



The Risks of RDP and How to Mitigate Them

Olivier Bilodeau (@obilodeau), GoSecure

Lisandro Ubiedo (@_lubiedo), GoSecure





Some The Risks of RDP and How to Mitigate Them

Olivier Bilodeau (@obilodeau), GoSecure

Lisandro Ubiedo (@_lubiedo), GoSecure





Some

The Risks of RDP and

How to Mitigate Them

And a vuln reported to Microsoft

Olivier Bilodeau (@obilodeau), GoSecure

Lisandro Ubiedo (@_lubiedo), GoSecure



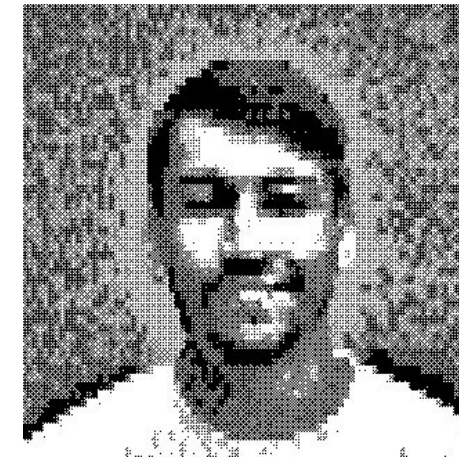
About Us



Olivier Bilodeau

Cybersecurity Research Lead at GoSecure

- Jack of all trades, master of none
- Speaker BlackHat, RSAC, SecTor, etc.
- Co-founder MontréalHack (hands-on security workshops)
- NorthSec VP Training / Hacker Jeopardy



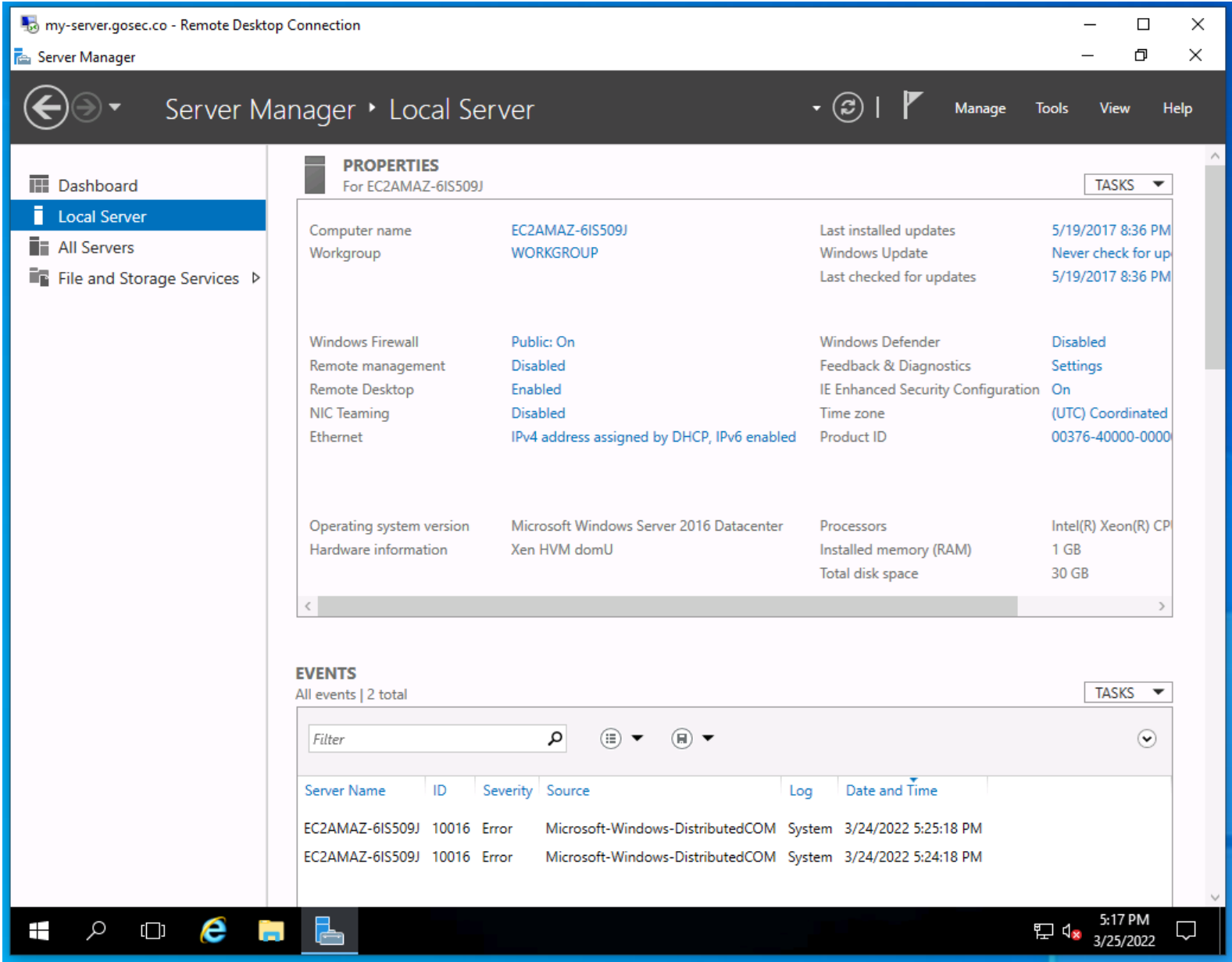
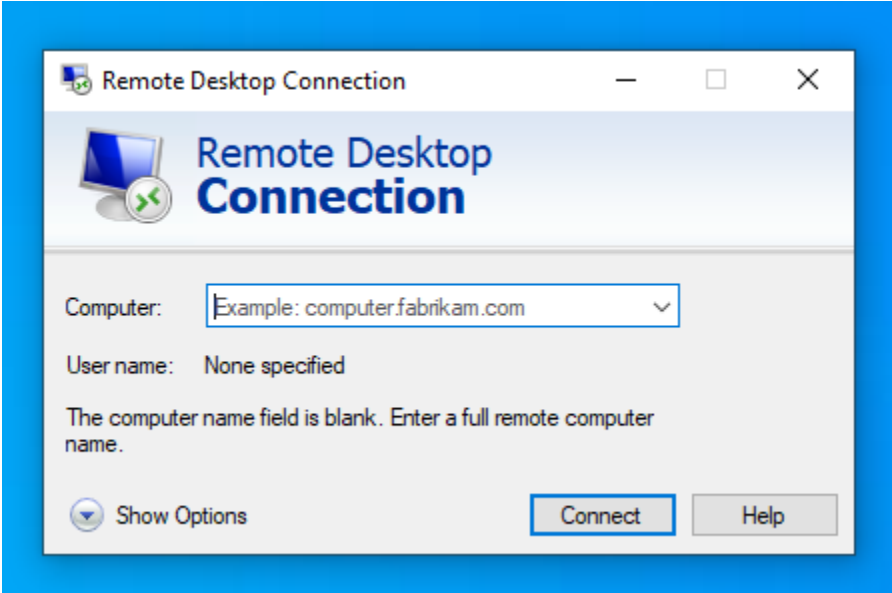
Lisandro Ubiedo

