



An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

- October 25th Class – Virtual Zoom Session
- October 12th Class (Tuesday) – No Meeting / Cancel

Required Week Five Readings

1. “Password Authentication with Insecure Communication,” Leslie Lamport
<https://lamport.azurewebsites.net/pubs/password.pdf>
2. Chapters 12 through 16: *From CIA to APT: An Introduction to Cyber Security*, E. Amoroso & M. Amoroso

Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso

Week 5



Week 5: Authentication Protocols

How Do Nation States Cryptanalyze Encrypted Data?
(Warm-Up Topic)

Three Methods for Cryptanalysis

- **Ciphertext Only**
 - Cryptanalyst only has encrypted text
 - No hints or codebooks

Three Methods for Cryptanalysis

- **Ciphertext Only**
 - Cryptanalyst only has encrypted text
 - No hints or codebooks
- **Known Plaintext**
 - Cryptanalyst observes hints (no control)
 - Tiny codebook examples can be developed

Three Methods for Cryptanalysis

- **Ciphertext Only**
 - Cryptanalyst only has encrypted text
 - No hints or codebooks
 - **Known Plaintext**
 - Cryptanalyst observes hints (no control)
 - Tiny codebook examples can be developed
 - **Chosen Plaintext**
 - Cryptanalyst has the encryption function
 - Codebook can be developed

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	W	E	A	O	S	H	T	S	I	E	C	A	V	E	F	E	T	O	V
/	D	Y	C	As	o	w	T	\$	g	a	-	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z			
//	E	O	O	R	X	C	L	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z					
X	E	S	A	z	g	q	d	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z						
X	E	E	A	z	u	b	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z	z						
Notes. x. x. +. F. T. z. x. - z. ff. a. A. v. B. +. w. S. M. C. +. +. h. C. H. f. v. b. g. a. D.																																									
January. February. March. April. May. June. July. August. September. October. November. December. Lent. Easter. Pentecost. Whitsunday. Corpus Christi. Ascension Day. Pentecost Sunday.																																									
X	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:	F	:								
Note. I shall always double the Consonants, preceding the same.																																									
Tis. p. for the pronouncing, Tis. v. for Iambification, Tis. j. to avoid his preposition, of particles & sentences.																																									
X	The Duke	+	the Duke of Lancast.	-	the Duke of Roane.	+	the Duke of Roane.	+	Madame	+	wage	+	you	X	for																										
X	The King of France	+	the Duke of Oxford	-	the Duke of Roane	+	the Duke of Roane	+	Madame	+	reueue	+	your	X	to																										
+	the E. of Gloucest.	=	the Duke of Sussex	+	the E. of Gloucest.	+	the E. of Gloucest.	+	your Maistrie	+	day	+	will																												
+	the E. of Gloucest.	=	the Duke of Northum.	+	the E. of Roane	+	the E. of Roane	+	My god brother	+	sent	+	whic																												
+	the E. of Denmark	+	the E. of Lecester	+	the E. of Gloucest.	+	the E. of Gloucest.	+	My leid	+	send	+	what																												
+	the Q. of England	+	the E. of H. Howard	+	the E. of H. Howard	+	the E. of H. Howard	+	Master	+	affect	+	where																												
X	The Q. of Ireland	+	the E. of Shrewsbury	+	the E. of Gloucest.	+	the E. of Gloucest.	+	I pray you	+	counsell	+	sace	X	wee																										
+	the Q. of France	+	the E. of H. Howard	+	the E. of H. Howard	+	the E. of H. Howard	+	maste	+	service	+	had																												
+	the Q. of Navarre	+	the E. of H. Howard	+	the E. of H. Howard	+	the E. of H. Howard	+	comfetti	+	support	+	hatte																												
+	the E. of Navarre	+	the E. of H. Howard	+	the E. of H. Howard	+	the E. of H. Howard	+	comfetti	+	comfetti	+	religion																												
+	the Q. of Navarre	+	the E. of H. Howard	+	the E. of H. Howard	+	the E. of H. Howard	+	comfetti	+	comfetti	+	comfetti																												
+	the E. of Scotland	+	the Lord Hunsdon	+	the Lord Hunsdon	+	the Lord Hunsdon	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Anjou	+	the E. of Westm.	+	the E. of Westm.	+	the E. of Westm.	+	comfetti	+	comfetti	+	comfetti																												
+	the Imperator	+	the E. of Bedford	+	the E. of Bedford	+	the E. of Bedford	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Anjou	+	the E. of Bedford	+	the E. of Bedford	+	the E. of Bedford	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Florence	+	the Comte of S. Rom.	+	the Comte of S. Rom.	+	the Comte of S. Rom.	+	comfetti	+	comfetti	+	comfetti																												
M	the Duke of Leonne	+	the Lord Talbot	+	the Lord Talbot	+	the Lord Talbot	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Guyenne	+	the Lord Talbot	+	the Lord Talbot	+	the Lord Talbot	+	comfetti	+	comfetti	+	comfetti																												
+	the Prince of Orage	+	S. Will Cecil	+	S. Will Cecil	+	S. Will Cecil	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Mayne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Mayne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Barne	+	his Lord Sonne	+	his Lord Sonne	+	his Lord Sonne	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Barne	+	his Lord Sonne	+	his Lord Sonne	+	his Lord Sonne	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+	comfetti																												
+	the Duke of Leonne	+	the Lord Strange	+	the Lord Strange	+	the Lord Strange	+	comfetti	+	comfetti	+																													

Three Methods for Cryptanalysis

- **Ciphertext Only**
 - Cryptanalyst only has encrypted text
 - No hints or codebooks
- **Known Plaintext**
 - Cryptanalyst observes hints (no control)
 - Tiny codebook examples can be developed
- **Chosen Plaintext**
 - Cryptanalyst has the encryption function
 - Codebook can be developed

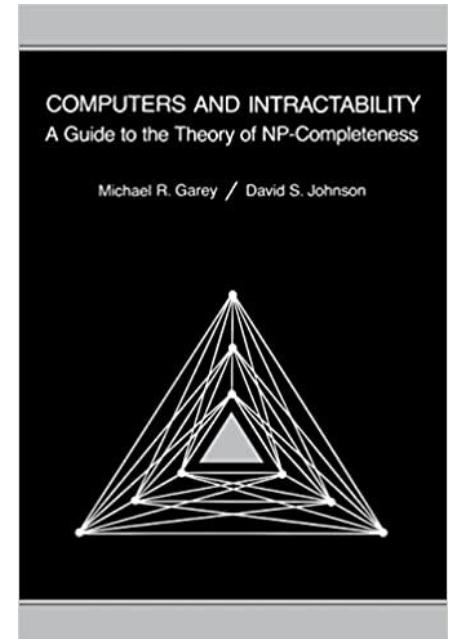
Two requirements protect encrypted text:

1. The encryption function must be cryptographically hard
2. The cleartext and ciphertext domains must be huge

Two Implications:

You must try every possible case to find the encryption function

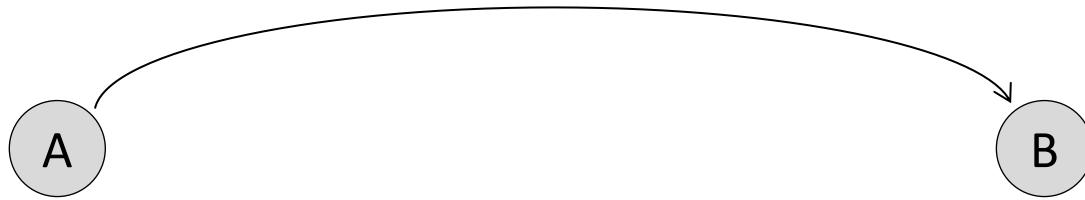
The number of possible cases cannot feasibly be covered



What is Authentication?

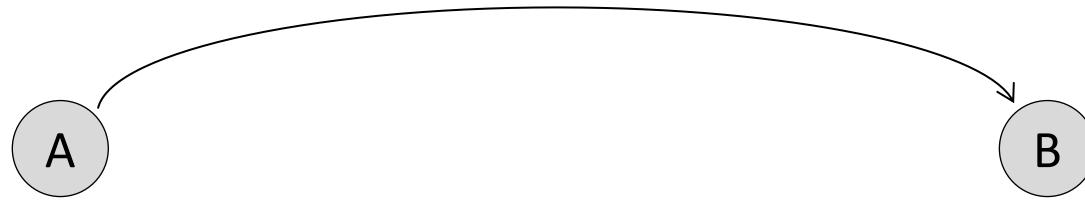
Authentication Schema

Step 1: Identification “I am Alice.”



Authentication Schema

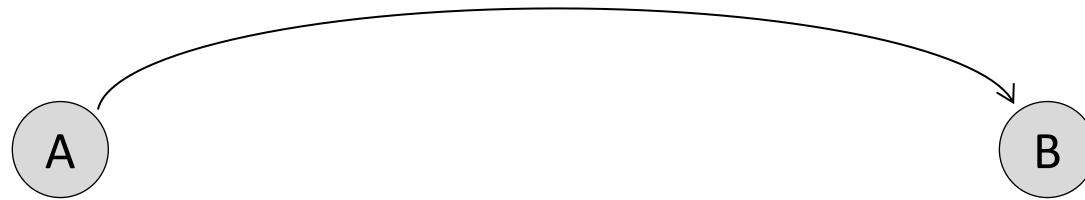
Step 1: Identification “I am Alice.”



Server Validates Client: “Client Authentication”

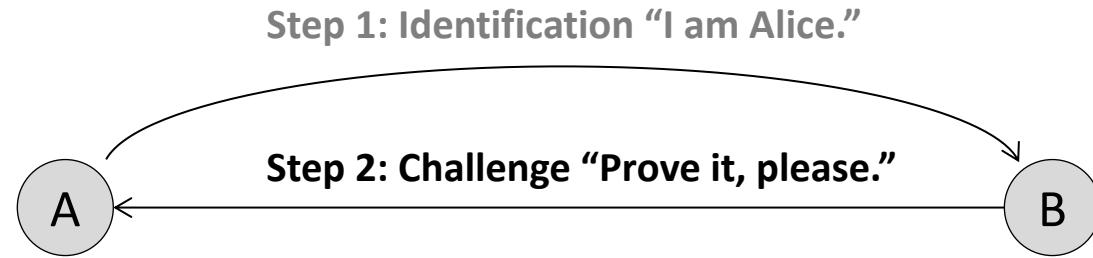
Authentication Schema

Step 1: Identification “I am Alice.”

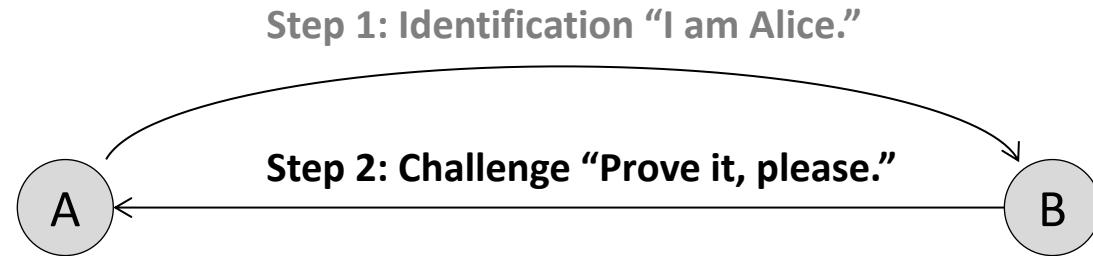


Client Validates Server: “Server Authentication”

Authentication Schema



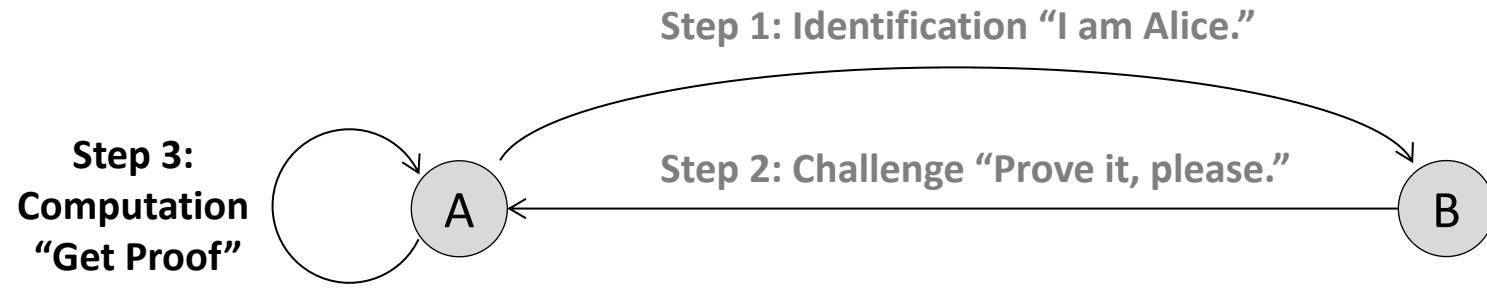
Authentication Schema



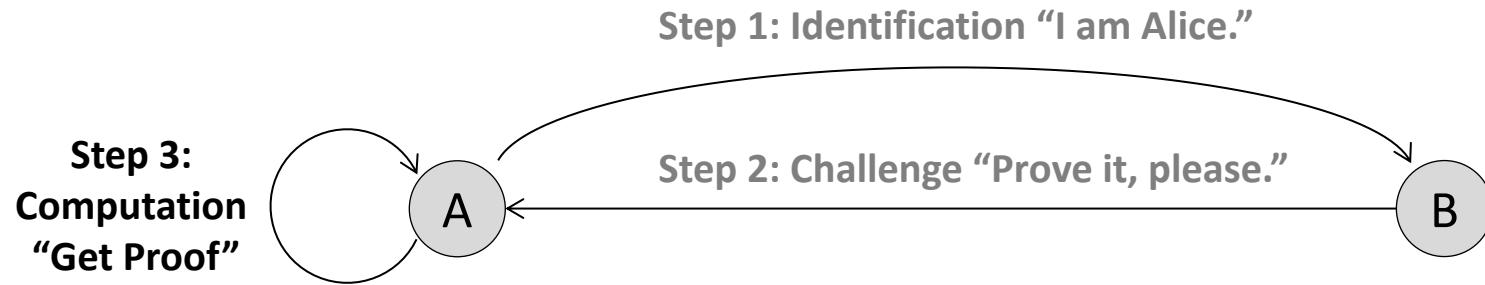
Challenge includes tangible domain value – possible “known plaintext” attacks

Challenge includes no tangible domain value – likely to restrict to “ciphertext-only attacks”

Authentication Schema



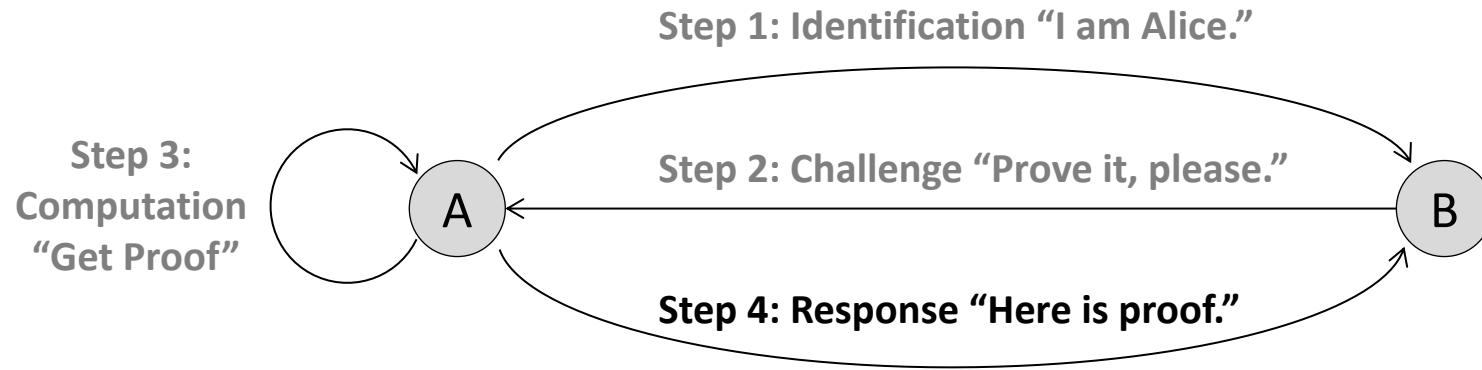
Authentication Schema



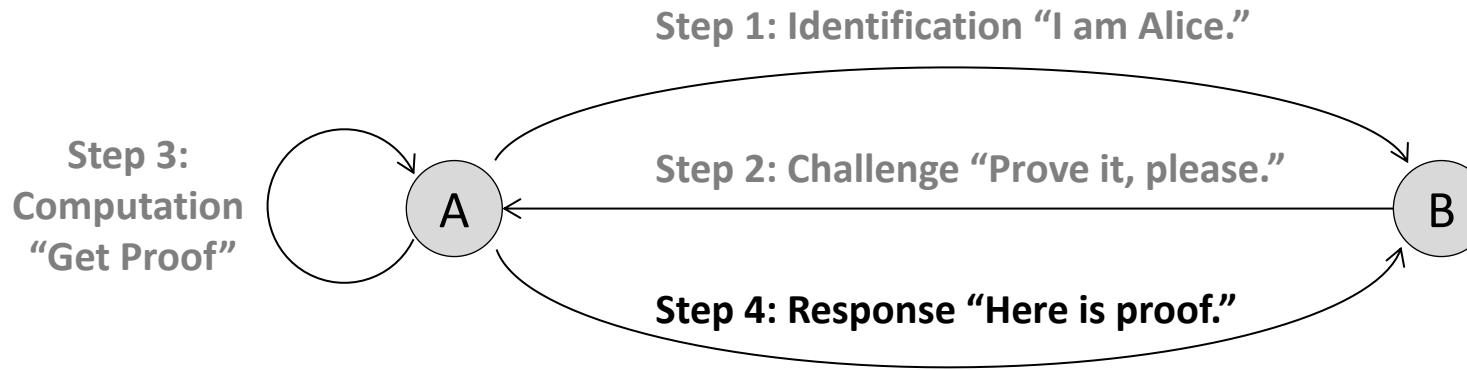
Computation might involve simple look-up/locate process (e.g., passwords)

Computation might be more deliberate mathematical operation on domain value

Authentication Schema



Authentication Schema



Types of Proof:

- "Something You Know" – Passwords
- "Something You Are" – Biometrics
- "Something You Have" – Token
- "Somewhere You Are" – Location

- **Adaptive Authentication** considers context
- **Two-Factor Authentication** uses at least two types

MyStevens Two-Factor Authentication

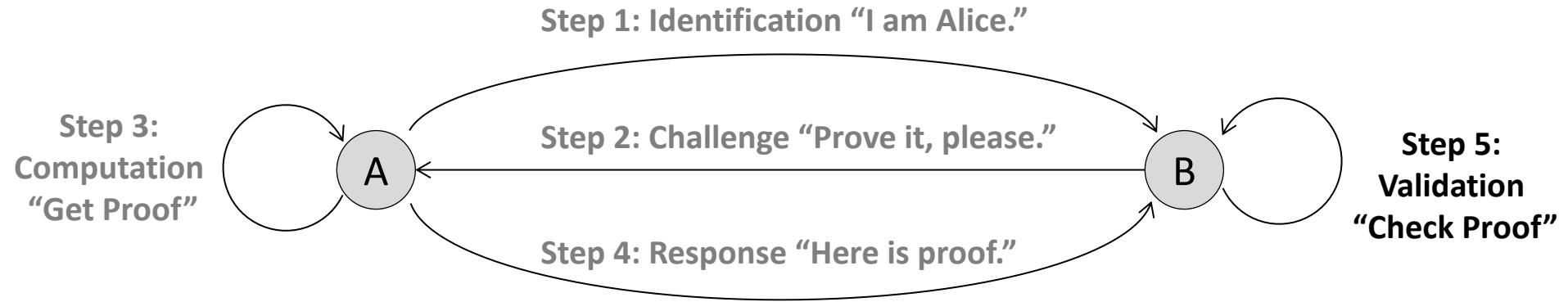
[Product](#)[Editions & Pricing](#)[Solutions](#)[Partnerships](#)[Support](#)[Documentation](#)[Resources](#)[Contact Sales](#)[Free Trial](#)

Protect your workforce with simple, powerful access security.

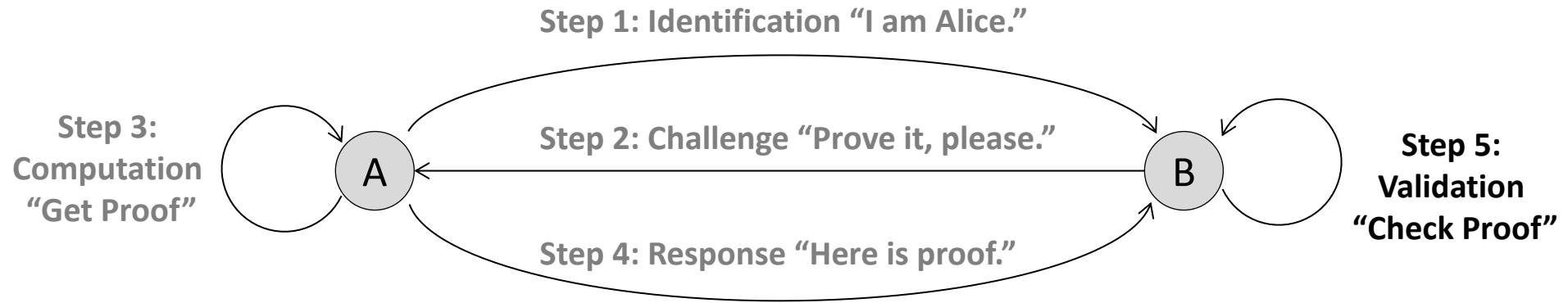
We're Duo. Our modern access security is designed to safeguard all users, devices, and applications — so you can stay focused on what you do best.



Authentication Schema



Authentication Schema



Validation might involve simple look-up/locate process (e.g., passwords)

Validation might be more deliberate mathematical operation on domain value

ZenKey Mobile Carrier Authentication (Metadata)

[WHAT IS ZENKEY ▾](#)[BUSINESS ▾](#)[DEVELOPERS ▾](#)[RESOURCES ▾](#)[CONTACT](#)[Get ZenKey](#)

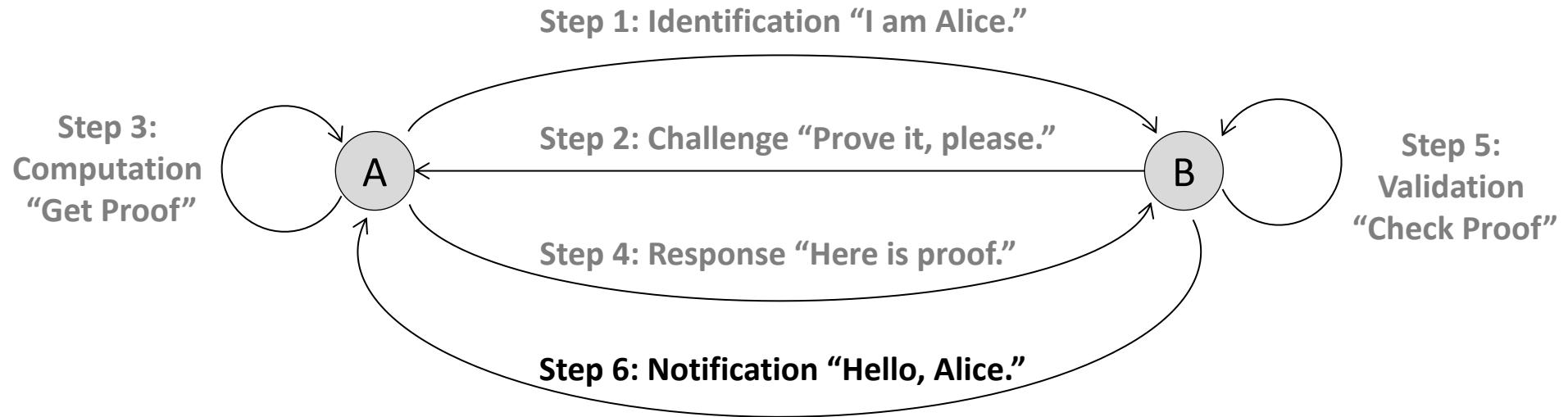
Unlock Trust

ZenKey gives you a fast and safe way to register for apps and websites. It also makes sure that the device you're using matches the device info you registered with your wireless carrier. This helps to secure your logins and transactions.

Be one of the first to try ZenKey and get the peace of mind you deserve.

