OST
Ostschweizer
Fachhochschule

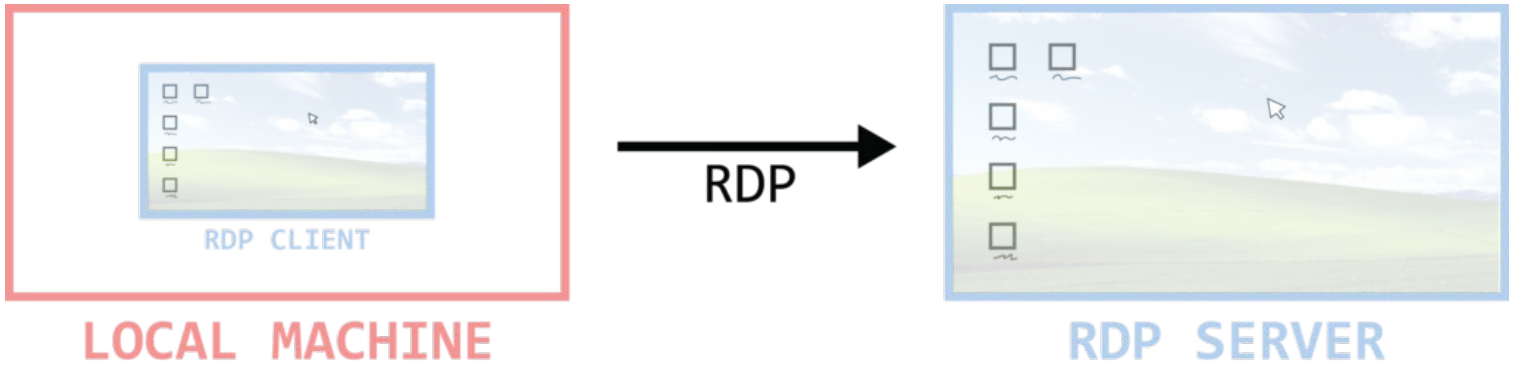
RDP Man-in-the-Middle

HS2024 Cyber Defense

Informatik

RDP (Remote Desktop Protocol)

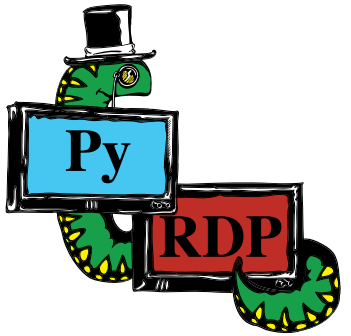
- Netzwerkprotokoll für den Remote-Zugriff auf Windows-Rechner
- Grundfunktionalität:
  - Übertragung von Monitor (Ausgabegerät) vom Remote-Server zum Client
  - Übertragung von Tastatur und/oder Maus (Eingabegeräte) vom Client zum Remote-Server
- Kommunikation basiert auf mehreren Kanälen



RDP Security

- Standard Security:
  - Datenverkehr wird mit RC4 verschlüsselt (= symmetrischer Schlüssel)
  - Zufallswerte werden während der Verbindungsaufbau ausgetauscht
- Enhanced Security:
  - Ermöglicht das Auslagern sämtlicher Sicherheitsoperationen an ein externes Sicherheitsprotokoll.
    - TLS
    - **CredSSP (mit NLA möglich)**
    - RDSTLS
  - Die Entscheidung des Sicherheitsprotokoll kann entweder "negotiation-based" oder "direct" sein.

PyRDP



- Python Man-in-the-Middle Tool und Bibliothek
- Von GoSecure für Pentests & Forschungszwecke entwickelt (2018)
- Features:
  - RDP Man-in-the-Middle
  - RDP Player
  - RDP Zertifikat Cloner