Security Researcher at GoSecure

- Cloud-based trickery
- Malware analysis and Threat research
- Stratosphere Labs collaborator

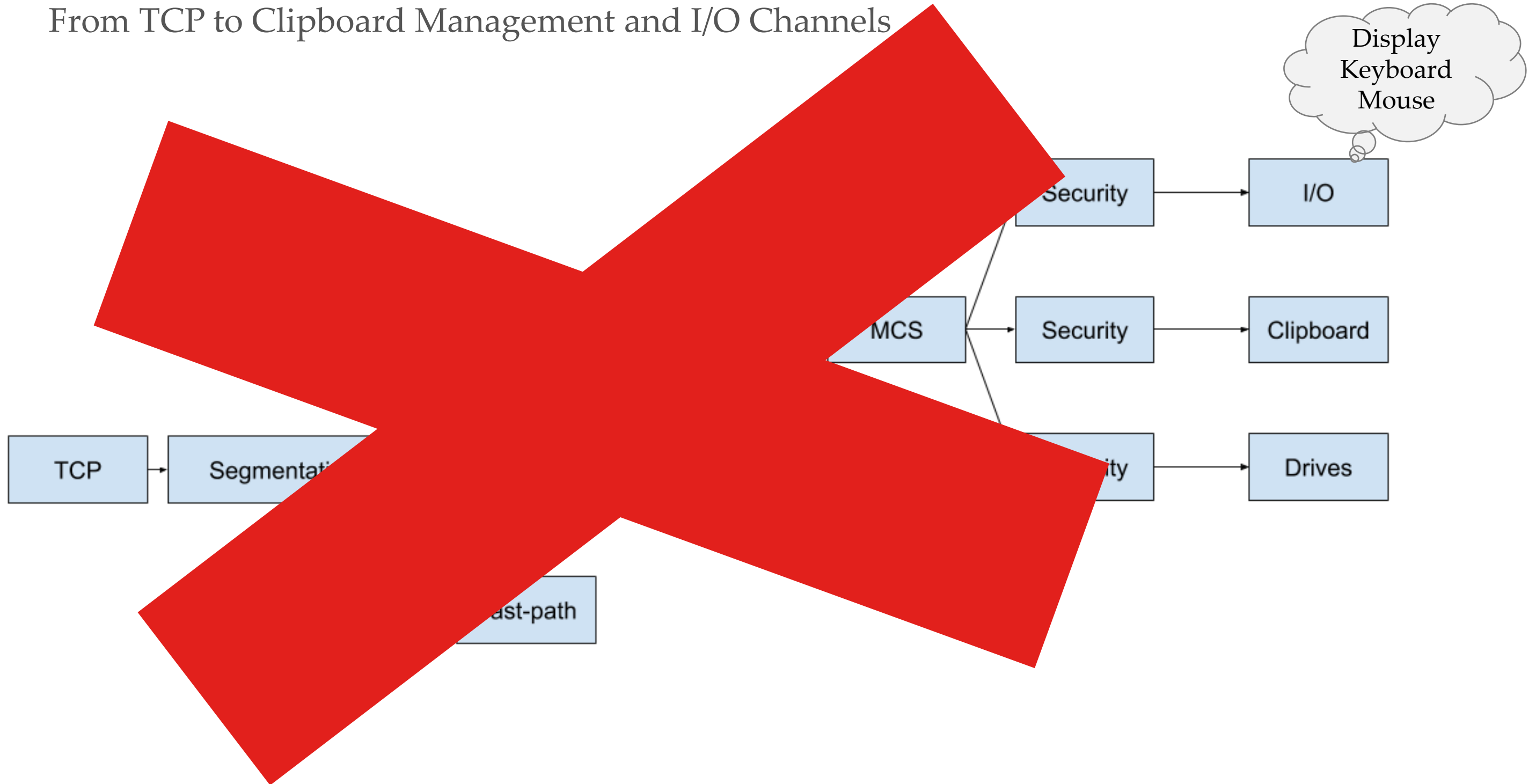
Introduction to RDP

Remote Desktop Protocol



RDP Layers

From TCP to Clipboard Management and I/O Channels



RDP Security



- RC4 + Graphical login (dead)
- TLS + Graphical login (legacy)
- TLS + Network Level Authentication (NLA) which relies on CredSSP
- Remote Desktop Credential Guard and Restriction



