OST
Eastern Switzerland
University of Applied Sciences

Secure Protocols

Get to know each other

Cyrill Brunschwiler, Managing Director Compass Security Schweiz AG

7.11.2020

CAS Cyber Security

Intro

Goals of Secure Protocols

- Neither a passive eavesdropper nor malicious, active adversary can defeat this.
- Apply crypto mechanisms the correct way to achieve a secure protocol

Participants

- Alice, Bob, Trent, Eve, Mallory
- Trent (trusted third party TTP, CA, KDC)
- Eve (passive eavesdropper - cannot influence protocol)
- Mallory (may alter, drop, inject, replay, delay, hijack traffic, but cannot break crypto or cause DoS)

Authentication

What is authentication?

- Data origin authentication (ISO 7498-2 origin verification)
- Entity authentication (ISO 7498-2 identity verification)

Entity authentication

- Unilateral (entity) authentication
- Mutual (entity) authentication
- Both might be encryption, MAC or signature-based

Authentication requirements (avoid reflection and replay attacks)

- **Authenticity of data origin**
- **Freshness (not being used before -> eg. nonce)**
- **Liveness (its not an old message -> eg. time-stamp, logical-ts, sequence nr)**
- **Protocol must embed identities**

See ISO-9798 for more details on entity authentication

Key Agreement

Motivation for key agreement

- Communicate securely for the duration of a session
- For that reason the authentication protocol gets pimped
- Result is a authenticate key agreement protocol (AKE)

Public/Private Key Agreement

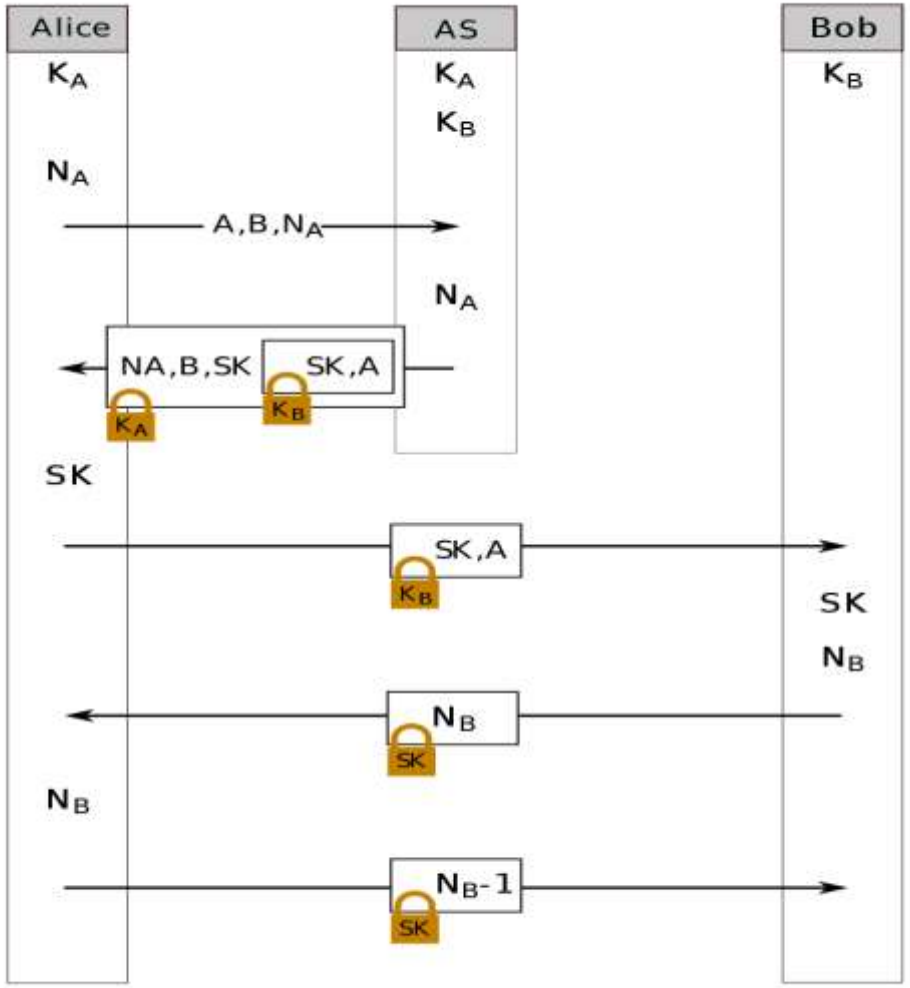
- Alice => Bob: {Session-Key}Public-Key$_{Bob}$
- K_{MAC} = HMAC(Session-Key || 'MAC')
- K_{ENC} = HMAC(Session-Key || 'ENC')

Diffi-Hellmann Key Agreement

- Alice --> Bob: g^X modulo p
- Bob --> Alice: g^Y modulo p
- $(g^Y)^X$ modulo p = g^{XY} modulo p

