Network Security - Week 4

Manuel E. Correia

DCC/FCUP

2025

Alternative authentication - Kerberos

In Greek mythology

- A ferocious 3-headed dog
- Guards the entrance to Hades' realm

Alternative authentication - Kerberos

In Greek mythology

- A ferocious 3-headed dog
- Guards the entrance to Hades' realm

In Security

- An authentication protocol
- Guards the entrance to some realms
- Designed for smaller scale, e.g. LANs
- Relies on a Trusted Third Party (TTP)

Motivation for Kerberos

- Authentication using public keys
  - N users $\Rightarrow$ N key pairs
  - Slow

Motivation for Kerberos

- Authentication using public keys
  - N users $\Rightarrow$ N key pairs
  - Slow
- Authentication using symmetric keys
  - Fast
  - N users requires N^2 keys (roughly)

Motivation for Kerberos

- Authentication using public keys
  - N users $\Rightarrow$ N key pairs
  - Slow
- Authentication using symmetric keys
  - Fast
  - N users requires N^2 keys (roughly)
- Symmetric key case **does not scale**

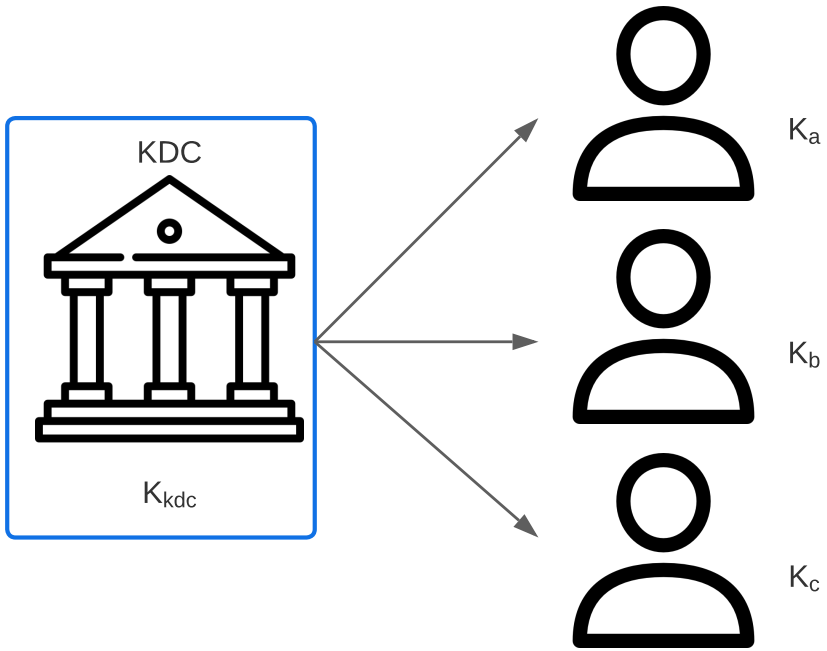
Motivation for Kerberos

- Authentication using public keys
  - N users $\Rightarrow$ N key pairs
  - Slow
- Authentication using symmetric keys
  - Fast
  - N users requires N^2 keys (roughly)
- Symmetric key case **does not scale**

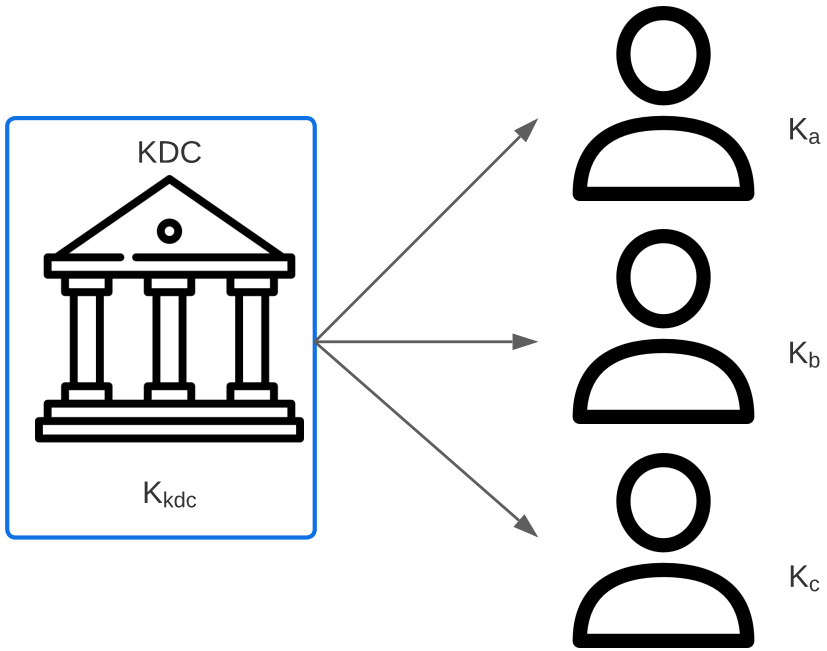
Kerberos is based on symmetric keys, but only requires N keys.

