Kerberos

with comments on WEP

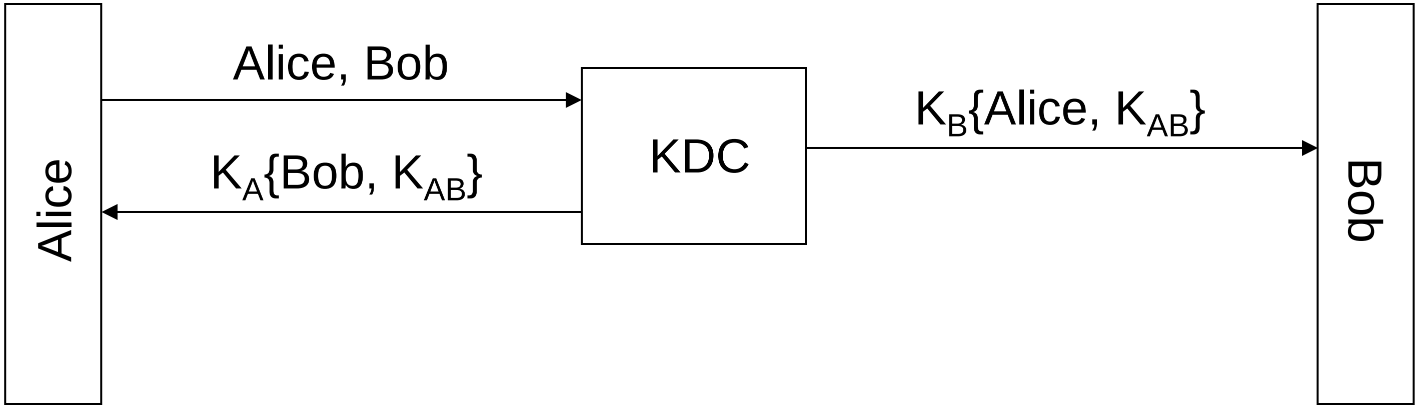
BİL 448/548

Internet Security Protocols

Ali Aydın Selçuk

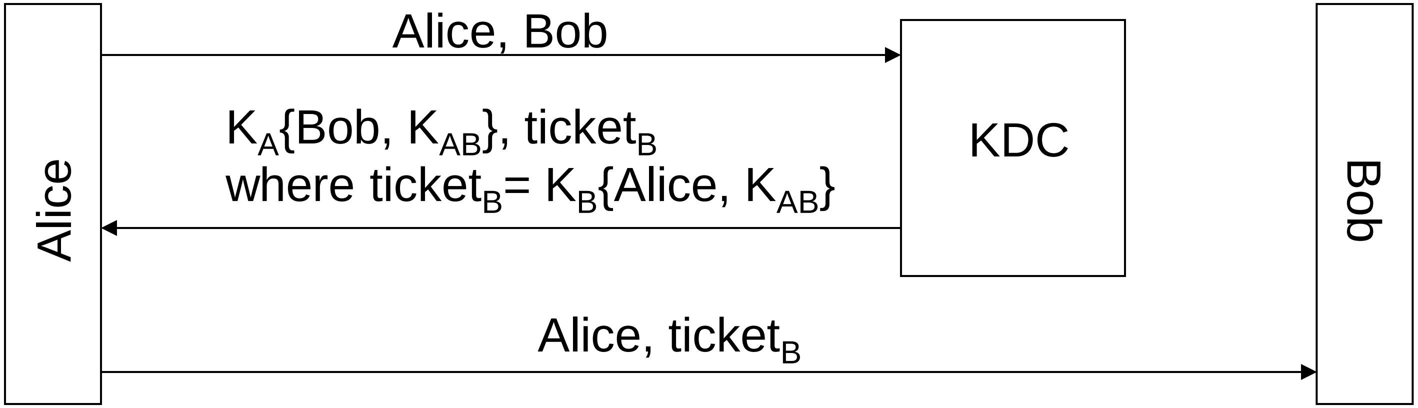
Key Establishment and Authentication with KDC