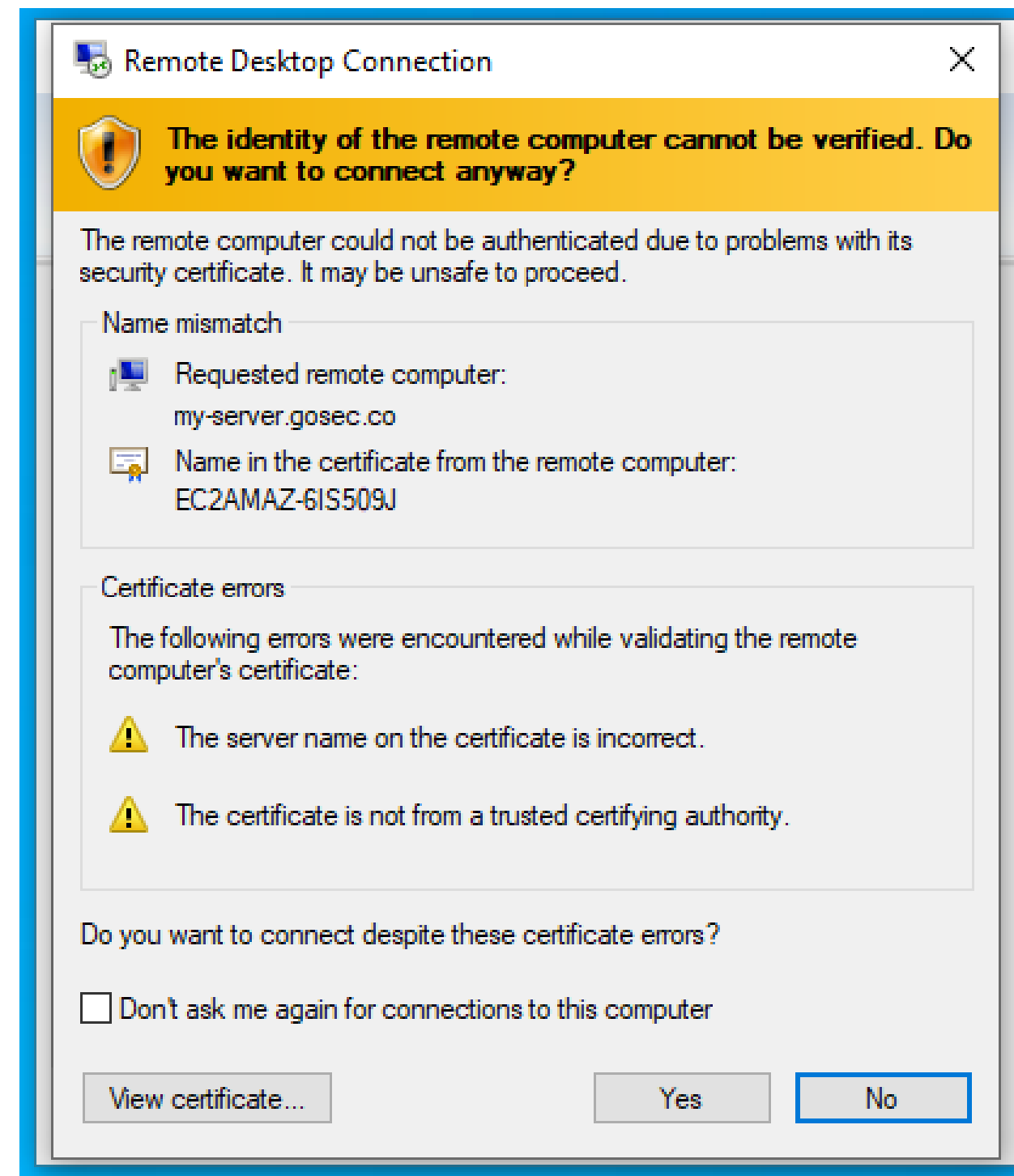
A Risk of RDP: MITM

MITM Risks



- **Security Downgrade Attacks**
 - NLA -> TLS
- **Clicking Through Warnings**
- **Impact**
 - Display
 - Keyboard
 - Clipboard
 - Server-side takeover
 - Client-side file stealing
 - Client-side takeover*

*: implementation pending



How? By Our Open Source Attack Tool: PyRDP

Learn More About It!