- *Assumption:* Security depends on TTP
- No PKI necessary!

A Trusted Key Distribution Center

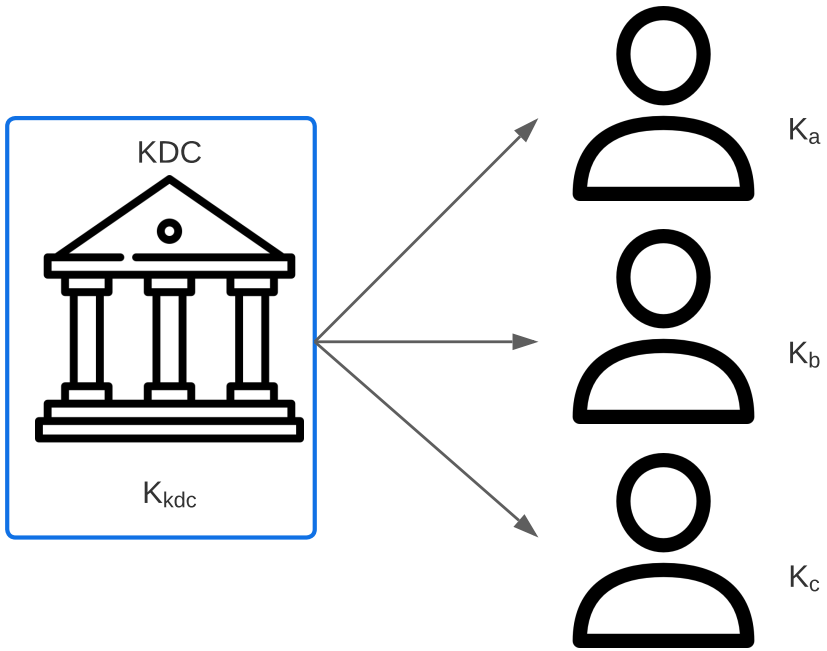


A Trusted Key Distribution Center



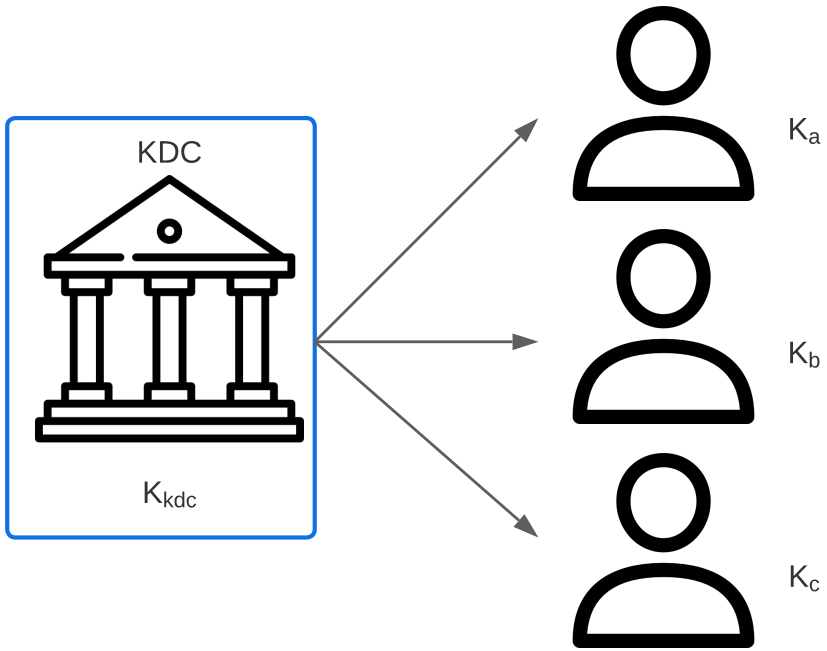
- KDC acts as a TTP (CA in PKIs)
- Cannot be compromised (by assumption)

A Trusted Key Distribution Center



- KDC acts as a TTP (CA in PKIs)
- Cannot be compromised (by assumption)
- Shares symmetric keys with all participants (K_a, K_b, K_c)
- ... and an extra master key K_{kdc}

A Trusted Key Distribution Center



- KDC acts as a TTP (CA in PKIs)
- Cannot be compromised (by assumption)
- Shares symmetric keys with all participants (K_a, K_b, K_c)
- ... and an extra master key K_{kdc}
- Enables authentication and session keys

