Countering Jamming Attacks Against Mobile Communications

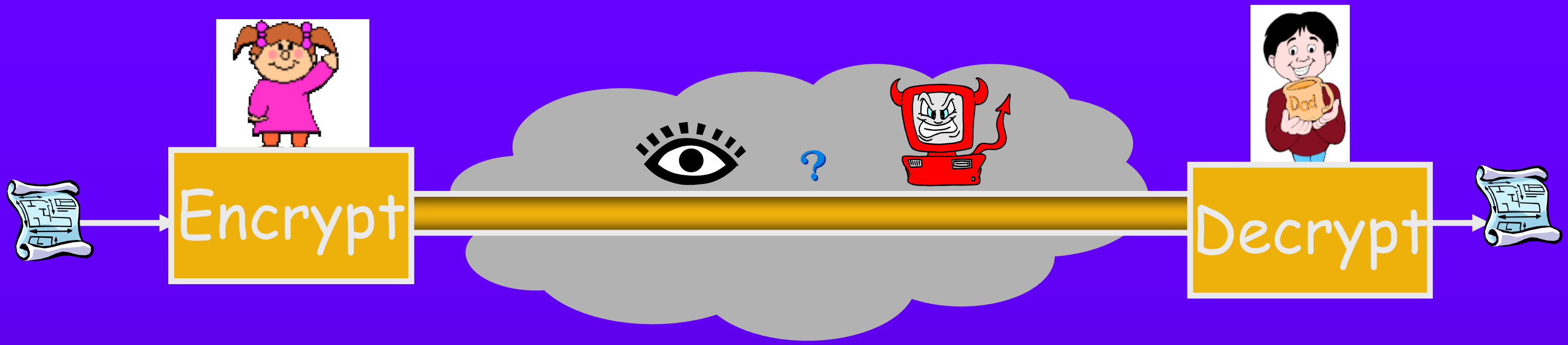
Dr. Reiner Dojen
Data Communications Security Laboratory,
Department of Electronic & Computer Engineering
University of Limerick, Ireland

Presentation Overview

- Security Protocols
- Jamming
- Jamming attack against a mobile communications protocol: Suppress & Desynchronise Attacks
- Sample: Chen-Lee-Chen

Cryptographic Security Protocols

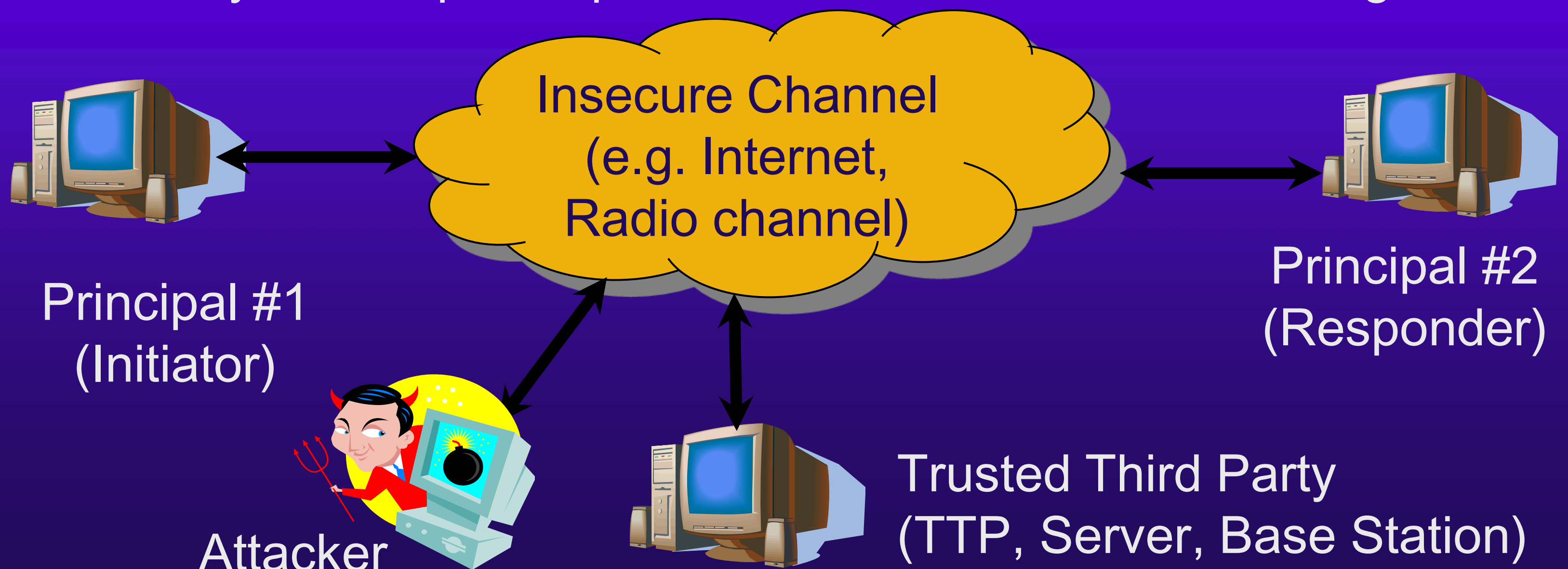
Cryptographic Security Protocols



- A communication protocol that is based on a cryptographic system
- A prescribed sequence of interactions between principals designed to achieve certain goals
- Goals include:
  - Secrecy, Key distribution, Key agreement, Integrity Protection, Authentication, Non-repudiation, Anonymity

Participants

- Honest Principals
  - follow particular protocol faithfully, do not cheat
- Trusted Third Parties (Servers)
  - trusted by all principals
  - Have authority over certain information
- Dishonest Principals (Attacker, Intruder)
  - Try to manipulate protocol to achieve unfair advantage



Security Protocols vs Communication Protocols

- Communication Protocols:
  - reachability of all legal states
  - avoidance of infinite loops
  - deal with accidental/random modifications (interference, bit flips)
- Security Protocols:
  - gain of information by attacker/intruder
  - passive attacker (listening only)
  - active attacker (modifies, may use multiple sessions)
  - “Attacker never play by the rules”

Attacker Ability

- Eavesdrop/Packet Sniffing
- Send Messages
- Replay recorded messages
- Modify/tamper with Messages in transit
- Jamming/Stopping Message
- Spoofing Addresses/Identities
- Impersonate an address and lie in wait
- Attacker may also be legitimate principal
- Summary: Attacker has full control over communication environment!!!

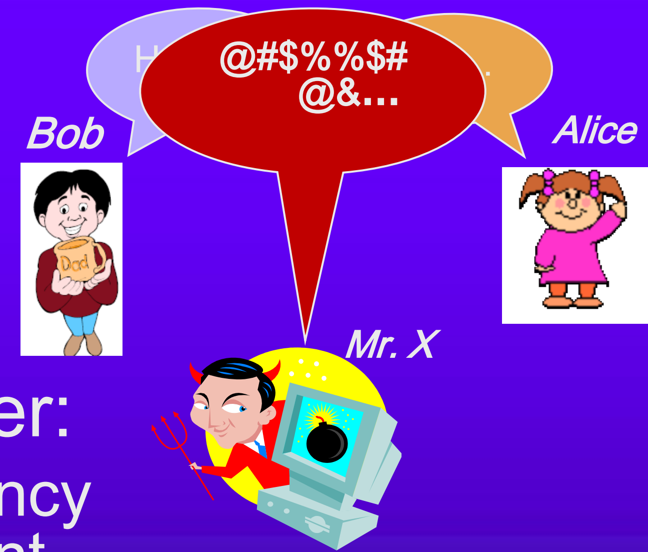
Attacks on Protocols

- Replay Attack
  - Attacker records old messages and replays them at later stage
- Parallel Session
  - Attacker starts a new session to obtain further information
- Type Flaw
  - Using one component instead of another (e.g. swap key with identity)
- Denial of Service (DoS)
  - Prevent legitimate use of system

Jamming Attacks against Mobile Communications

What is Jamming?

- Transmission of radio signals that disrupt communications by decreasing the signal to noise ratio.



