Authentication: Part 5

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

NPTEL

References

- J. Kurose, K. Ross, “*Computer Networking: A Top Down Approach*”, Sixth Edition, Pearson Education, 2013
- C. Kaufman, R. Perlman, M. Speciner, “*Network Security: Private Communication in a Public World*”, Pearson Education, 2nd edition, 2002

NPTEL

Authentication Using a Key Distribution Center (KDC)

NPTEL

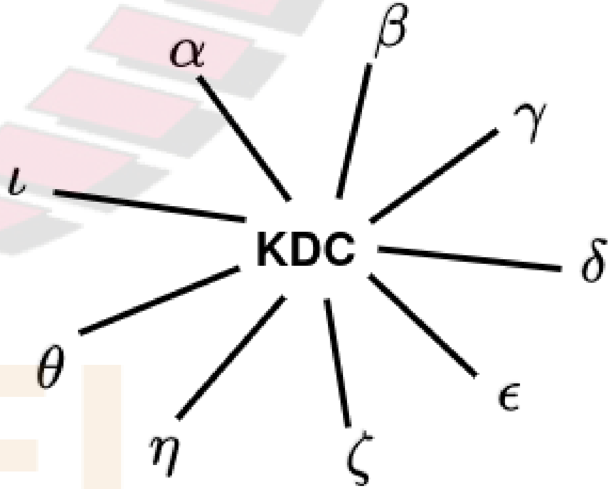
Establishing Shared Symmetric Keys

- Suppose two network nodes, Alice and Bob, want to securely communicate over a network
- Recall: they need to first agree on a shared secret key K_{AB}
- One way: public key cryptography
- However, this requires public key infrastructure
- Now, assume that public key infrastructure is not available
- Want a mechanism using which any two nodes in a network can agree on a shared secret key
- One way is to use a trusted node called Key Distribution Center (KDC)

NPTEL

Key Distribution Center (KDC)

- Whenever a new node is installed in the network:
  - ❑ that node and the KDC are configured (e.g., manually, via post) with a shared secret key
- If node α wants to talk to node β:
  - ❑ α connects with KDC and asks for a key with which to talk to β
  - ❑ KDC authenticates α, chooses a random number, say $R_{\alpha\beta}$, and sends $R_{\alpha\beta}$ after encrypting it to α
  - ❑ KDC also encrypts and sends $R_{\alpha\beta}$ to β, with the instruction that it is to be used for communicating with α
    - ○ Alternatively, KDC encrypts $R_{\alpha\beta}$ and gives it to α for forwarding to β
  - ❑ Now α and β have a shared secret key $R_{\alpha\beta}$; they mutually authenticate and then start exchanging data
- Above is an outline with some details omitted; we will later discuss, in detail, protocols for KDC-mediated authentication