Kerberos Authentication

Tickets within tickets

- KDC grants tickets needed to access network resources

Kerberos Authentication

Tickets within tickets

- KDC grants tickets needed to access network resources
- But also grands Ticket-Granting Tickets (TGTs)
  - Issued upon first login
  - Used to obtain regular tickets

Kerberos Authentication

Tickets within tickets

- KDC grants tickets needed to access network resources
- But also grands Ticket-Granting Tickets (TGTs)
  - Issued upon first login
  - Used to obtain regular tickets

TGTs

- Each TGT contains:
  - Session key
  - User ID
  - Expiration time

Kerberos Authentication

Tickets within tickets

- KDC grants tickets needed to access network resources
- But also grands Ticket-Granting Tickets (TGTs)
  - Issued upon first login
  - Used to obtain regular tickets

TGTs

- Each TGT contains:
  - Session key
  - User ID
  - Expiration time
- Used to avoid having the KDC manage a database
- KDC remains (mostly) stateless

Kerberos Login

1. Alice enters her password

Kerberos Login

1. Alice enters her password
2. Alice retrieves the TGT
   - Derives K_A from its password.
   - Uses K_A to request TGT from the KDC

Kerberos Login

1. Alice enters her password
2. Alice retrieves the TGT
   - Derives K_A from its password.
   - Uses K_A to request TGT from the KDC
3. Forward the TGT to access network resources

Kerberos Login

1. Alice enters her password
2. Alice retrieves the TGT
   - Derives K_A from its password.
   - Uses K_A to request TGT from the KDC
3. Forward the TGT to access network resources

The good and the bad

Kerberos Login

1. Alice enters her password
2. Alice retrieves the TGT
   - Derives K_A from its password.
   - Uses K_A to request TGT from the KDC
3. Forward the TGT to access network resources

The good and the bad

- **Good:** Security is transparent for Alice

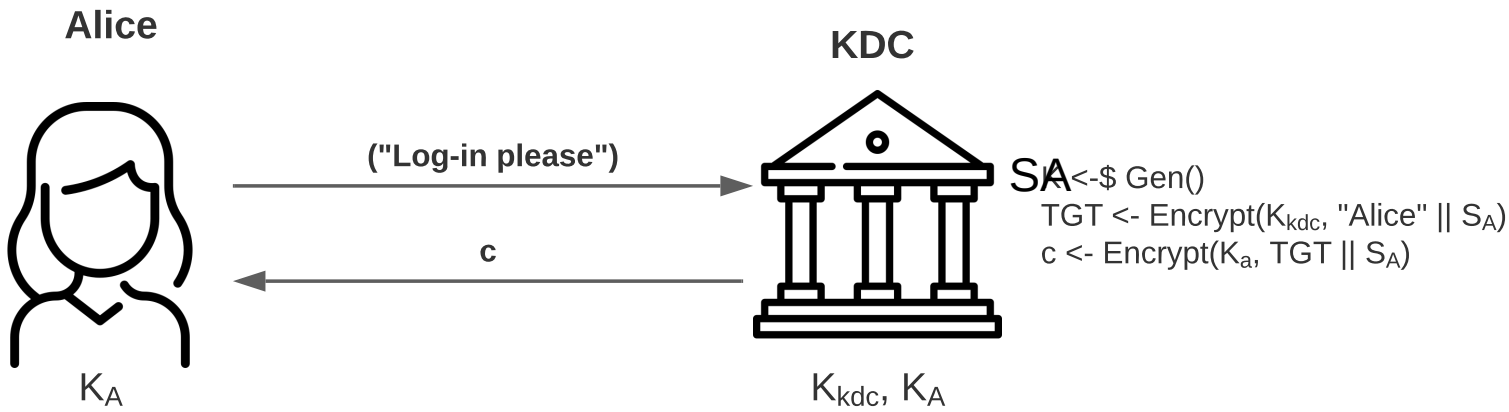
Kerberos Login

1. Alice enters her password
2. Alice retrieves the TGT
   - Derives K_A from its password.
   - Uses K_A to request TGT from the KDC
3. Forward the TGT to access network resources