- Jamming uses transmitter:
  - tuned to the same frequency as the receiving equipment
  - uses the same type of odulation
  - enough power
- Overrides any signal at the receiver

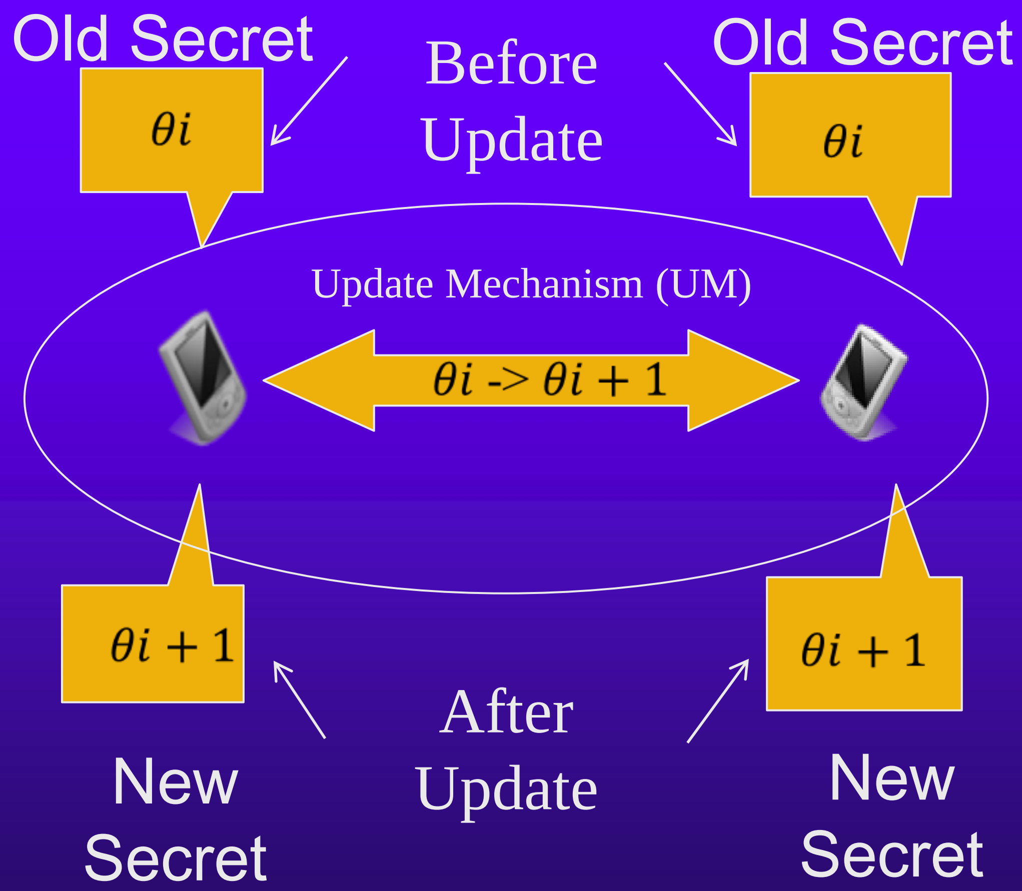
Defence Strategies

- Constant Jammer:
  - Spread-spectrum techniques
  - Frequency hopping (physical layer)
  - Channel Surfing (link layer)
  - Spatial retreat (escape jammer)
  - Hard to defend against at application layer
  - Sufficient power: impossible to stop ☹
- Deceptive/Random Jammer
  - Ensure communication continues after jamming has stopped - application layer ☺

Dynamic Shared Secrets

- Many security protocols for wireless communications use one-time shared secrets for authentication purposes
- Used by the owning principals to prove their identity
- Same protocol run establishes a new instance of the shared secret (for next session).
- Messages of the protocol that establish the new shared secret => update mechanism (UM)
- UM serves two purposes:
  - generation of a new instance of the shared secret
  - agreement on the same new shared secret
- UM aims to ensure synchronous storage of the shared secret

Update Mechanism for Dynamic Shared Secrets

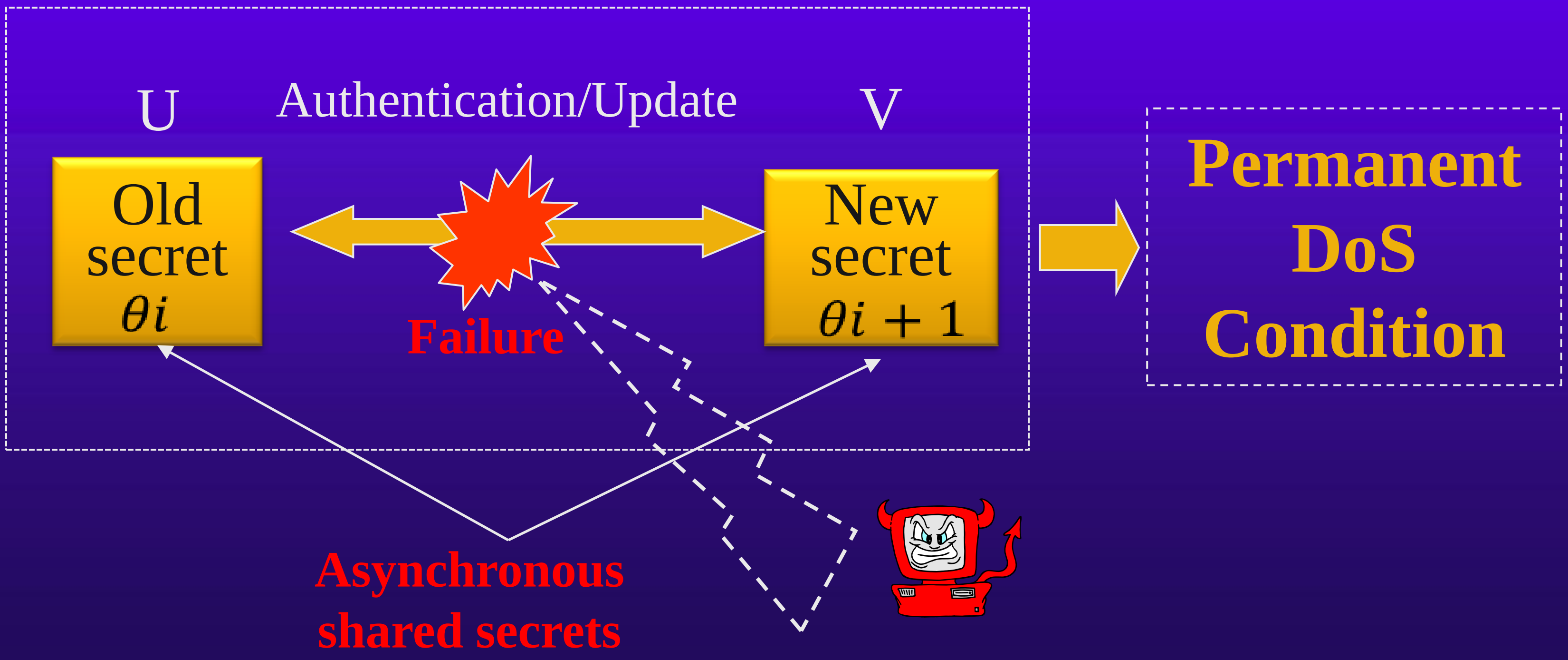


Atomic Update Mechanism?