OST

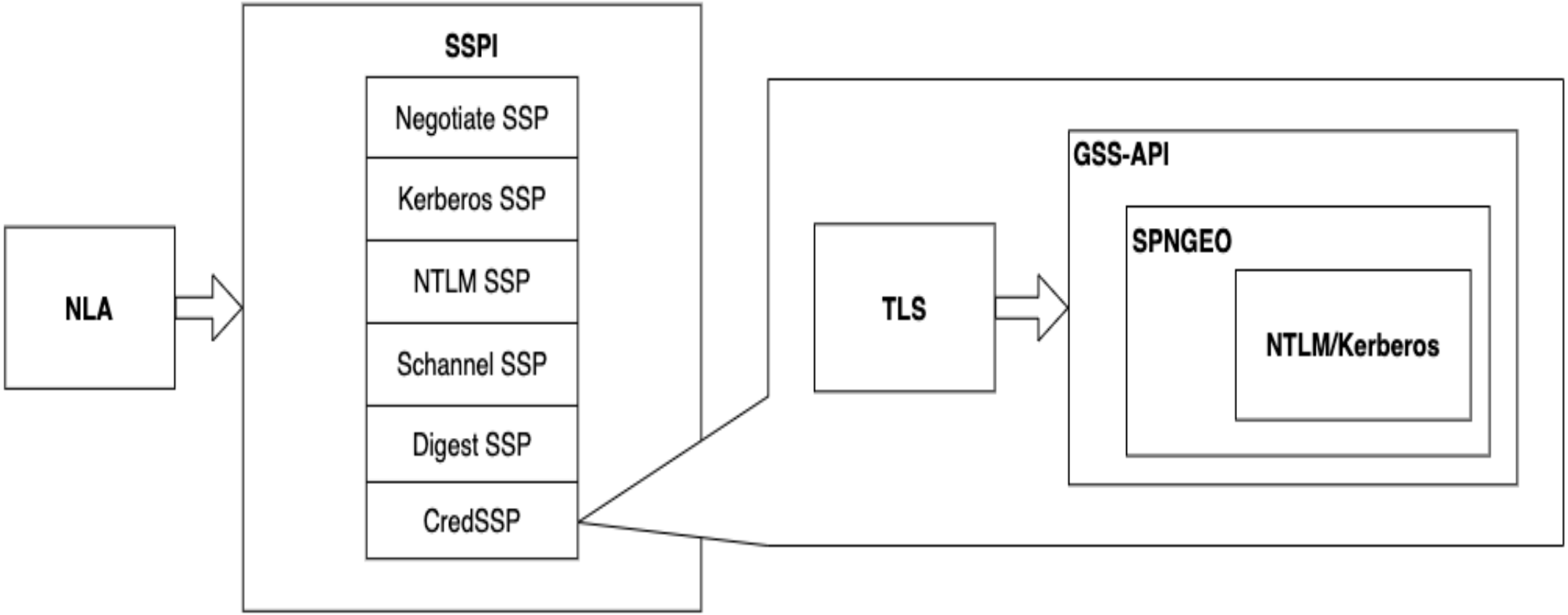
Kann NLA mit PyRDP umgangen werden?

- «Im vergangenen Oktober 2020 wurde behauptet, dass PyRDP auch RDP-Verbindungen, die mit NLA/CredSSP geschützt sind, intercepten kann.» Dieser Frage ist eine BA der OST nachgegangen. Hier ein Ausschnitt aus deren Ergebnissen.