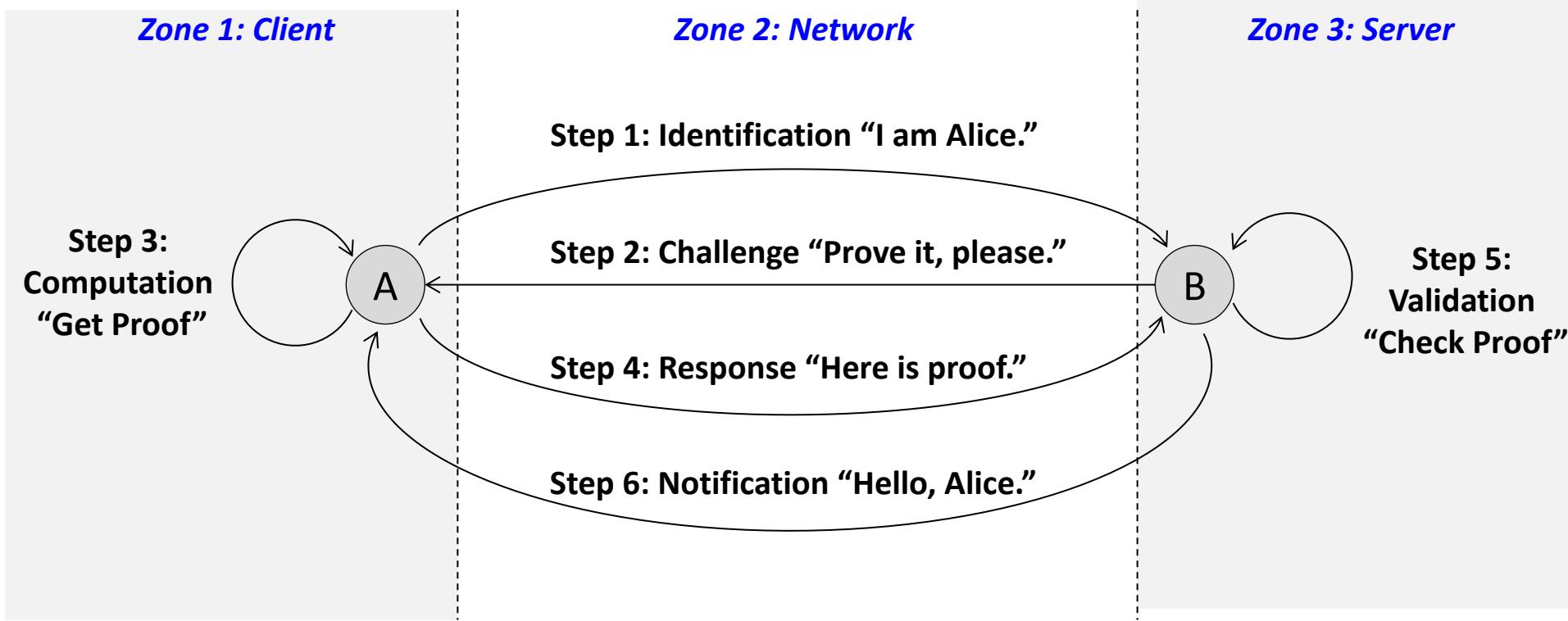


Authentication Schema

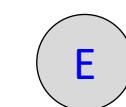
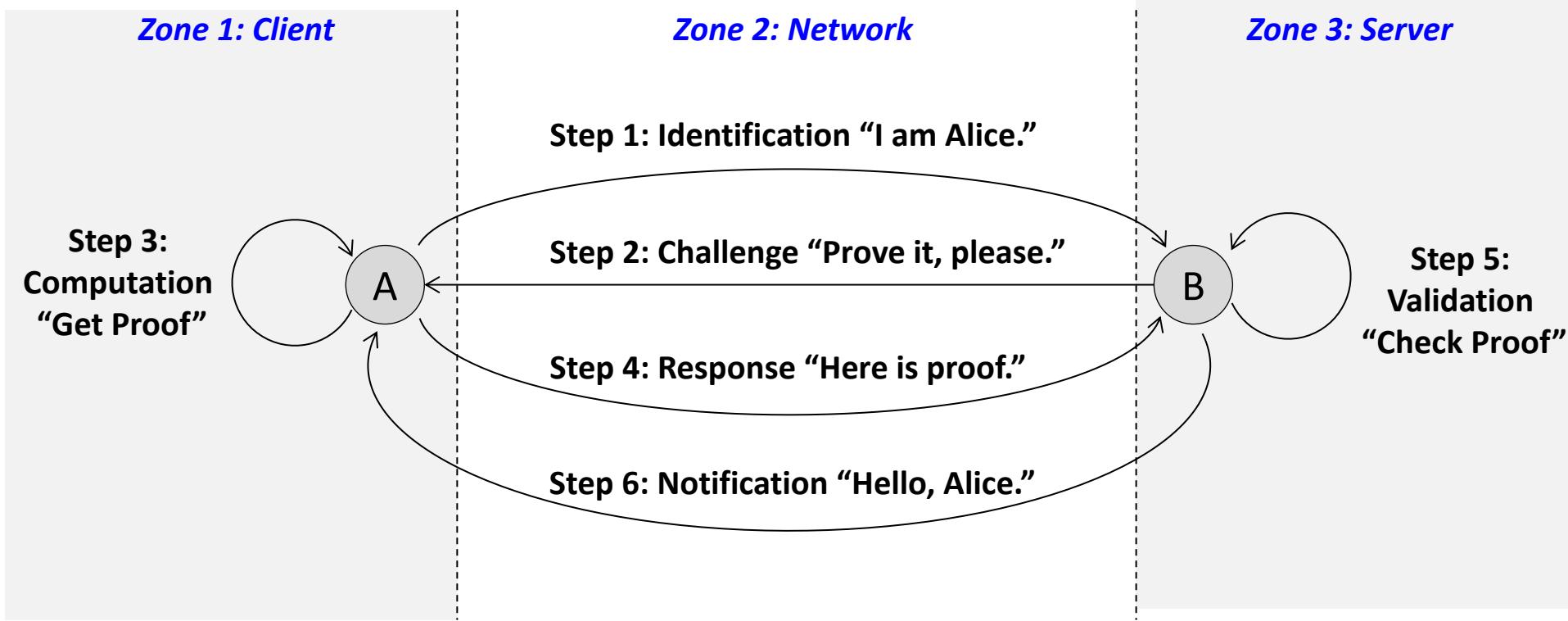


How Do Hackers Try to Bypass Authentication?

Authentication Schema

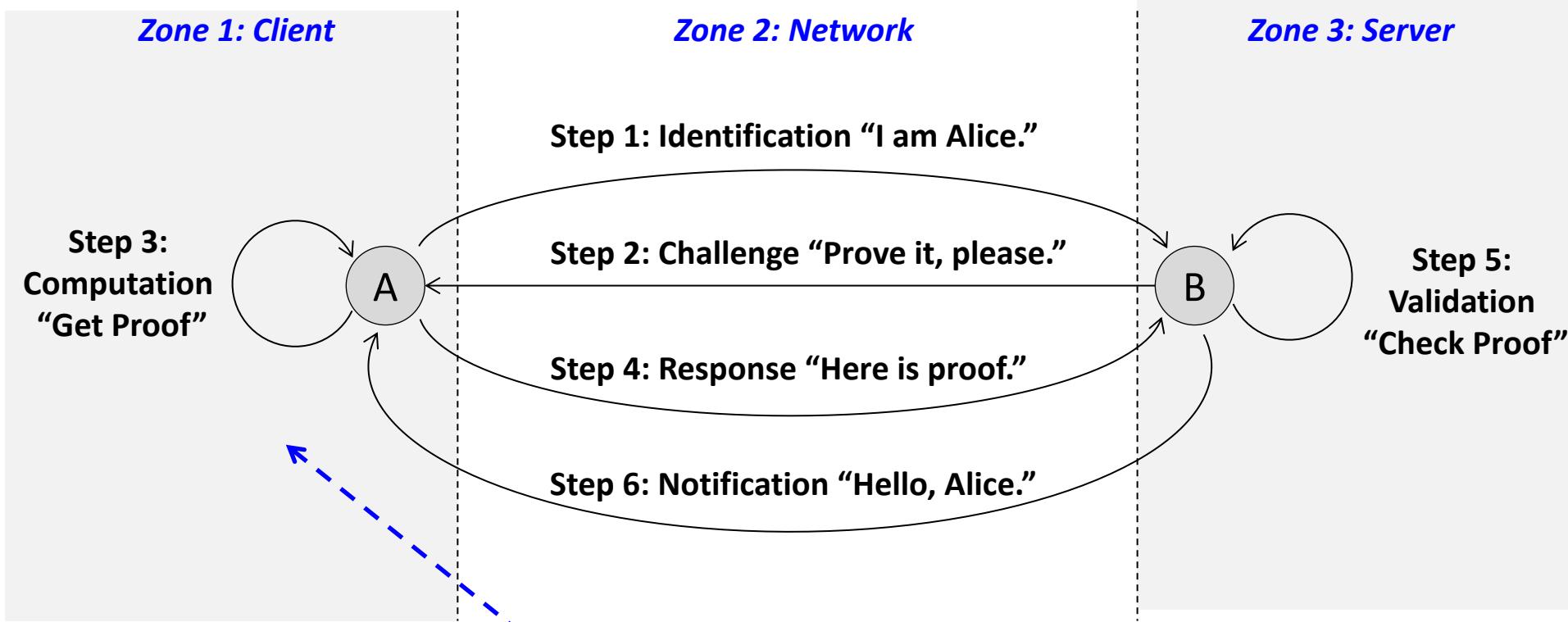


Authentication Schema



Eve is the
Attacker

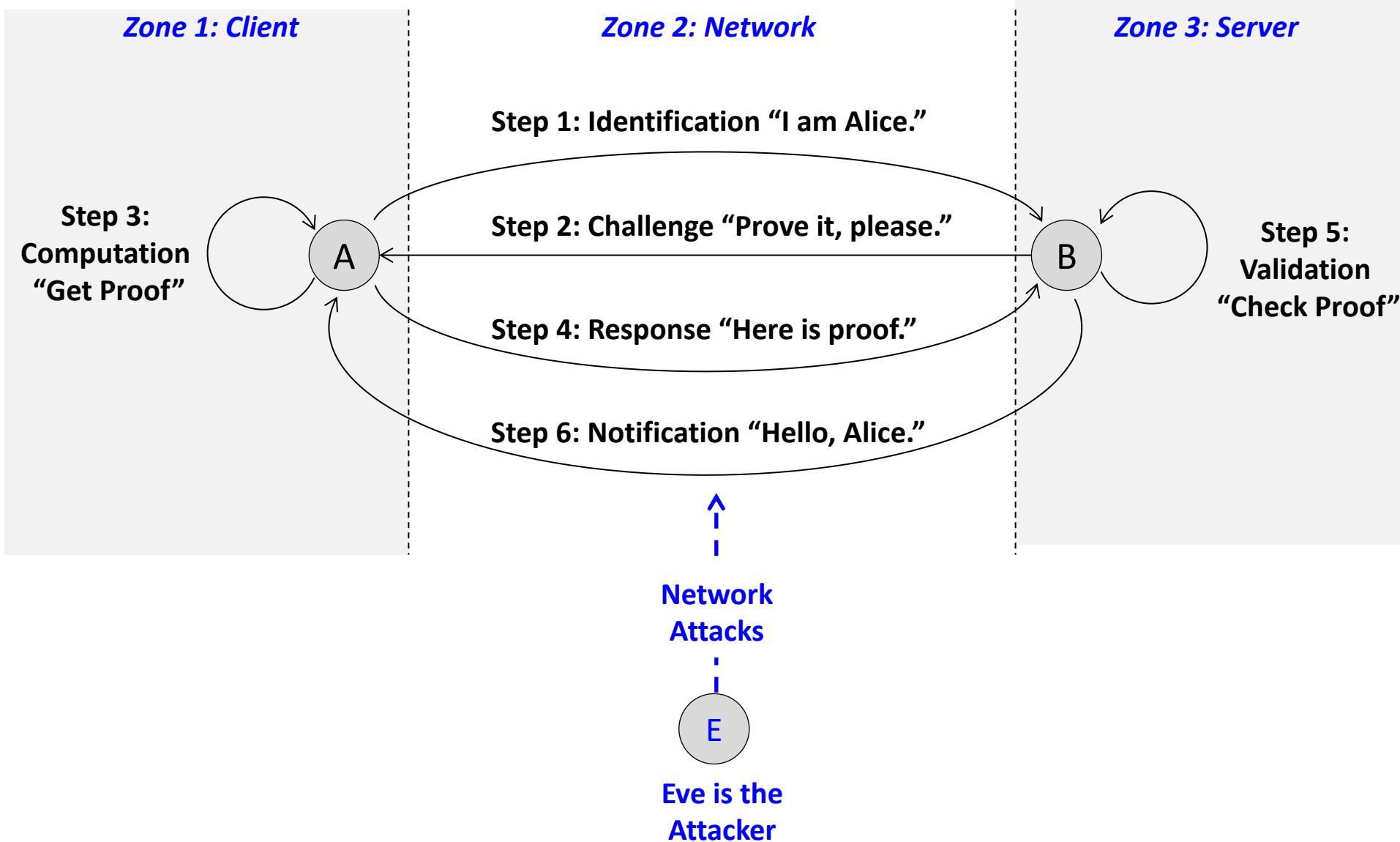
Authentication Schema



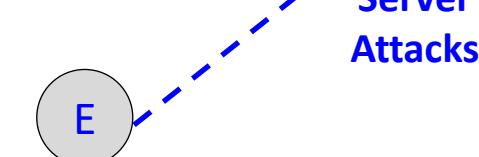
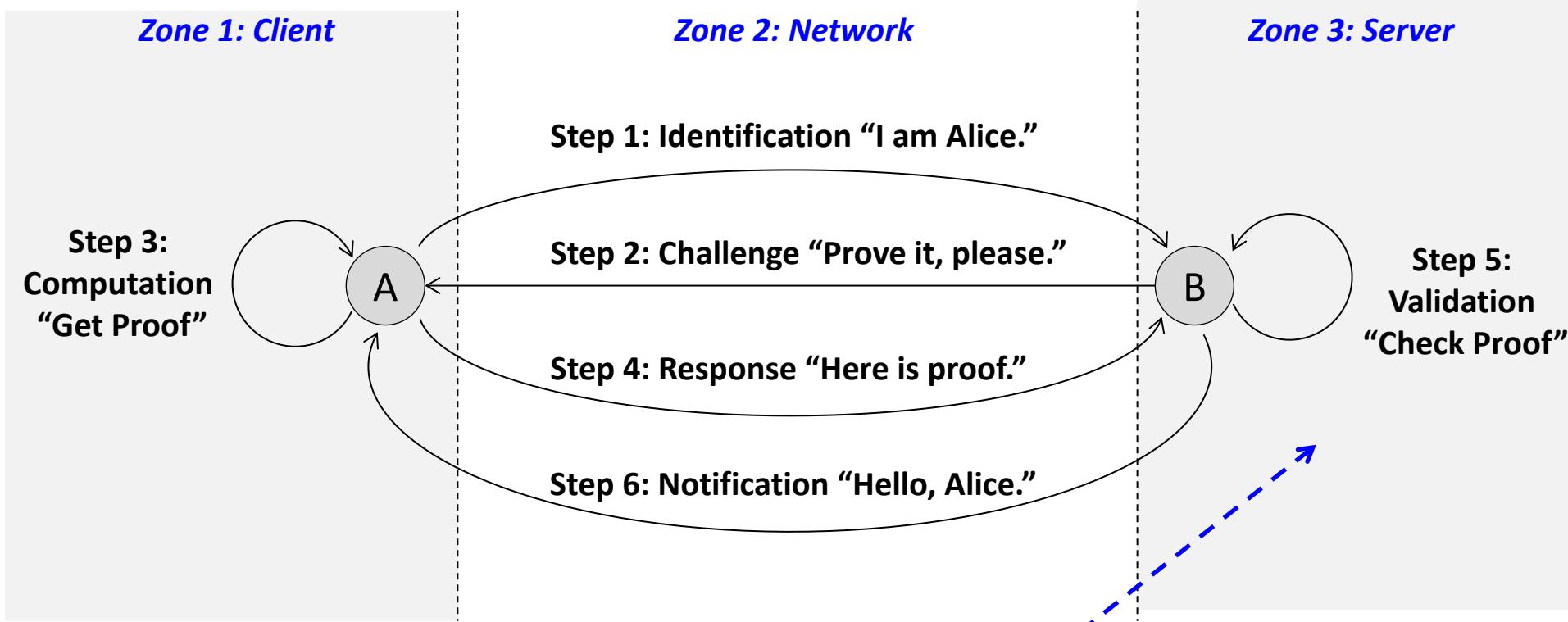
Client
Attacks

Eve is the
Attacker

Authentication Schema



Authentication Schema



Eve is the
Attacker

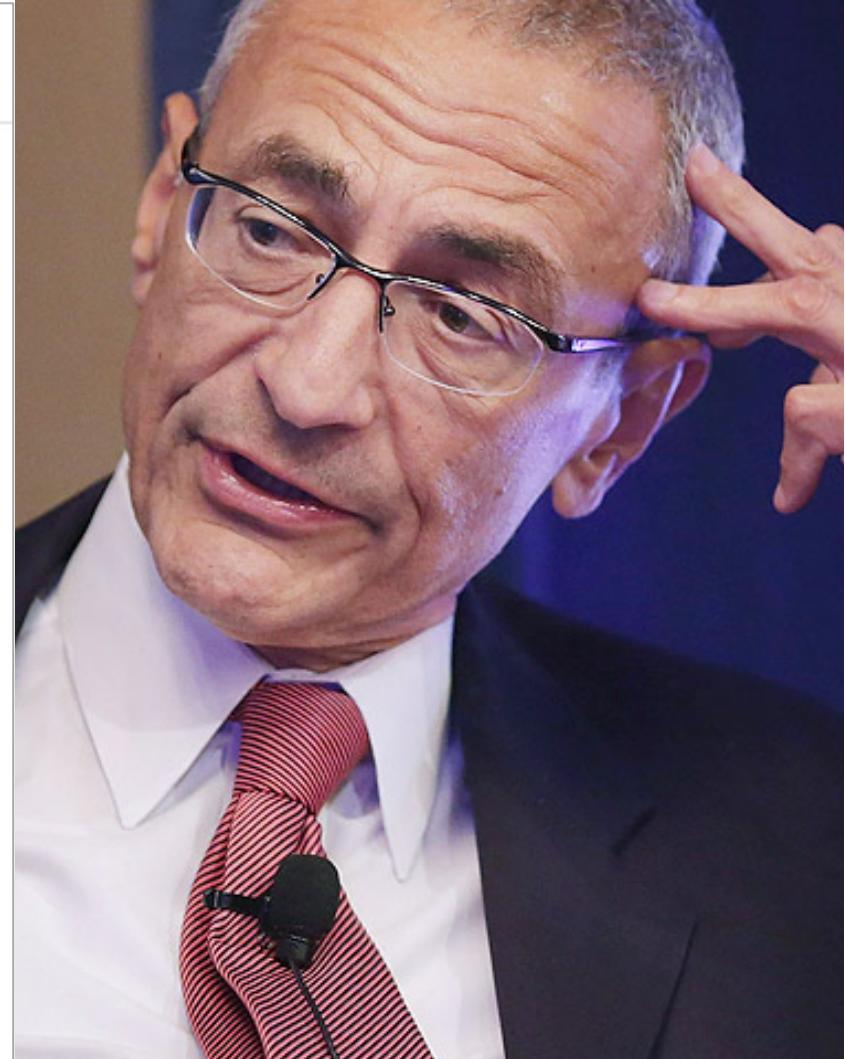
Are Passwords Acceptable for Authentication?