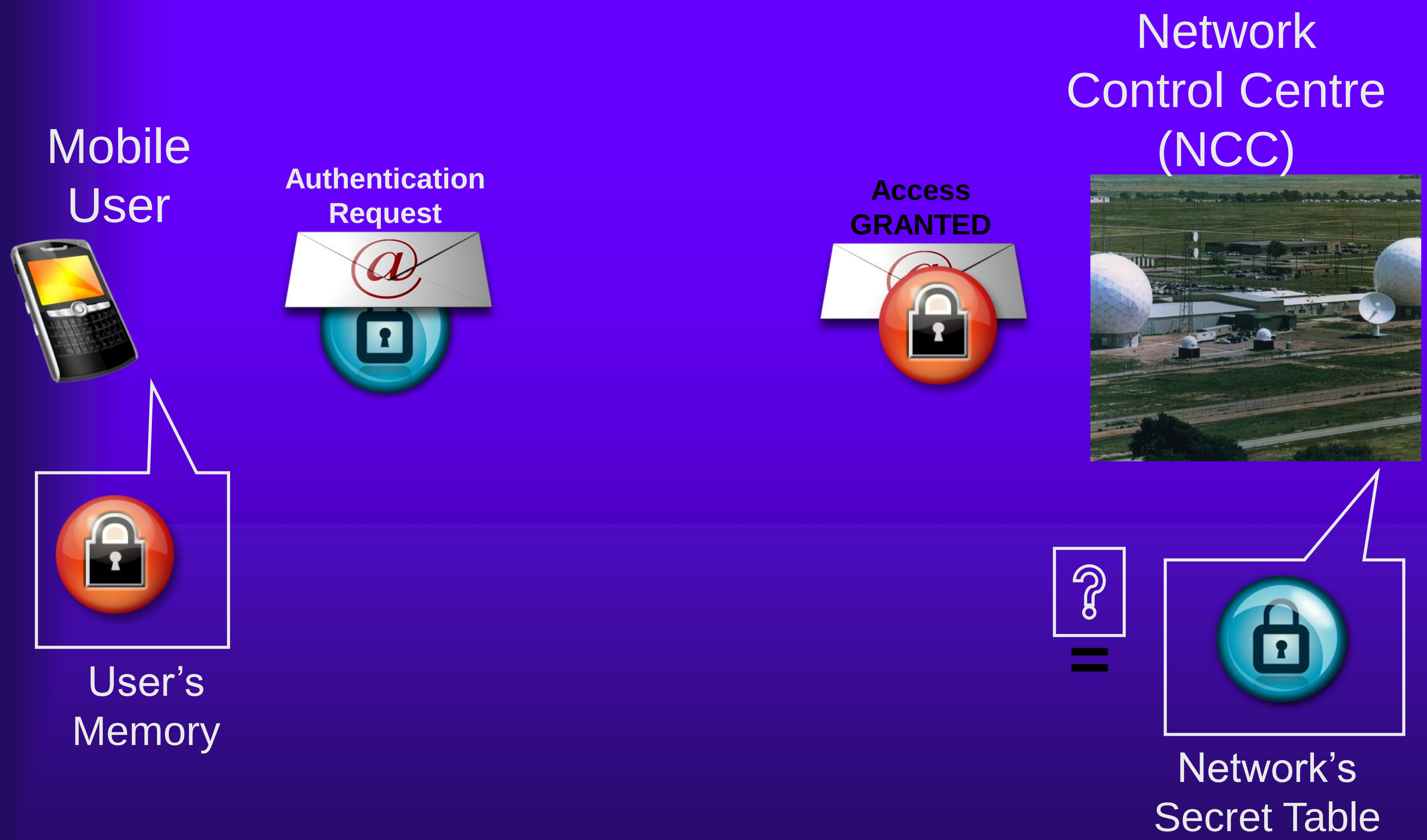
- Update mechanism often regarded as an atomic unit.
- However, UM is a sequential process:
  1. One principal (A) updates the shared secret first from θ_i to θ_{i+1}.
  2. A computes the message containing the new operating value θ_{i+1}.
  3. A sends the message to the other principal (B).
  4. B receives the message from A.
  5. On successful authentication of A, B updates its shared secret to θ_{i+1}.

Suppress-and-Desynchronise Attacks

- Suppress-and-Desynchronise (SD) attacks interfere with update mechanism
- Message in UM is suppressed to desynchronise storage of secrets
- Successful SD attack leads to permanent DoS condition