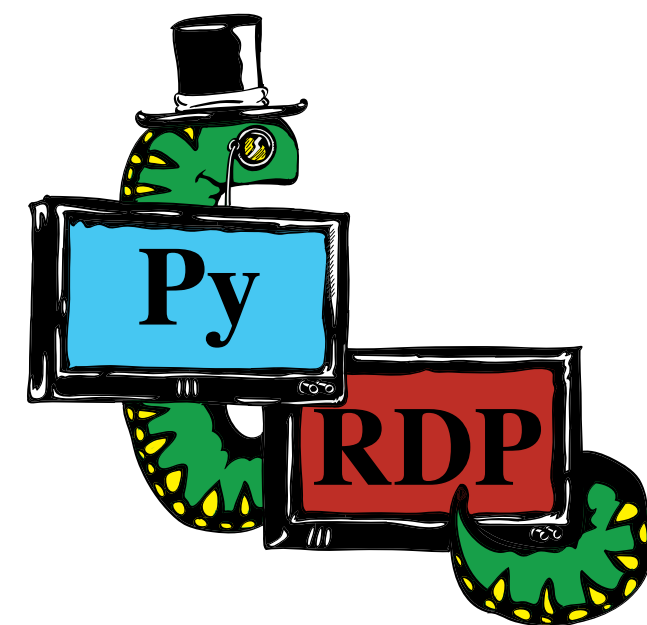


Source Code / Documentation

- <https://github.com/GoSecure/pyrdp>
- [PyRDP ReadMe](#)
- [PyRDP Transparent Proxying Guide](#)
- [Windows RDP Certificate Extraction](#)
- [RDP Connection Sequence](#)
- [RDP Basic Protocol Specification](#)

Past Presentations & Blogs

- [Introduction Blog Post](#)
- [NorthSec 2019 Talk](#)
- [BlackHat Arsenal 2019](#)
- [Blog: PyRDP on Autopilot](#)
- [DerbyCon 2019 \(Video\)](#)
- [DEFCON 28 Demo Labs](#)
- [Blog: Announcing PyRDP 1.0](#)
- [1.0 released at SecTor 2020](#)