Password-Related Incident: Democratic National Committee 2016



Leaks News About Partners

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* john.podesta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
```



Password-Related Incident: Colonial Pipeline Ransomware 2021

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By [William Turton](#) and [Kartikay Mehrotra](#)

June 4, 2021, 3:58 PM EDT

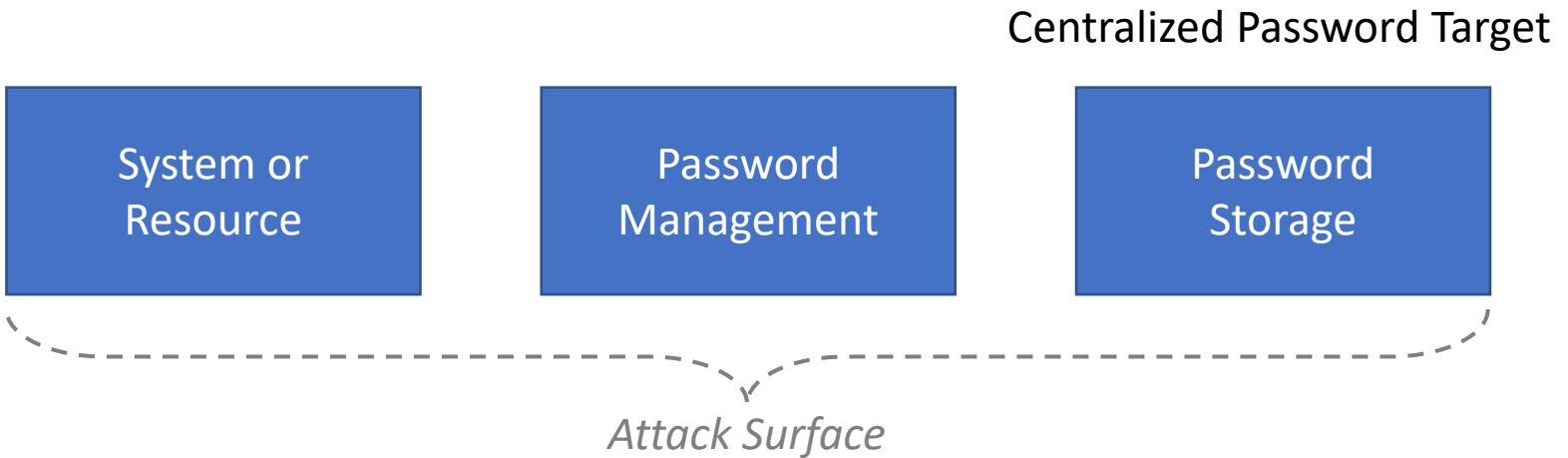
The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked, he said. However, Carmakal said he isn't certain that's how hackers obtained the password, and he said investigators may never know for certain how the credential was obtained.

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

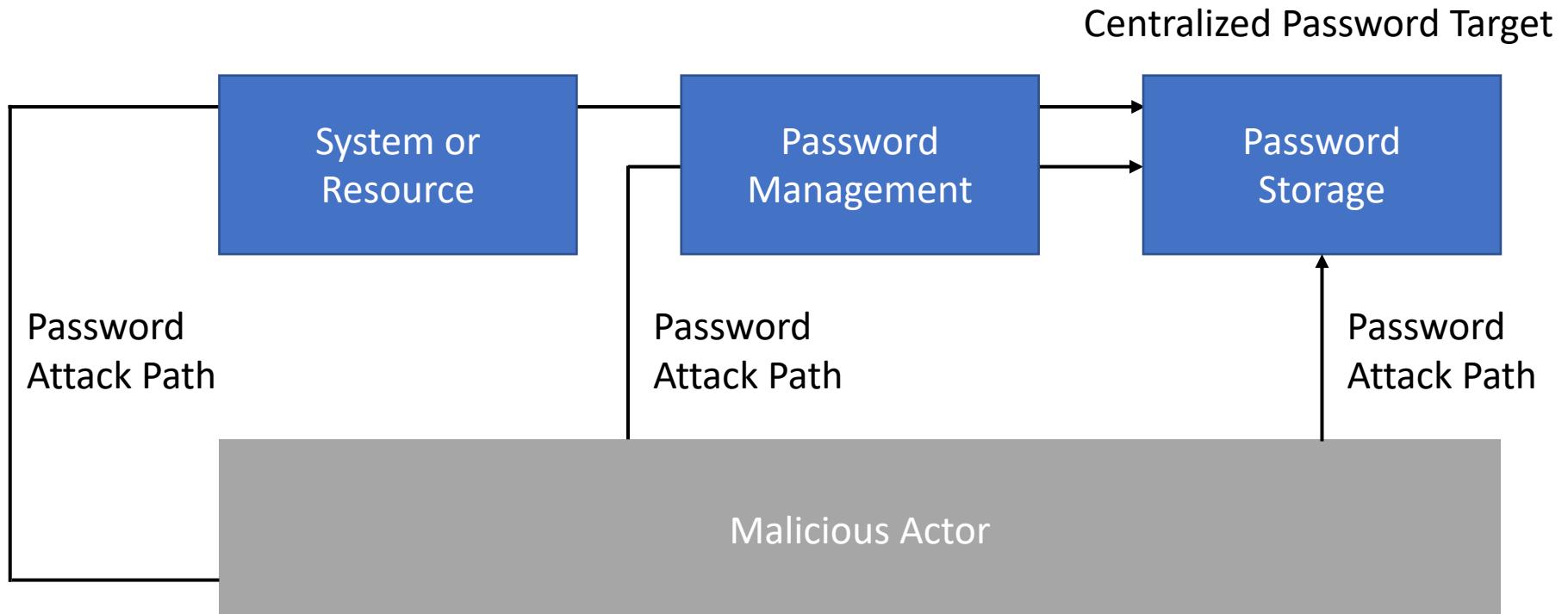
Hackers gained entry into the networks of [Colonial Pipeline Co.](#) on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm [Mandiant](#), part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said.



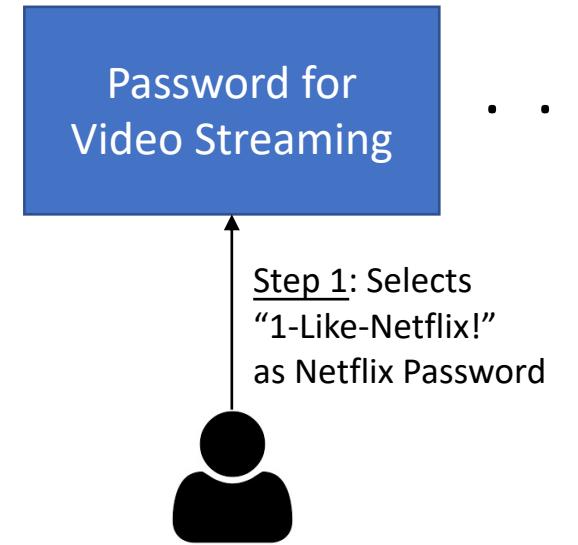
Inherent Threat of Password Repositories



Inherent Threat of Password Repositories



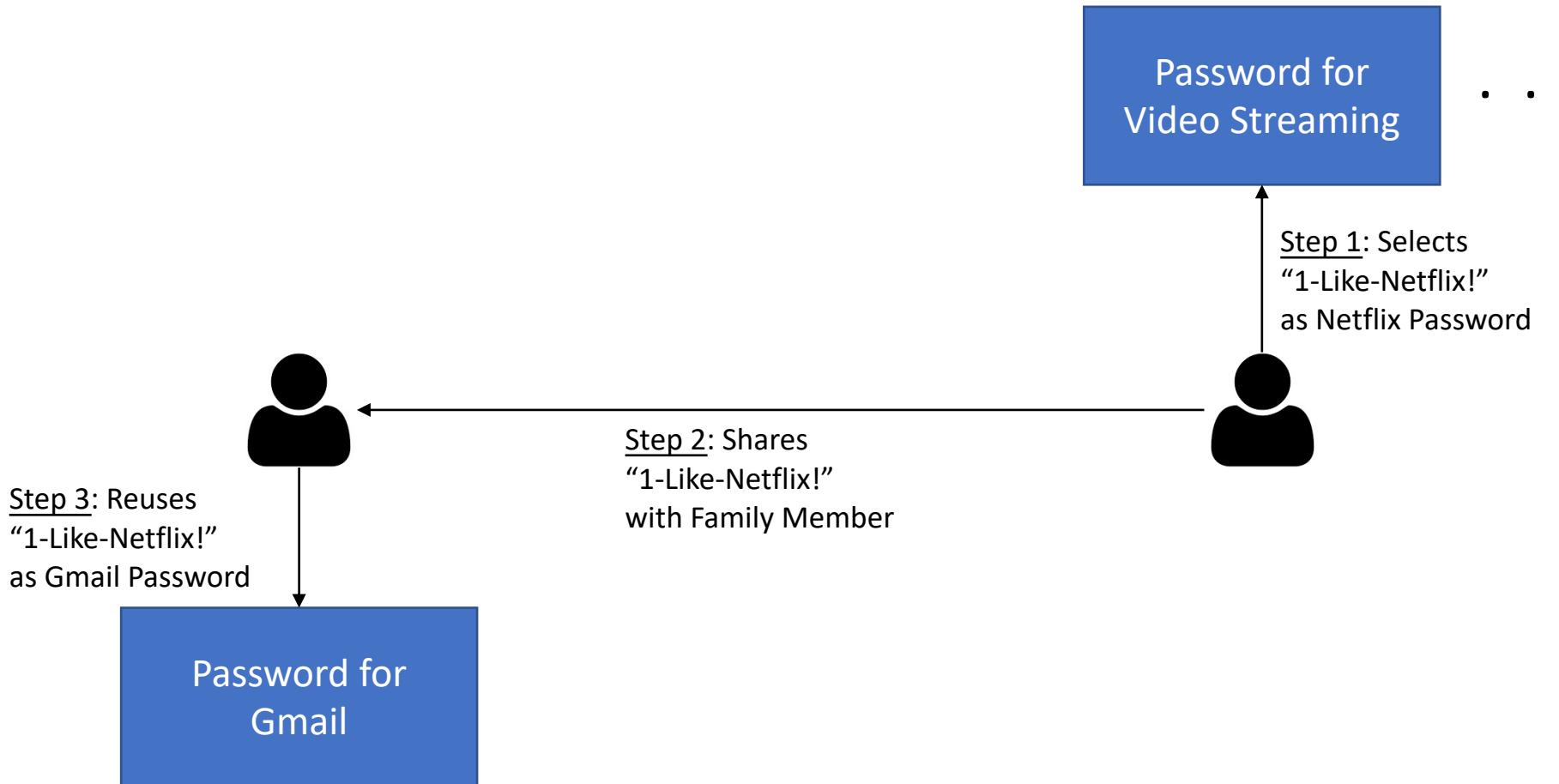
Inherent Threat of Password Reuse



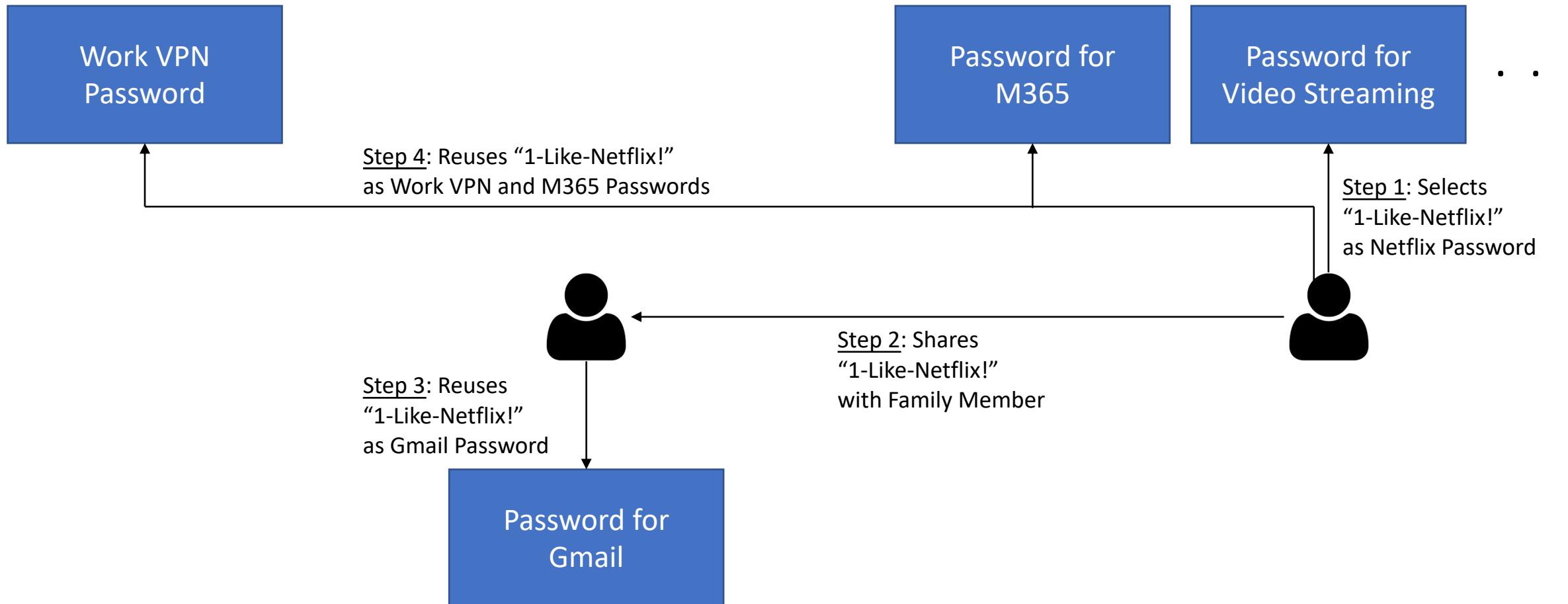
Inherent Threat of Password Reuse



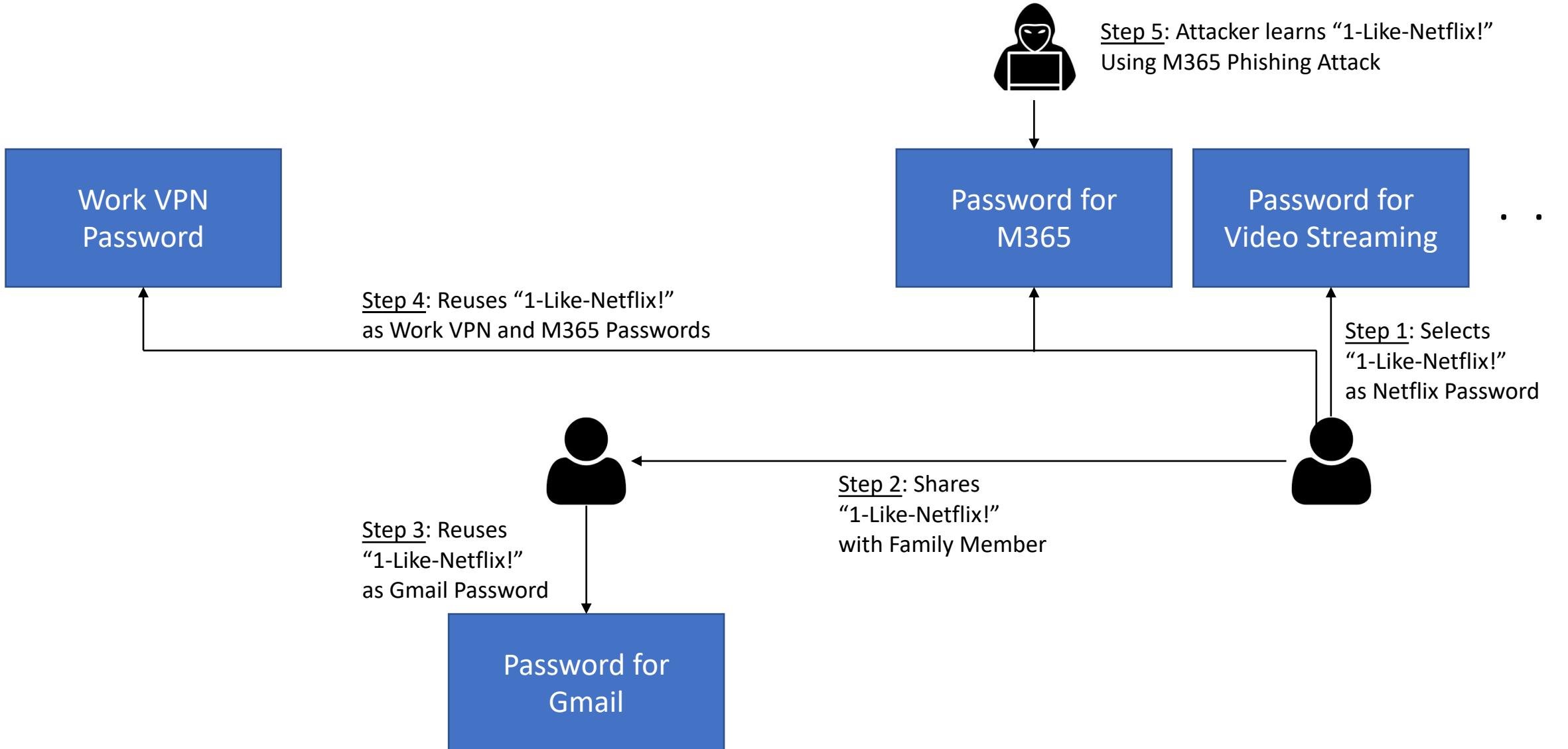
Inherent Threat of Password Reuse



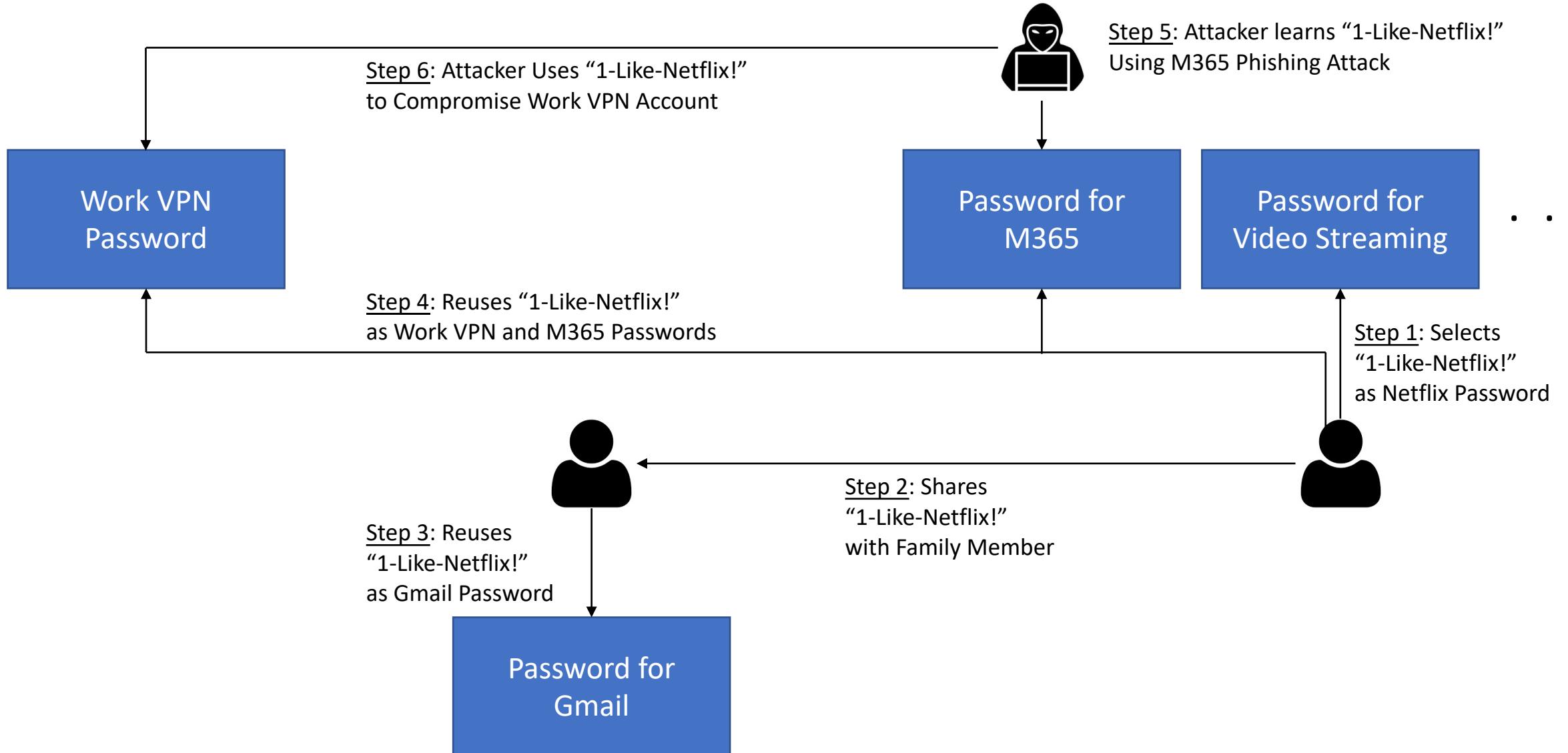
Inherent Threat of Password Reuse



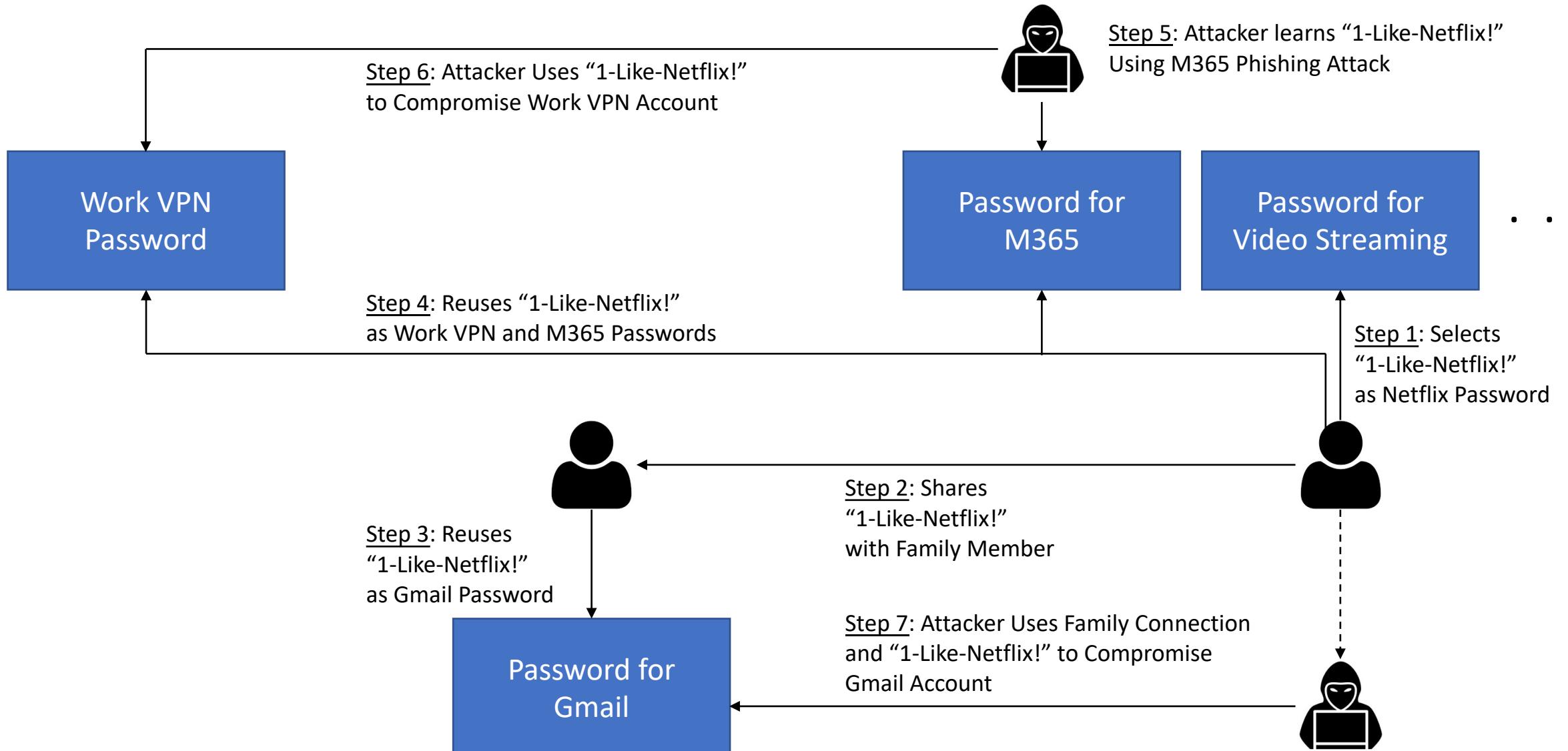
Inherent Threat of Password Reuse



Inherent Threat of Password Reuse



Inherent Threat of Password Reuse



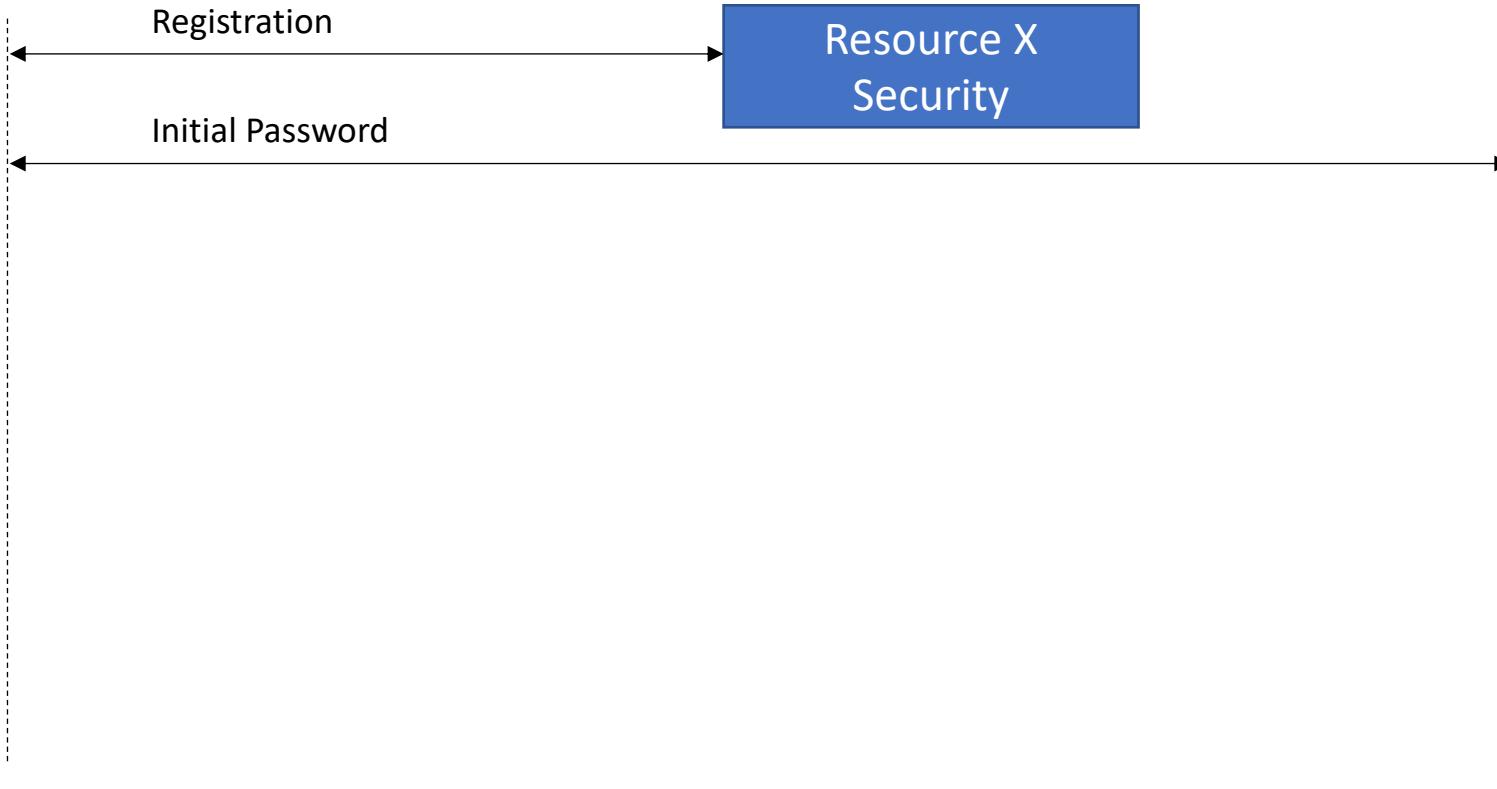
Inherent Friction from Password Usage



Friction:
Process, Help Desk,
Accessibility, etc.