The good and the bad

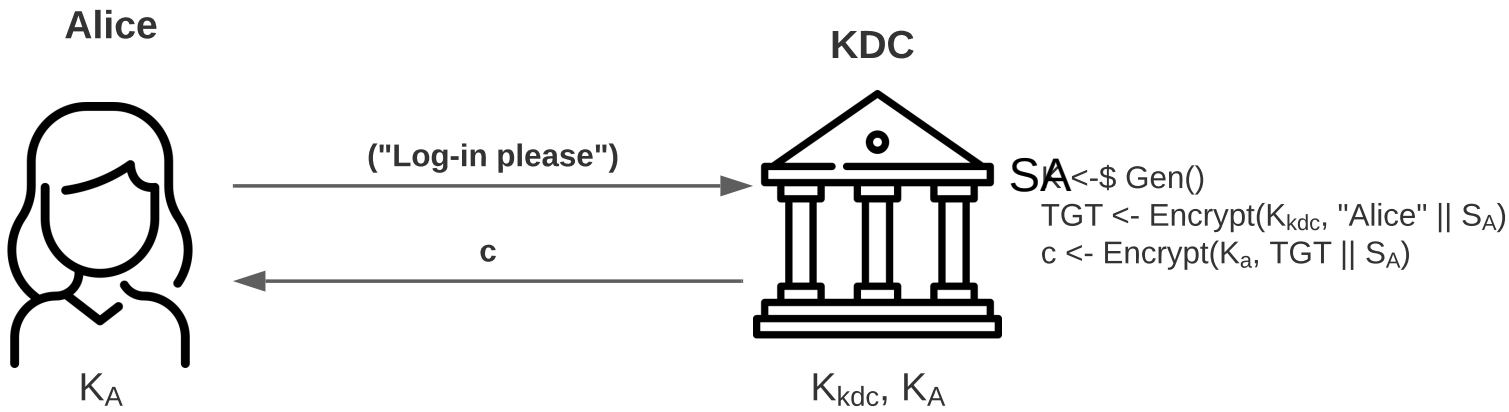
- **Good:** Security is transparent for Alice
- **Bad:** KDC must always be secure!

Kerberos Login



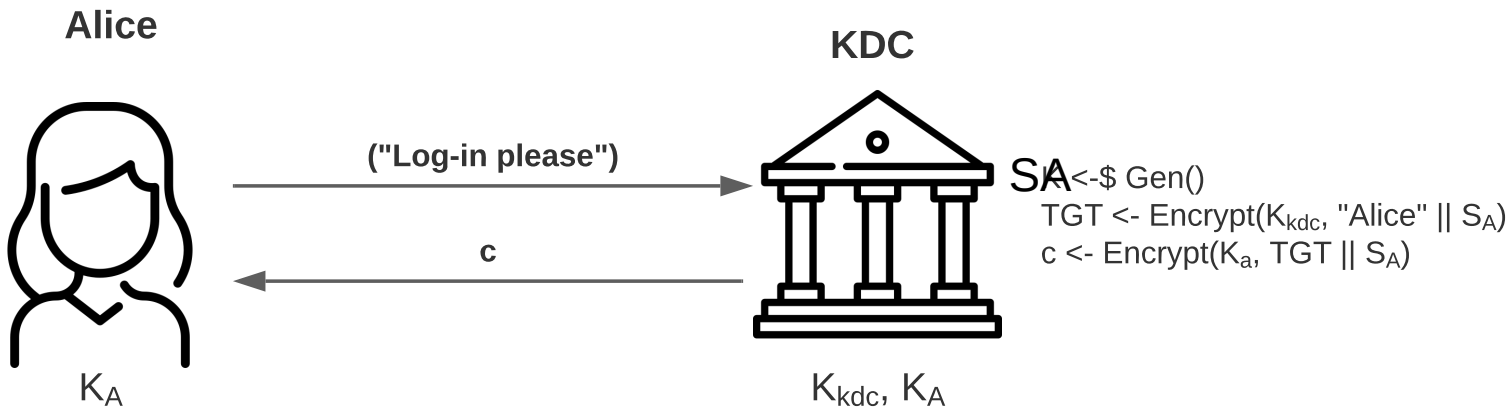
- K_A is Alice's key (e.g. generated from password)

Kerberos Login



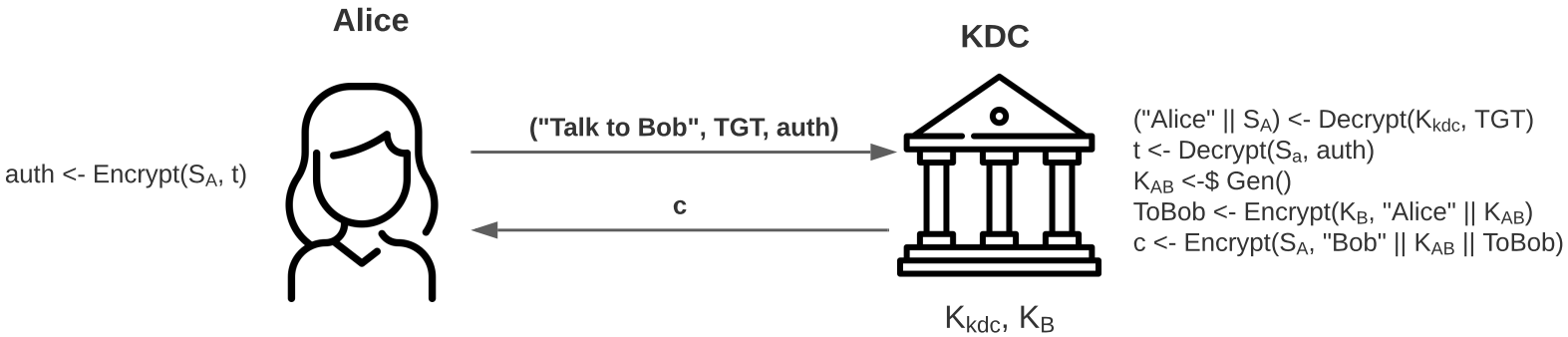
- K_A is Alice's key (e.g. generated from password)
- KDC generates session key S_A and constructs TGT