Trusted Third-Party

Needham-Schroeder Protocol



Mutual Authentication

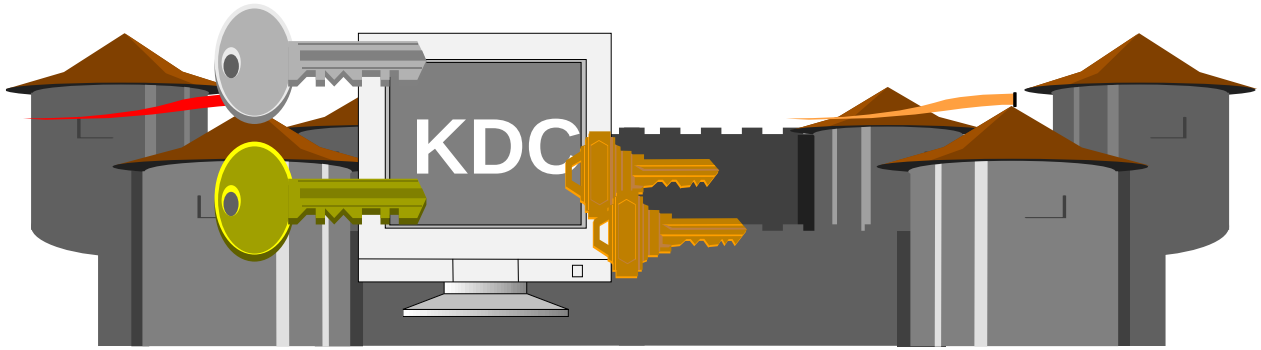
- Messages 4 and 5 must contain an Nonce to be able to authenticate B to A

Warning

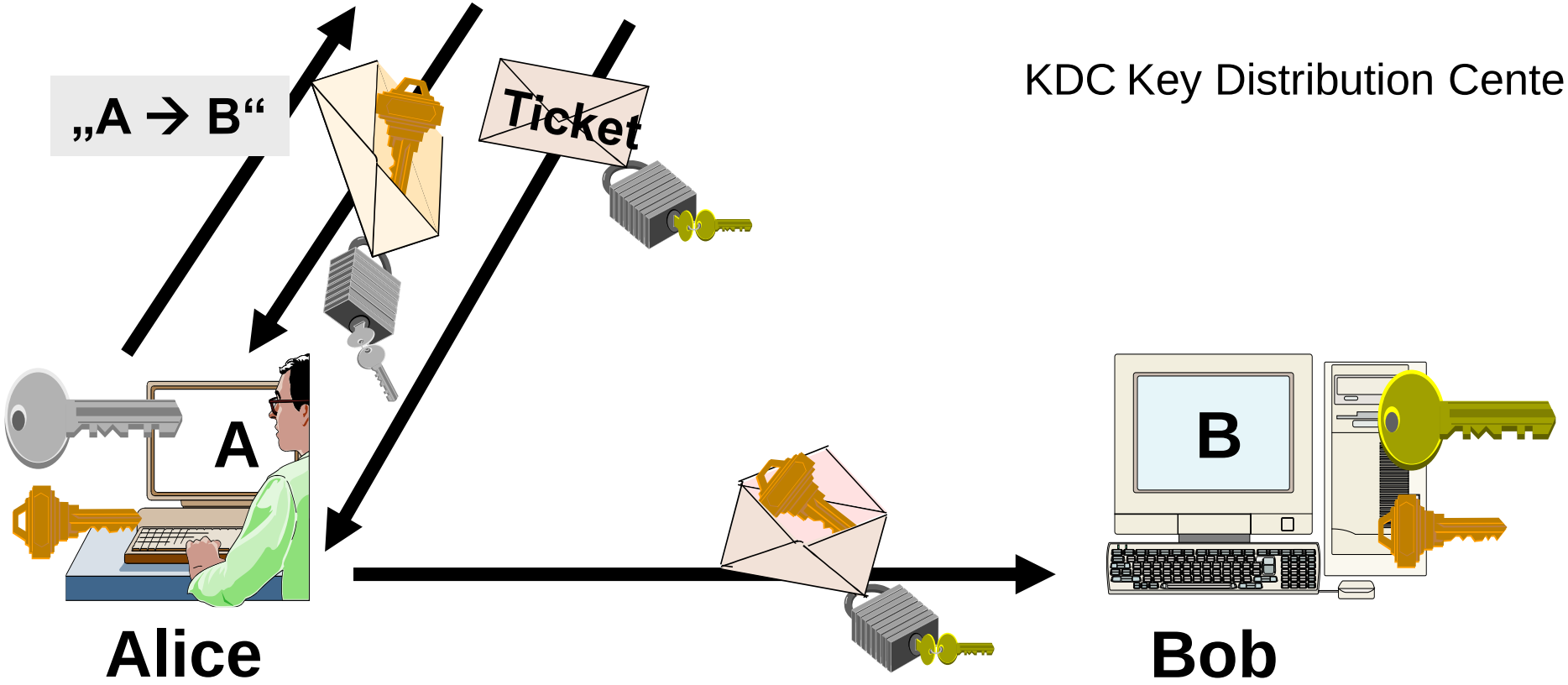
- The protocol is vulnerable to replay attacks

