Securing RDP deep dive
Agenda

- RDP transport security history
- TLS for RDP over TCP 3389
- NLA authentication with Kerberos and NTLM
- RDP single-sign-on (SSO)
- TLS for RDP over RD Gateway
  - TCP 3389 tunneled in HTTPS
- Limiting pass-the-password and pass-the-hash
- RestrictedAdmin mode
Sample environment
Windows 2003 and older

- RDP security layer
  - DH key exchange *(unauthenticated)*
  - safe against passive eavesdropping
  - prone to MITM attacks
  - no server authentication

- Windows 2003 SP1
  - TLS 1.0 support
  - manual certificate selection
Windows 2003 TLS certificate requirements

- **Subject or SAN**
  - CN or DNS name of the RDP server used by client

- **Enhanced Key Usage (EKU)**
  - Server Authentication (OID 1.3.6.1.5.5.7.3.1)

- **Key Usage**
  - Key encipherment
  - TLS 1.0 only supported by Windows 2003
  - TLS 1.0 does not have ECDH/RSA suites

- **CSP**
  - Microsoft RSA SChannel Cryptographic Provider

- **Signature**
  - might be signed by SHA2 (SHA256) if updates installed (KB938397, KB968730)
Windows 2003 RDP TLS configuration

- **Security layer:** SSL
- **Encryption level:** Client Compatible
- **Certificate:** R1.GOPAS.virtual
Incorrect or no certificate on the server

- The remote computer requires that authentication be enabled to connect. The connection cannot proceed because authentication is not enabled.
Negotiate or explicit TLS?

- Client compatibility (TLS requires MSTSC 5.2)
- Active MITM **downgrade** possible with Negotiate
- Must enforce TLS on client

---

![Diagram showing client, MITM, and RDP server with decision points and outcomes.]

- **Client**
  - TLS or RDP?
  - RDP only
  - OK, then RDP

- **MITM**
  - ??? whatever ???

- **RDP Server**
Enforce server authentication on client (KB895433)

- .RDP file setting authentication level: 1
- HKLM\Software\Microsoft\Terminal Server Client AuthenticationLevelOverride DWORD = 1

- No authentication = 0
- Attempt authentication = 2
Windows 2008 RDP TLS certificate

- Remote Desktop Configuration service
- **Self-signed** auto-generated TLS server certificate
  - changed with primary DNS suffix or computer name change
  - untrusted
- **Manually** selected TLS server certificate
  - manual configuration
- **GPO based** automatically enrolled TLS server certificate
  - automatically enrolled from enterprise online AD CS
Windows Vista/2008+ TLS certificate requirements

- Subject or SAN
  - CN or DNS name of the RDP server used by client
- Enhanced Key Usage (EKU)
  - Remote Desktop Authentication (OID 1.3.6.1.4.1.311.54.1.2)
  - Server Authentication (OID 1.3.6.1.5.5.7.3.1)
- Key Usage
  - Key encipherment
  - Windows 7/2008 R2 still uses only TLS 1.0, does not have ECDH/RSA suites
  - Digital signature
  - Windows 8/2012 supports TLS 1.1+ with ECDH/RSA suites
- CSP or CNG/KSP
  - any
- Signature
  - might be signed by SHA2 (SHA256)
GPO certificate template selection

Certificate Template Name: GOPASDomainRSARDPServerCSP

This policy setting allows you to specify the name of the certificate template that determines which certificate is automatically selected to authenticate an RD Session Host server when SSL (TLS 1.0) is used to secure communication between a client and an RD Session Host server during RDP connections.
GPO certificate template selection

- certificate enrollment performed by Remote Desktop Configuration service
GPO configuration for TLS on server

Require use of specific security layer for remote (RDP) connections

- Enabled
- Not Configured
- Disabled

Comment:

Supported on: At least Windows Vista

Options:
- Security Layer: SSL (TLS 1.0)
- Choose the security layer:
  - SSL (TLS 1.0)
  - Negotiate
  - RDP

Help:
This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this policy setting, all communication between RD Session Host servers and clients will use the selected security layer.
Network Level Authentication (NLA)

- Additional authentication during channel establishment
  - Kerberos or NTLM
- Requires TLS
- Removes the TLS certificate quality requirement
- With Kerberos provides mutual authentication of the channel
- Supported with MSTSC 6.0+
NLA requirement on the server

- With Kerberos the authentication is mutual and as such does not require enforcement on client
RDP is basic authentication

- Password transported in "full" or "plaintext" form
- Client LSASS does not supply plaintext password to client applications
  – always typed or stored locally
RDP single-sign-on (SSO)

- With TLS and NLA with Kerberos
  - requires server authentication with Kerberos
- Client LSASS passes plaintext password to the remote server encrypted by TGS key
LSAS (local security authority sub system)

- **LSASS**
  - full-text pwd
  - pwd #
  - Kerberos tickets
  - IE
  - Outlook
  - Explorer
  - Client
  - HTTP, SMB, DCOM

- **Server**
  - SmbSrv
  - WebSrv

- **Client**
  - IE
  - Outlook
  - Explorer

- **In-band transport**

- **AD**
  - SMB SAM pipe
  - DCOM Netlogon
  - Secure Channel

- **DC**
Stealing user password from LSASS memory

- Local administrator on the RDP server
  - just read it from LSASS memory
- Windows 10 can store LSASS private data in Hyper-V Virtual Secure Mode (VSM) outside of the OS
  - just like a smart card
RD Gateway

RDP Server

GPS-WFE1.gopas.virtual

RDP Certificate

3389

RDP Gateway

rdp.gopas.cz

HTTPS Certificate

HTTPS

RDP + TLS

Client
RD Gateway certificate requirements

- **Subject or SAN**
  - CN or DNS name of the RD Gateway server used by client

- **Enhanced Key Usage (EKTU)**
  - **Server Authentication** (OID 1.3.6.1.5.5.7.3.1)

- **Key Usage**
  - Key encipherment
  - Windows Vista/2008 still uses only TLS 1.0, does not have ECDH/RSA suites
  - Digital signature
  - Windows 7/2008 R2 supports TLS 1.1+ with ECDH/RSA suites

- **CSP or CNG/KSP**
  - any

- **Signature**
  - might be signed by SHA2 (SHA256)
Trust over RD Gateway

- Client would have to trust both the **internal certificate** and the **RD Gateway public certificate**
- Windows 2012 offers KDC Proxy Service (KPS) – requires Windows 8 client
MSTSC and KDC proxy

- To enable KDC proxy on client, set the RDP file property
  - rdgiskdcproxy:i:1
- To set the property centrally
  - Set-RDSessionCollectionConfiguration -CustomRdpProperty "rdgiskdcproxy:i:1"
Limit pass-the-hash attacks

- Use smart-cards with Kerberos PKINIT
  - no password
  - cannot be copied
- Limit TGT lifetime (1 hour)
  - 1 hour ~ session duration
- Disable NTLM
  - since Windows 7/2008 R2

or use Restricted Admin mode
  - since Windows 8/2012 RDP server
RestrictedAdmin mode

- `mstsc /restrictedAdmin`
- Does NOT send plaintext password
  - authenticates only with the NLA Kerberos
- Cannot access network resource
  - by default receives RDP computer's credentials
- Must be configured
  - `HKLM\System\CurrentControlSet\Control\LSA DisableRestrictedAdmin = DWORD = 0`
  - `DisableRestrictedAdminOutboundCreds = DWORD = 1/0`
RestrictedAdmin with GPO preferences
Děkuji za pozornost!

Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security | CHFI | CEH | CISA |
ondrej@sevecek.com | www.sevecek.com |