Kerberos Login



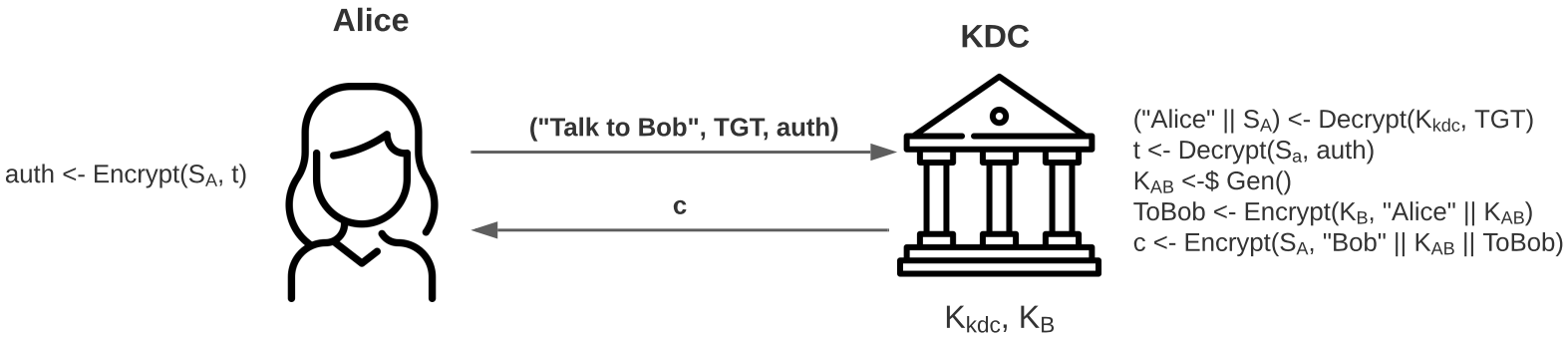
- K_A is Alice's key (e.g. generated from password)
- KDC generates session key S_A and constructs TGT
- Alice retrieves S_A and TGT