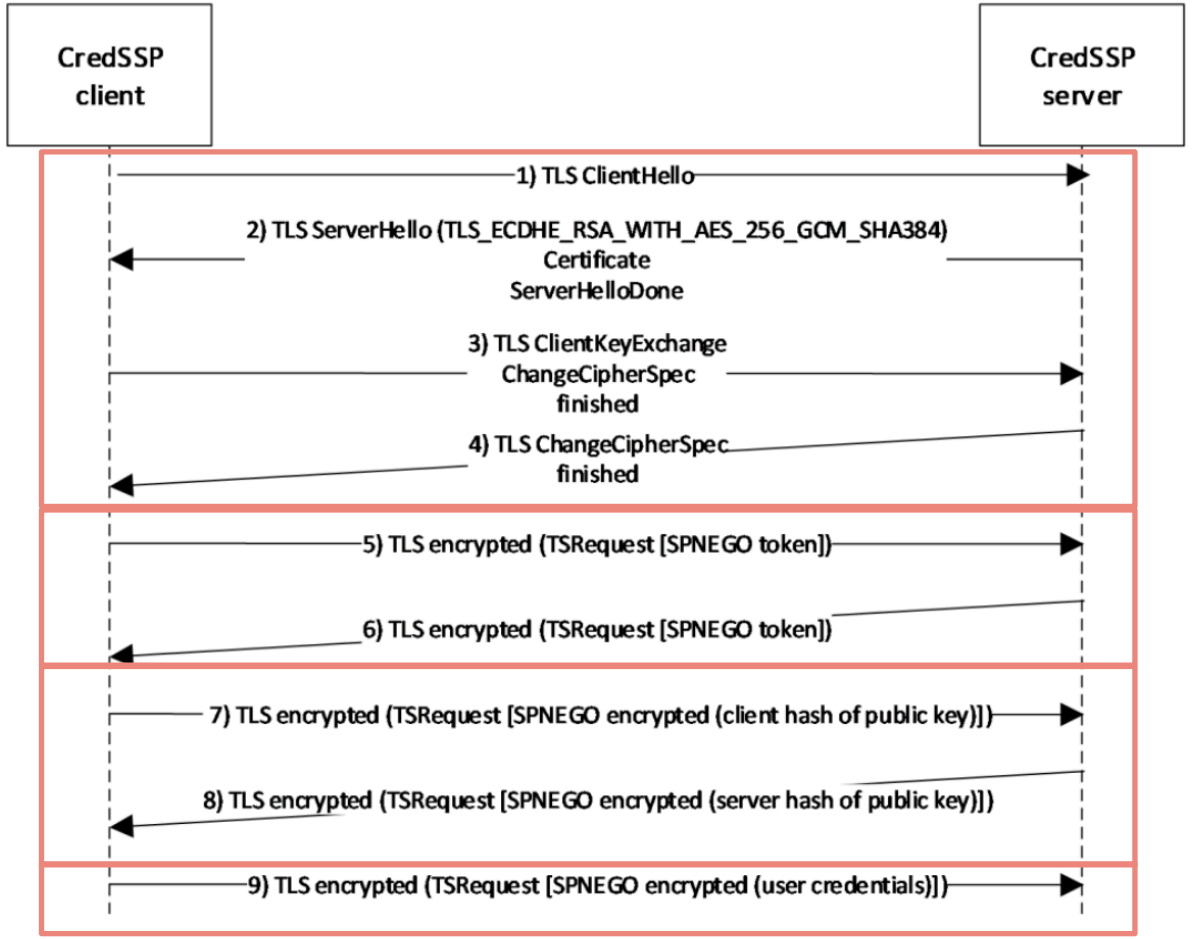
- Challenge:
  - Analyse von RDP mit NLA/CredSSP
    - Studium der NLA, SSPI, SPNEGO, CredSSP
  - Aufzeigen der Machbarkeit des MitM oder eben Sicherheit
  - Analyse der verschiedenen RDP Varianten (Historie)
  - Aufzeigen von bereits «gebrochenen» Protokollvarianten
  - Analyse der PyRDP-Implementation
  - Implementation eines MitM PoC basierend auf PyRDP (falls möglich)