- [BlackHat Arsenal 2021](#)



Detect Security Protocol Downgrade



Normal Flow

Windows Security

Enter your credentials

These credentials will be used to connect to my-server.gosec.co.

User name

Password

☐ Remember me

OK

Cancel



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
EC2AMAZ-BMCNDLD

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

☐ Don't ask me again for connections to this computer

View certificate...

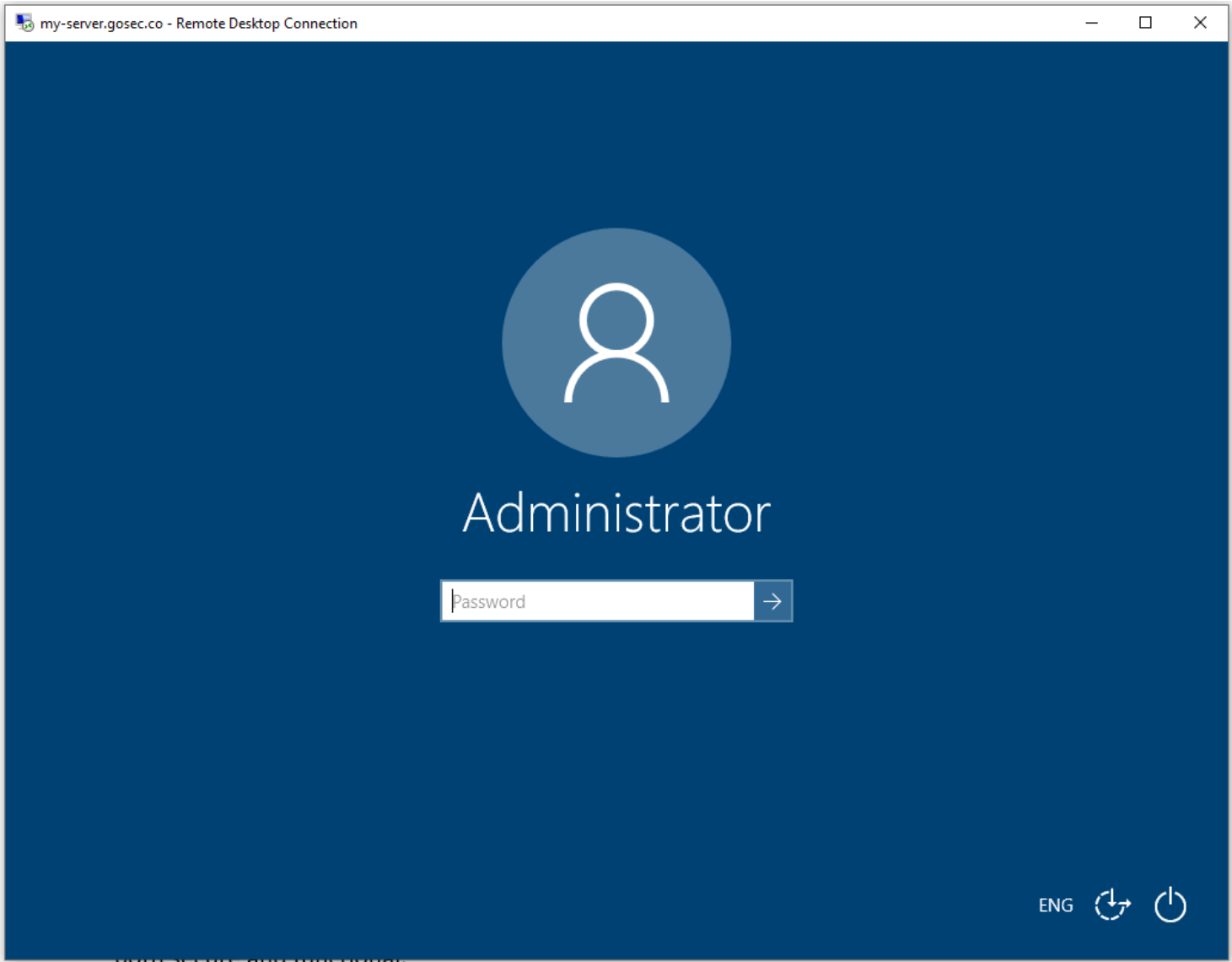
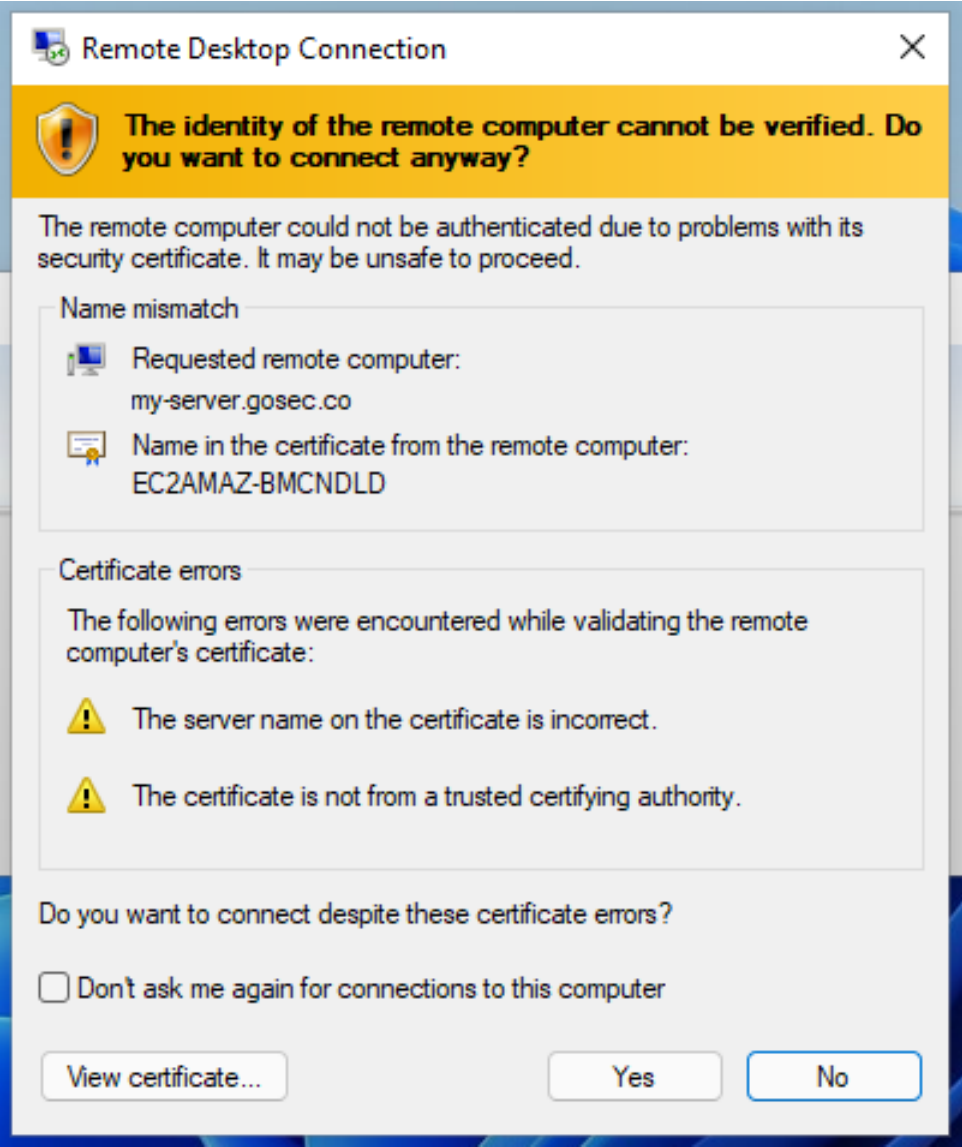
Yes