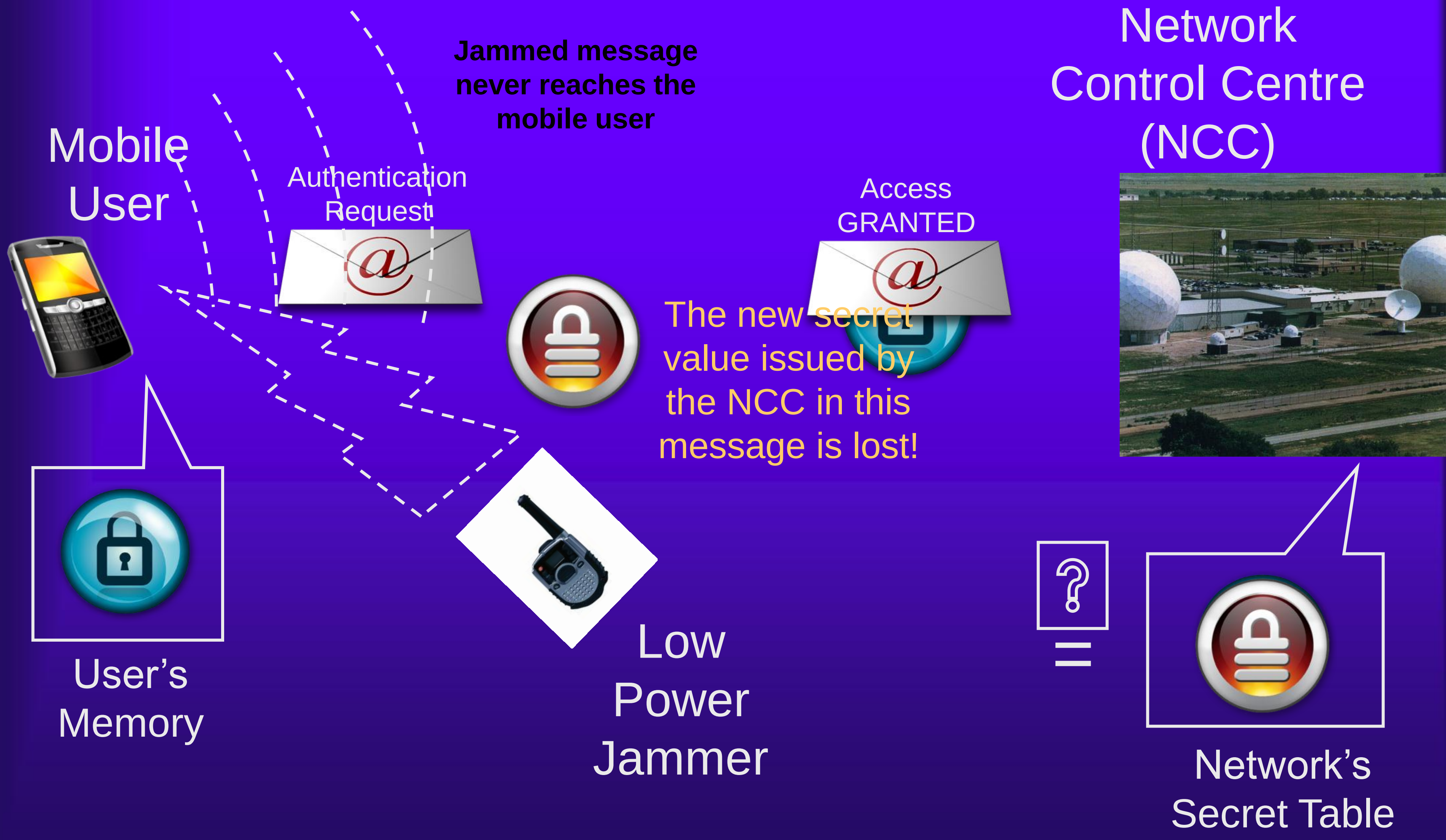


Normal Protocol Execution

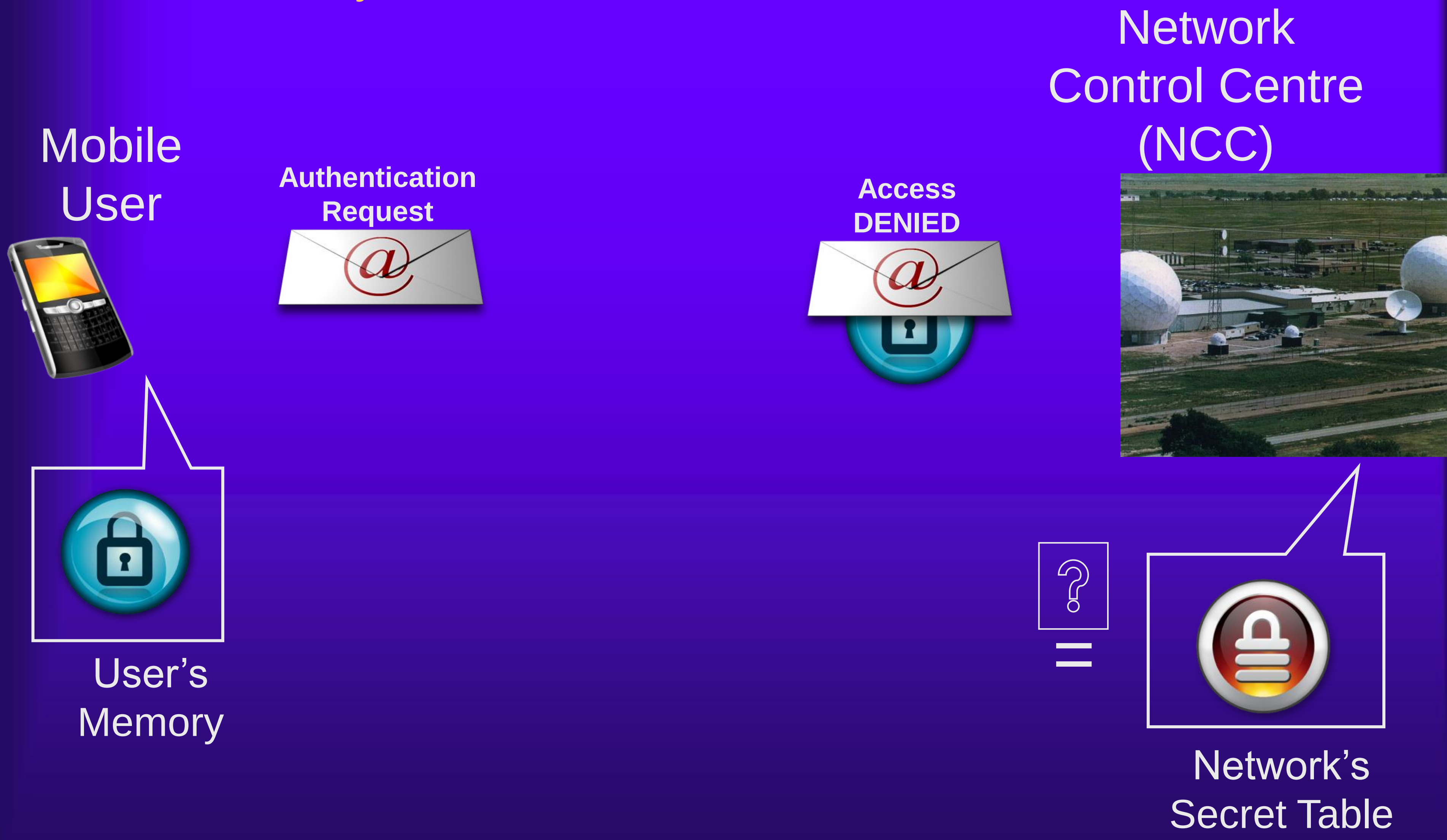


Mutual Authentication by Proving Possession of Shared Secret

Attacker Mounting SD-Attack
SD Attack against a Mutual Authentication Protocol



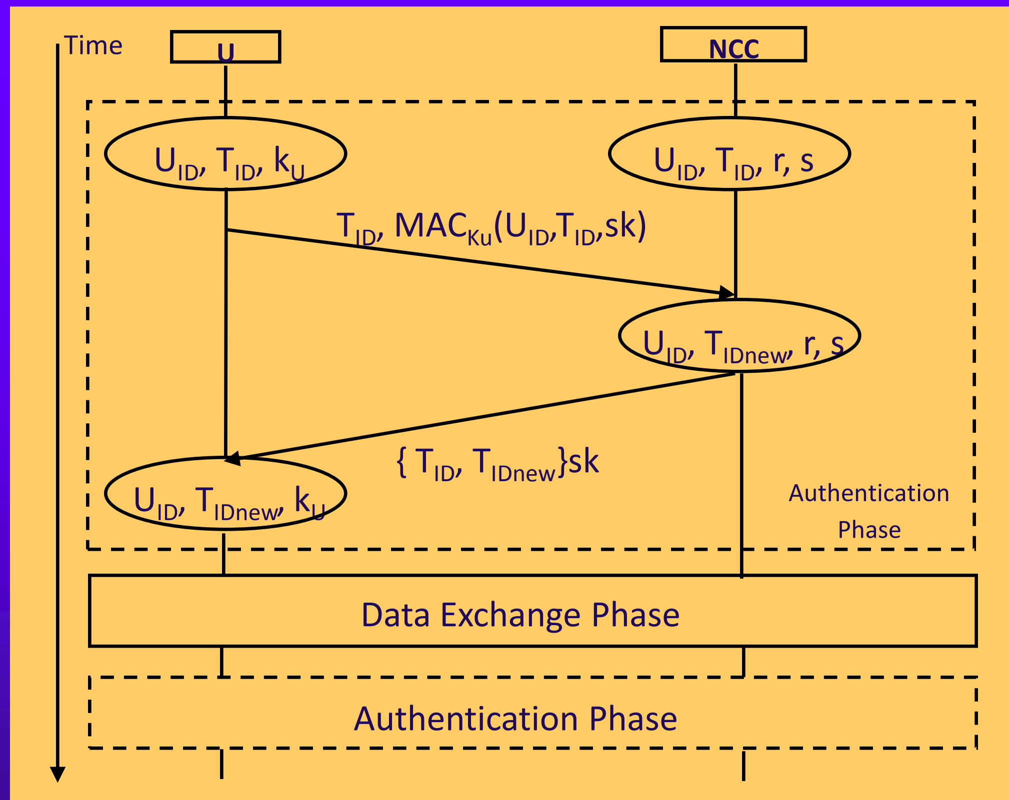
Authentication Request after SD-Attack
Desynchronised Users Fail Authentication



Vulnerable Protocols

- Mutual authentication and session key in terrestrial wireless fixed and mobile networks
  - A. Aziz and W. Diffie - "*Privacy and Authentication for Wireless Local Area Networks*", IEEE Personal Communications, First Quarter 1994
- Certificate distribution for nodes in a mobile ad-hoc network for satellite communications using VSATs, cellular networks (GPRS), unmanned aerial vehicle (UAV) communications
  - Tseng, YM., "*A heterogeneous-network aided public-key management scheme for mobile ad hoc networks*", International Journal of Network Management, vol. 17, pp. 3–15, 2007
- Mutual authentication between a mobile user and the service provider in a LEO satellite communications system
  - Hwang, MS., Yang, CC., Shiu, CY.- "*An authentication scheme for mobile satellite communication systems* ", ACM SIGOPS Operating Systems Review, Vol. 37, No. 4, October 2003, pp. 42-47.
  - YF. Chang and CC. Chang - "*An efficient authentication protocol for mobile satellite communication systems*", ACM SIGOPS Operating Systems Review, Vol. 39, Issue 1 (January 2005), 70-84.
  - Chen T.H., Lee W.B. and Chen H.B. - "*A self-verification authentication mechanism for mobile satellite communication systems*", Computers and Electrical Engineering, Volume 35, Issue 1 (January 2009), 41-48.

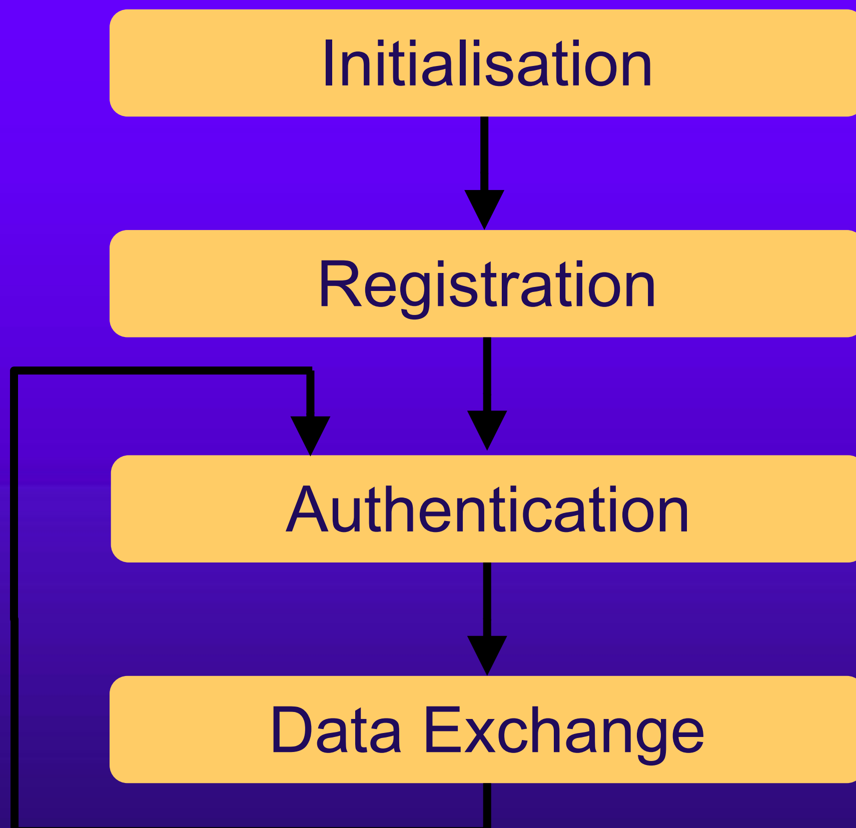
Example: CLC Protocol (2009)



