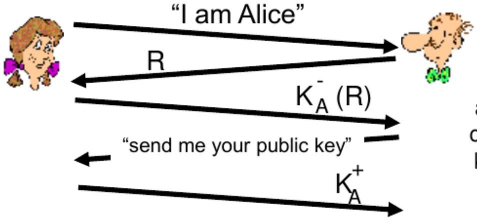
11.4

Authentication: ap5.0

ap4.0 requires shared symmetric key

- can we authenticate using public key techniques?

ap5.0: use nonce, public key cryptography

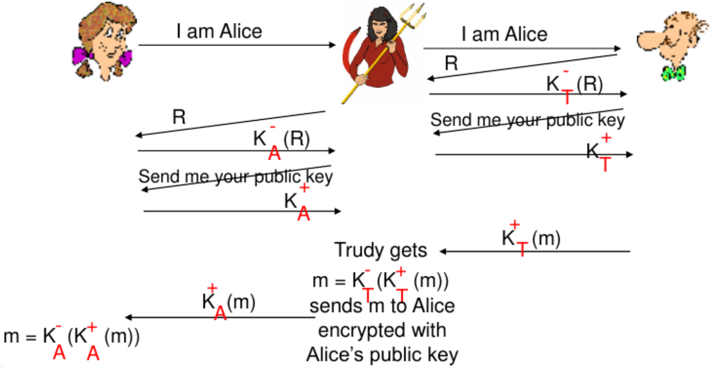


Bob computes
$K_A^+(K_A^-(R)) = R$
and knows only Alice could have the private key, that encrypted R such that
$K_A^+(K_A^-(R)) = R$

11.4

ap5.0: security hole

Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



11.4

ap5.0: security hole

Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)

Difficult to detect:

- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation)
- problem is that Trudy receives all messages as well!

11.4

AP 1.0/2.0 Just faking IDs ("I am Alice") or spoofing an IP address

AP 3.0/3.1 Often record and playback attacks

AP 5.0 Man-in-the-middle attack

11.5

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

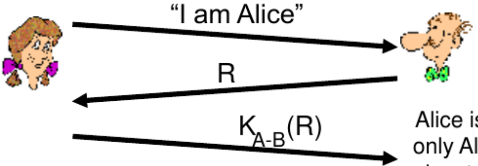
11.4

Authentication: yet another try

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



Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

Failures, drawbacks?

11.5

- Brings freshness
- Prevents replay attacks