Resource X

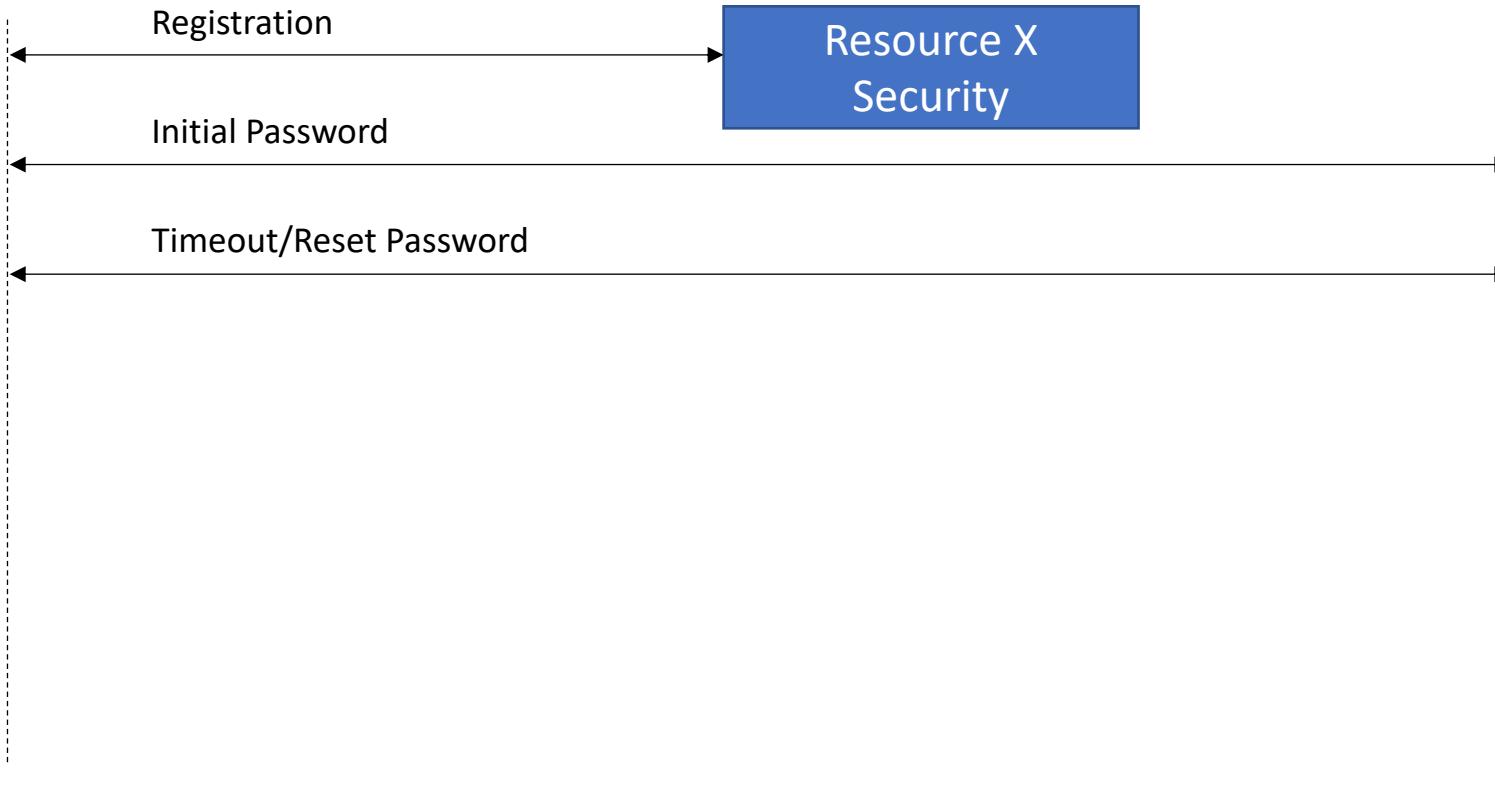
Inherent Friction from Password Usage



Friction:
Machine Generated,
User Selected, etc.

Resource X

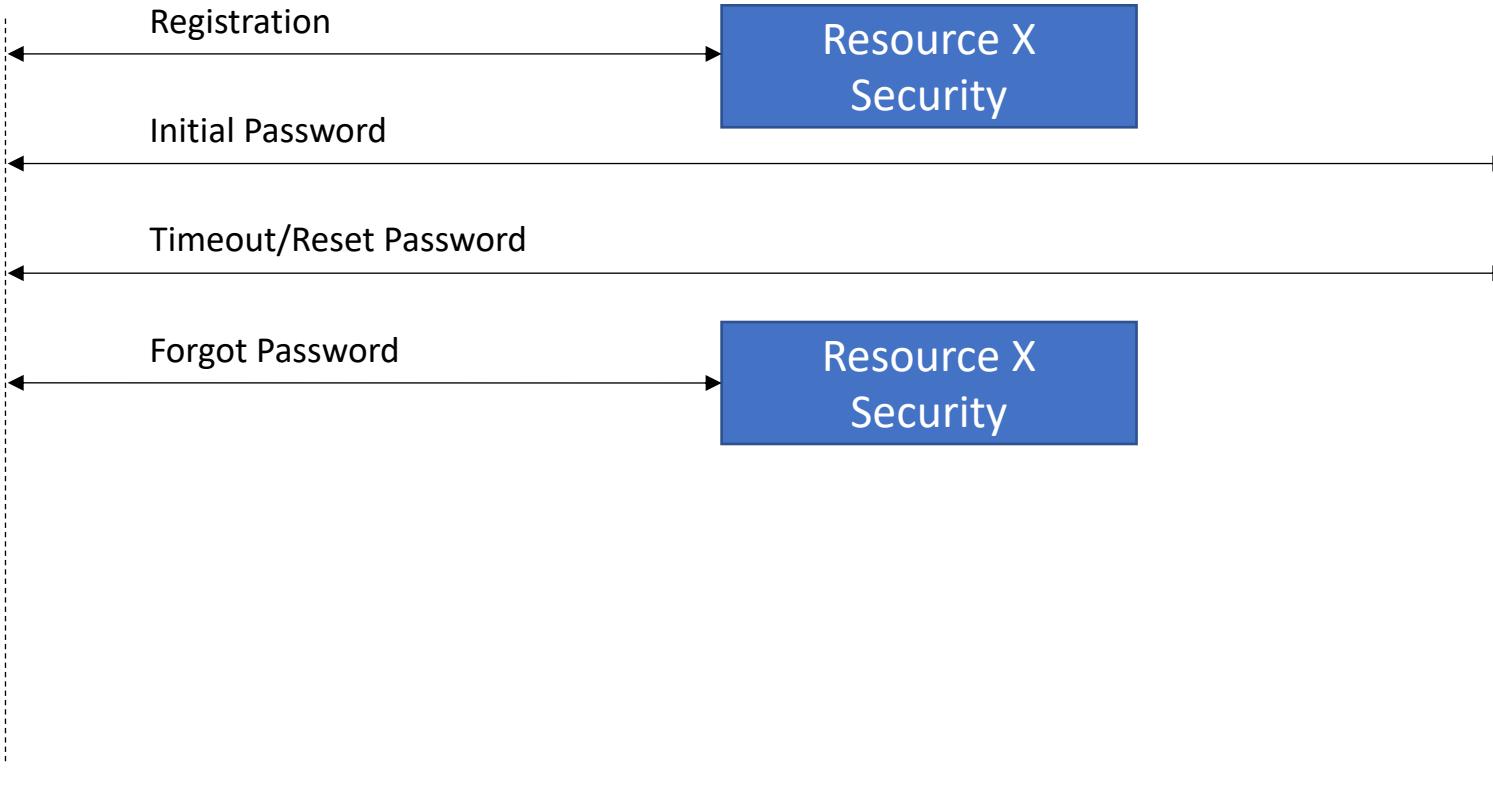
Inherent Friction from Password Usage



Friction:
Blocked Resource,
Frustration, etc.

Resource X

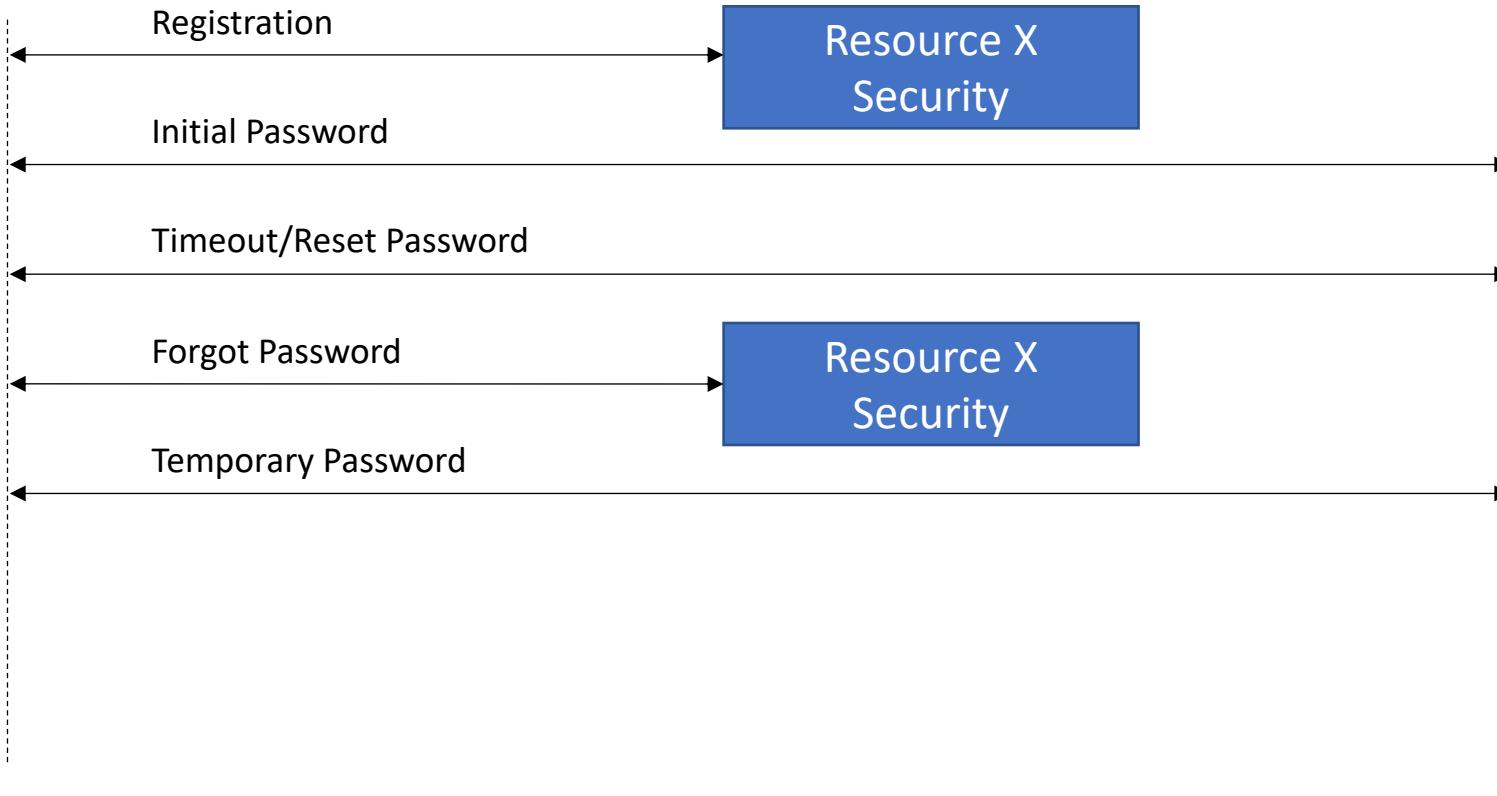
Inherent Friction from Password Usage



Friction:
Annoyance,
Frustration, etc.



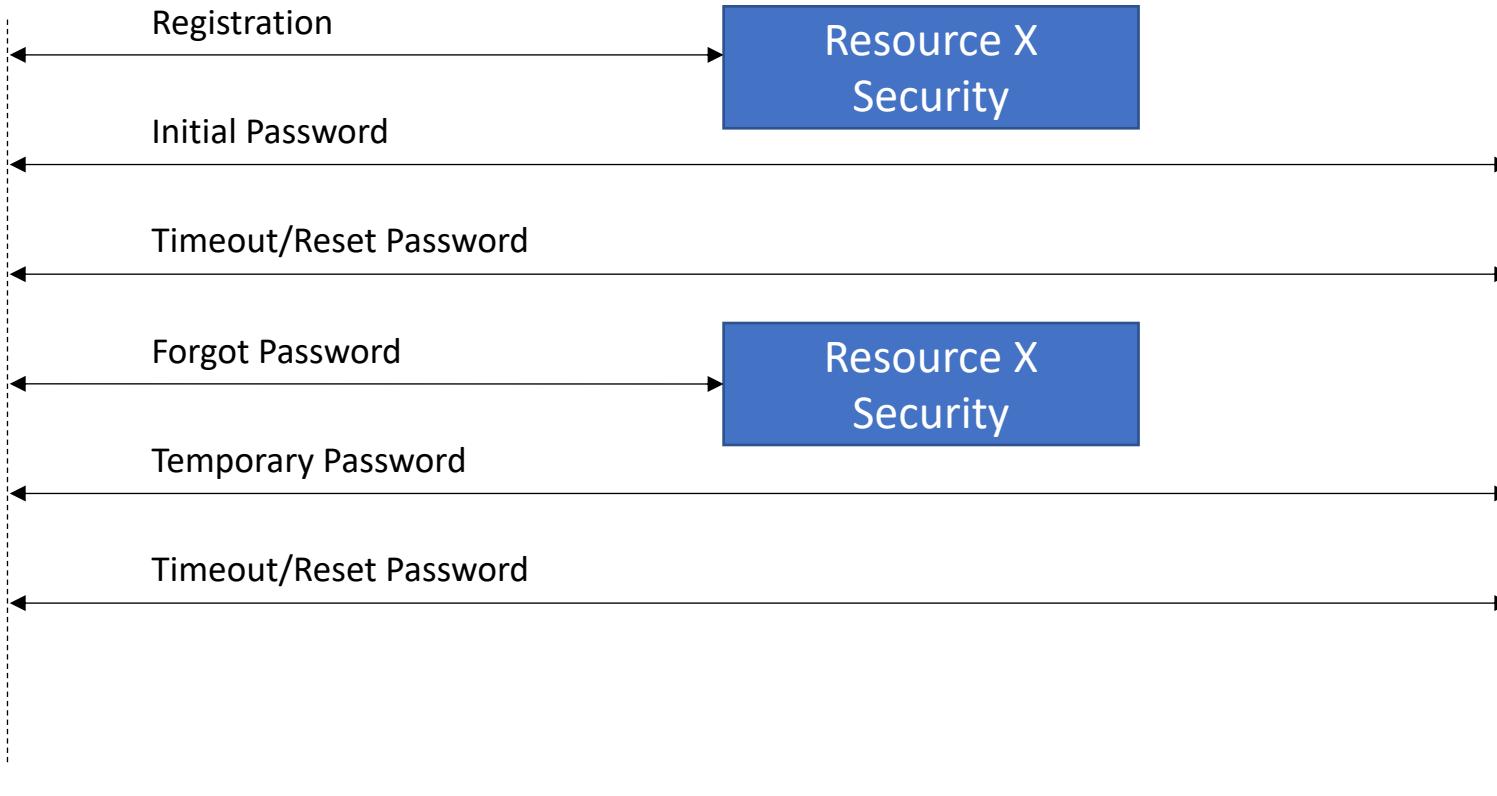
Inherent Friction from Password Usage



Friction:
Inconvenience,
New Password, etc.

Resource X

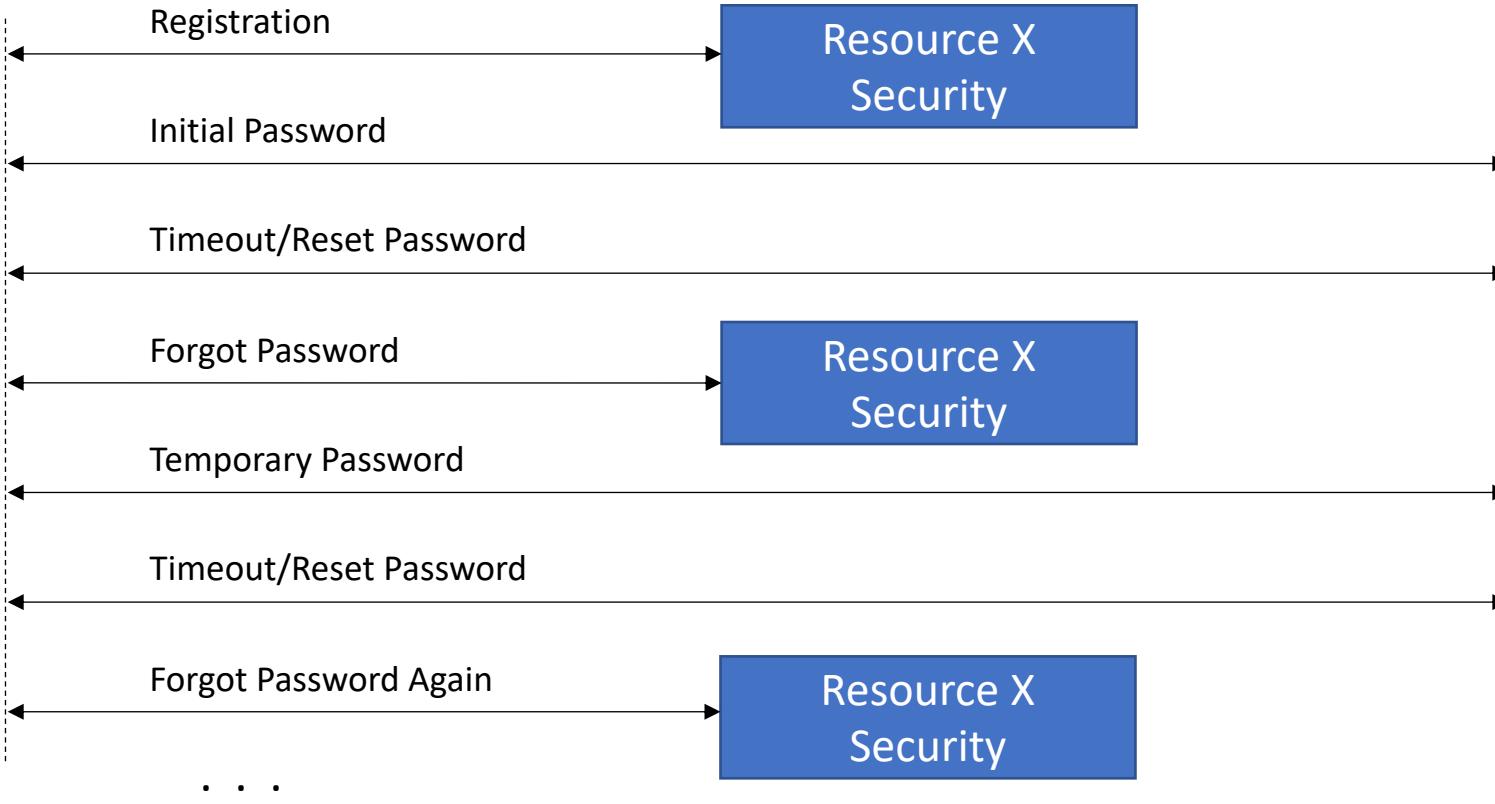
Inherent Friction from Password Usage



Friction:
Blocked Resource,
More Frustration, etc.

Resource X

Inherent Friction from Password Usage

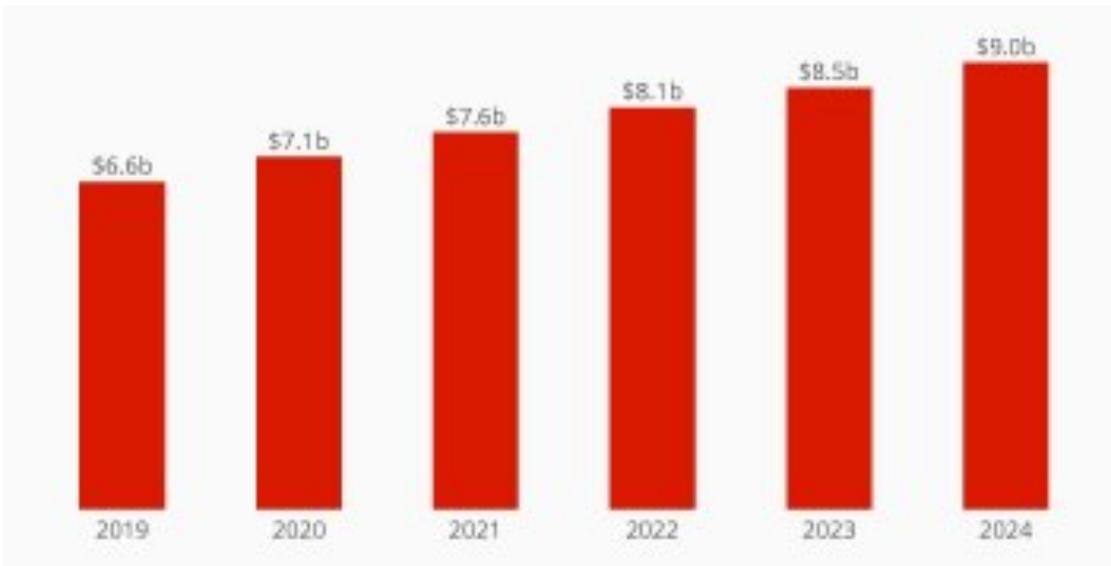


Friction:
Annoyance,
Frustration, etc.



Password Issues with Smart TV/Streaming Channels

Estimated Revenue Losses for US Pay TV Industry from Piracy and Account Sharing



Source: Statista

<https://www.statista.com/chart/19914/estimated-revenue-loss-for-the-us-pay-tv-industry-from-piracy-and-account-sharing/>



How Did Handheld Authenticators Work?

Handheld Authentication Device

A

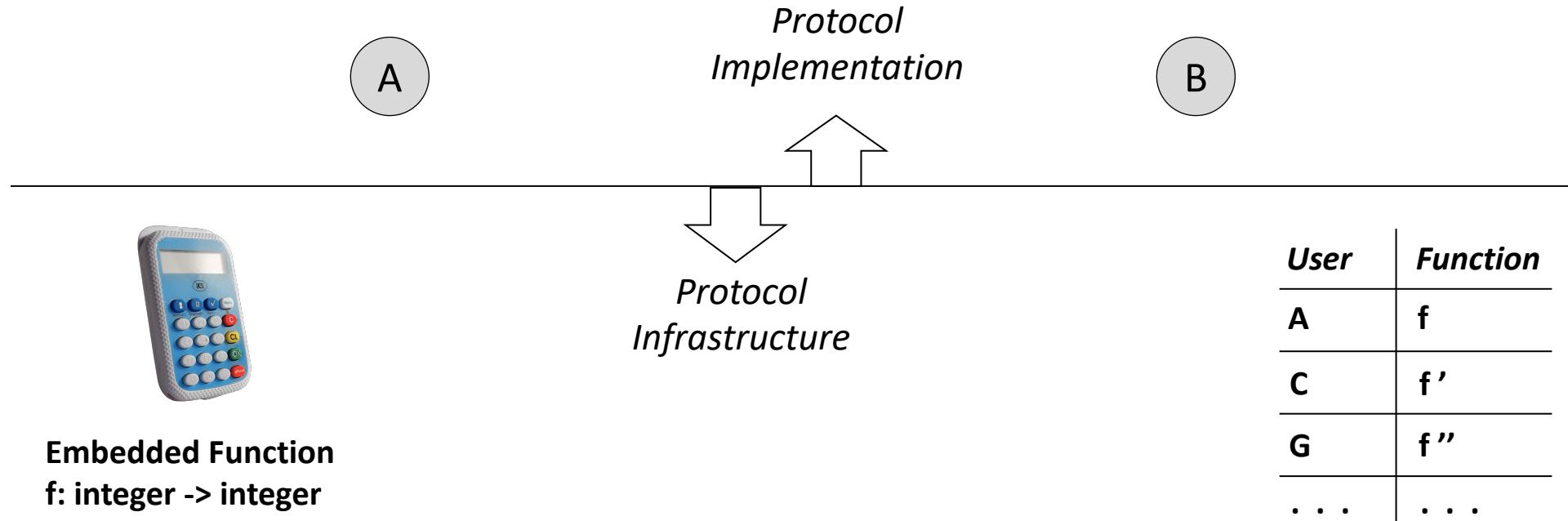


Embedded Function
 $f: \text{integer} \rightarrow \text{integer}$

B

User	Function
A	f
C	f'
G	f''
...	...

Handheld Authentication Device



Handheld Authentication Device

Step 1: I am Alice

A

B



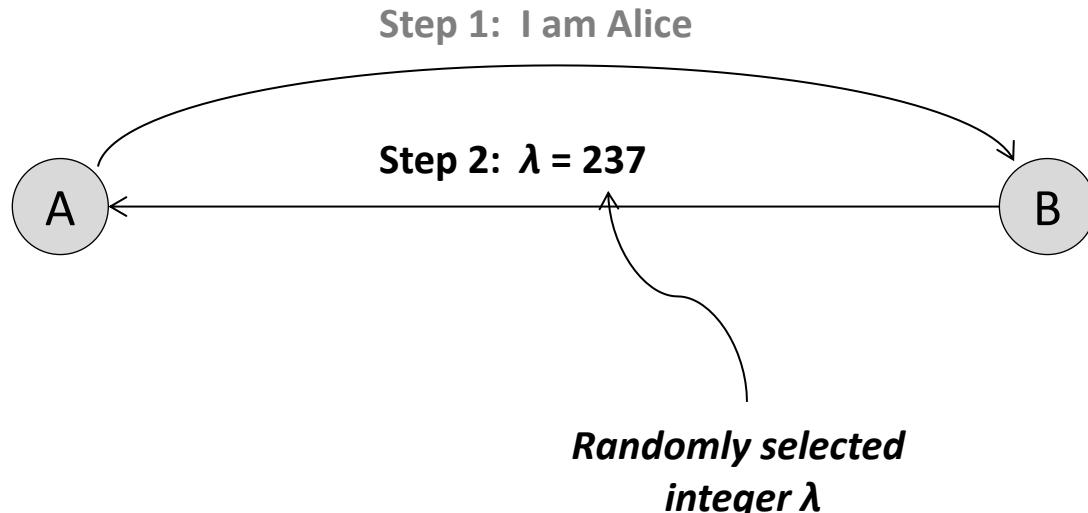
Embedded Function
 $f: \text{integer} \rightarrow \text{integer}$

User	Function
A	f
C	f'
G	f''
...	...

Handheld Authentication Device

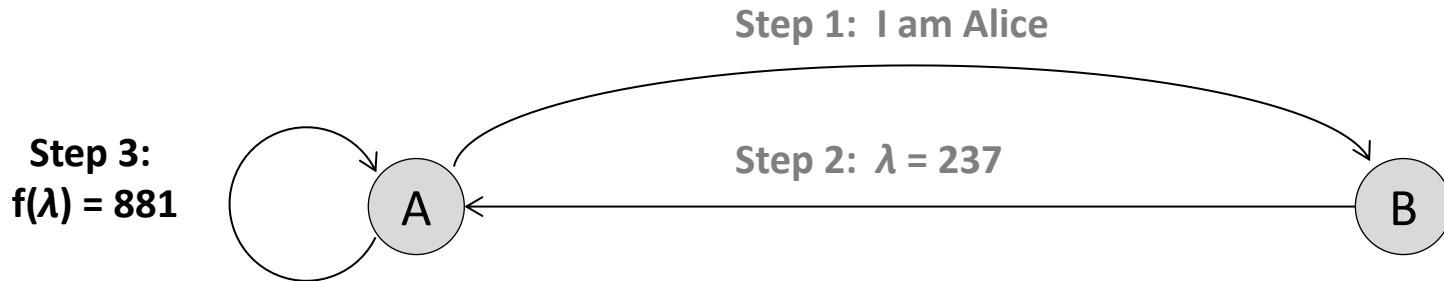


Embedded Function
 $f: \text{integer} \rightarrow \text{integer}$



User	Function
A	f