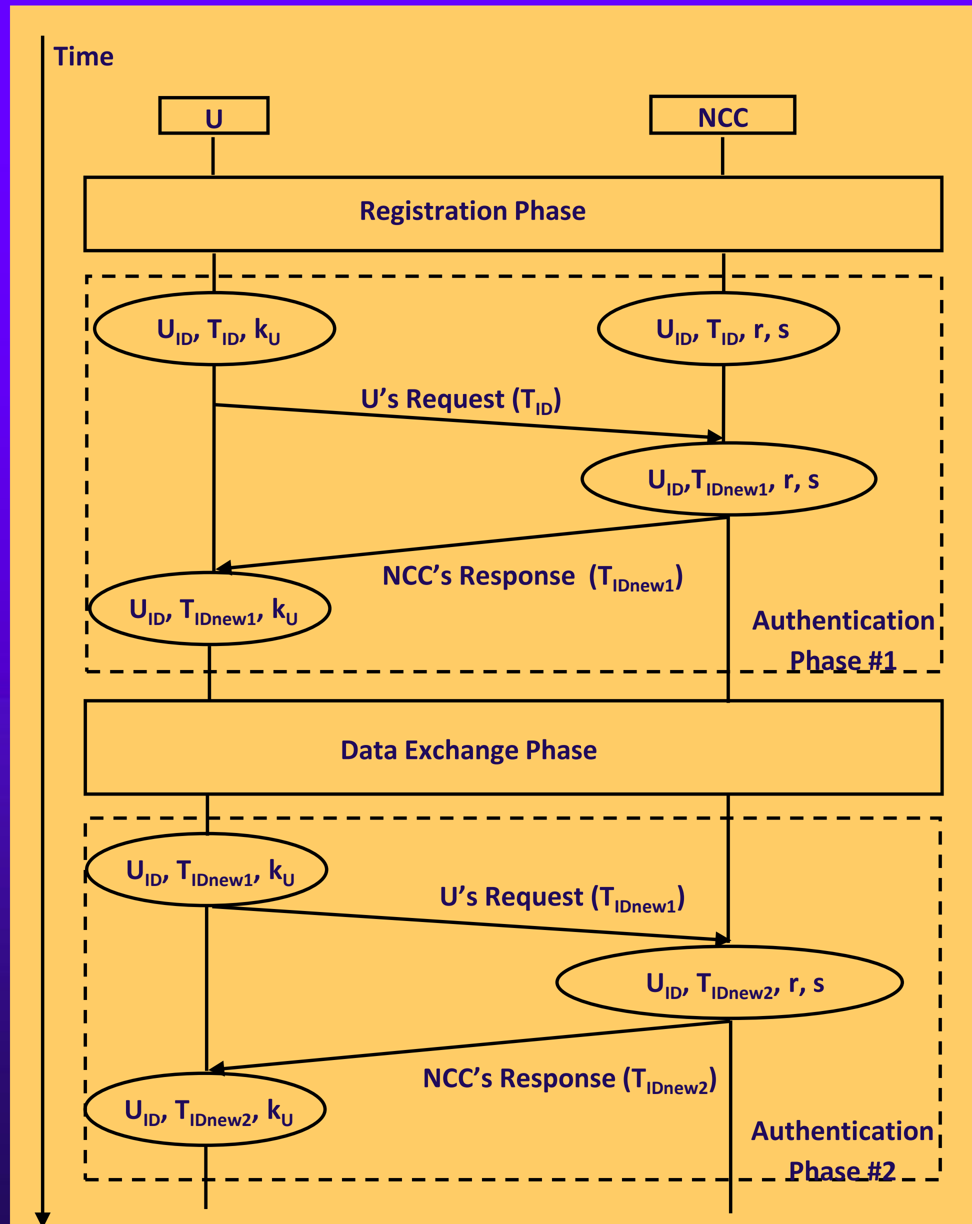
1. U -> LEO: T_{ID}, MAC-$k_U(U_{ID}, T_{ID}$, sk)
2. LEO -> NCC: T_{ID}, MAC-$k_U(U_{ID}, T_{ID}$, sk), LEO_{ID}
3. NCC -> LEO: $\{T_{ID}, T_{IDnew}\}$sk, LEO_{ID}
4. LEO -> U: $\{T_{ID}, T_{IDnew}\}$sk