No

Detect Security Protocol Downgrade



Degraded Flow

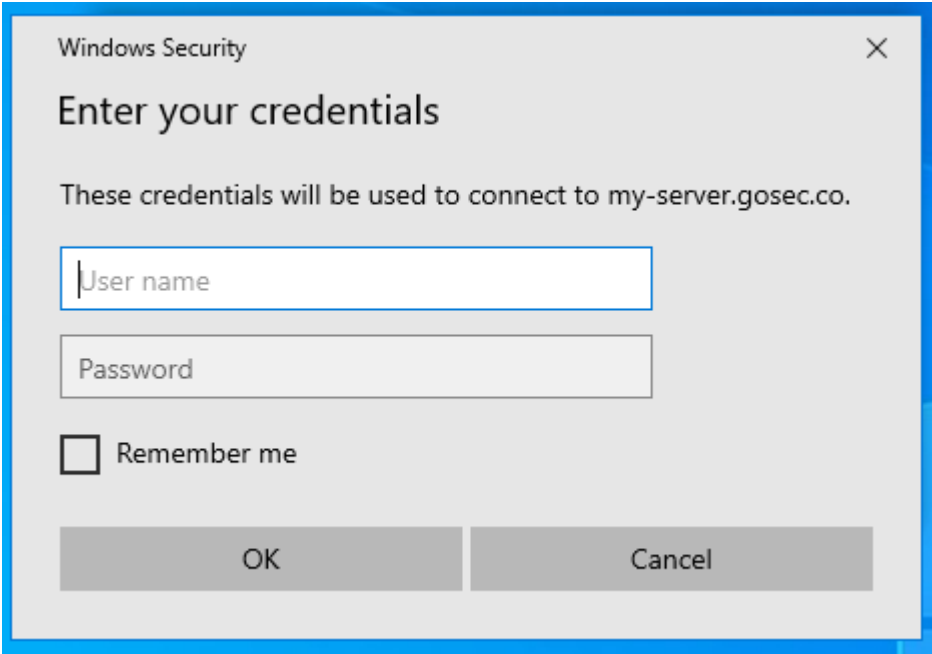
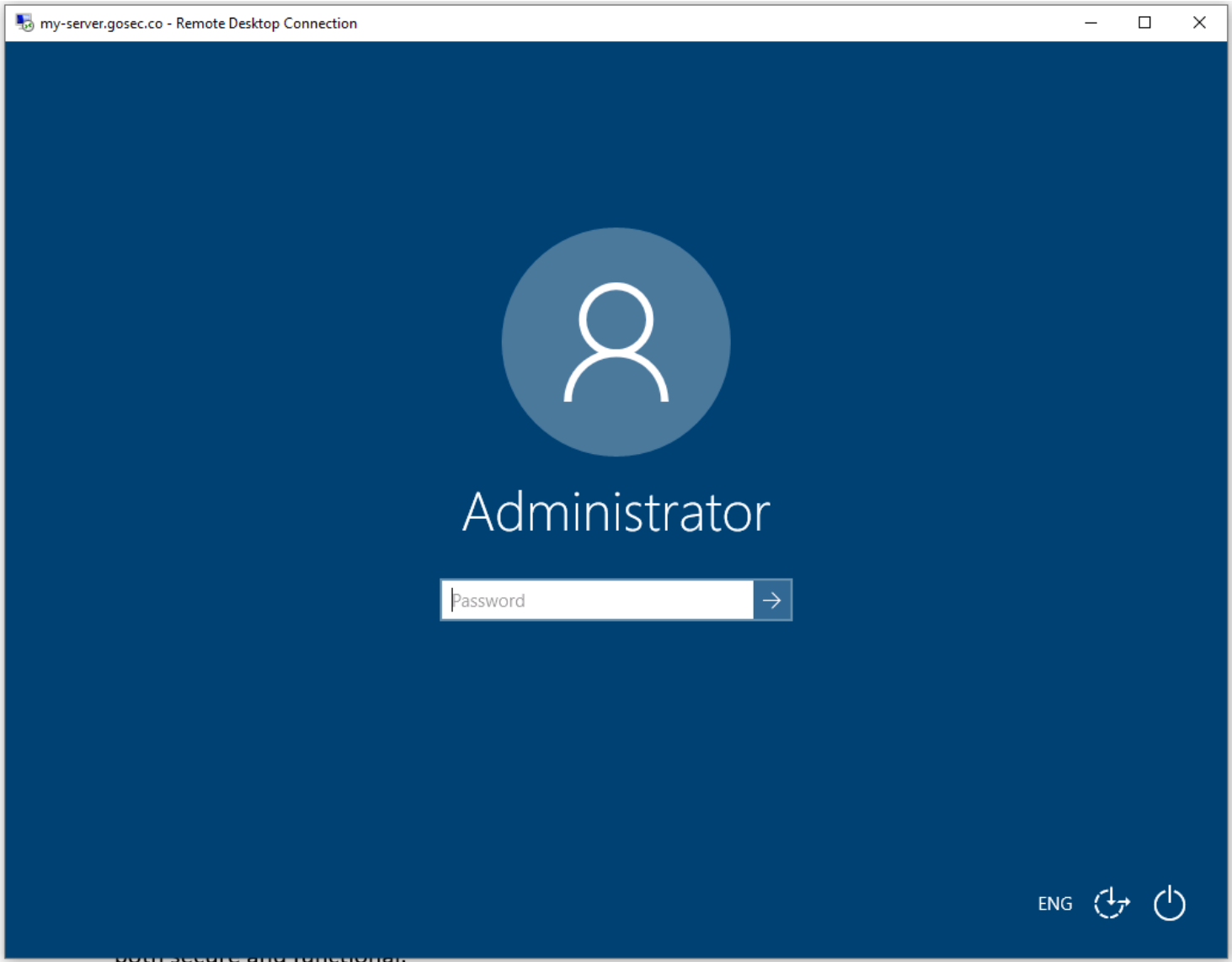


both secure and functional.