C	f'
G	f''
...	...

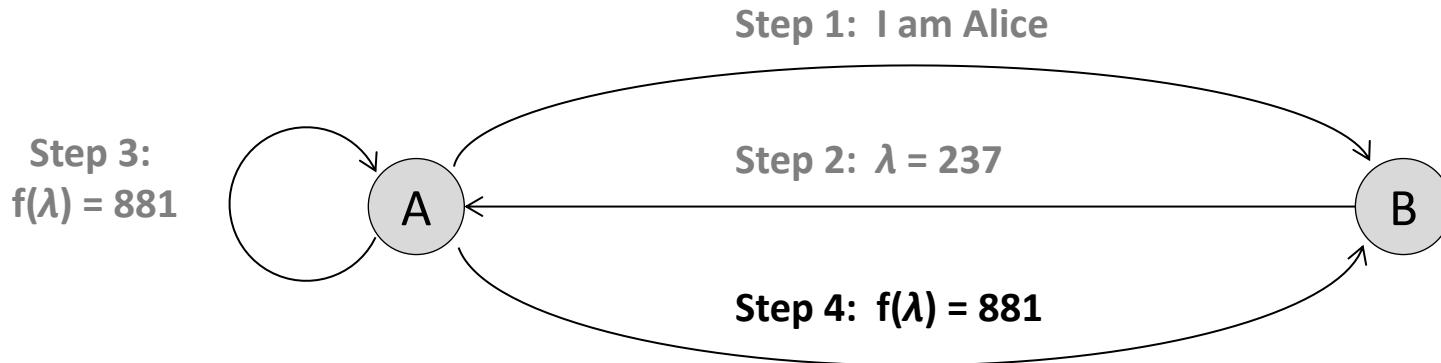
Handheld Authentication Device



Embedded Function
 $f: \text{integer} \rightarrow \text{integer}$

User	Function
A	f
C	f'
G	f''
...	...

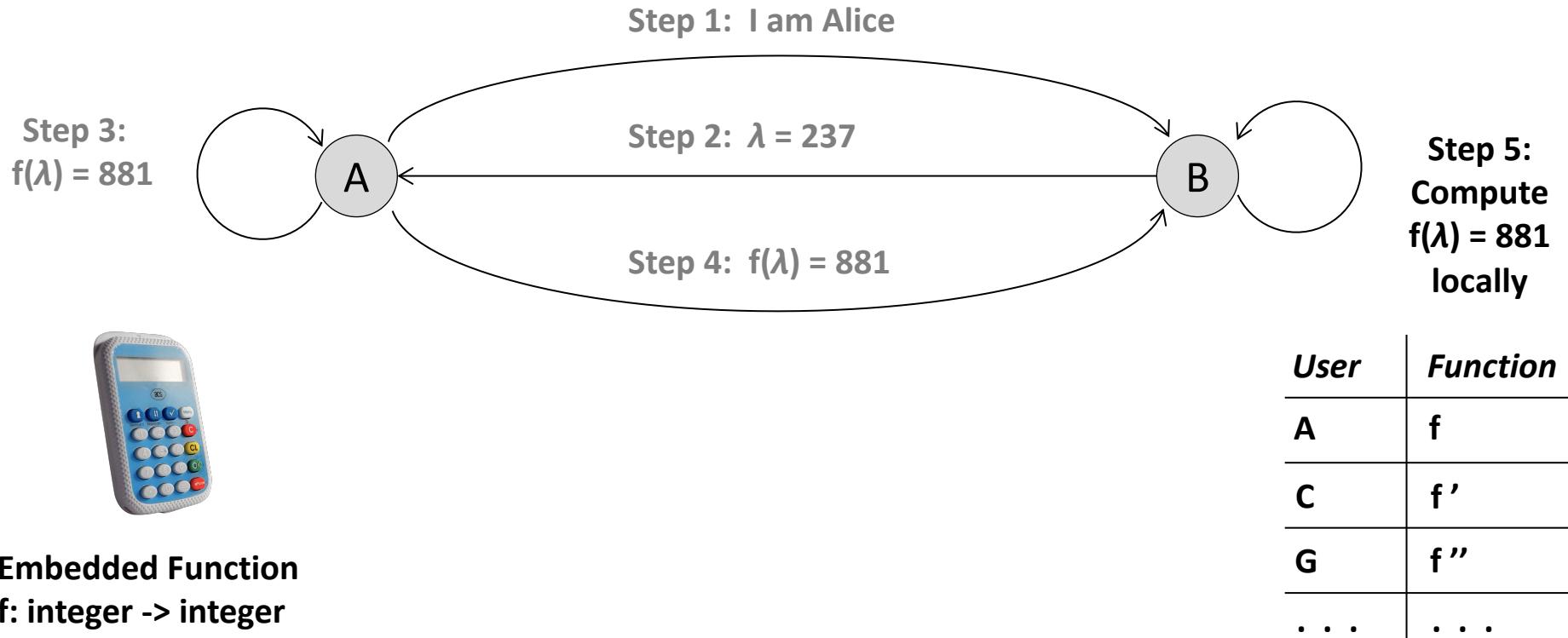
Handheld Authentication Device



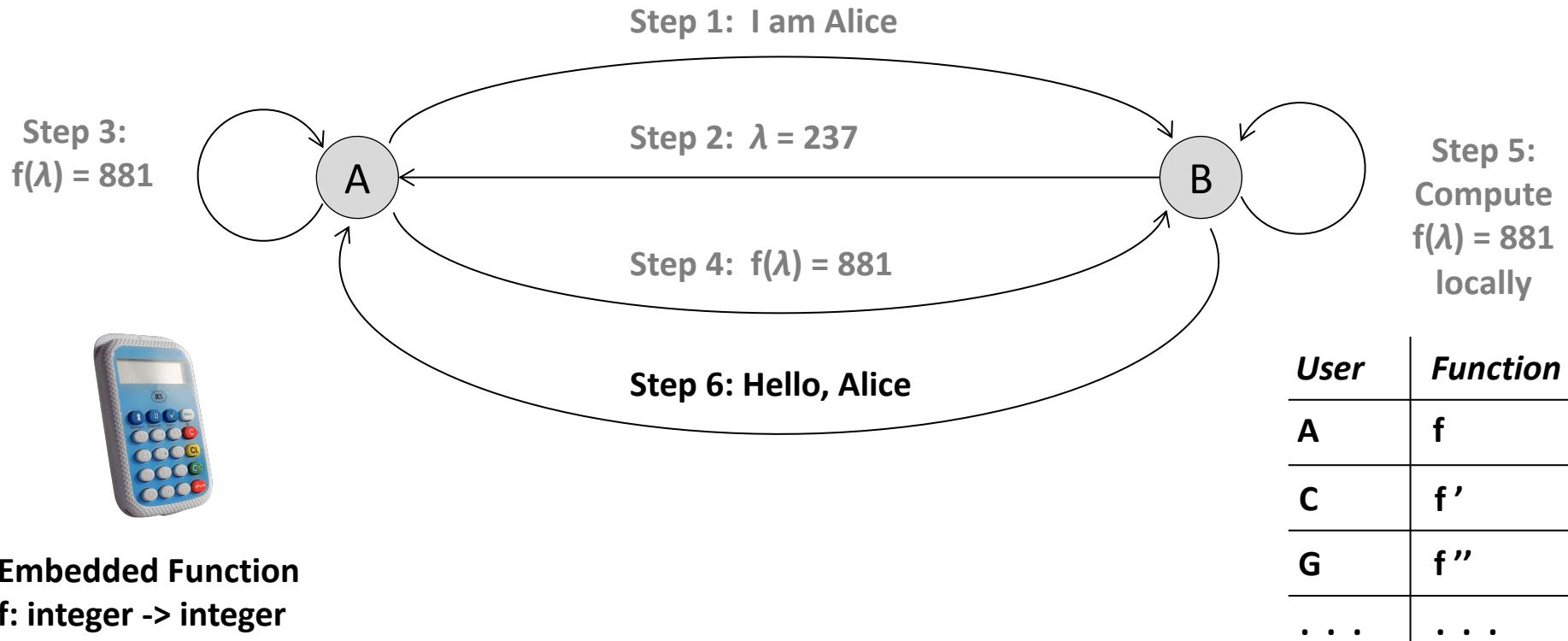
Embedded Function
 $f: \text{integer} \rightarrow \text{integer}$

User	Function
A	f
C	f'
G	f''
...	...

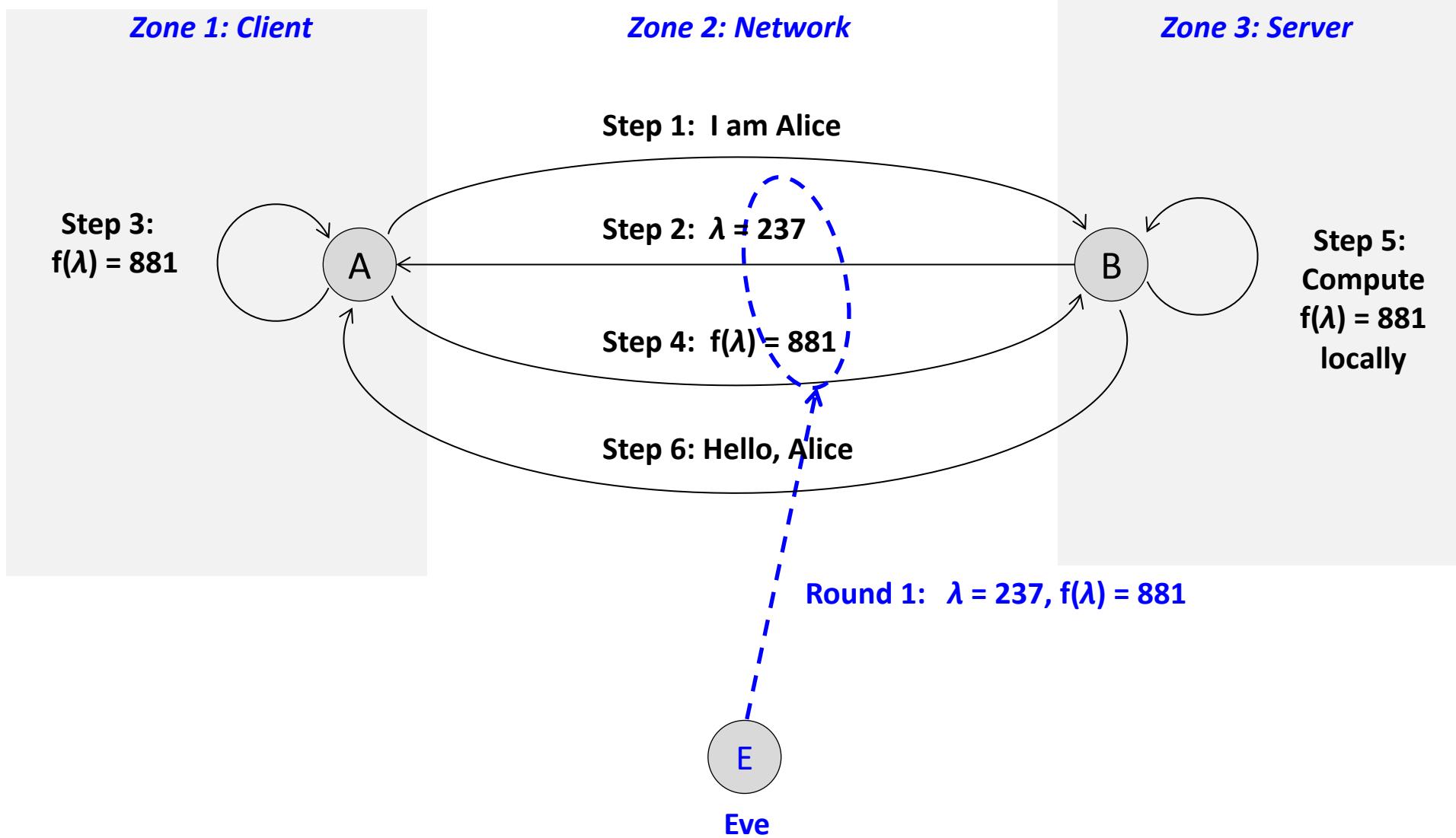
Handheld Authentication Device



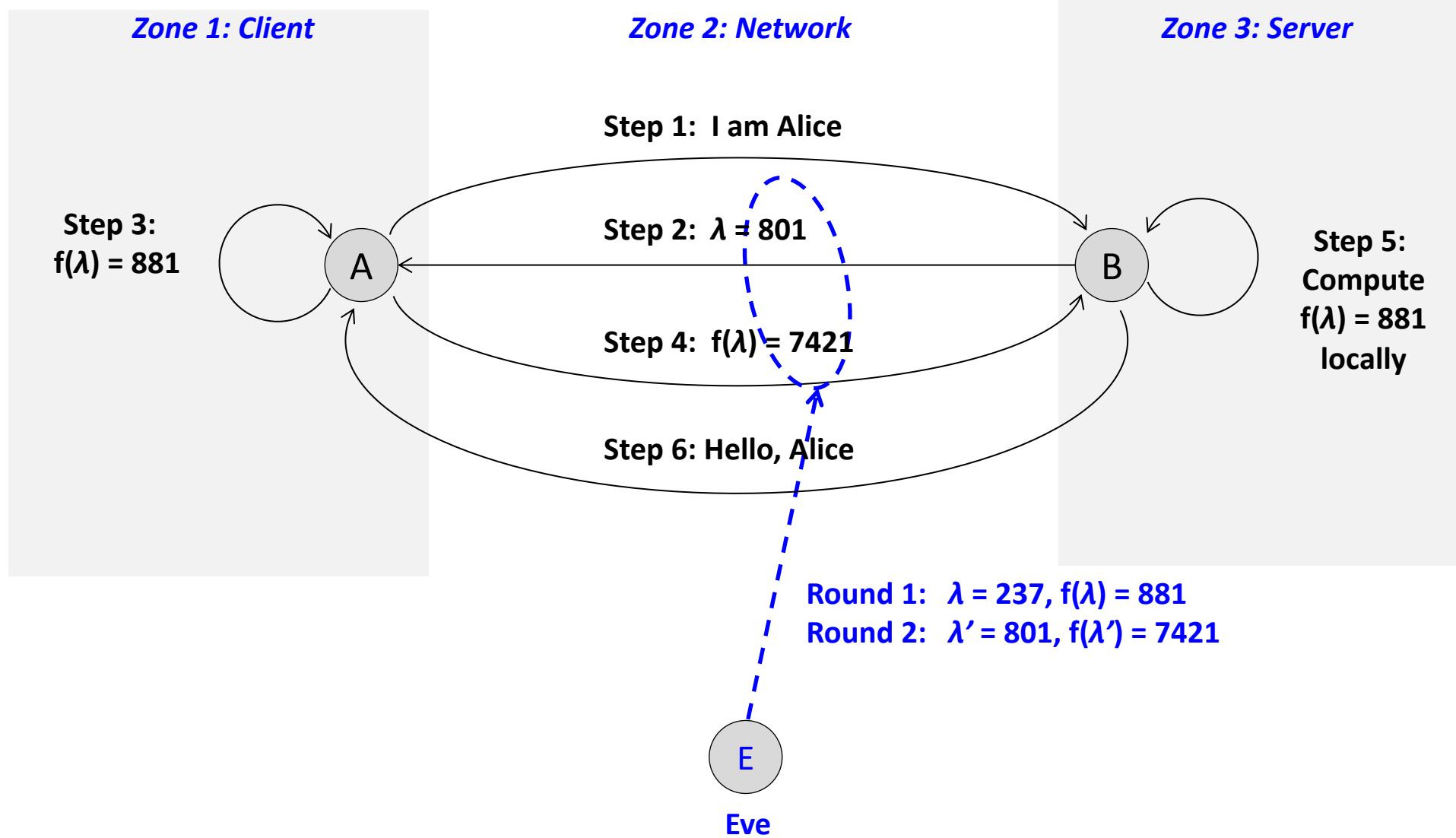
Handheld Authentication Device



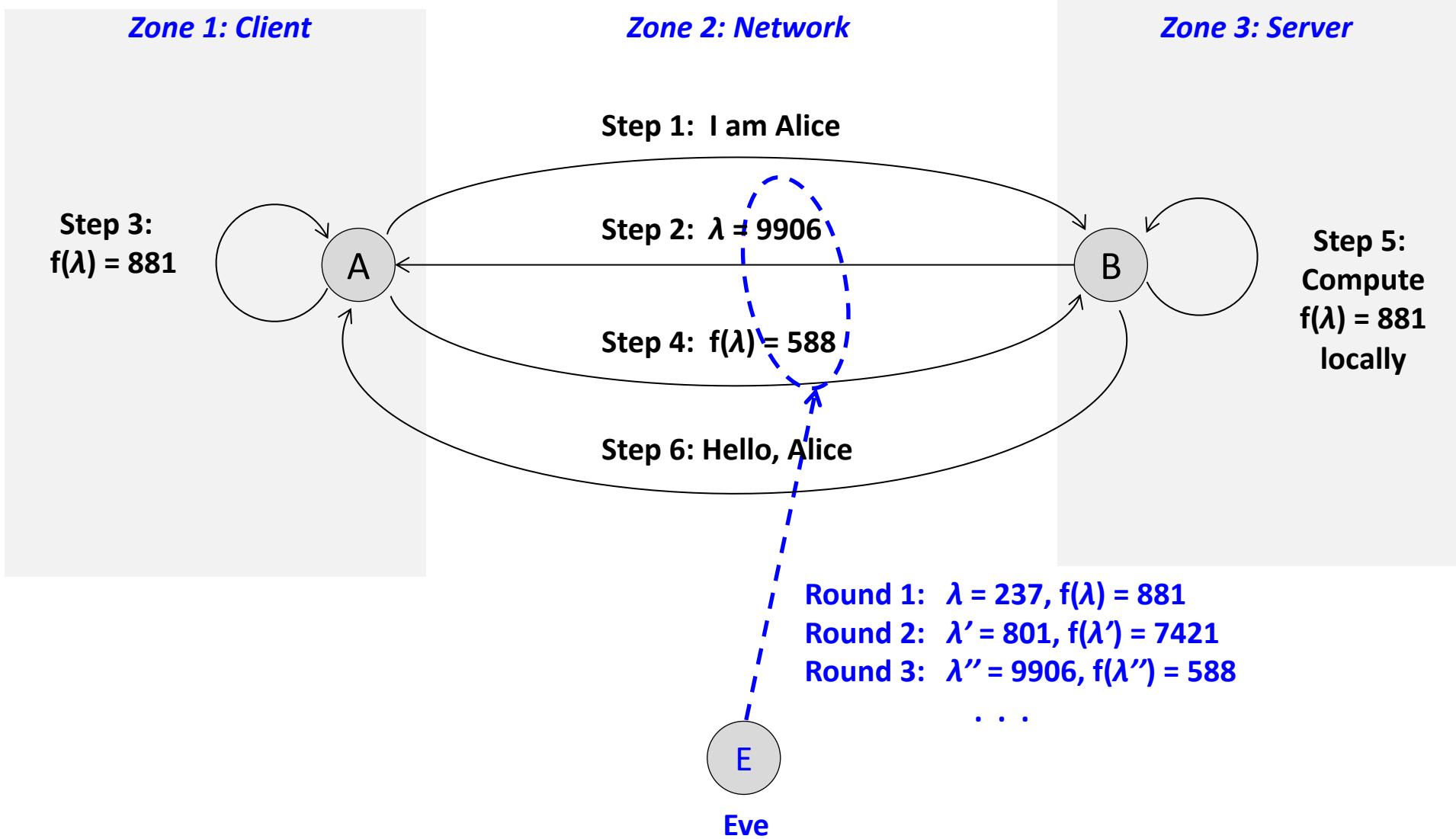
Handheld Authentication Device Protocol



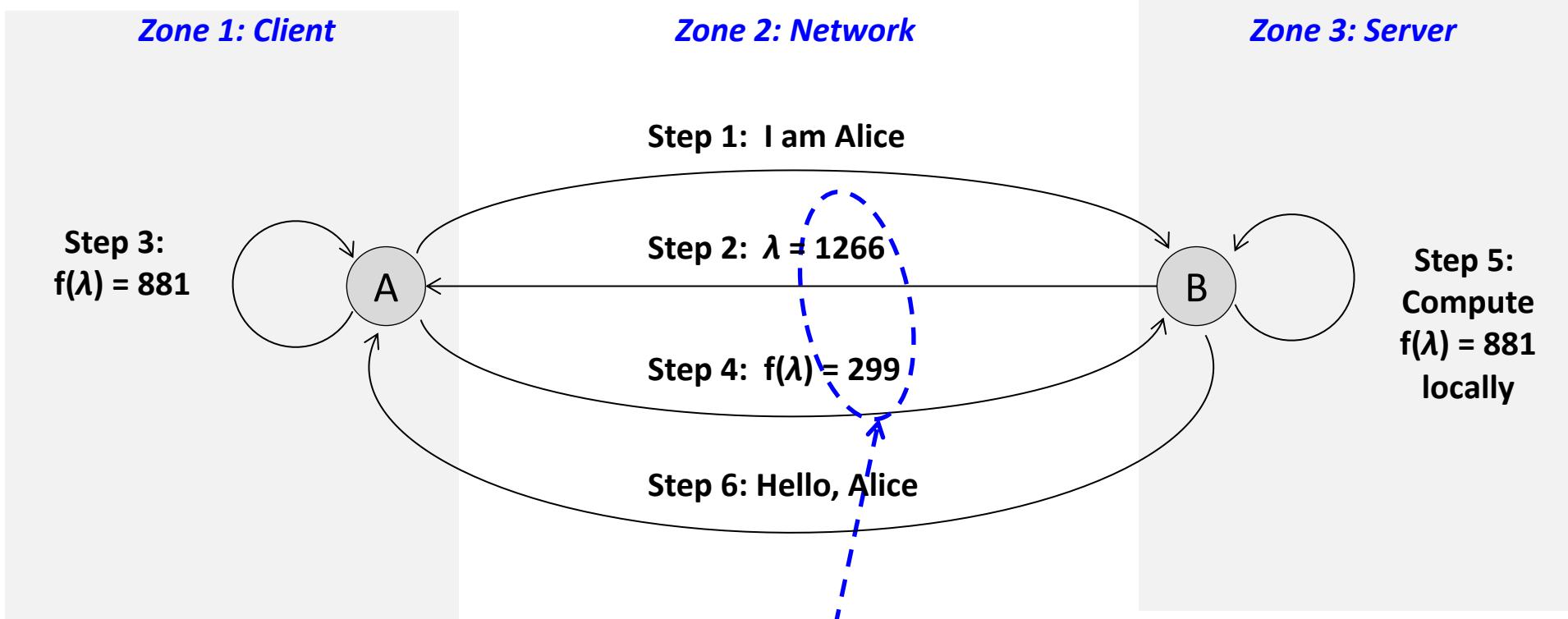
Handheld Authentication Device Protocol



Handheld Authentication Device Protocol



Handheld Authentication Device Protocol



How Does RSA SecureID OTP Work?

RSA SecurID One-Time Password (OTP) Algorithm



f : integer \rightarrow integer

λ : integer seed

t_0 : initial time

t_c : current time

Δt : time interval

$$n = (t_c - t_0) / \Delta t$$



RSA SecurID One-Time Password (OTP) Algorithm



f : integer \rightarrow integer

λ : integer seed

t_0 : initial time

t_c : current time

Δt : time interval

$n = (t_c - t_0) / \Delta t$

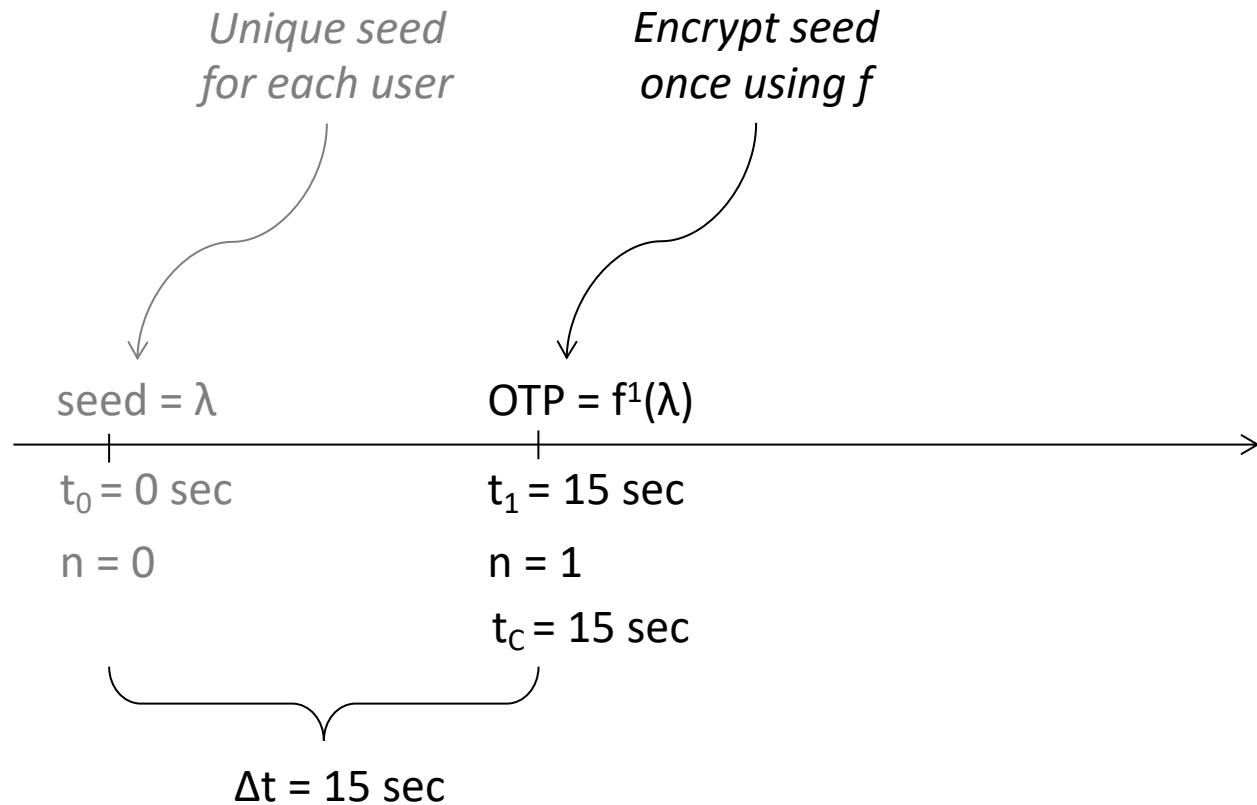
*Unique seed
for each user*



RSA SecurID One-Time Password (OTP) Algorithm



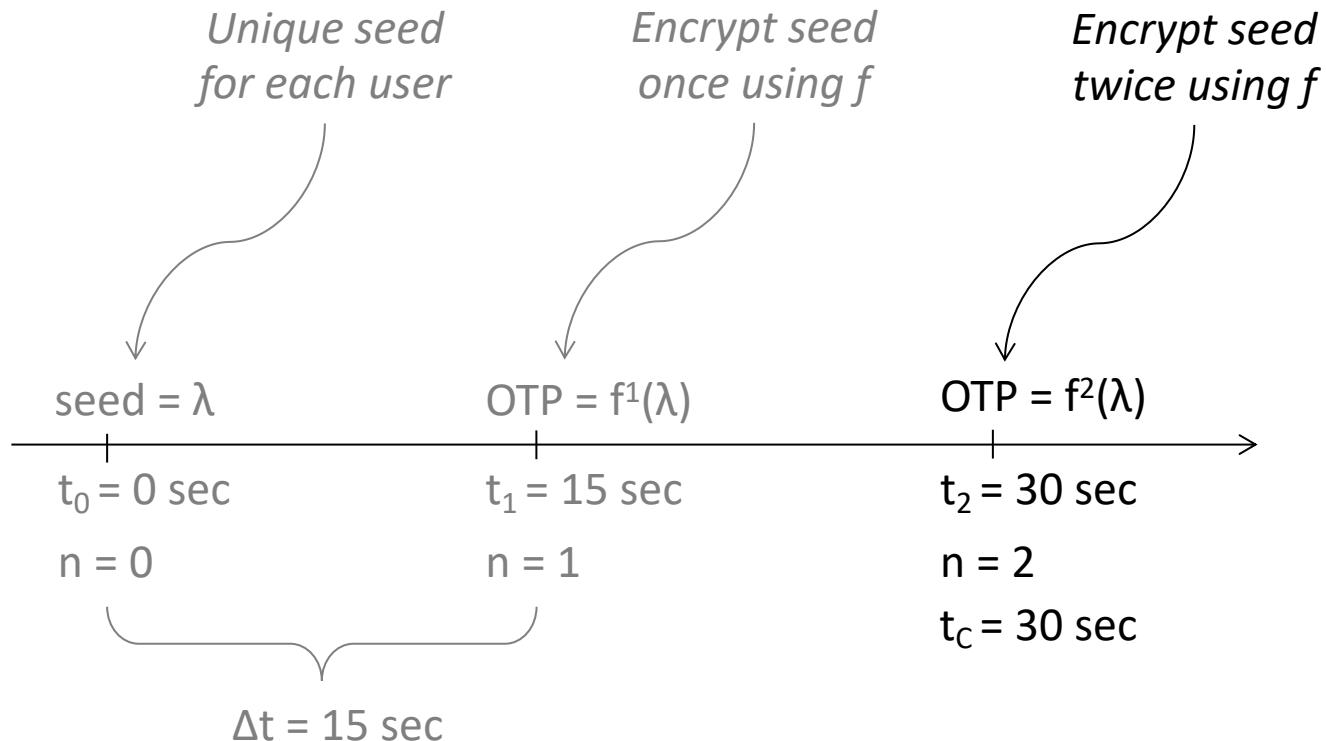
f : integer \rightarrow integer
 λ : integer seed
 t_0 : initial time
 t_c : current time
 Δt : time interval
 $n = (t_c - t_0) / \Delta t$



RSA SecurID One-Time Password (OTP) Algorithm



f : integer \rightarrow integer
 λ : integer seed
 t_0 : initial time
 t_c : current time
 Δt : time interval
 $n = (t_c - t_0) / \Delta t$