Source https://upload.wikimedia.org/wikipedia/commons/4/4b/Symetric_Needham-Schroeder-Protocol_%E2%80%93_linear.svg

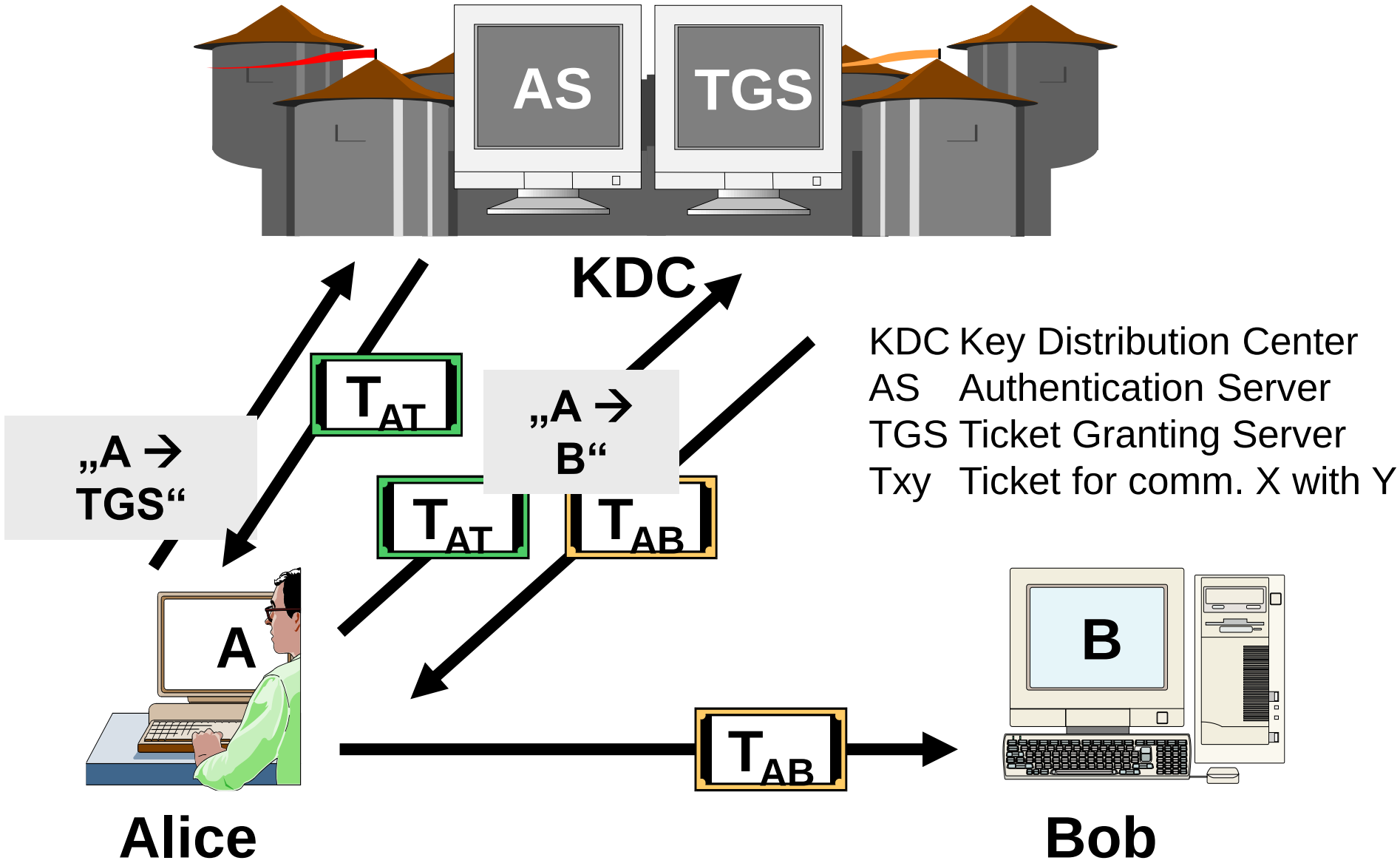
Kerberos Basic Principles



KDC Key Distribution Center



Kerberos Standard Procedure



KDC Key Distribution Center
AS Authentication Server
TGS Ticket Granting Server
Txy Ticket for comm. X with Y


COMPASS
SECURITY