Kerberos Talk to Bob - P1



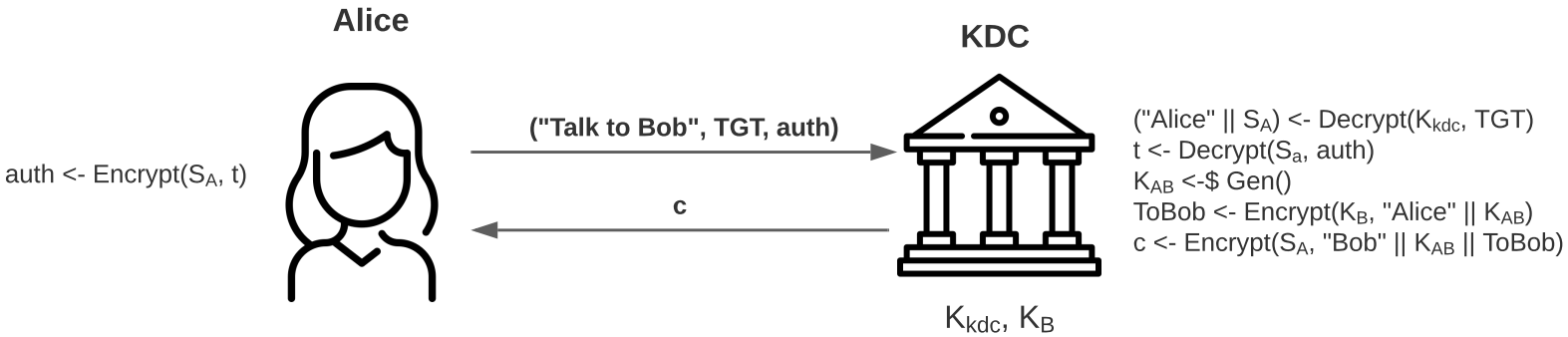
- KDC knows Bob's key K_B

Kerberos Talk to Bob - P1



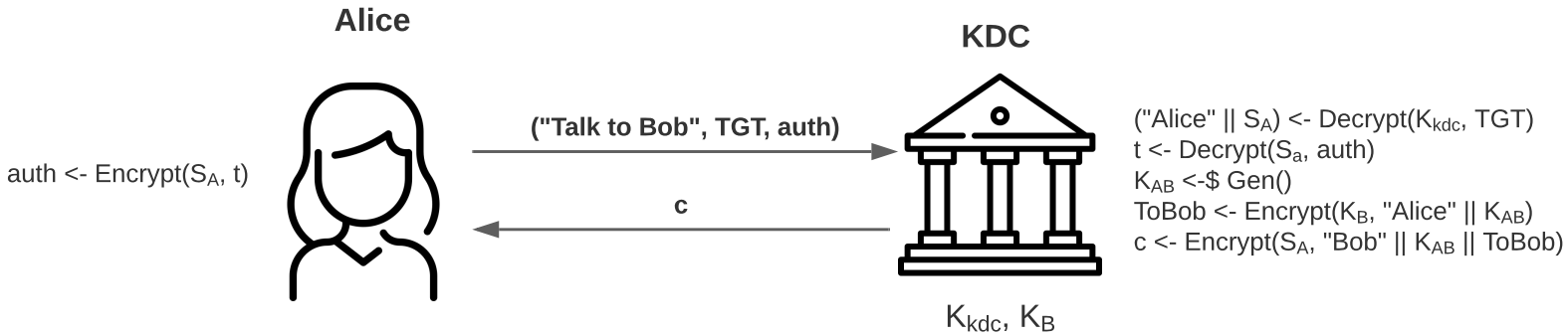
- KDC knows Bob's key K_B
- Alice sends the request, alongside the TGT and an authenticator

Kerberos Talk to Bob - P1



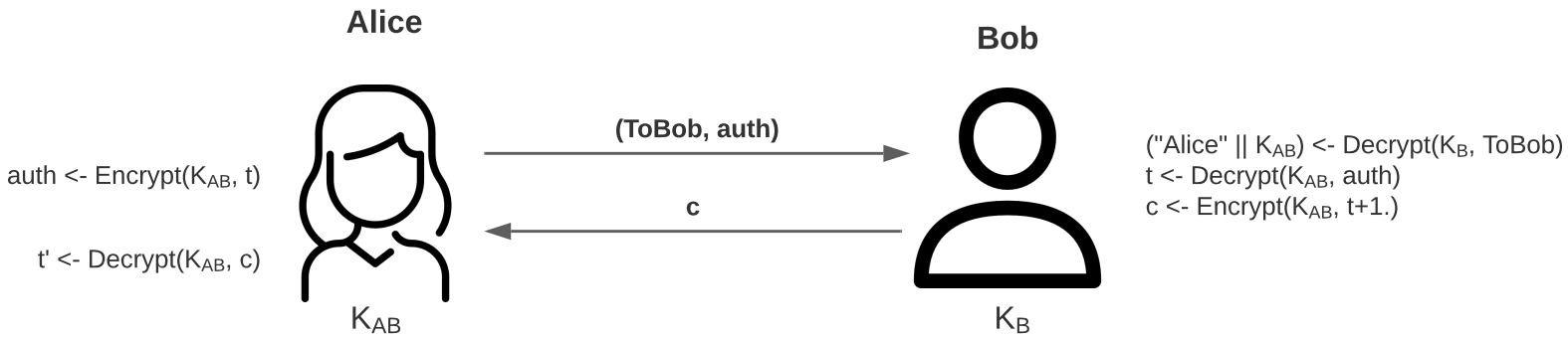
- KDC knows Bob's key K_B
- Alice sends the request, alongside the TGT and an authenticator
- KDC prepares a communication key for K_{AB}
  - Encrypts it also with K_B
  - And tags Alice (to avoid reflection attacks)