1. U -> NCC: T_{ID}, MAC-$k_U(U_{ID}, T_{ID}$, sk)
2. NCC -> U: $\{T_{ID}, T_{IDnew}\}$sk

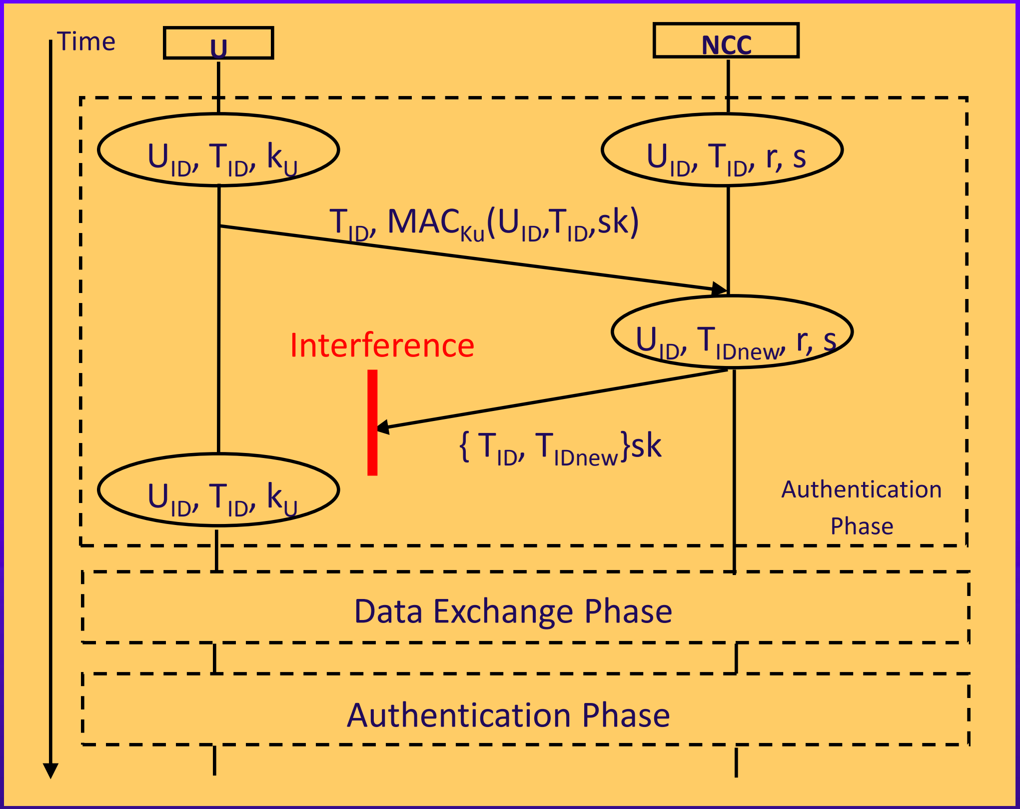
CLC Structure



CLC – Normal Execution

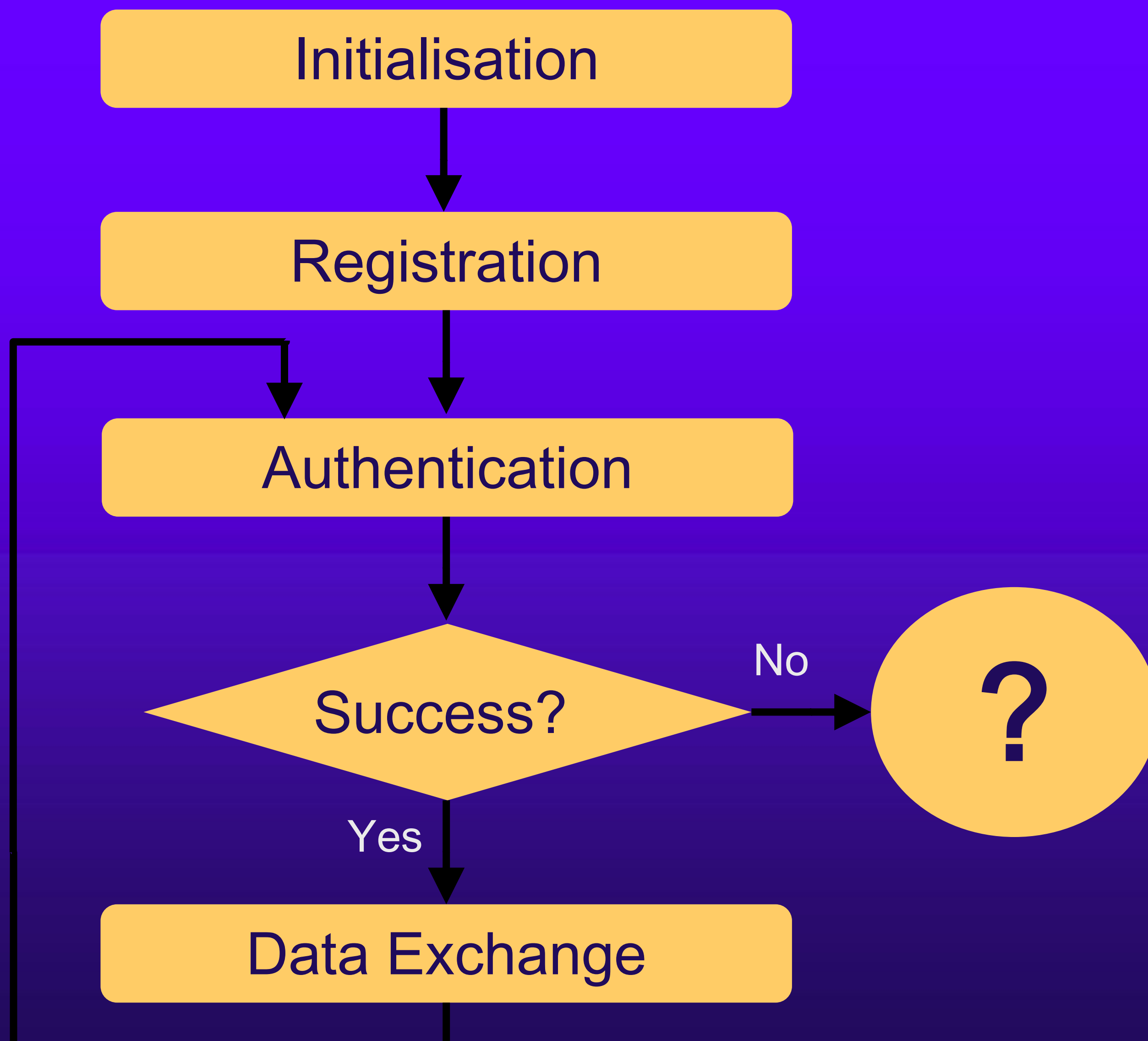


Attacking CLC



An SD attack inflicts asynchronous T_{ID} values for the NCC and U.

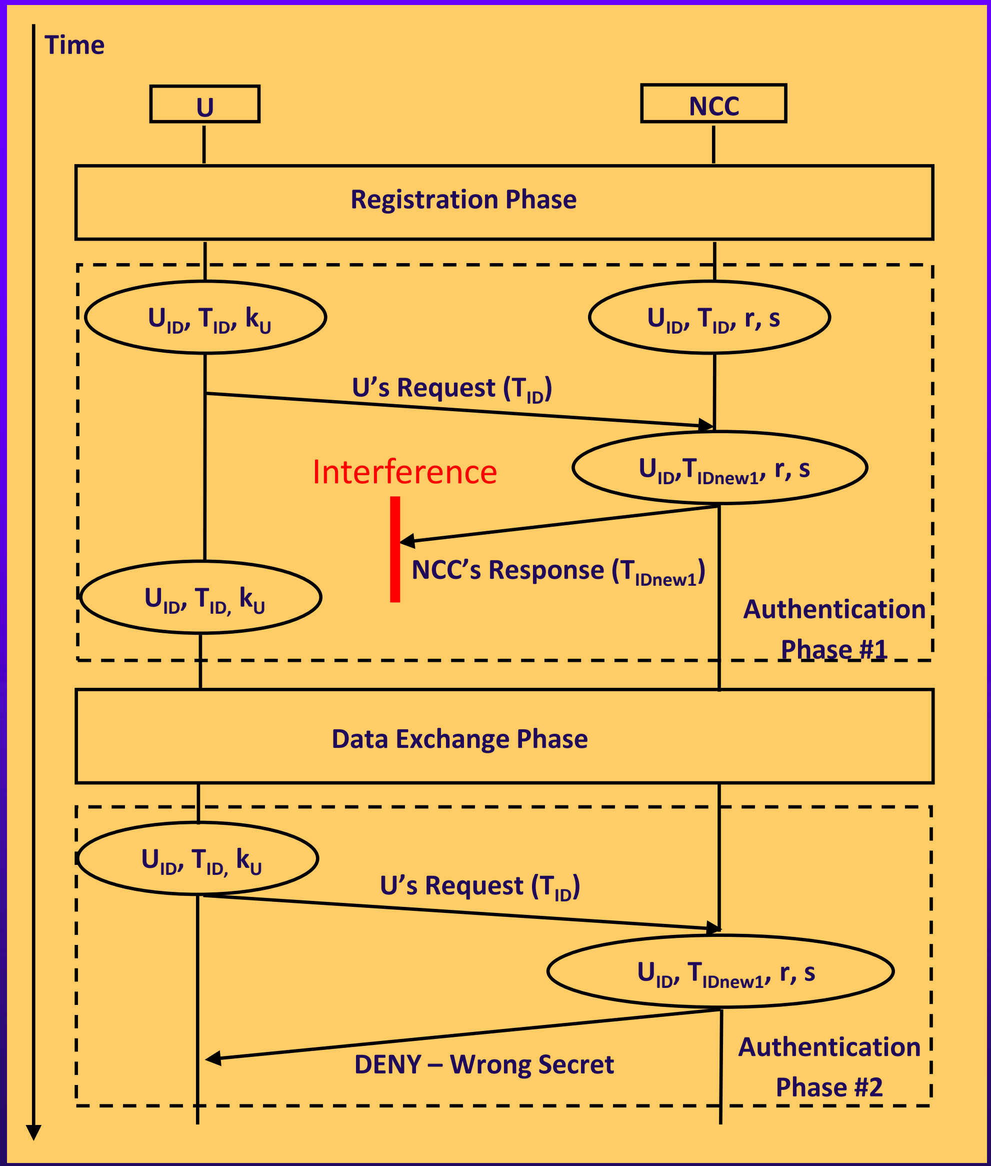
CLC Structure



CLC Problems

- U times out and resends using old T_{ID}
- NCC: no knowledge of earlier failure, expects U to use updated value T_{IDnew}
- NCC denies access - assumes replay of previous message
- U and NCC can not enter Data Exchange Phase
- U and NCC fail any further attempt to authenticate
- No resynchronisation phase or means are provided with the protocol
- Permanent Denial-of-Service Condition !!!