A simple protocol:



Problem: Potential delayed key delivery to Bob. (besides others)

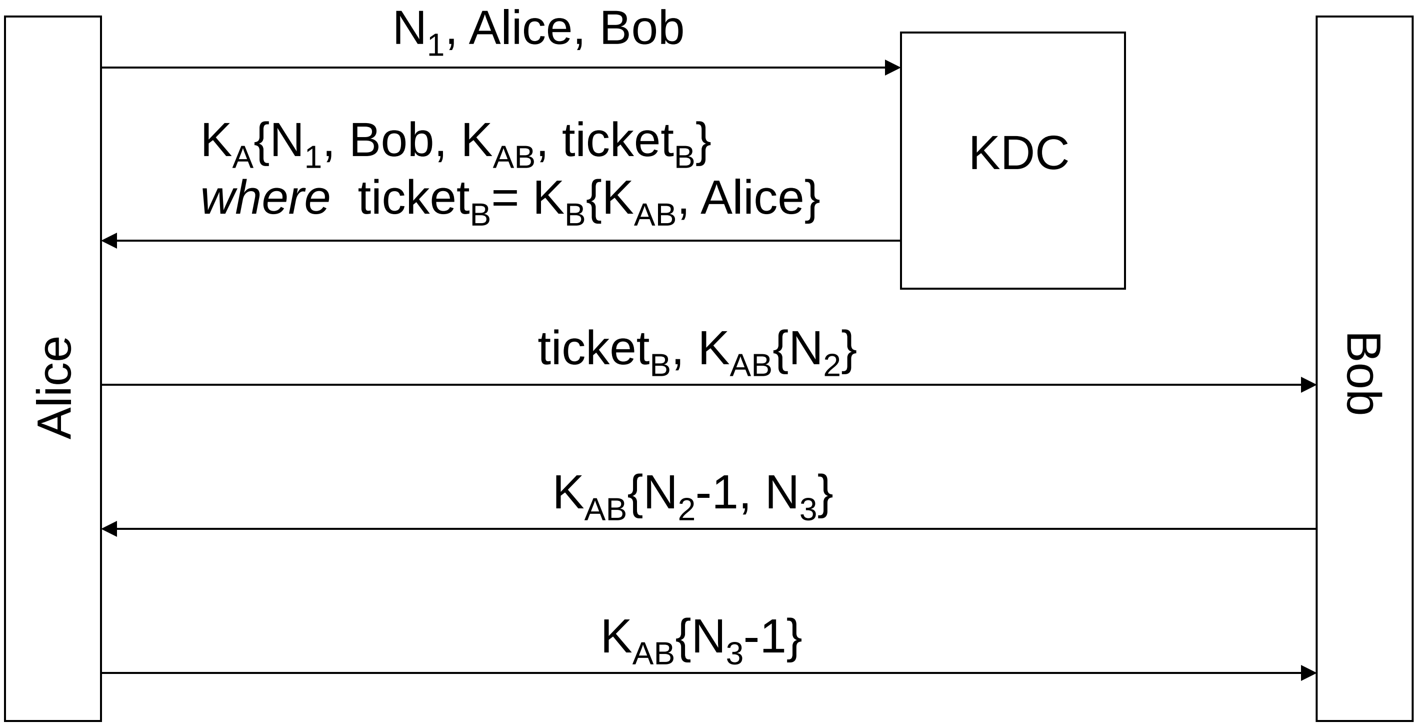
Another simple protocol:


Alice, Bob
K_A\{Bob, K_{AB}\}, ticket_B
where ticket_B= K_B\{Alice, K_{AB}\}
KDC
Alice
Bob
Alice, ticket_B