OST

RDP Protokoll Stack



CredSSP Handshake mit NTLM



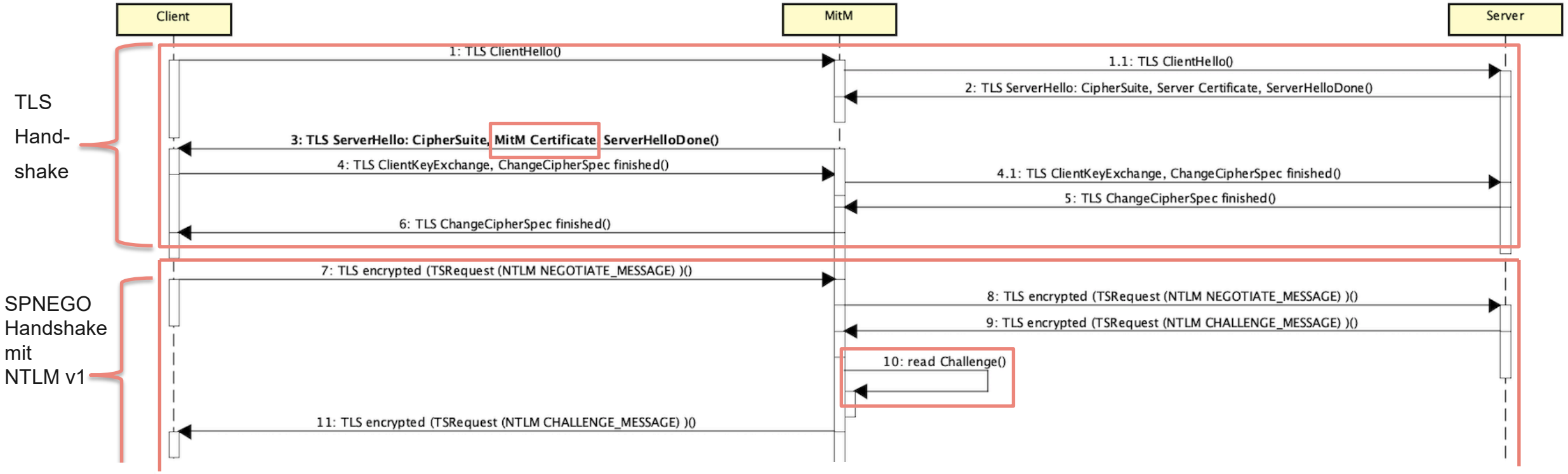
Cipher Spec Phase

TLS SPNEGO Exchange

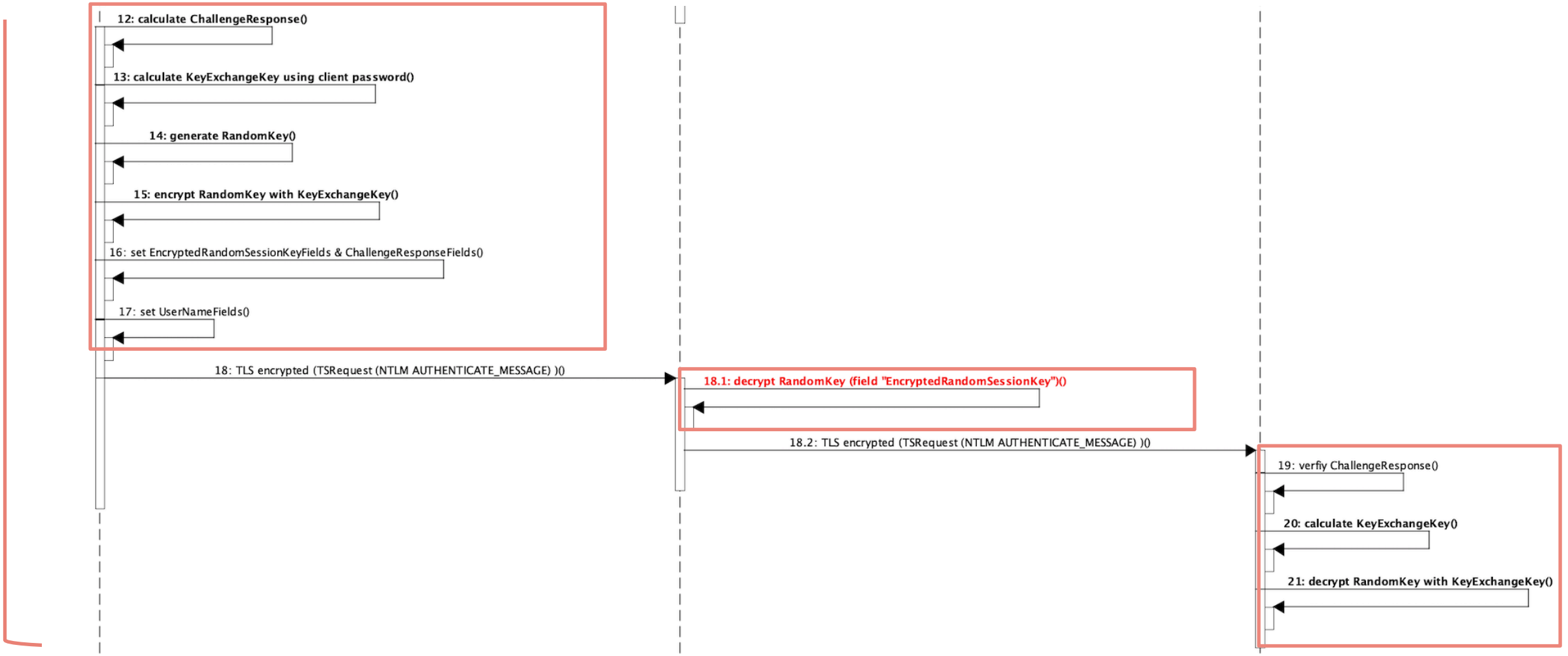
TLS PubKey Verification

User Credentials

CredSSP mit NTLM Auth – MitM (1/2)



CredSSP mit NTLM Auth – MitM (2/2)

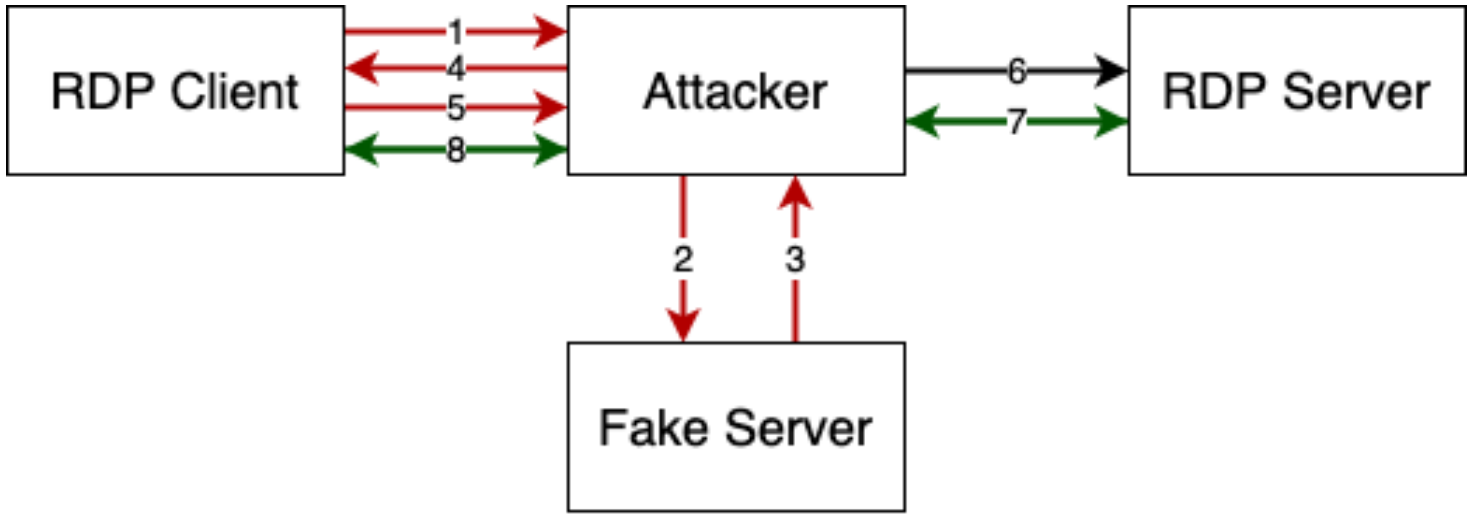


OST

Ergebnisse der Machbarkeitsanalyse

- Passwort des Benutzer beim MitM nicht bekannt (Challenge Response Verfahren)
- Randomkey (NTLM) für MitM kann nicht ausgelesen werden
- PubKeyAuth Feld nicht austauschbar
- Fazit: Umgehung NLA Protection nicht möglich

Wie könnte MITM bei RDP und NLA trotzdem funktionieren?



Schritte 1-5: Anmeldedaten mittels gefälschtem Login-Screen auslesen

Schritt 6: Anhand erhaltene Anmeldedaten sich beim RDP Server authentifizieren (NLA)

Schritt 7-8: Hergestellte RDP-Verbindung dem Client weiterleiten

OST