RSA SecurID Protocol

Step 1: I am Alice

A

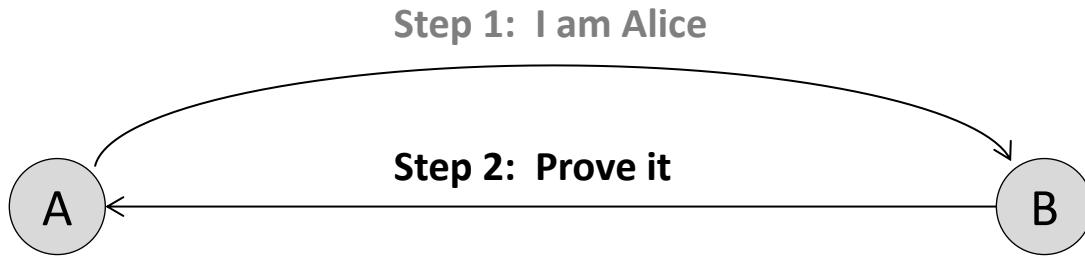
B



f: integer \rightarrow integer
 λ : integer seed
 t_0 : initial time
 t_c : current time
 Δt : time interval
 $n = (t_c - t_0) / \Delta t$

User	Information
A	f: integer \rightarrow integer λ : integer seed t_0 : initial time t_c : current time Δt : time interval $n = (t_c - t_0) / \Delta t$

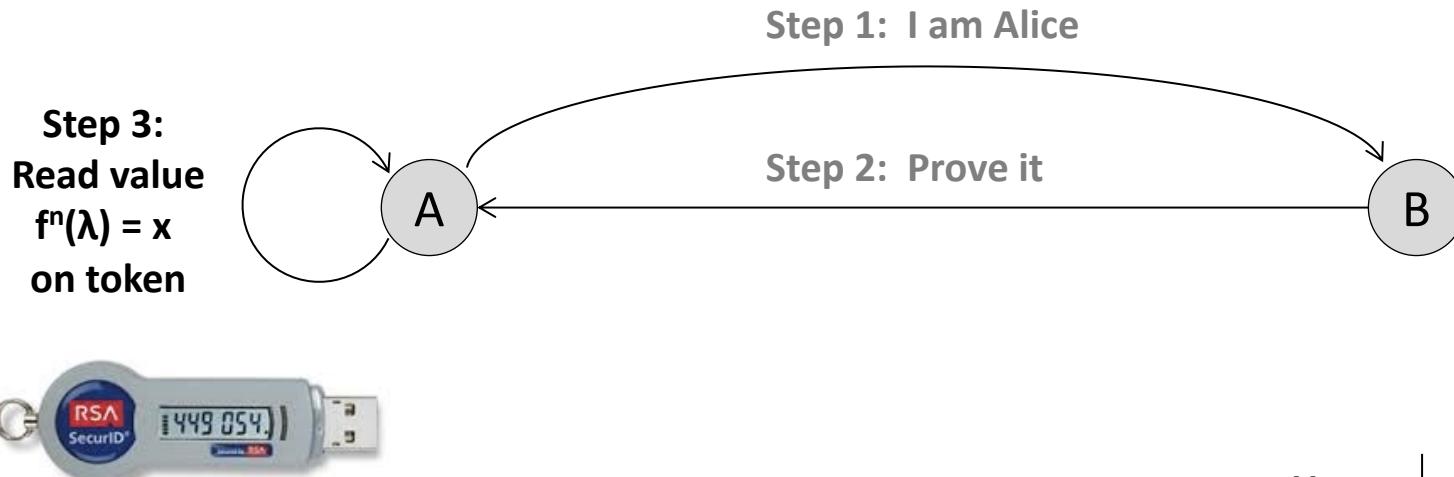
RSA SecurID Protocol



f: integer \rightarrow integer
λ: integer seed
t₀: initial time
t_c: current time
Δt: time interval
 $n = (t_c - t_0) / \Delta t$

User	Information
A	f: integer \rightarrow integer λ: integer seed t ₀ : initial time t _c : current time Δt: time interval $n = (t_c - t_0) / \Delta t$

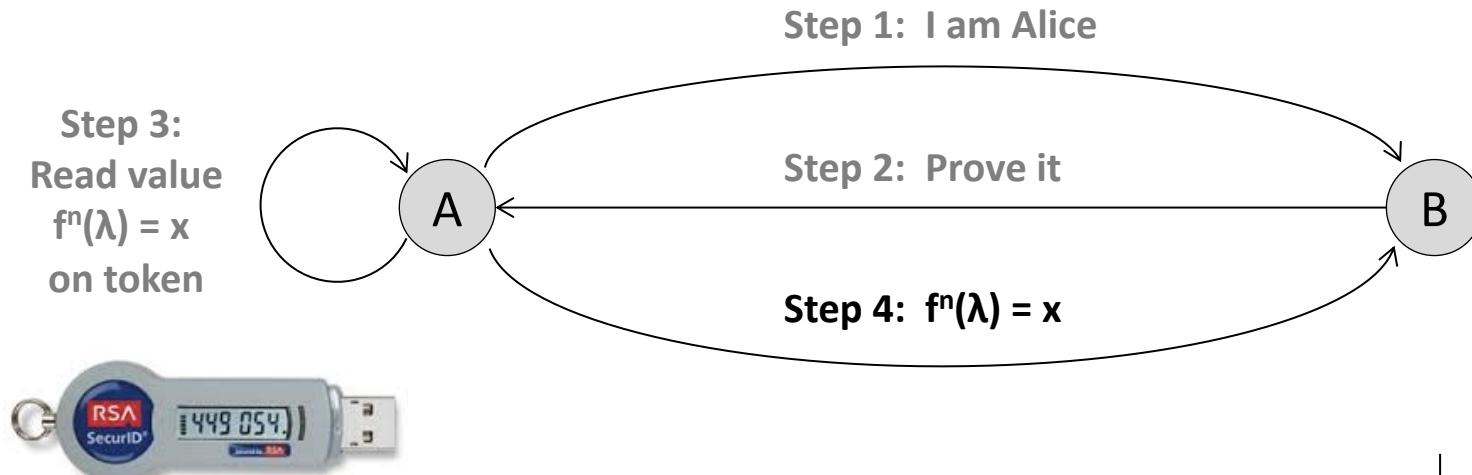
RSA SecurID Protocol



f : integer \rightarrow integer
 λ : integer seed
 t_0 : initial time
 t_C : current time
 Δt : time interval
 $n = (t_C - t_0) / \Delta t$

User	Information
A	f : integer \rightarrow integer λ : integer seed t_0 : initial time t_C : current time Δt : time interval $n = (t_C - t_0) / \Delta t$

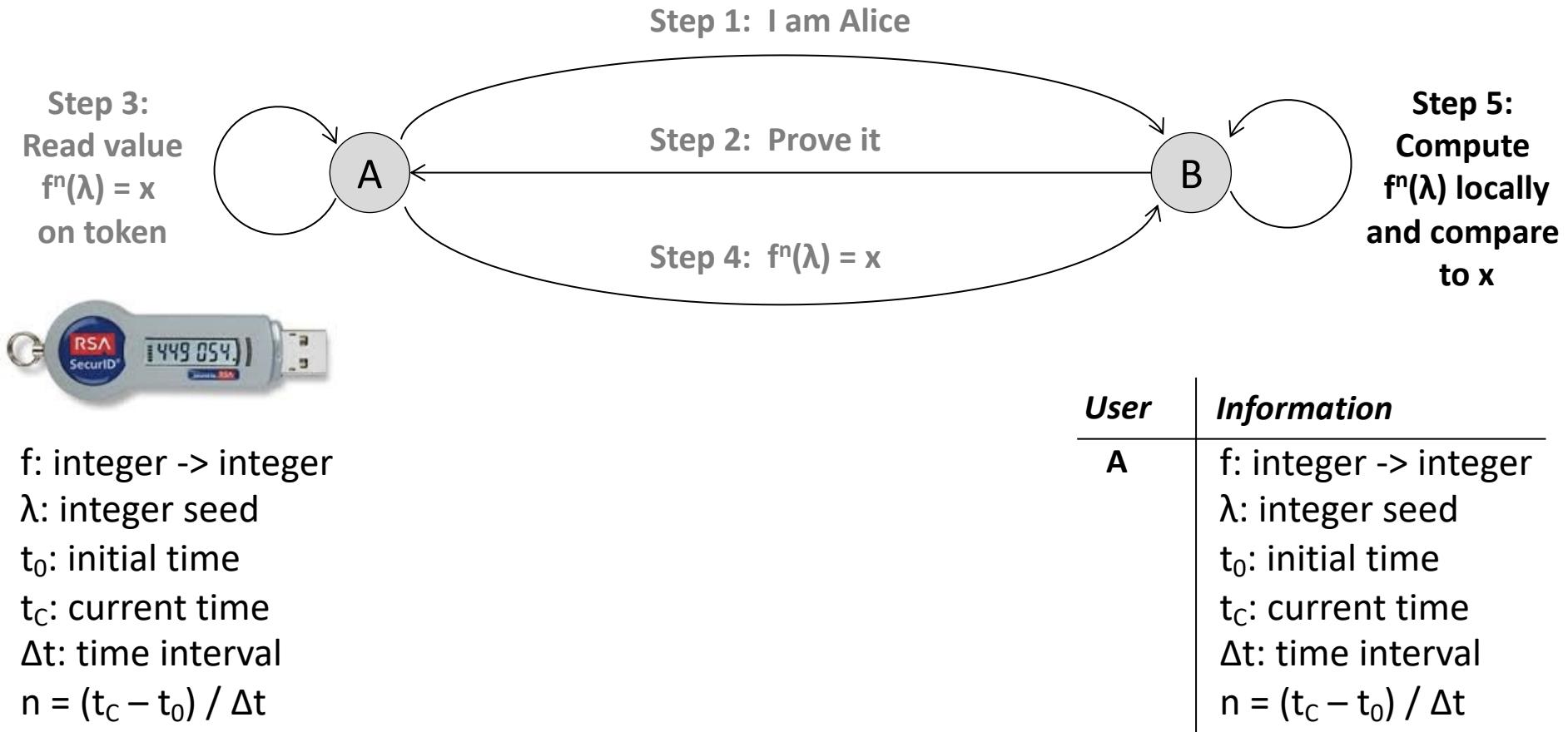
RSA SecurID Protocol



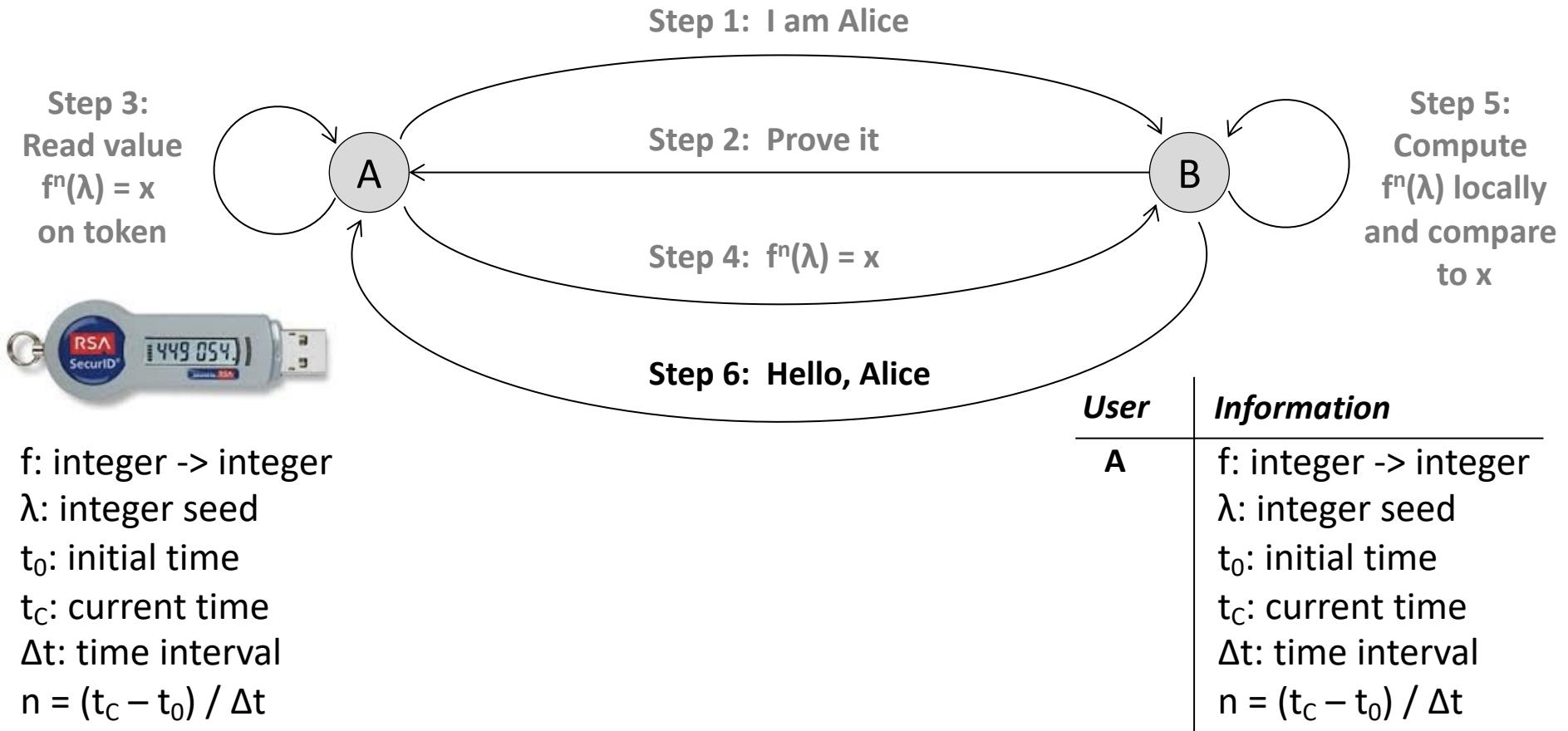
f : integer \rightarrow integer
 λ : integer seed
 t_0 : initial time
 t_C : current time
 Δt : time interval
 $n = (t_C - t_0) / \Delta t$

User	Information
A	f : integer \rightarrow integer λ : integer seed t_0 : initial time t_C : current time Δt : time interval $n = (t_C - t_0) / \Delta t$

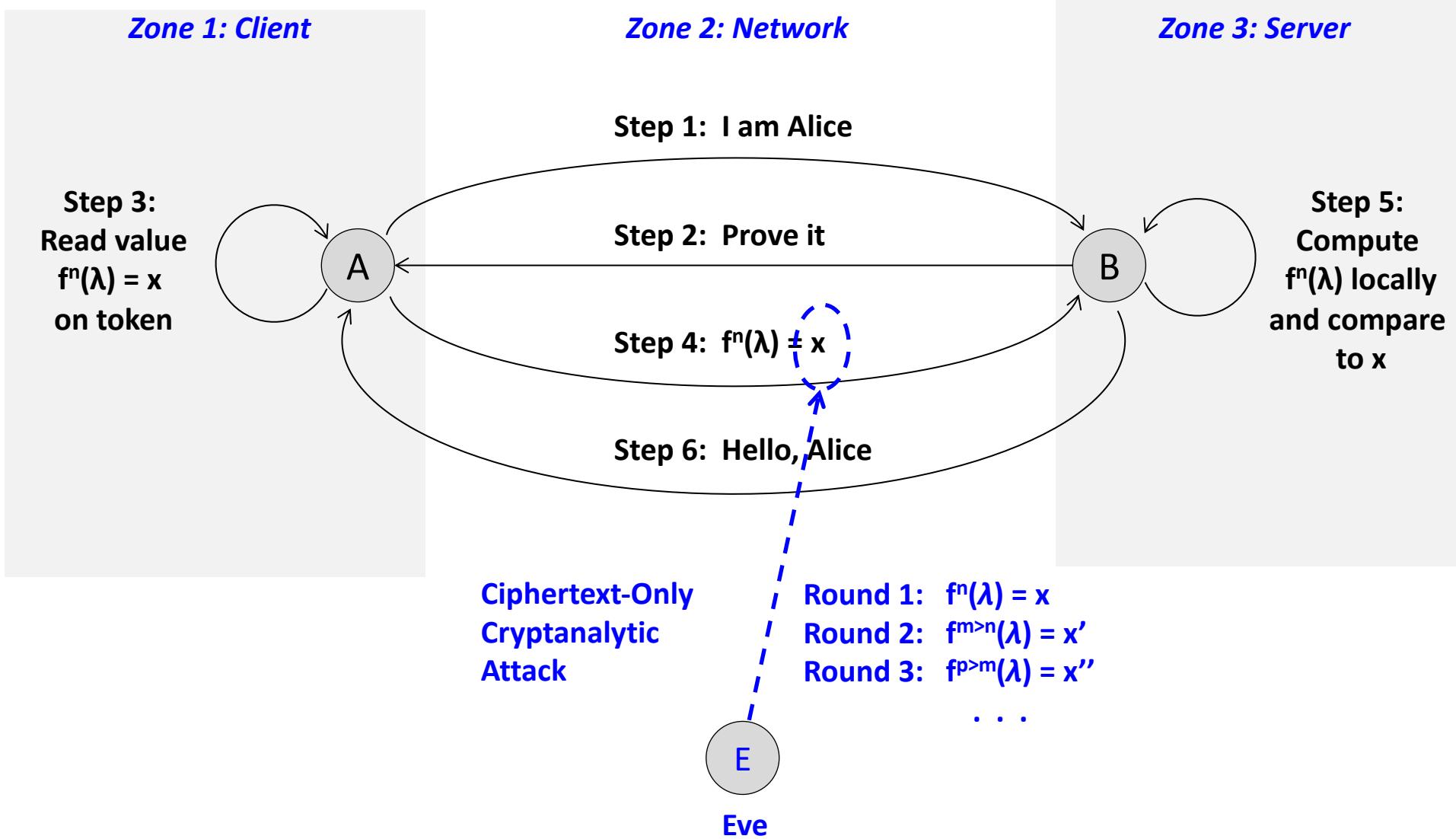
RSA SecurID Protocol



RSA SecurID Protocol



RSA SecurID Protocol



RSA SecurID App



App Store Preview

Open the Mac App Store to buy and download apps.



RSA SecurID Software Token 4+