Kerberos Talk to Bob - P1



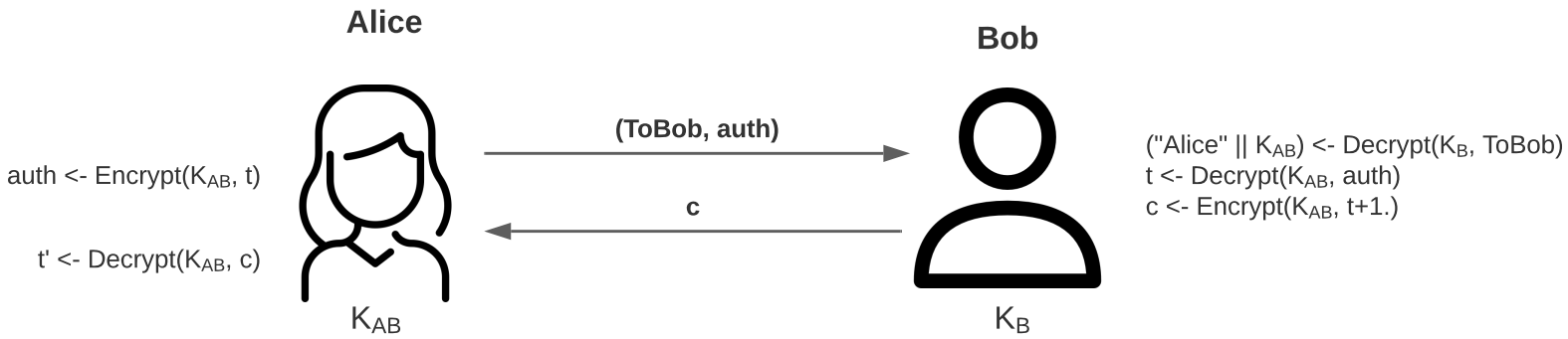
- KDC knows Bob's key K_B
- Alice sends the request, alongside the TGT and an authenticator
- KDC prepares a communication key for K_{AB}
  - Encrypts it also with K_B
  - And tags Alice (to avoid reflection attacks)
- Alice retrieves K_{AB} and an authenticator it can send to Bob

Kerberos Talk to Bob - P2



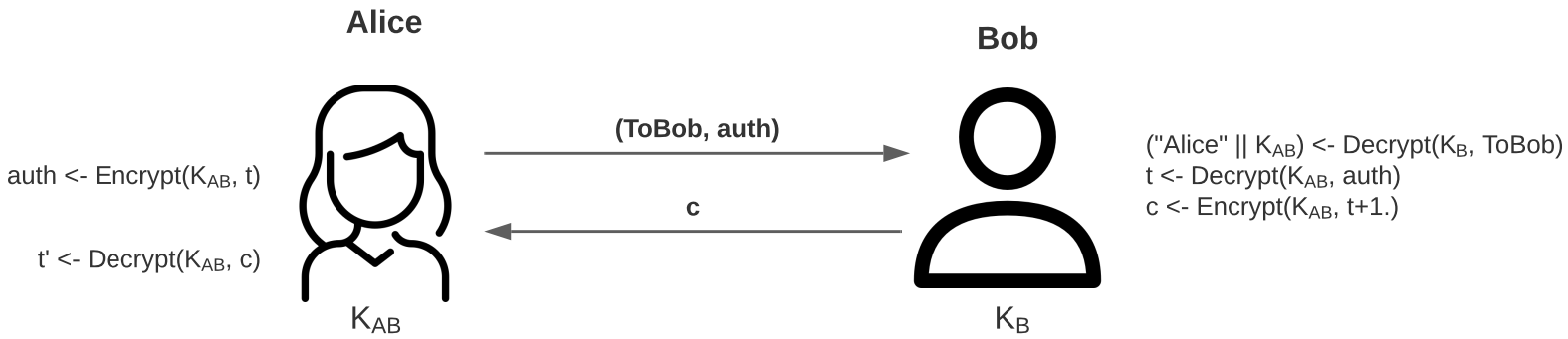
- Bob knows its own key K_B

Kerberos Talk to Bob - P2



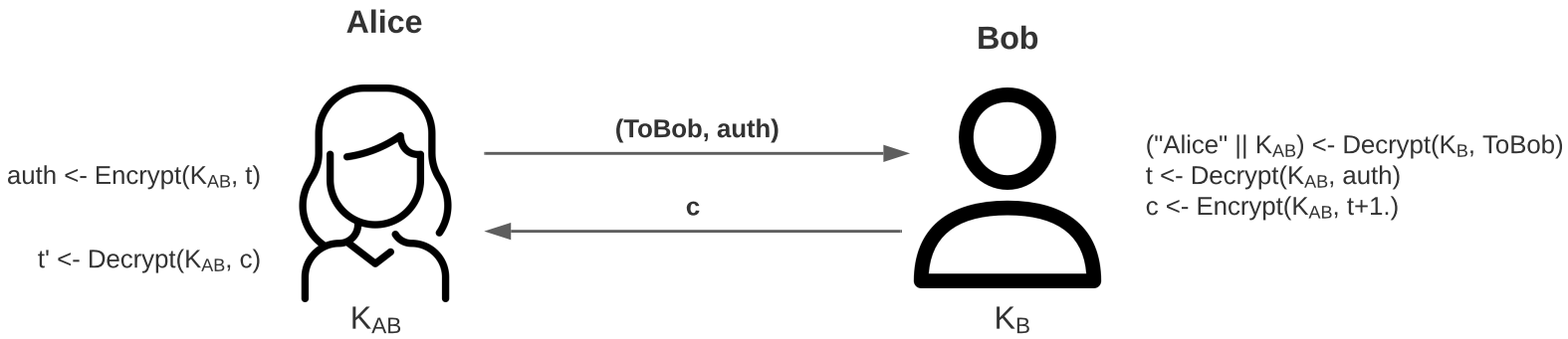
- Bob knows its own key K_B
- Alice sends ToBob, and an authenticator encrypted with K_{AB}

