Lecture 3

Tuesday, 22 November 2022 12:31

PKI → (for solving) key exchange problem

↳ symmetric crypto : how to transport keys ?

for n people, one key per pair

↓

$\frac{n(n-1)}{2} = O(n^2)$ keys

↓

not scalable

↓

solutions:

1. key server — must be trusted ..., available (single point of failure) — key server is main the middle

   but this model is used in mobile telecom

2. public key crypto — public key server (availability solved, but main in the middle still possible)

   ↓

   authentication still a problem (key ownership)

   performance may be an issue

   not everyone's key may be on the server

   key validity → should not be infinite, since compromise becomes more likely over time ...

hybrid encryption → Encrypt symmetric key with asymmetric cryptography

signing has similar key exchange problems

but might be less sensitive to key availability issues

PKI used for web security

↓

authenticity, validity

binding between identity and public key

↑ asserted by CA (signature)

↑ subjects

X.509

PGP

validity → lifetime

↓

should be revocable → either binding between

key and subject

attributes and subject

↓

CRL + OCSP