RSA Security

Designed for iPhone

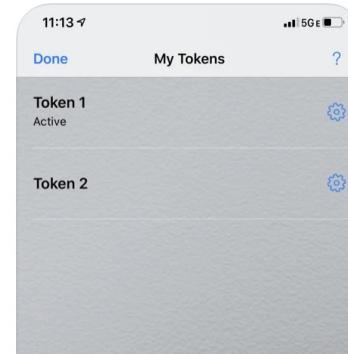
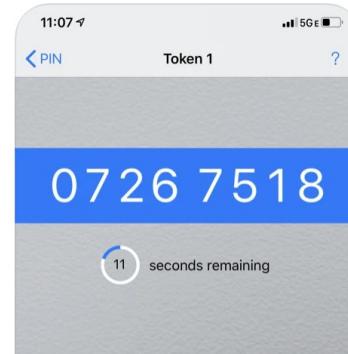
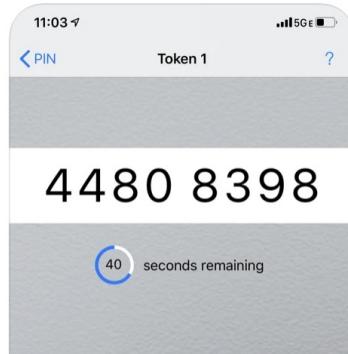
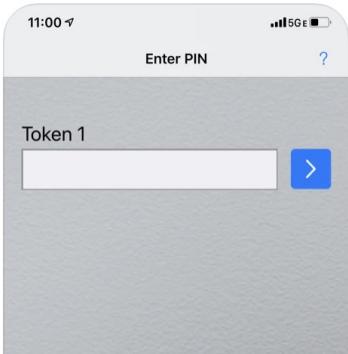
#69 in Business

★★★★★ 3.1 • 334 Ratings

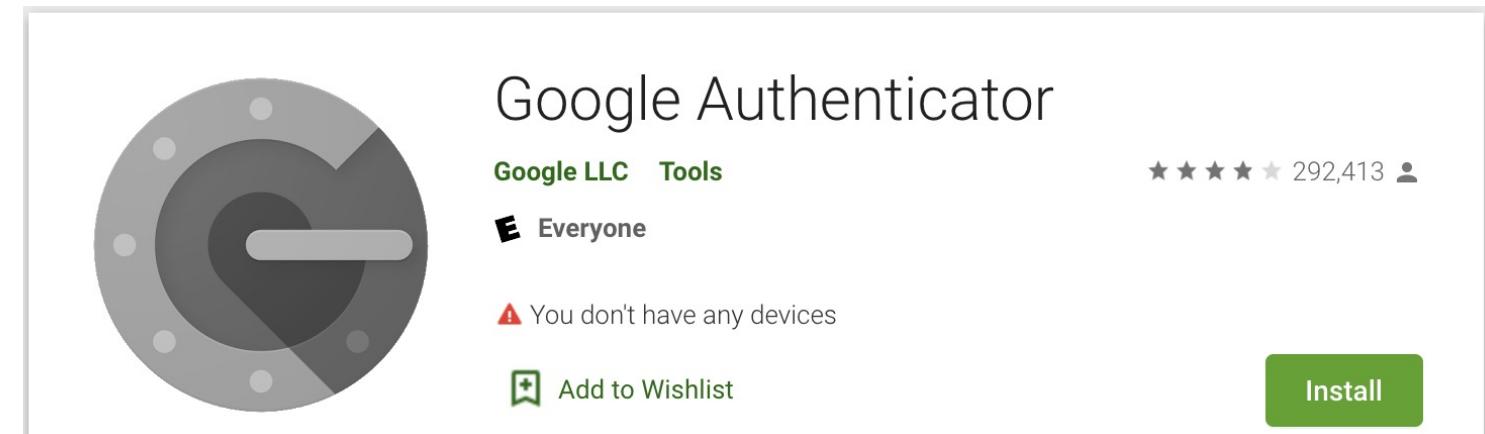
Free

[View in Mac App Store ↗](#)

iPhone Screenshots



Google Authenticator App



Google Authenticator

Google LLC Tools

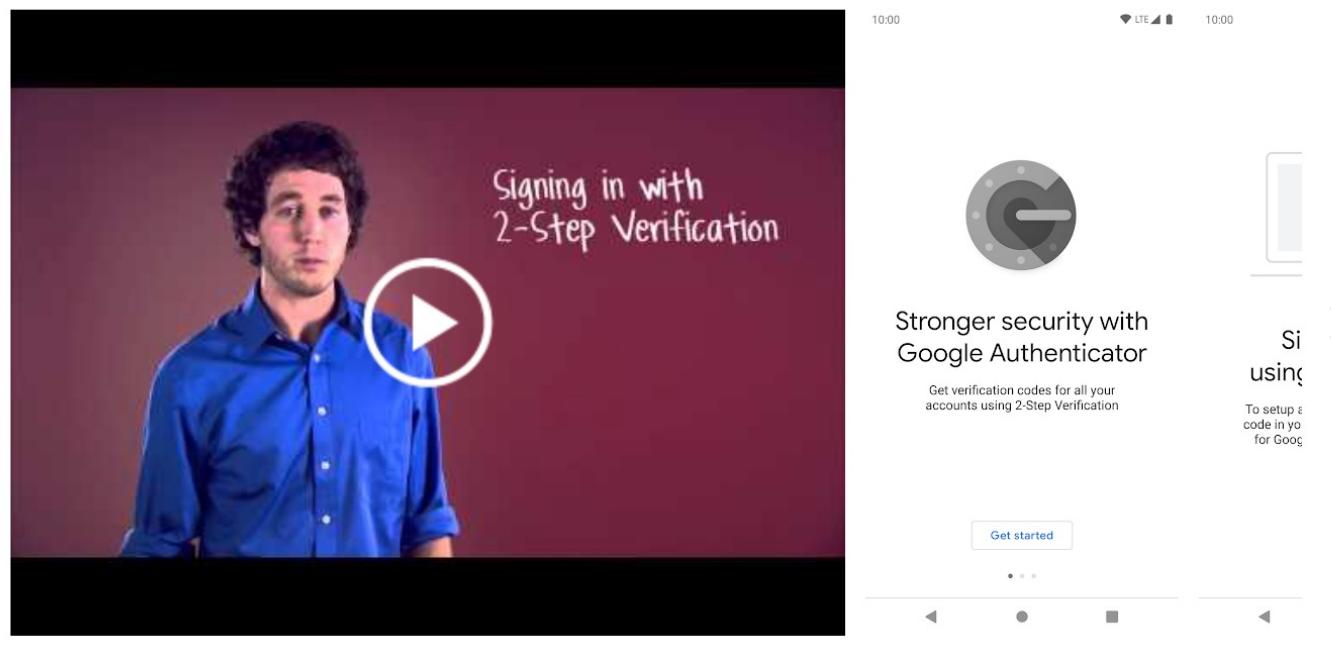
E Everyone

⚠ You don't have any devices

Add to Wishlist

Install

★★★★★ 292,413 reviews



10:00 LTE 10:00

Signing in with 2-Step Verification

Get verification codes for all your accounts using 2-Step Verification

Get started

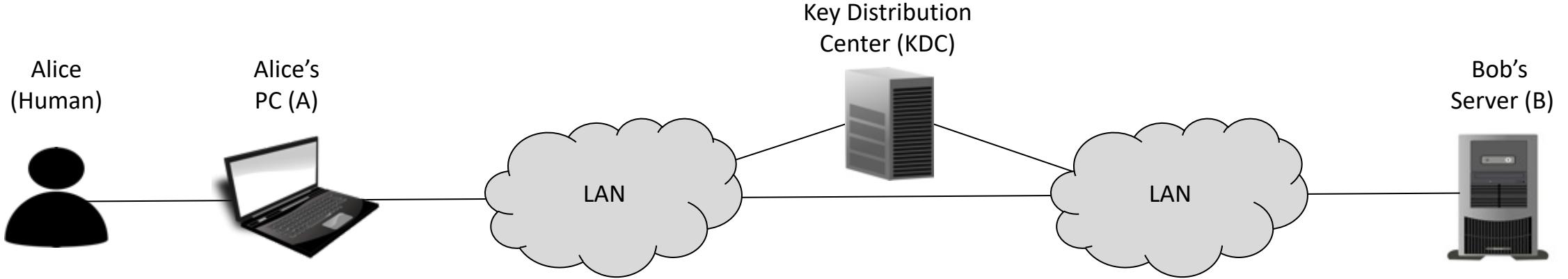
Stronger security with Google Authenticator

To setup a code in yo for Goog

Si using

How Does Kerberos Work?

Kerberos: A Complex Solution to a Simple Password Problem



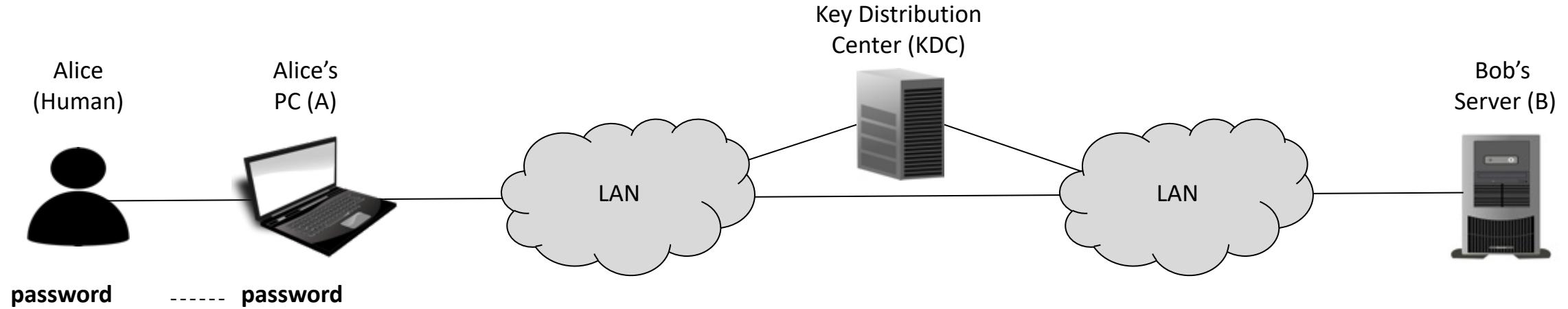
Basic Kerberos Concept:

- Invented at MIT in 1980's as part of Project Athena
- Goal is that Alice (client) can authenticate to Bob (server) without using a password on the local area network (LAN);
- Key Distribution Center (KDC) enables this process using conventional cryptography (i.e., no public key technology)
- **Used primarily for Single Sign-On (SSO)**



Kerberos – Preconditions

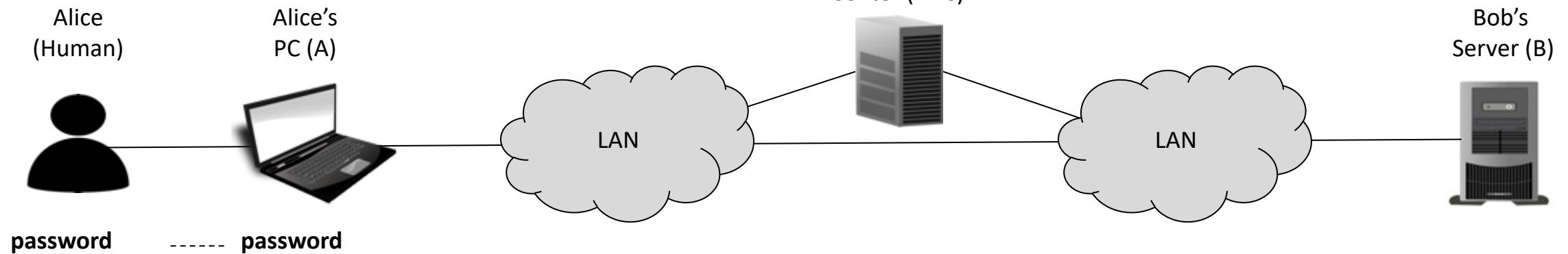
Infrastructure
Preconditions:



Kerberos password set up
for Alice to log into her PC
(Never used over any LAN)

Kerberos – Keys

Infrastructure
Preconditions:



Key (Issued by KDC)
 K_A : Alice's Encryption

Kerberos KDC creates and issues
three cryptographic keys: K_A , K_B , K_{KDC}

$$\{ \{ m \}_{K_A} \}_{K_A} = m$$

↑
Encrypt ↑
Decrypt