Detect Security Protocol Downgrade



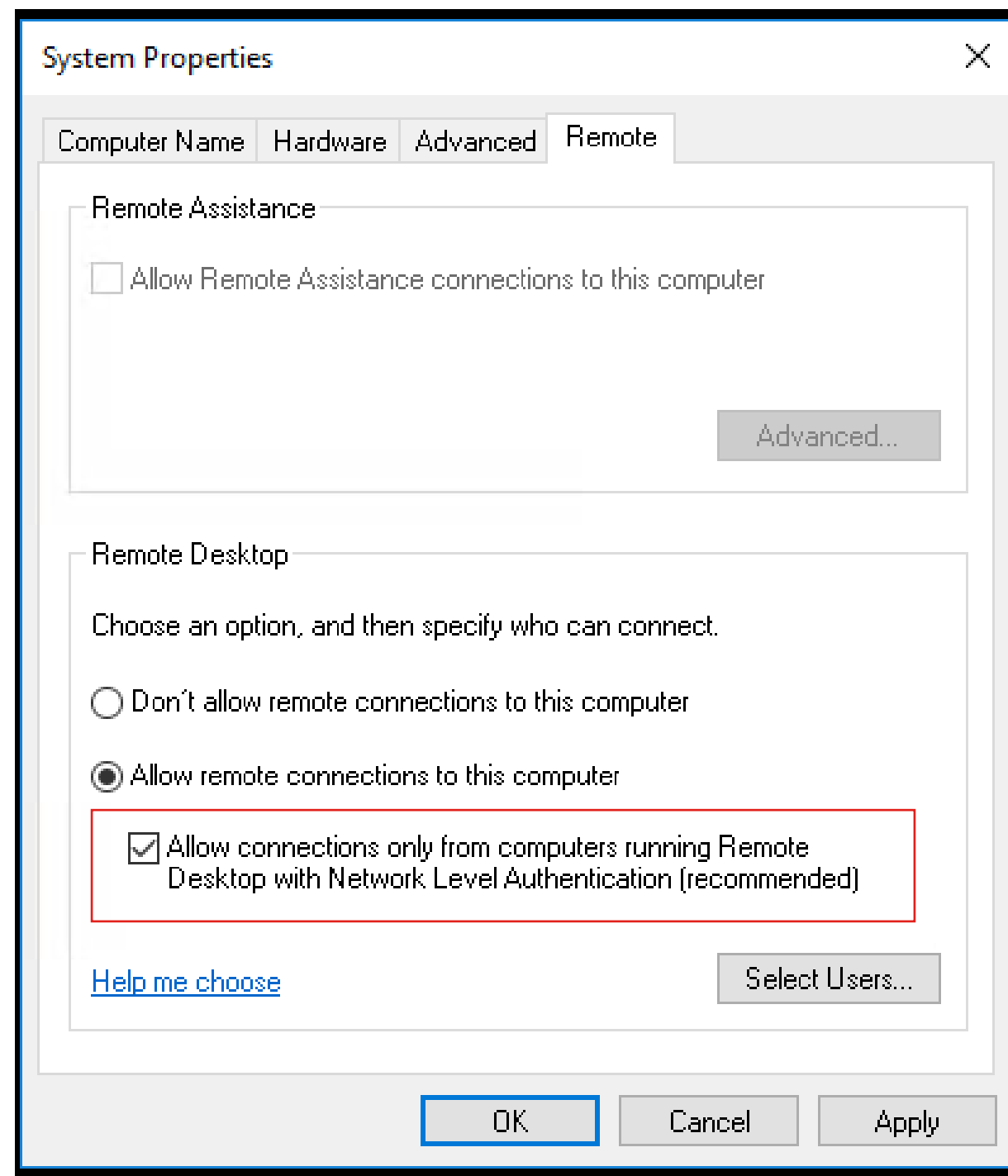
Graphical Login instead of NLA Prompt



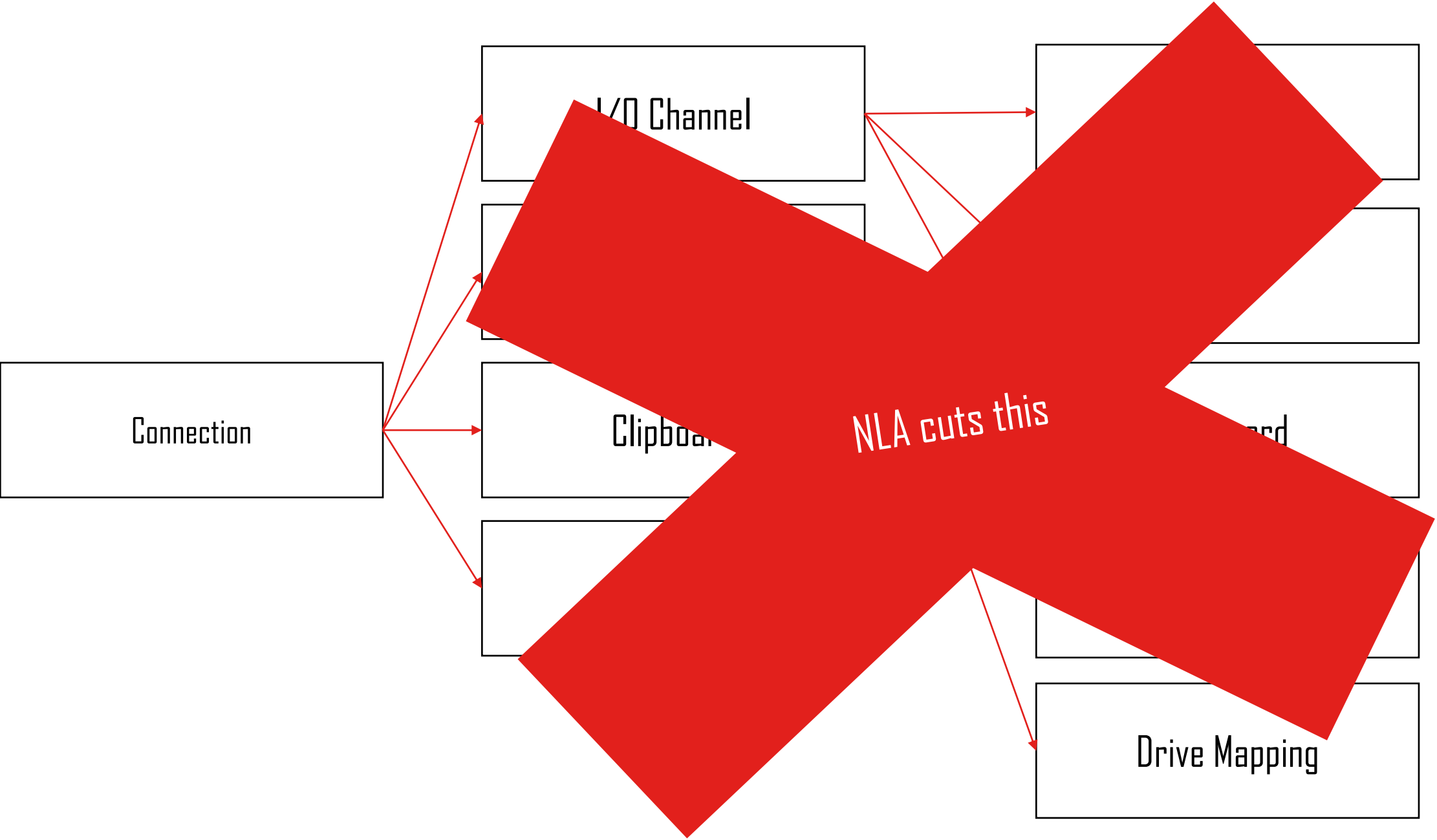
What is Network Level Authentication (NLA)?