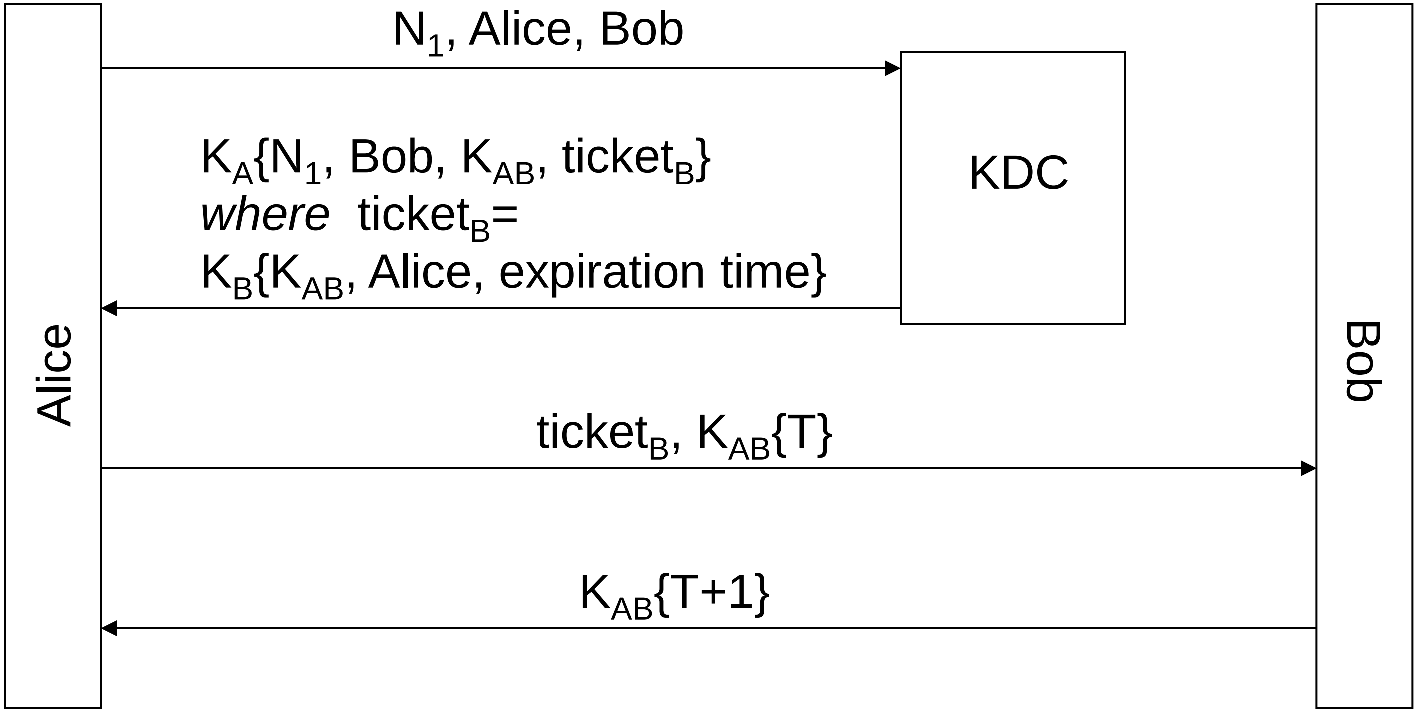
Problems:

- No freshness guarantee for K_{AB}
- Alice & Bob need to authenticate

Needham-Schroeder Protocol


N_1, Alice, Bob
KDC
$K_A\{N_1$, Bob, K_{AB}, $\text{ticket}_B\}$
where $\text{ticket}_B = K_B\{K_{AB}$, Alice$\}$
Alice
Bob
ticket_B, $K_{AB}\{N_2\}$
$K_{AB}\{N_2\text{-}1, N_3\}$
$K_{AB}\{N_3\text{-}1\}$

Basic Kerberos Protocol



Alice

KDC

Bob

N_1, Alice, Bob

$K_A\{N_1$, Bob, K_{AB}, $ticket_B\}$
where $ticket_B$=
$K_B\{K_{AB}$, Alice, expiration time$\}$

$ticket_B$, $K_{AB}\{T\}$

$K_{AB}\{T+1\}$

T: timestamp

Kerberos

- Cryptographic authentication for distributed systems.
- Designed as the security protocol of Project Athena at MIT in the ’80s.
- Supported widely in current systems: Linux, Windows, Mac OS X, FreeBSD, Oracle… for network authentication.