NPTEL

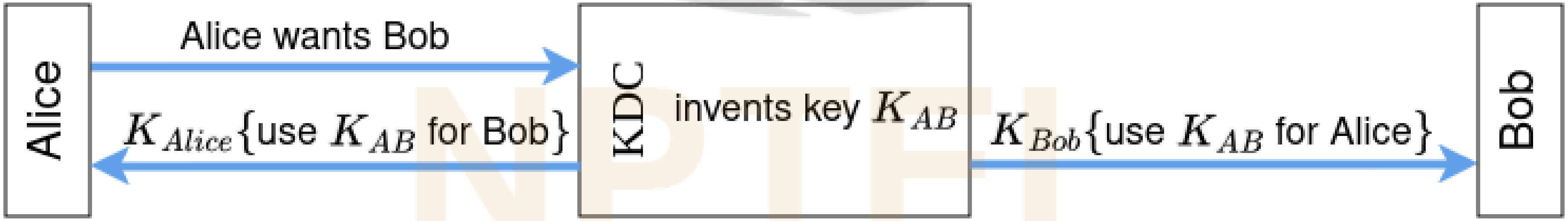
Advantages and Disadvantages of KDC

- Advantages:
  - ❑ When a new user is being installed into network, or a user’s key is compromised and needs to be changed, there is a single location (KDC) that needs to be configured
    - o Alternative: install the user’s information at every server to which the user might need access (difficult)
- Disadvantages:
  - ❑ If KDC is compromised, all network resources are vulnerable
  - ❑ Single point of failure: if KDC fails (e.g., crashes), no new communication can be initiated, although keys previously distributed can continue to be used
  - ❑ KDC can be a performance bottleneck, since all network nodes frequently need to communicate with it
- Alternative that overcomes second and third of above disadvantages:
  - ❑ have multiple KDCs, which share same database of keys
- Disadvantages:
  - ❑ all copies of KDC need to be protected
  - ❑ additional cost and complexity; need for replication protocols

NPTEL

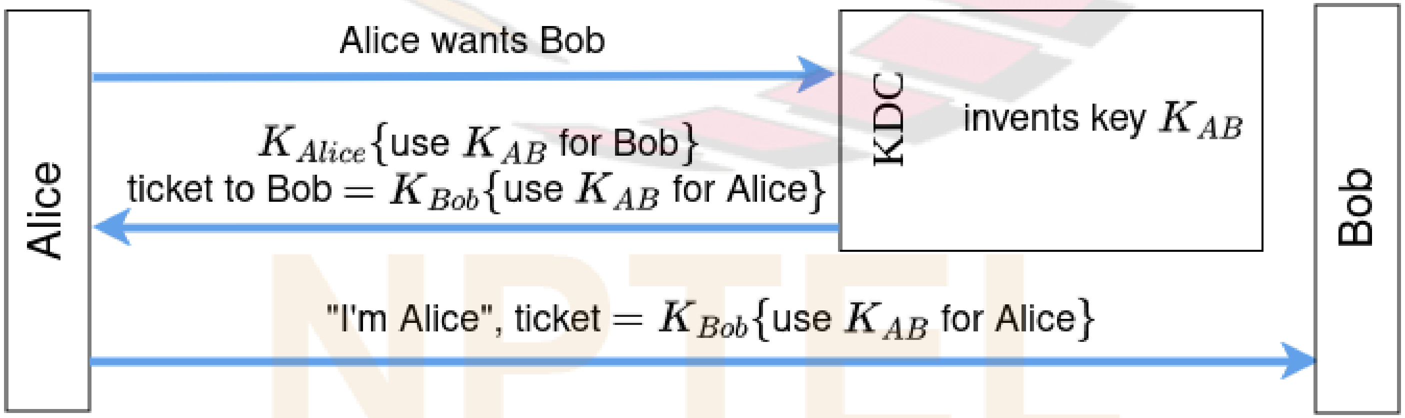
Mediated Authentication Using KDC

- Consider a network in which each user has a secret shared key with a KDC
- When Alice wants to communicate with Bob, protocol shown in fig. can be used
- Shortcoming of this protocol:
  - ❑increases load on KDC, since it needs to initiate connection with Bob and share K_{AB} with him
- Hence, instead, in message from KDC to Alice, a "*ticket*" is included, which Alice needs to send to Bob


Alice
Alice wants Bob
K_{Alice}\{use K_{AB} for Bob\}
KDC
invents key K_{AB}
K_{Bob}\{use K_{AB} for Alice\}
Bob

Mediated Authentication Using KDC (contd.)

- Fig shows revised protocol
- After protocol shown in fig., mutual authentication between Alice and Bob needs to be performed
- Can be performed:
  - ❑using one of the protocols we discussed for mutual authentication
- However, this protocol has some vulnerabilities, e.g.:
  - ❑Suppose an intruder, Trudy, stole Alice's key and also recorded msg. 2 when Alice contacted KDC to talk to Bob; later, Alice changed her key; but Trudy can still use the old key and recorded msg. 2 to impersonate herself as Alice to Bob
- We will discuss improved protocols


Alice
Alice wants Bob
KDC
invents key K_{AB}
K_{Alice}\{use K_{AB} for Bob\}
ticket to Bob = K_{Bob}\{use K_{AB} for Alice\}
"I'm Alice", ticket = K_{Bob}\{use K_{AB} for Alice\}
Bob