Kerberos Talk to Bob - P2



- Bob knows its own key K_B
- Alice sends ToBob, and an authenticator encrypted with K_{AB}
- Bob does not know K_{AB}...
  - But the ToBob token has K_{AB}, encrypted with K_B
  - Retrieves K_{AB} and checks the authenticator for freshness
  - Encrypts a reply with the updated timestamp

Kerberos Talk to Bob - P2



- Bob knows its own key K_B
- Alice sends ToBob, and an authenticator encrypted with K_{AB}
- Bob does not know K_{AB}...
  - But the ToBob token has K_{AB}, encrypted with K_B
  - Retrieves K_{AB} and checks the authenticator for freshness
  - Encrypts a reply with the updated timestamp
- Alice decrypts the reply and checks for freshness

Kerberos Security - P1

- Key S_A is used for authentication
  - Gives confidentiality/integrity for Alice-KDC communication

Kerberos Security - P1

- Key S_A is used for authentication
  - Gives confidentiality/integrity for Alice-KDC communication
- Key K_{AB} used for Alice-Bob communication
  - Trustworthiness from the fact that the KDC encrypt it with K_B
  - Only entity with knowledge of K_B
  - Bob trusts the KDC!

Kerberos Security - P1

- Key S_A is used for authentication
  - Gives confidentiality/integrity for Alice-KDC communication
- Key K_{AB} used for Alice-Bob communication
  - Trustworthiness from the fact that the KDC encrypt it with K_B
  - Only entity with knowledge of K_B
  - Bob trusts the KDC!
- Timestamps are used for authentication and replay protection

Kerberos Security - P1

- Key S_A is used for authentication
  - Gives confidentiality/integrity for Alice-KDC communication
- Key K_{AB} used for Alice-Bob communication
  - Trustworthiness from the fact that the KDC encrypt it with K_B
  - Only entity with knowledge of K_B
  - Bob trusts the KDC!
- Timestamps are used for authentication and replay protection
- Timestamps behave like a nonce that is known in advance

Kerberos Security - P1

- Key S_A is used for authentication
  - Gives confidentiality/integrity for Alice-KDC communication
- Key K_{AB} used for Alice-Bob communication
  - Trustworthiness from the fact that the KDC encrypt it with K_B
  - Only entity with knowledge of K_B
  - Bob trusts the KDC!
- Timestamps are used for authentication and replay protection
- Timestamps behave like a nonce that is known in advance
- “time” is a security-critical parameter!

Kerberos Security - P2

Common questions

- Why is TGT encrypted with K_A?
  - Allows for the anonymity of Alice!

Kerberos Security - P2

Common questions

- Why is TGT encrypted with K_A?
  - Allows for the anonymity of Alice!
- Why doesn't the KDC sent the ticket to Bob?
  - Bob would have to remember K_{AB}
  - It's good to remain stateless!

Kerberos Security - P2

Common questions

- Why is TGT encrypted with K_A?
  - Allows for the anonymity of Alice!
- Why doesn't the KDC sent the ticket to Bob?
  - Bob would have to remember K_{AB}
  - It's good to remain stateless!
- Can't we have the KDC remember the session key instead of using the TGT?
  - Yes... but it's good to have the KDC remain stateless
  - Scales better!

Wrap up

Authentication is core in network security

- Single or mutual authentication

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks
- Nonces/timestamps used for freshness

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks
- Nonces/timestamps used for freshness

Cryptogaphy

- Signatures used to ensure source is trustworthy

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks
- Nonces/timestamps used for freshness

Cryptogaphy

- Signatures used to ensure source is trustworthy
- Encryption used to ensure confidentiality

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks
- Nonces/timestamps used for freshness

Cryptogaphy

- Signatures used to ensure source is trustworthy
- Encryption used to ensure confidentiality

Kerberos

- An alternative system for authentication

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks
- Nonces/timestamps used for freshness

Cryptogaphy

- Signatures used to ensure source is trustworthy
- Encryption used to ensure confidentiality

Kerberos

- An alternative system for authentication
- Trusted hardware assumption - KDC

Wrap up

Authentication is core in network security

- Single or mutual authentication
- Vulnerable to replay, relay, mitm attacks
- Nonces/timestamps used for freshness

Cryptogaphy

- Signatures used to ensure source is trustworthy
- Encryption used to ensure confidentiality

Kerberos

- An alternative system for authentication
- Trusted hardware assumption - KDC
- Ticket Granting Tickets
  - Allows for stateless resource management

Network Security - Week 4

Manuel E. Correia

DCC/FCUP

2025