Kerberos

- Requirements:
  - Security, reliability, transparency, scalability

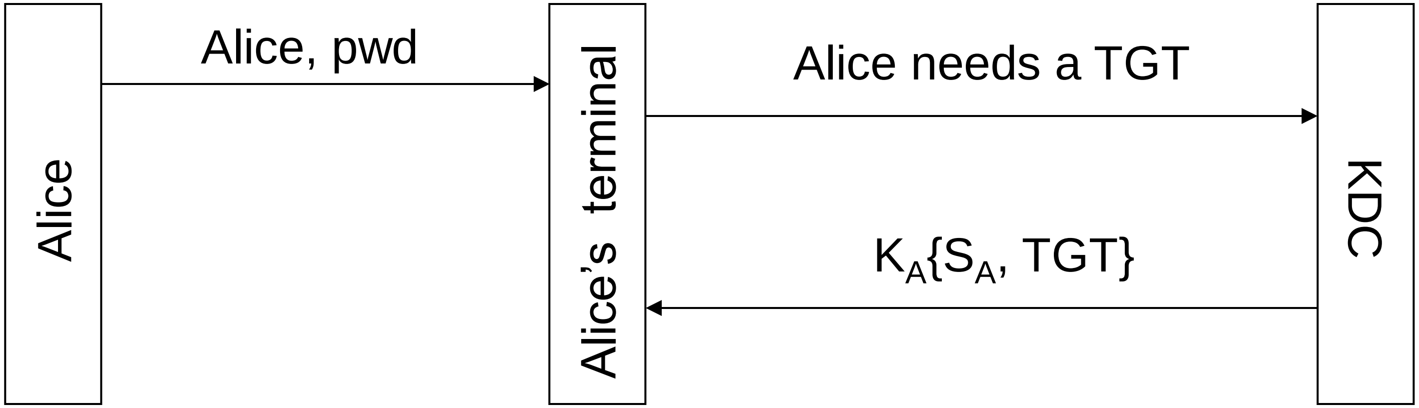
- Based on symmetric-key authentication with KDC

- Advantages:
  - secure authentication
  - single sign-on (!)
  - secure data flow

Kerberos Keys

- Each “principal” shares a “master key” with KDC
- K_A: Alice’s master key (pwd based for users). Used for initial authentication
- S_A: Alice’s session key. Created after initial authentication, used instead of K_A.
- K_{AB}: Alice-Bob session key.
- “Ticket Granting Tickets” (TGT):
  - issued to Alice by KDC after login
  - contains S_A encrypted with K_{KDC}
  - used to obtain session key K_{AB}