CLC – With Attack



Fixing CLC (1)

- "The transport layer guarantees delivery – indicated attack is not a problem"
- Problems:
  - Transport layer may report "cannot deliver" ⇒ actions taken by protocol must be specified
  - Many transport layer protocols are easily corrupted ⇒ attacker can create incorrect acknowledgements

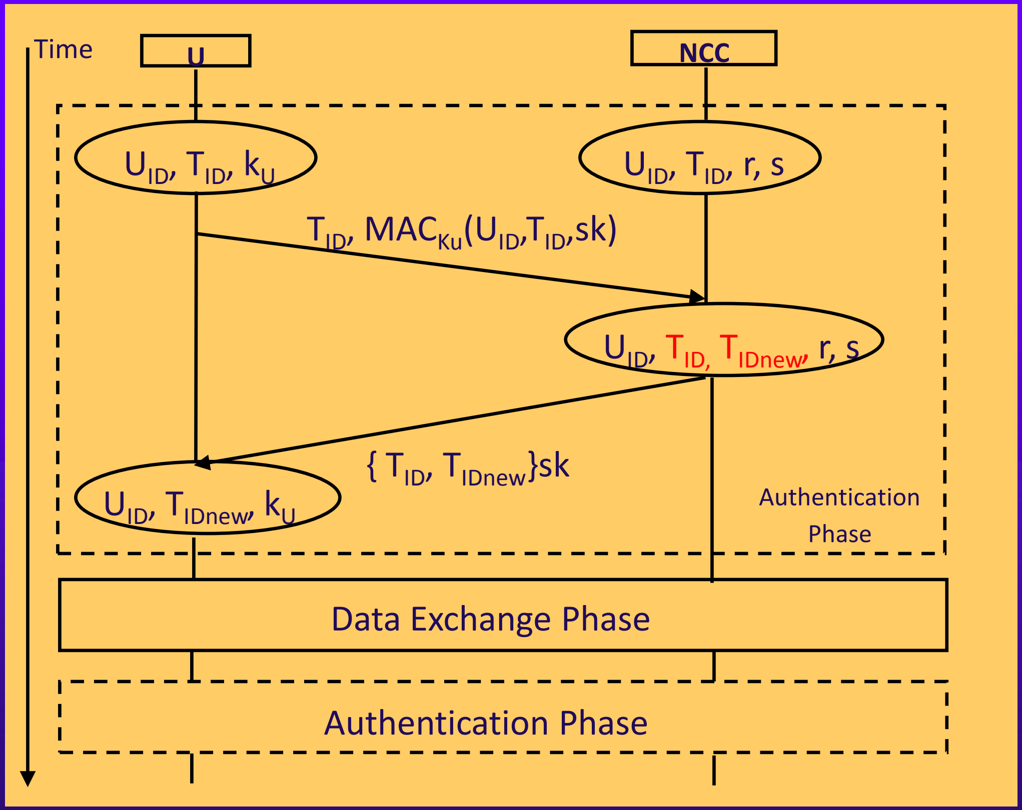
Fixing CLC (2)

- Accept current and previous secret (authenticate T_{ID} and T_{IDnew}), consider all earlier values as replays
- Problem:
  - Allows replay-attack: Intruder can repeatedly replay previous request to authenticate

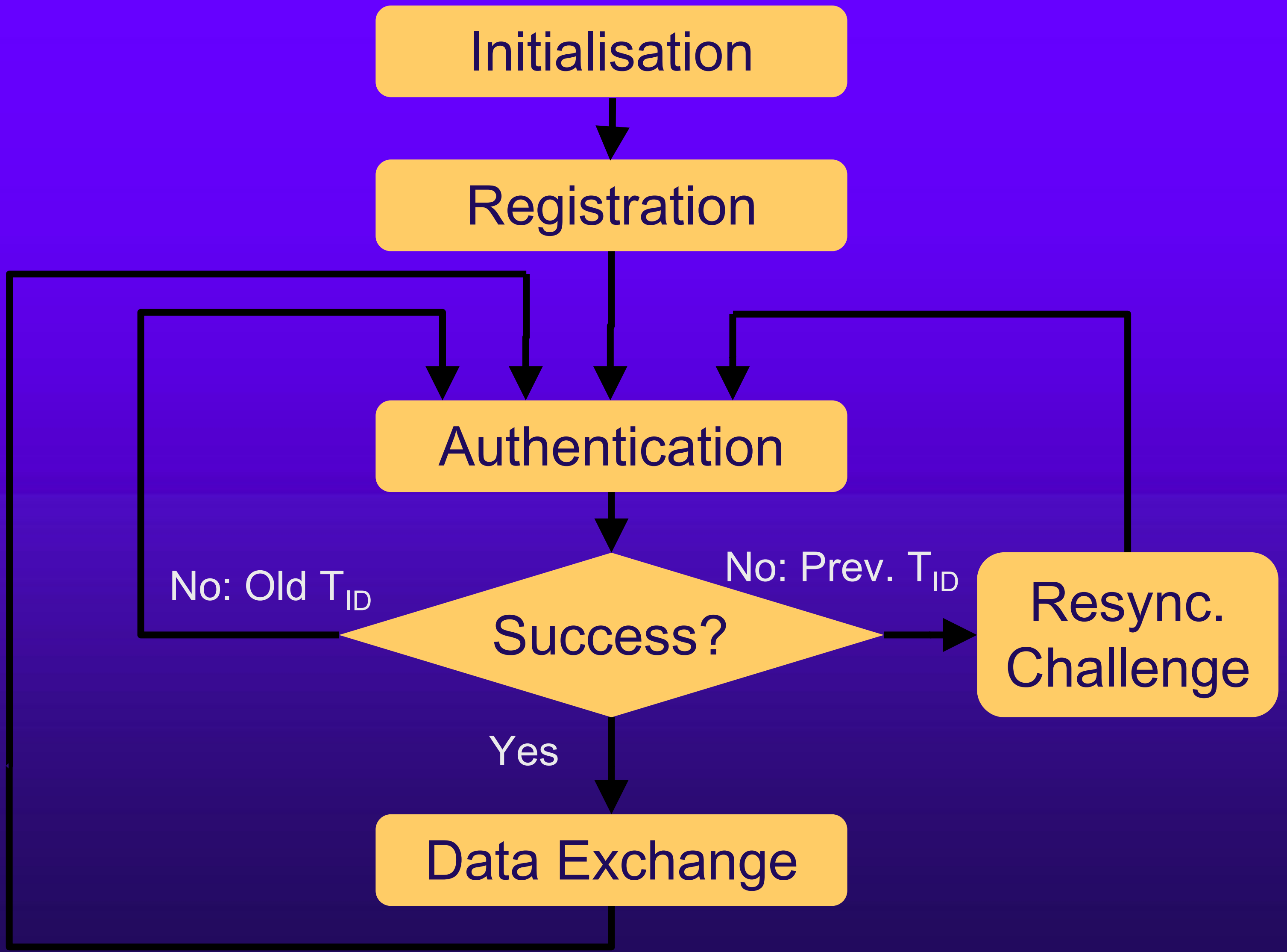
Fixing CLC (3)

- NCC stores current and previous (most recent) T_{ID} values.
- If correct T_{ID} is used, proceed as in original protocol.
- If previous T_{ID} is used, deny access & send resynchronisation challenge that allows user to catch up on current T_{ID}.