$$\{ \{ m \}_{K_B} \}_{K_B} = m$$

$$\{ \{ m \}_{K_{KDC}} \}_{K_{KDC}} = m$$

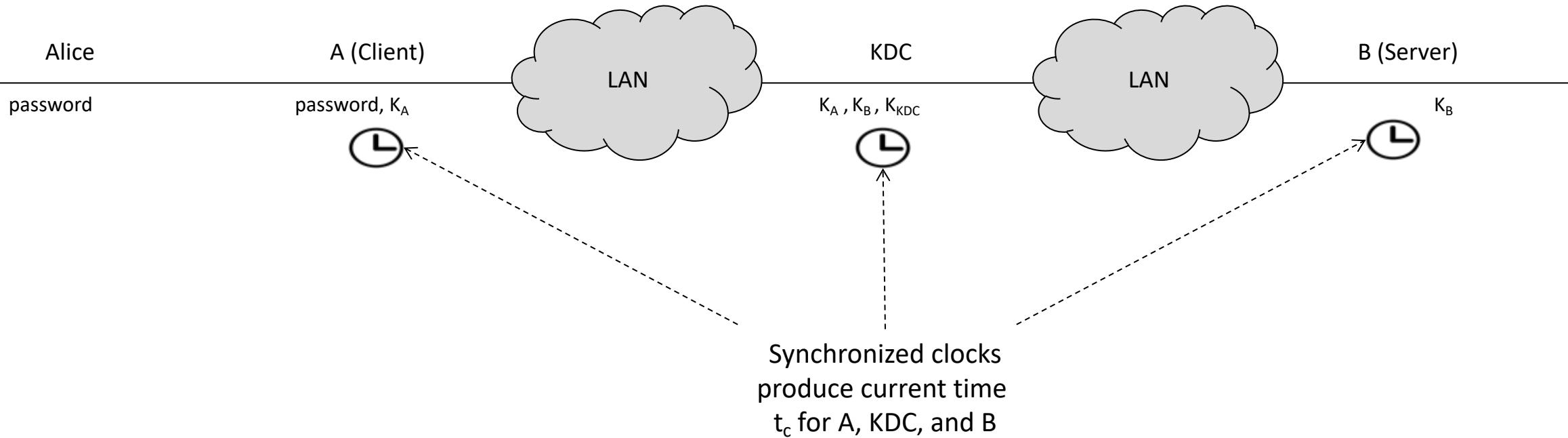
K_{KDC} : KDC's Encryption
Key (Created by KDC)

Key Distribution
Center (KDC)

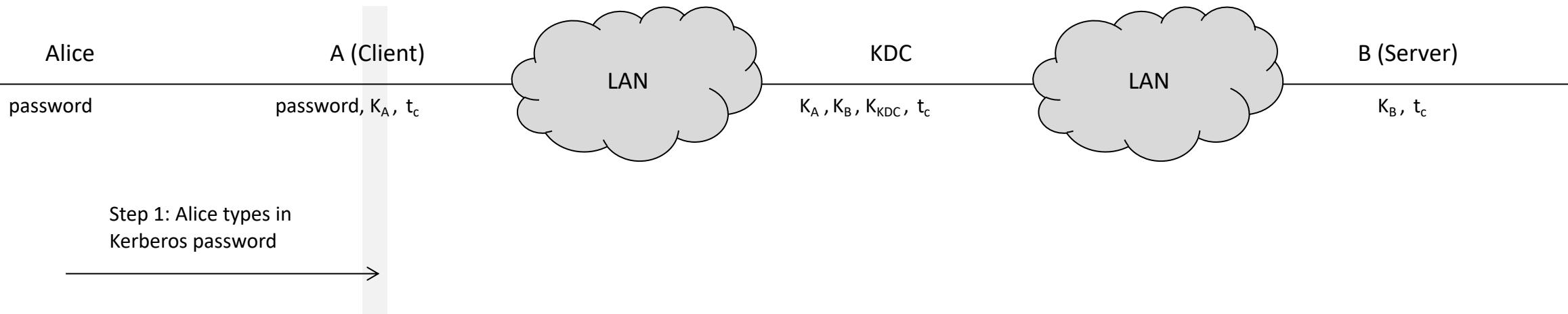
Bob's
Server (B)

K_B : Bob's Encryption
Key (Issued by KDC)

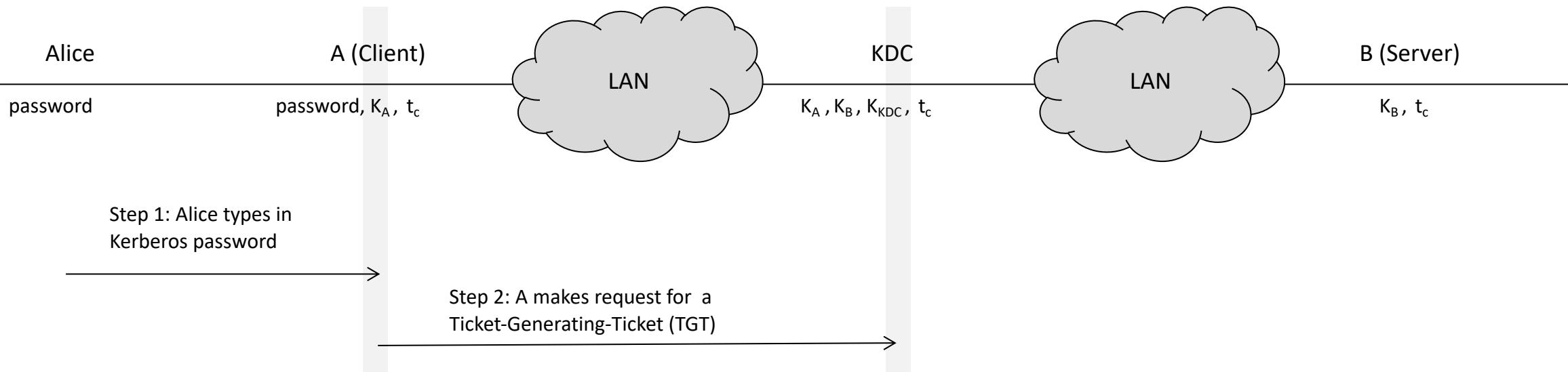
Kerberos – Clocks



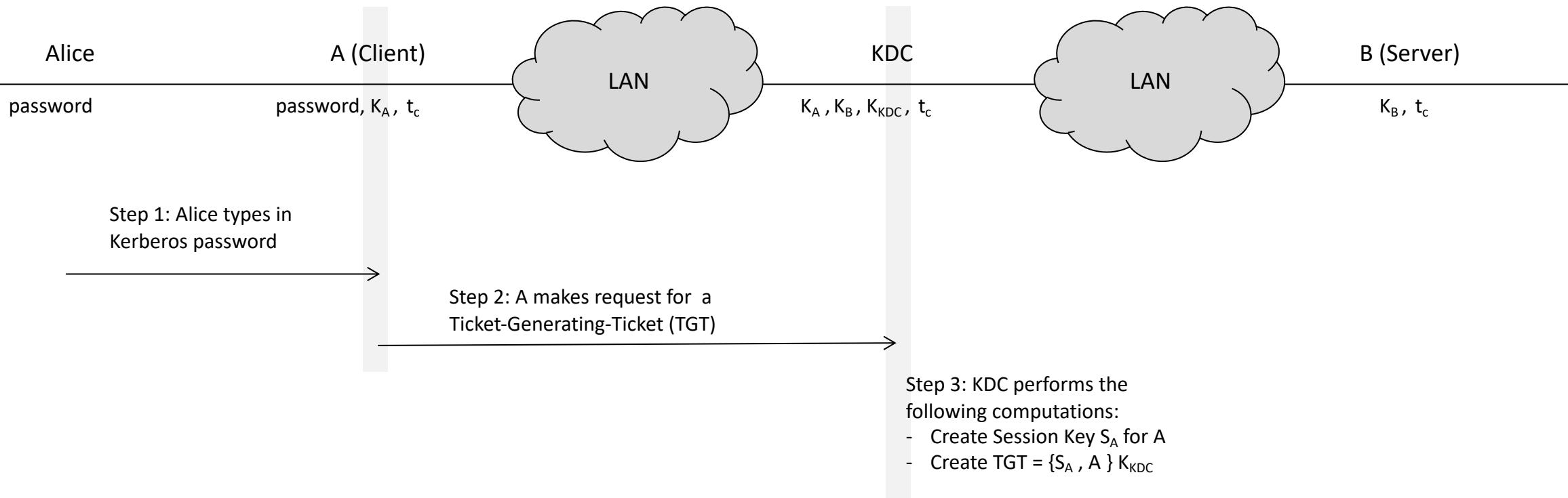
Kerberos Step 1: Type in Local Password



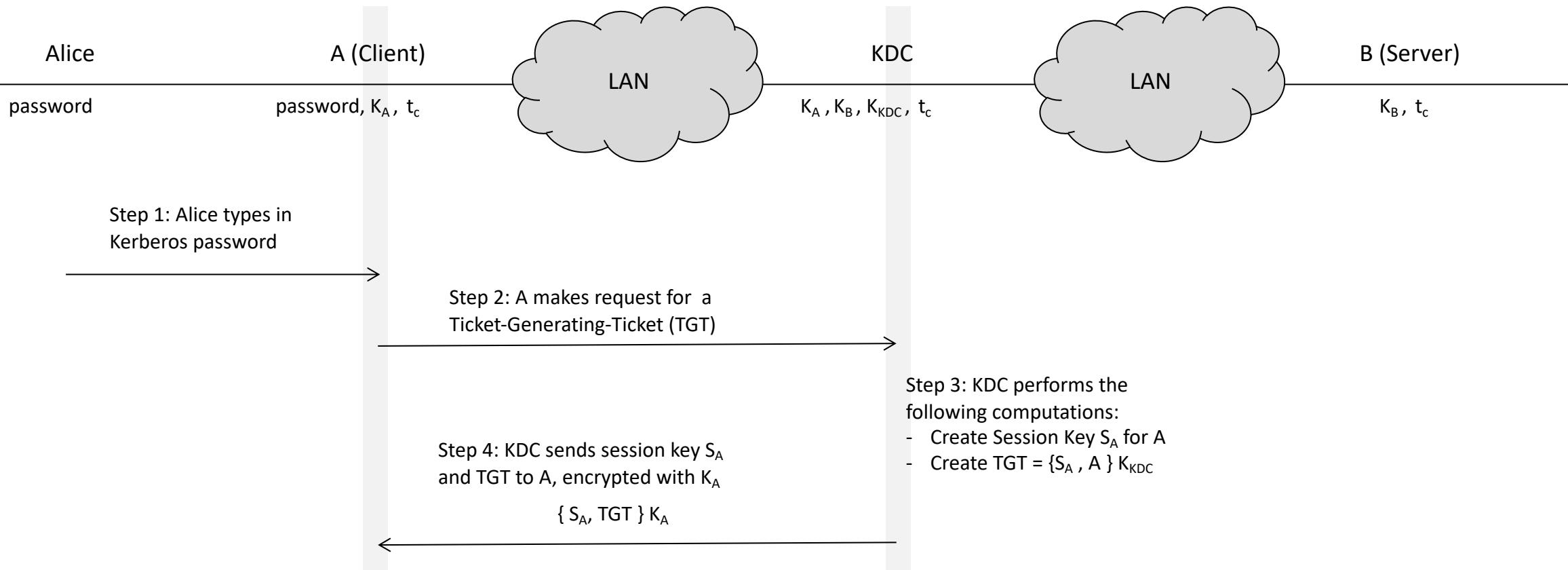
Kerberos Step 2: Request TGT and Session Key



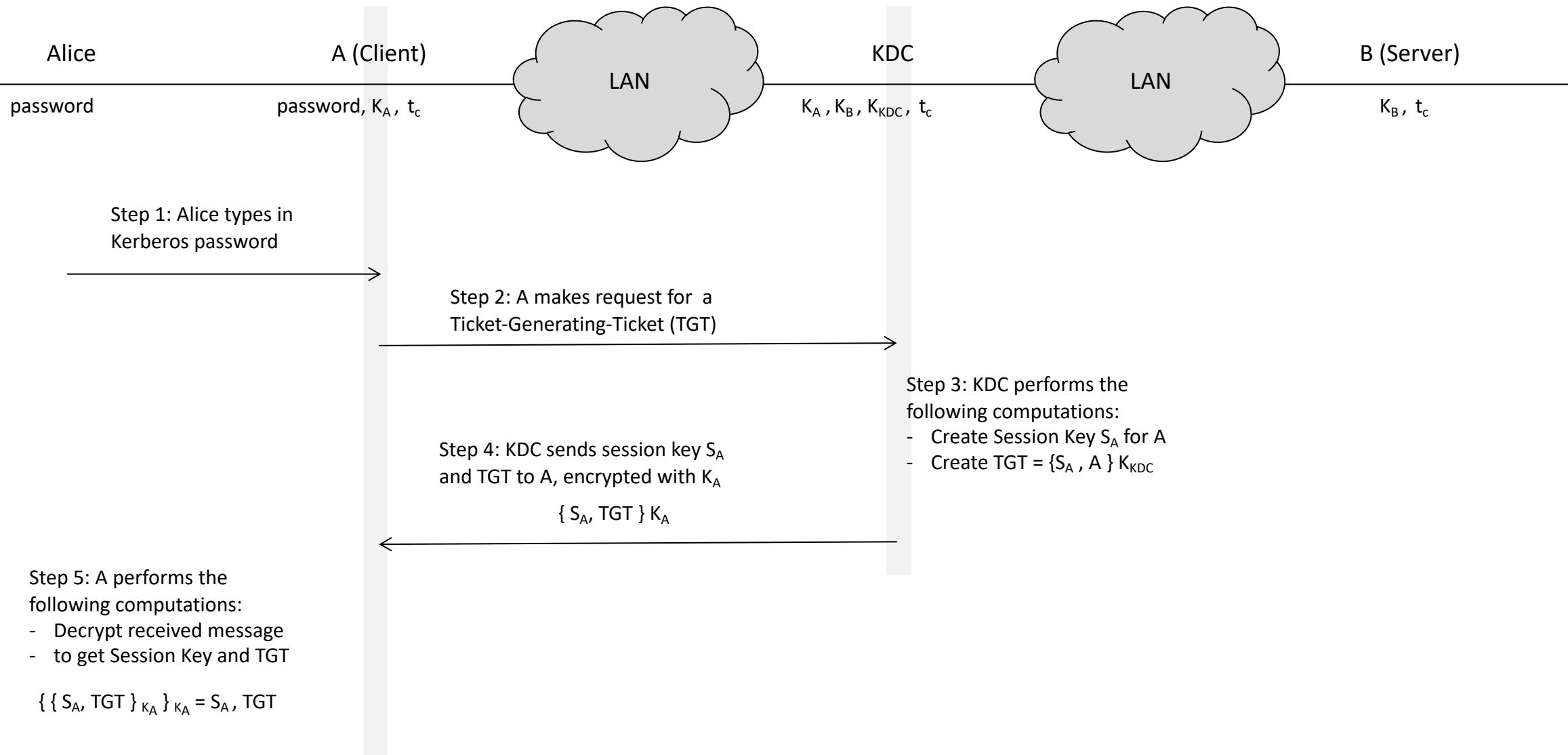
Kerberos Step 3: Create Session Key and TGT



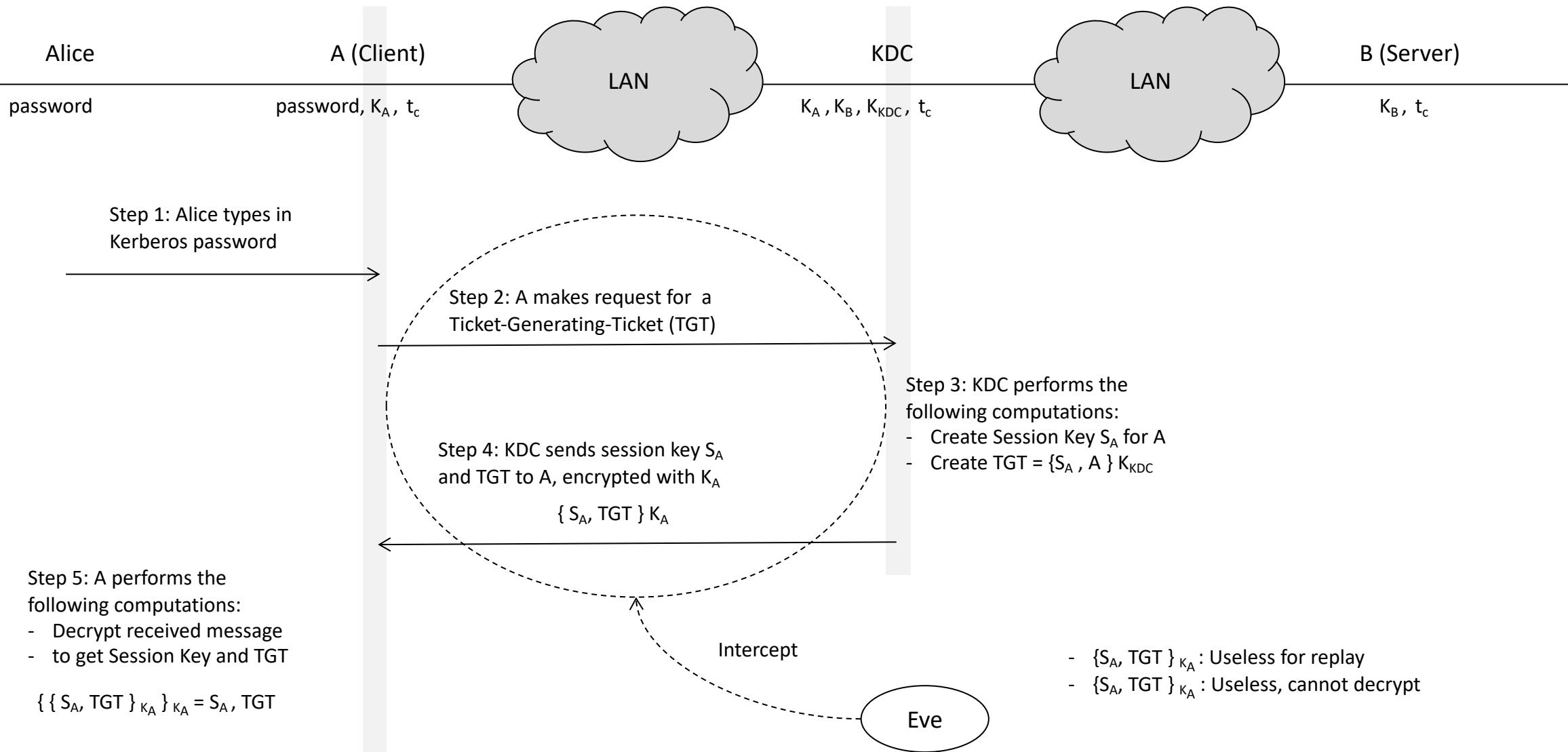
Kerberos Step 4: Provide Session Key and TGT



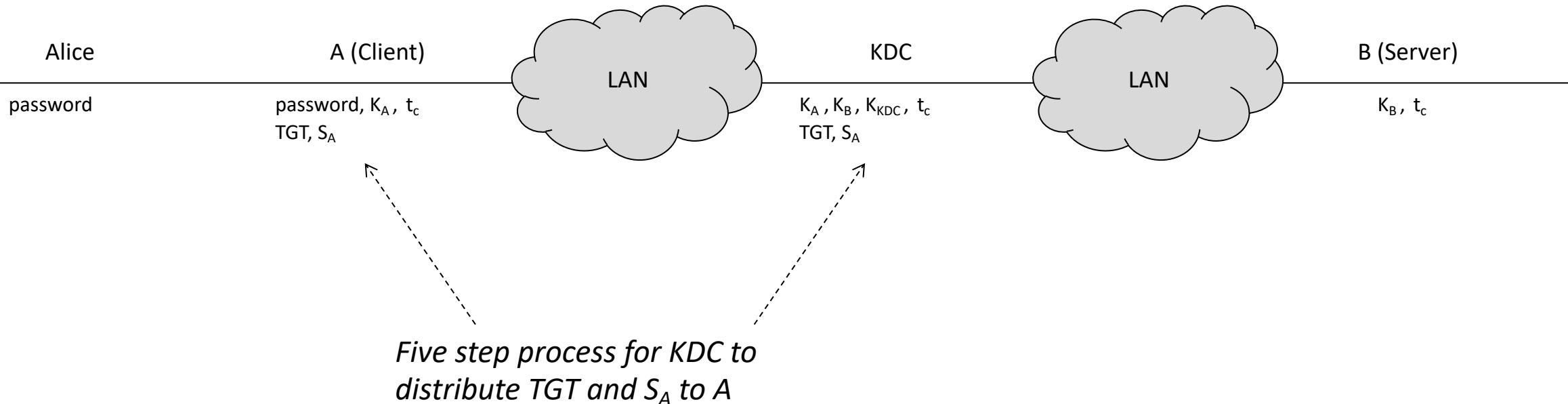
Kerberos Step 5: Decrypt Session Key and Store TGT



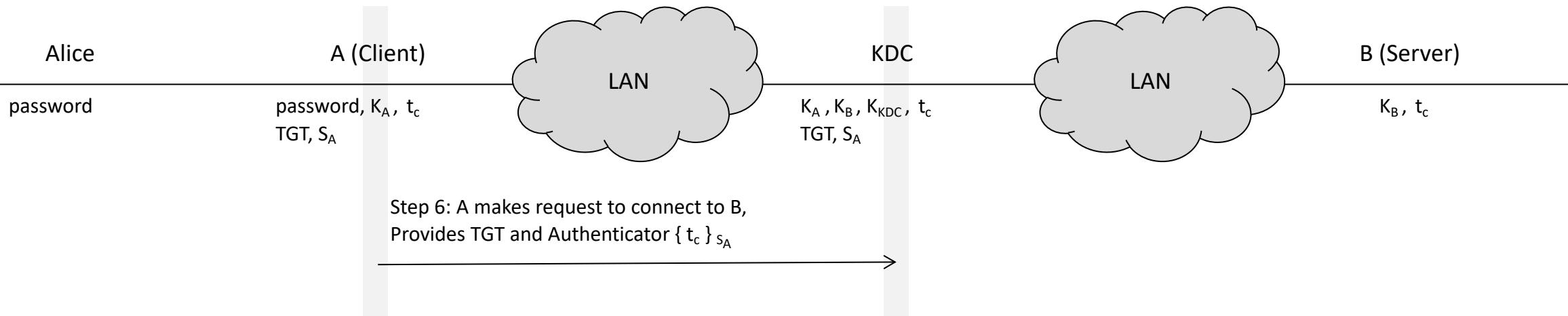
Kerberos – Through Five Steps: Eve Cannot Hack



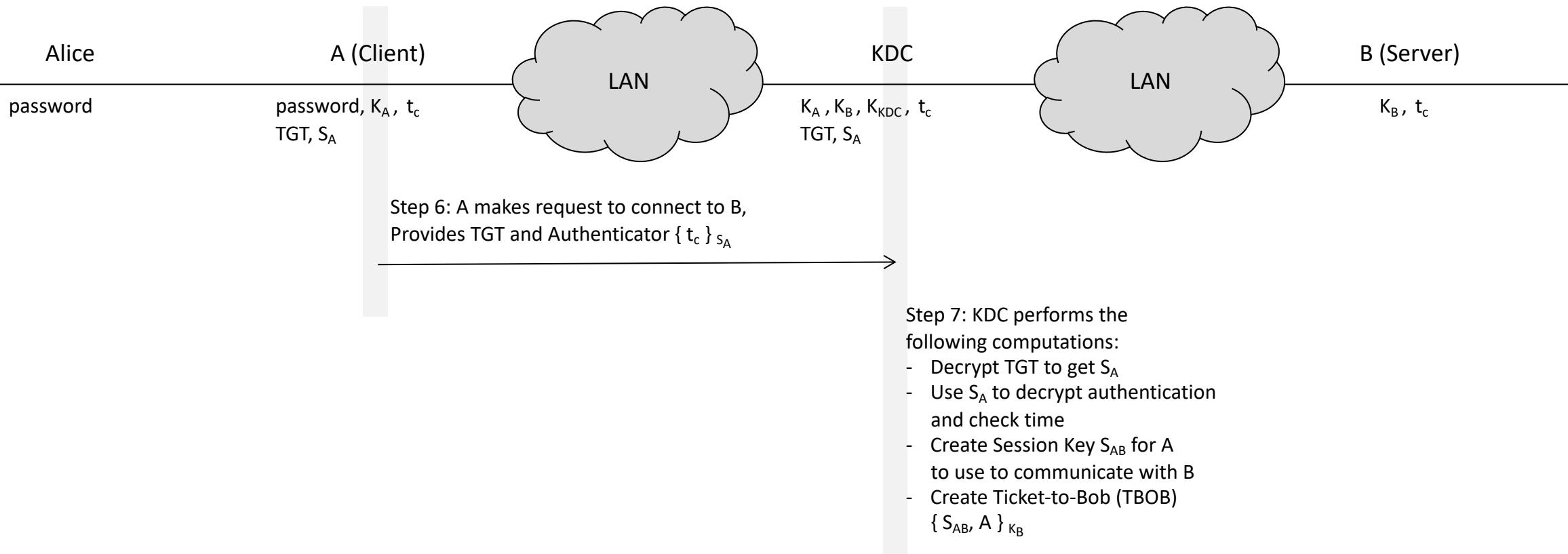
Kerberos – Result of Five Steps



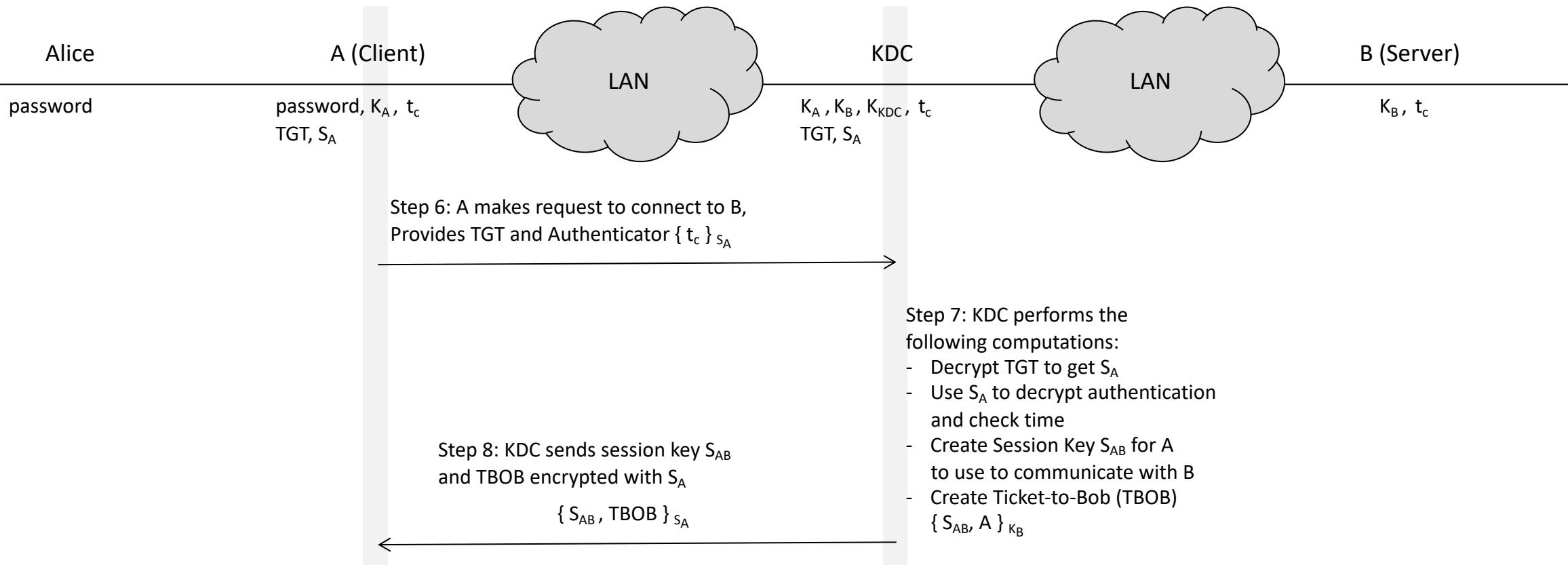
Kerberos Step 6: Request Login to B



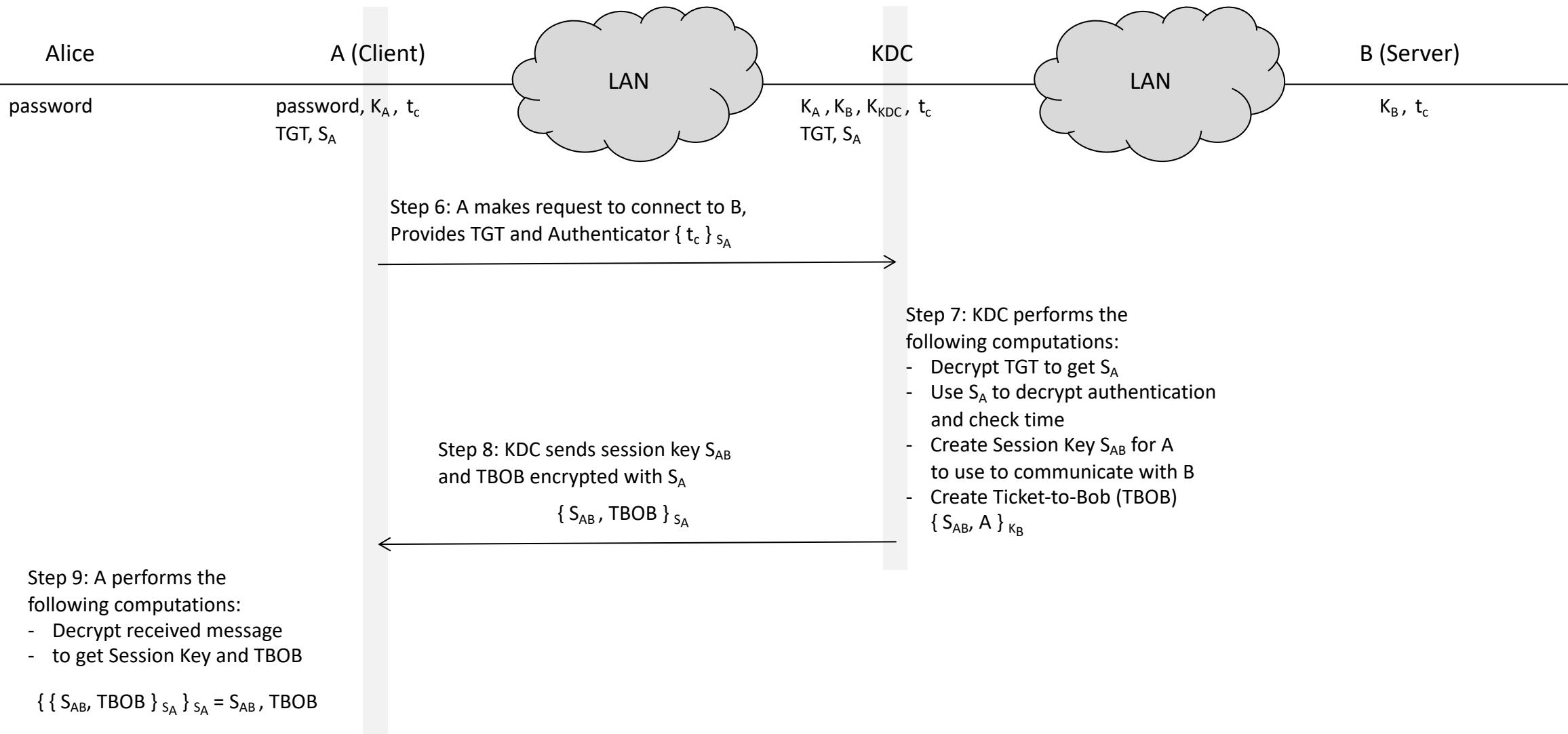
Kerberos Step 7: Create Session Key and Ticket to Bob



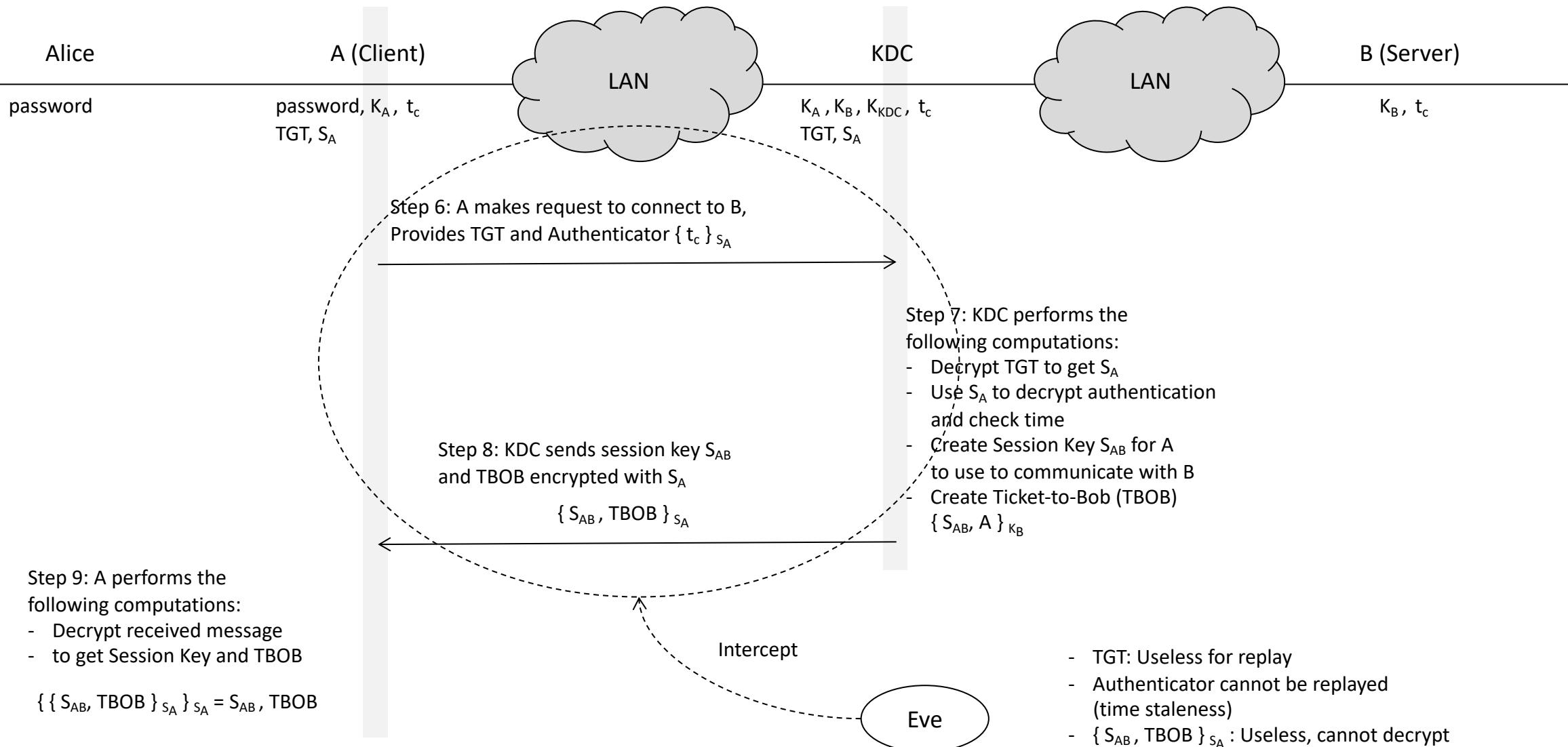
Kerberos Step 8: Send Session Key and Ticket to Bob



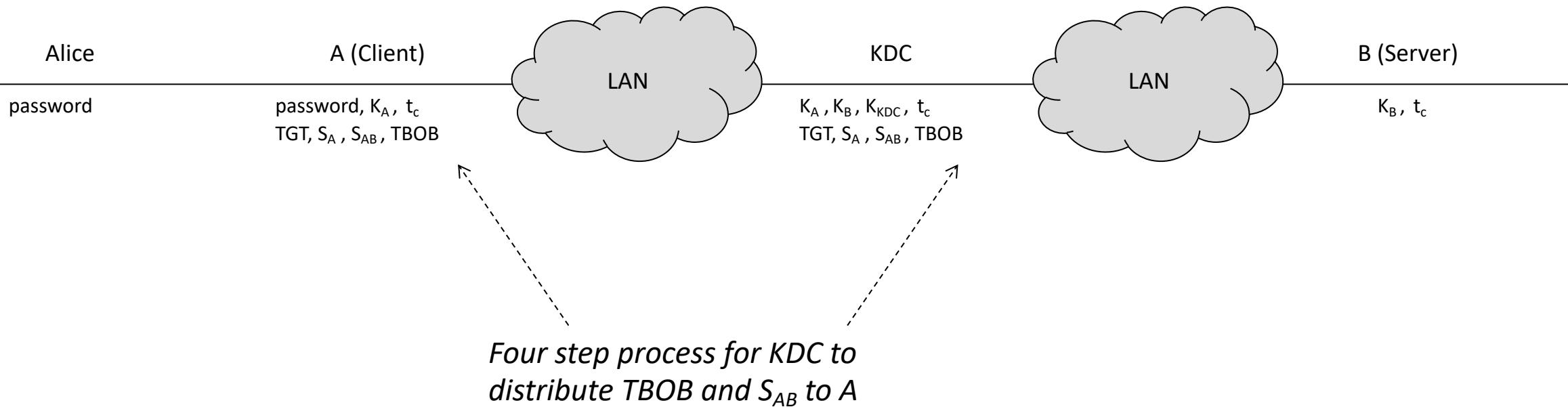
Kerberos Step 9: Decrypt Session Key and Store Ticket to Bob



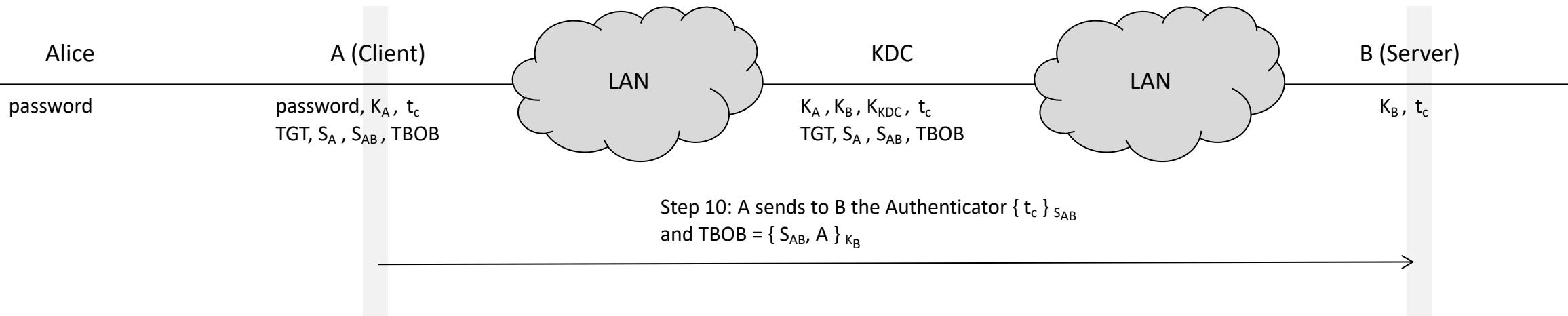
Kerberos – Through Nine Steps: Eve Cannot Hack



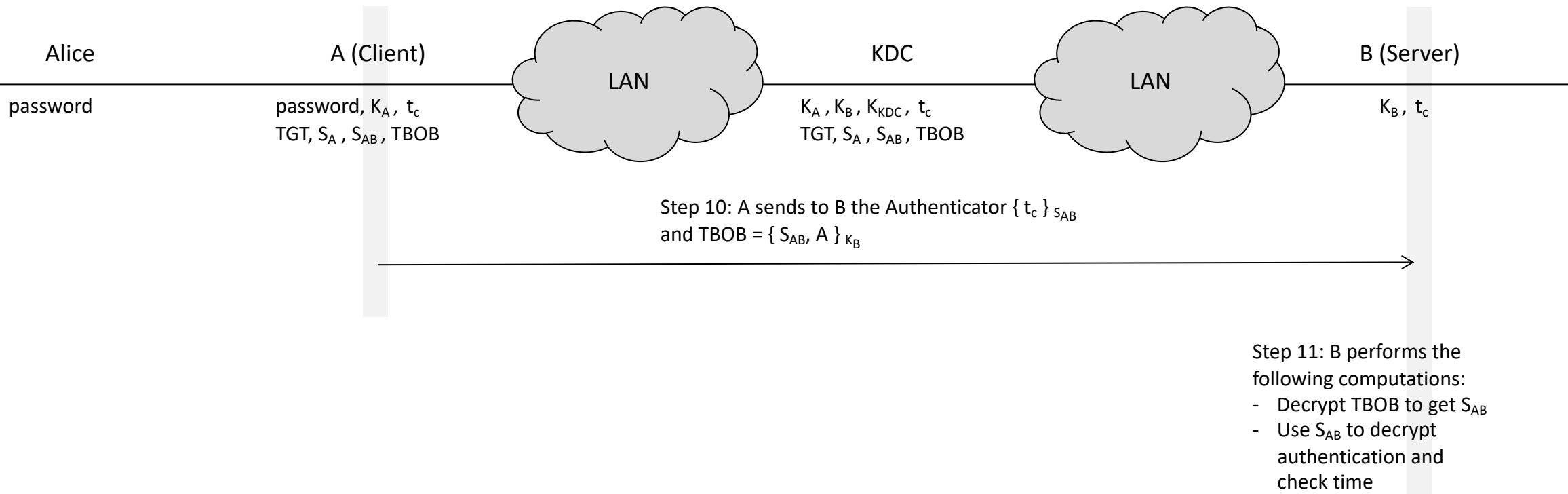
Kerberos – Result of Nine Steps



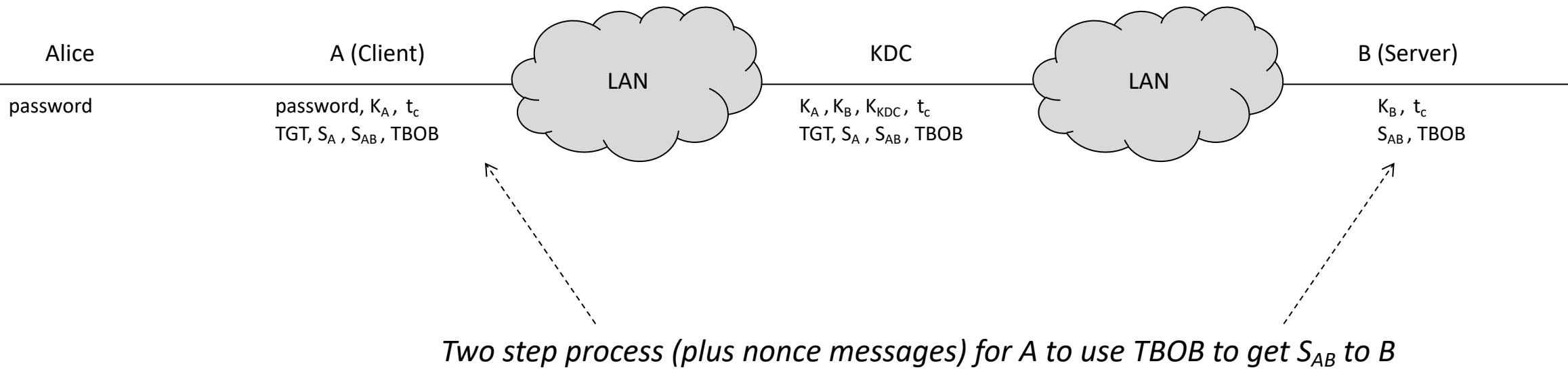
Kerberos Step 10: Send Bob the Ticket to Bob



Kerberos Step 11: Decrypt Ticket to Bob and Check Time



Kerberos – Result of Eleven Steps



Kerberos – Realms