Logging into the Network



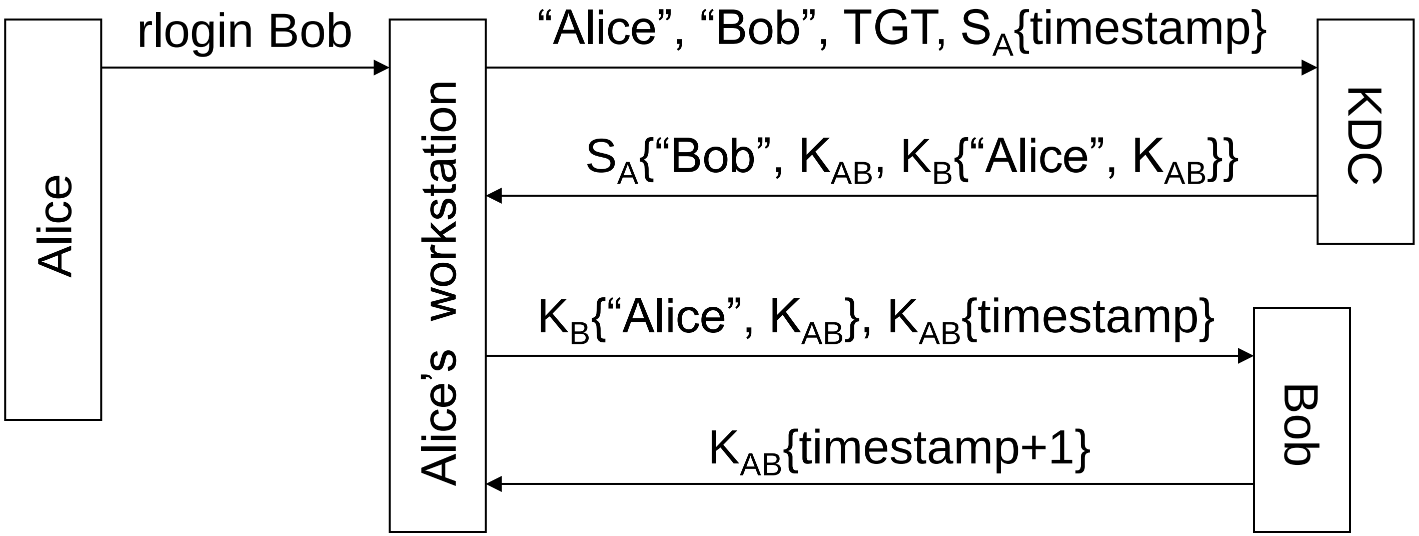
(doesn't protect against dictionary attacks with eavesdropping)

Logging into the Network (cont’d)

The workstation,

- converts Alice’s password into a DES key
- when receives the credentials from the server, decrypts them using this DES key
- if decrypts correctly, authentication is successful
- discards Alice’s master key; retains the TGT.
- TGT contains all the information KDC needs about Alice’s session; hence KDC can work without remembering any volatile data.