Fixed CLC Protocol



Fixed CLC Structure



Fixed CLC Messages

1. U -> LEO: T_{ID}, MAC-k_U(U_{ID}, T_{ID}, sk)
2. LEO -> NCC: T_{ID}, MAC-k_U(U_{ID}, T_{ID}, sk), LEO_{ID}

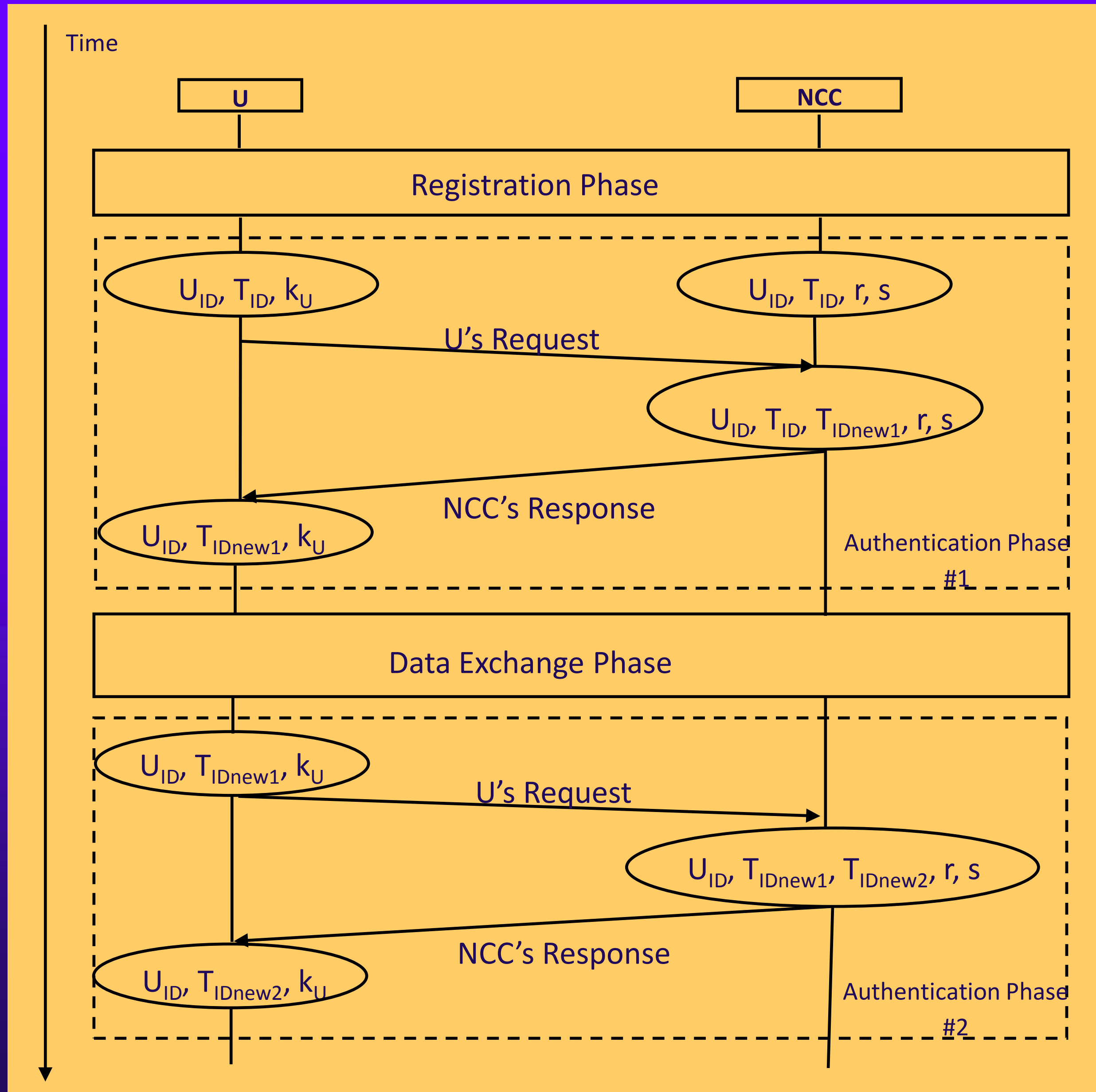
3.a. NCC -> LEO: $\{GRANT, T_{ID}, T_{IDnew}\}sk_{crt}$, LEO_{ID}
4.a. LEO -> U: $\{GRANT, T_{ID}, T_{IDnew}\}sk_{crt}$

Normal process

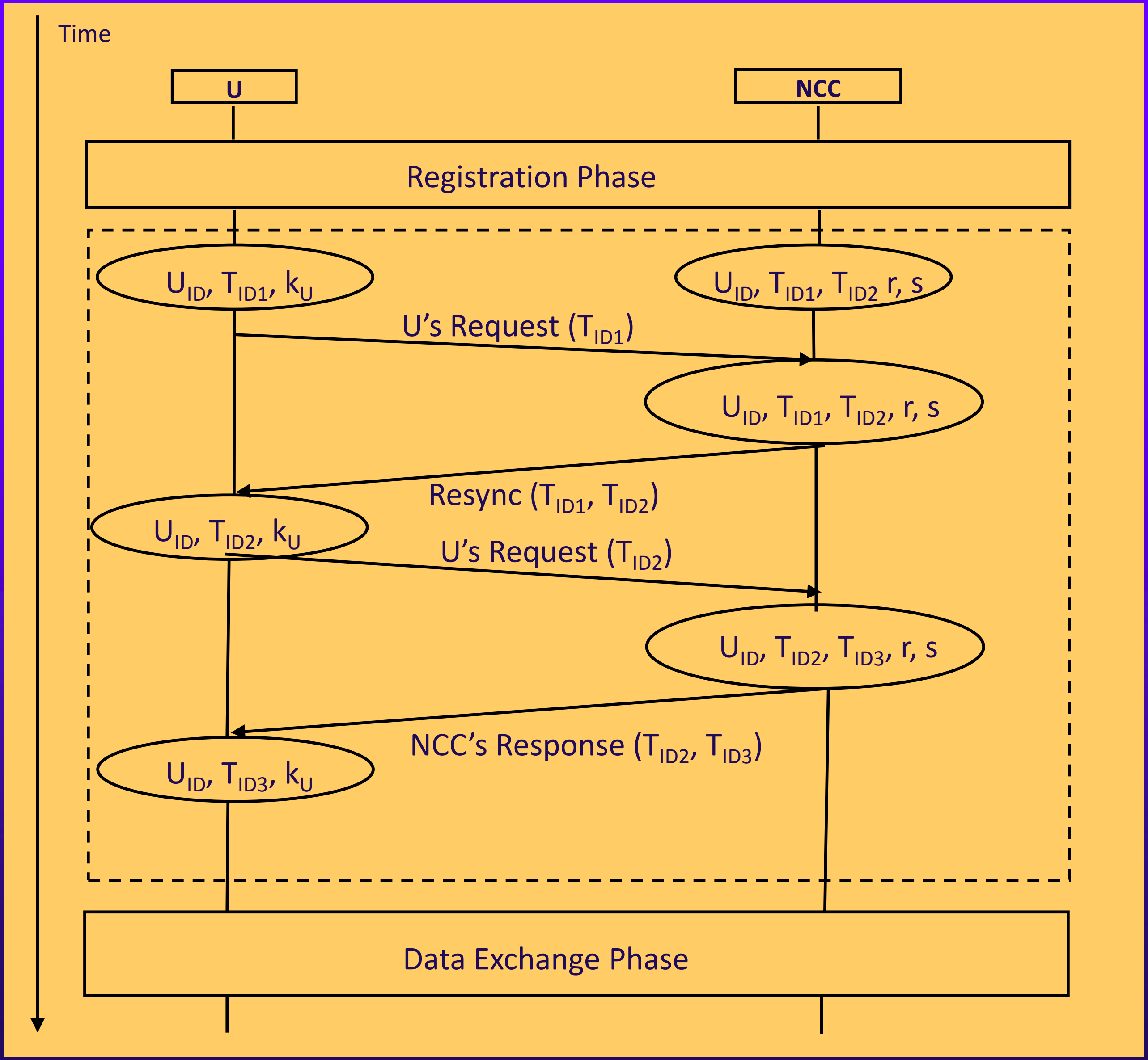
3.b. NCC -> LEO: $\{DENY, T_{ID}, T_{IDnew}\}sk_{prev}$, LEO_{ID}
4.b. LEO -> U: $\{DENY, T_{ID}, T_{IDnew}\}sk_{prev}$

Re-sync phase

Fixed CLC – Normal Run



Fixed CLC – After Attack



Summary

- Jamming is always possible
- Need mechanisms at application layer to recover if message are lost
- Cannot trust transport layer
- Sample jamming attack (suppress & desynchronise) against CLC protocol
- Fixed CLC allows resynchronisation after attack

Relevant Publications

- Lasc, I., Dojen, R. and Coffey, T., “A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications”, IGI International Journal of Information Security and Privacy, Volume 5, Issue 1, January 2011, pp. 33-49
- Lasc, I., Dojen, R. and Coffey, T., “Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications”, Elsevier Computers & Electrical Engineering (Special Issue on Modern Trends in Applied Security: Architectures, Implementations and Applications), Volume 37, Issue 2, March 2011, pp.160-168
- Lasc, I., Dojen, R., Coffey, T., “On Detecting New Attacks against Security Protocols that use Dynamic Shared Secrets”, to appear in Elsevier Computers & Security