RDP Man-in-the-Middle

Diplomanden

Aynkaran SUNDRALINGAM

Kevin Moro

Danusan PREMANANTHAN

Examinator
Cyrill Brunschwiler

Experte
Christoph Frei, Wallisellen, ZH

Themengebiet
Sicherheit, Software

Einleitung: Man-in-the-Middle ist eine Cyberangriffstechnik, bei der sich der Angreifer in den Datenverkehr zwischen zwei Kommunikationsteilnehmern einschleust und beiden vortäuscht, dass sie direkt mit dem jeweils anderen kommunizieren. Das Ziel dieses Angriffes ist es, die Kommunikation zwischen den Kommunikationsteilnehmern abzufangen, mitzulesen oder unbemerkt zu manipulieren.

In dieser Arbeit soll nun die Machbarkeit eines solchen Angriffes auf das Remote Desktop Protocol (RDP), ein Kommunikationsprotokoll von Microsoft, das den Fernzugriff auf Windows-Rechner ermöglicht, untersucht werden. Dabei soll aber die erweiterte Sicherheitsstufe «Enhanced Security NLA» von RDP verwendet werden.

Sollte die Machbarkeitsanalyse zeigen, dass ein Man-in-the-Middle-Angriff auf eine mittels NLA (CredSSP) authentifizierte RDP-Verbindung möglich sein sollte, soll ein Proof of Concept für das Tool "PyRDP" implementiert werden.

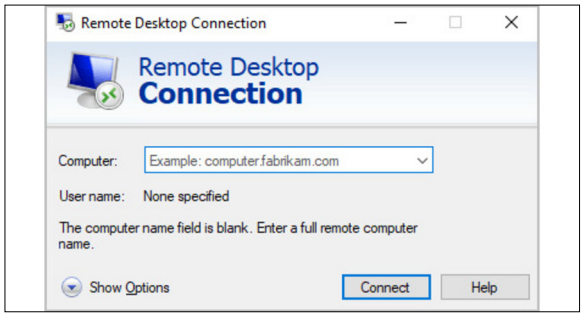
Vorgehen: Um die Durchführbarkeit dieses Angriffs beurteilen zu können, musste zunächst das RDP-Protokoll selbst näher untersucht werden. Denn es ist wichtig zu wissen, welche Sicherheitsaspekte RDP unterstützt bzw. verwendet und welche Schritte zum Aufbau einer Verbindung notwendig sind. Anschliessend wurden relevante Protokolle wie CredSSP, SPNEGO oder NTLM, die bei der vorherigen Untersuchung gefunden wurden, analysiert.

Die Machbarkeitsanalyse wurde auf Basis der Theorie und durch die Durchführung von Paketanalysen mit Tools wie Wireshark vorgenommen. Basierend auf diesen Analysen konnte schliesslich die Machbarkeit eines Man-in-the-Middle Angriffs evaluiert werden.

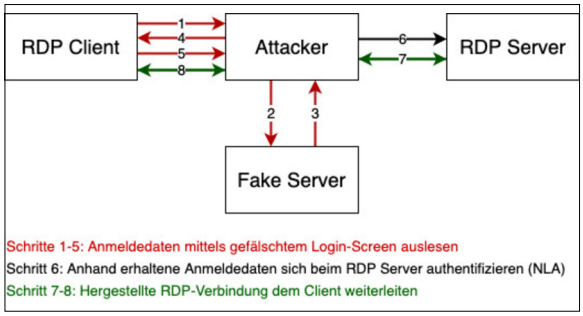
Ergebnis: Aufgrund der durchgeführten Machbarkeitsanalyse konnte festgestellt werden, dass ein direkter Man-in-the-Middle Angriff auf eine mit NLA authentifizierte RDP-Verbindung nicht möglich ist. Denn durch die theoretische Analyse konnte herausgefunden werden, dass das Passwort des RDP-Clients in die Berechnung eines Schlüssels einfliesst, der im Authentifizierungsverfahren verwendet wird.

Ein Man-in-the-Middle-Angriff wäre jedoch möglich, wenn der Angreifer bereits im Besitz des Client-Passwortes ist, bevor der Client und der Server das von NLA verwendete Authentifizierungsverfahren durchlaufen.
Um diese Variante zu realisieren, wurde ein alternativer Man-in-the-Middle-Ansatz gewählt. In einem ersten Schritt wird das Kennwort des Clients über einen vorgetäuschten Anmeldebildschirm eingelesen. Mit Kenntnis des Kennworts kann der Angreifer nun in einem zweiten Schritt eine gültige RDP-Verbindung zum Server aufbauen. Diese wird dann vom Angreifer an den Client weitergeleitet, so dass der Client den Eindruck hat, er sei direkt mit dem Server verbunden.

RDP-Client
Eigene Darstellung



Alternative Man-in-the-Middle Variante
Eigene Darstellung



Vorgetäuschter Anmeldebildschirm
Eigene Darstellung