Accessing a Remote Principal



Alice

rlogin Bob

Alice's workstation

"Alice", "Bob", TGT, S_A{timestamp}

KDC

S_A{"Bob", K_{AB}, K_B{"Alice", K_{AB}}}

K_B{"Alice", K_{AB}}, K_{AB}{timestamp}

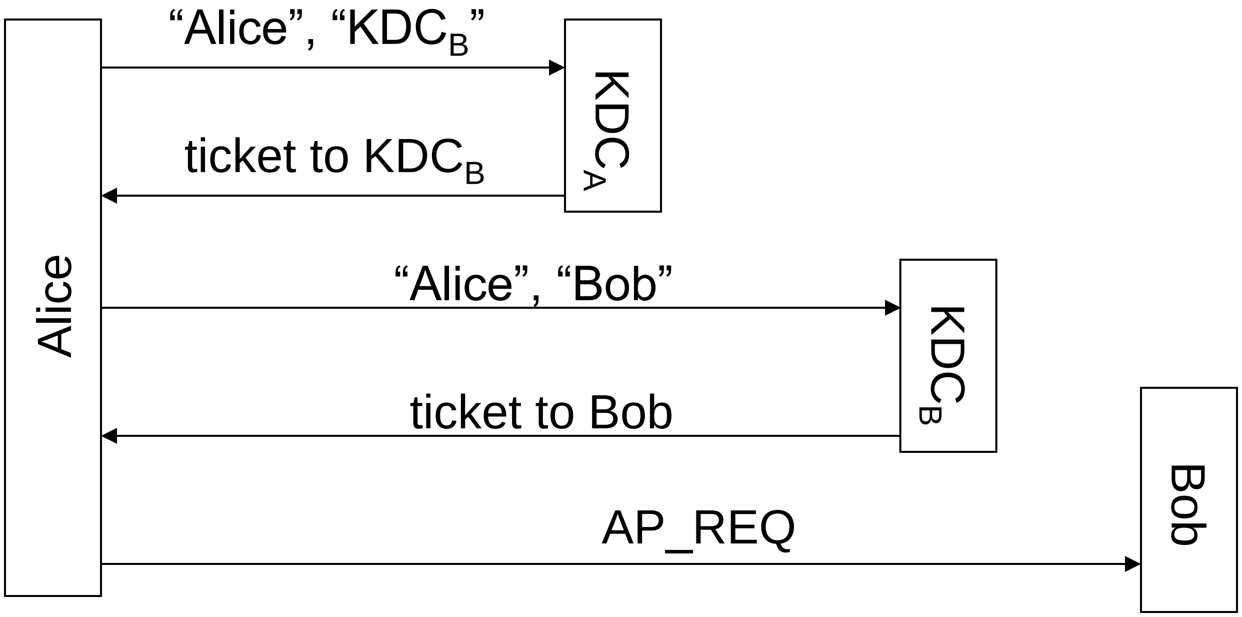
Bob

K_{AB}{timestamp+1}

Afterwards, the traffic between Alice & Bob can be

- unprotected
- authenticated
- encrypted & authenticated

Multiple Realms



- KDC$_A$ & KDC$_B$ must have registered with each other

Message Authentication

- Back in the ’80s, MACs were not an established concept.
- Kerberos initially used CRC-32 checksum, with DES encryption as the MAC.
- Non-crypto chksum, with encryption:
  - Not ok if message is in cleartext. (we know this)
  - May be ok if message is encrypted too.
  - With block cipher: Kerberos (mostly ok)
  - With a stream cipher: May be with MD5 checksum.
  - Definitely not with a stream cipher and a linear checksum as CRC; just as WEP did!

Major Problems with WEP

- WEP: “Wired Equivalent Privacy”, the first encryption protocol for 802.11 Wi-Fi.

- Major problems:
  - Using a stream cipher (RC4) for challenge-response authentication (!!)
  - Using a 24-bit IV
  - Using a linear checksum (CRC-32) with a stream cipher (RC4) as the MAC

Message Authentication in WEP

- MAC algorithm:
  - Compute CRC-32 checksum over the message.
  - Encrypt both the message and the chksum with RC4.

- Problem: RC4 is a stream cipher.
  - You can do controlled changes on the message and fix the checksum over the ciphertext!

- Can be more significant than just flipping a few bits.

Attack on MAC in WEP

Attacker can get the whole plaintext packets by flipping bits over the ciphertext:

- Parts of the plaintext is predictable (e.g., the upper-layer protocol headers).
- Attacker sniffs a packet and changes its IP address to his machine from the ciphertext.
  (If the attacker’s machine is outside the firewall, the TCP port number could also be changed, to 80 for example, which most firewalls would not block.)
- Hence, the attacker obtains the decrypted text without breaking the encryption!

More Attacks on WEP

- The final nail in the coffin:
(Fluhrer, Mantin, Shamir, 2001)
The way RC4 is used in WEP can be broken completely: When IV is known, it is possible to get k in RC4(IV || k).

- WEP2 proposal: 128-bit key, 128-bit IV.
This can be broken even faster!

Replacements for WEP

- WPA
  - encryption: RC4, but with a complex IV-key mixing
  - integrity: cryptographic checksum (by lightweight Michael algorithm)
  - replay protection: 48-bit seq.no.; also used as IV

- WPA2 (long-term replacement, 802.11i std.)
  - encryption: AES-CTR mode
  - integrity: AES-CBC-MAC