- Authentication **before** session establishment
- Security Advantages
 - Attack Surface Reduction
 - DoS Resistance
 - Single Sign-On
- Introduced in RDP 6.0
- By default since Server 2012 and Windows 8



Attack Surface Reduction

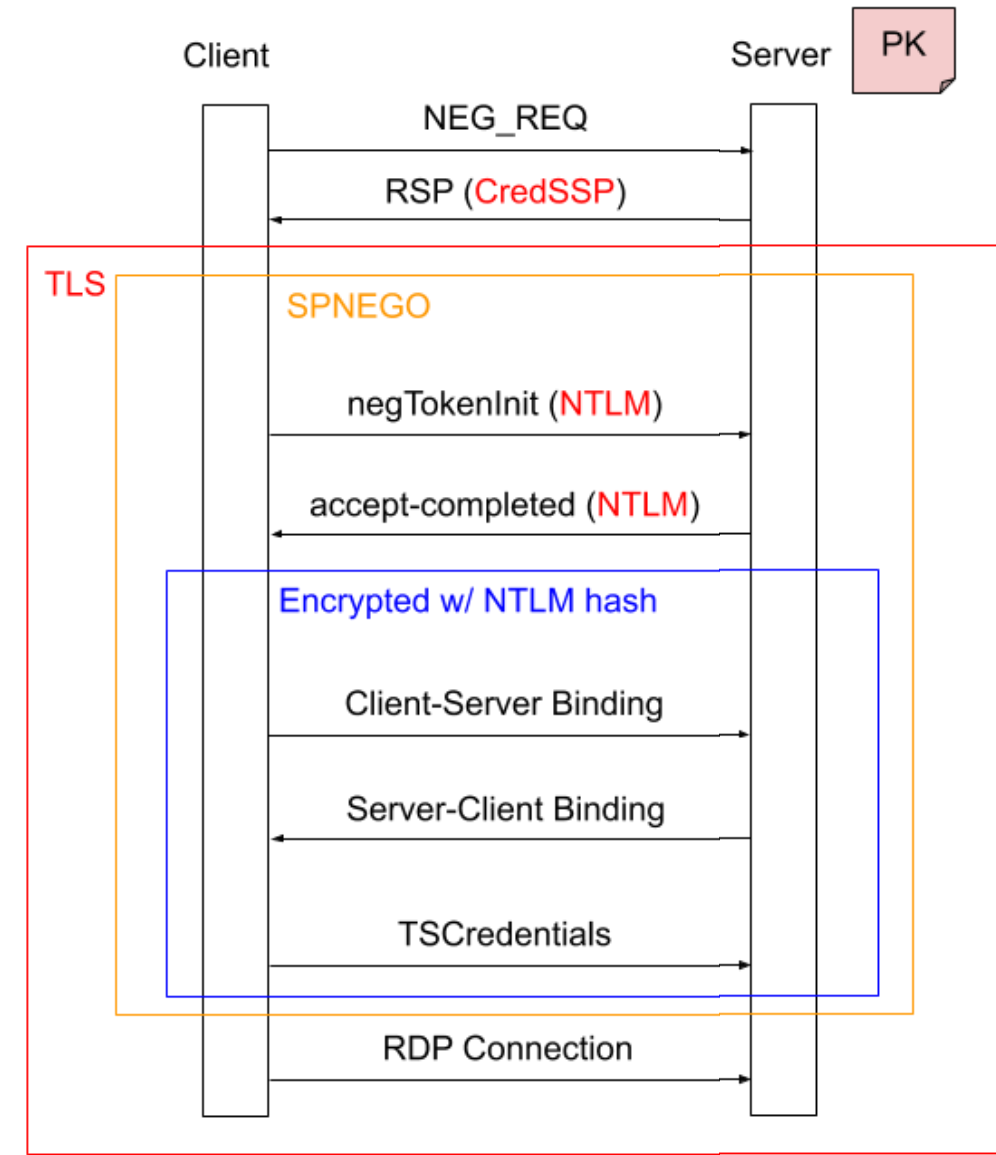


Authentication: CredSSP

NLA's Authentication Mechanism



- Initial plaintext negotiation method
- TLS Channel
- SPNEGO
 - NTLM
 - Kerberos
- Crypto should prevents MITM
 - $E(H(PK \parallel Challenge), NTLM-Hash)$



NLA Attack #1: Downgrade Attack



Downgrade the NEG_REQ to remove CredSSP from supported protocols

Windows Security

Enter your credentials

These credentials will be used to connect to my-server.gosec.co.

User name

Password

☐ Remember me

OK Cancel



my-server.gosec.co - Remote Desktop Connection

Administrator

Password

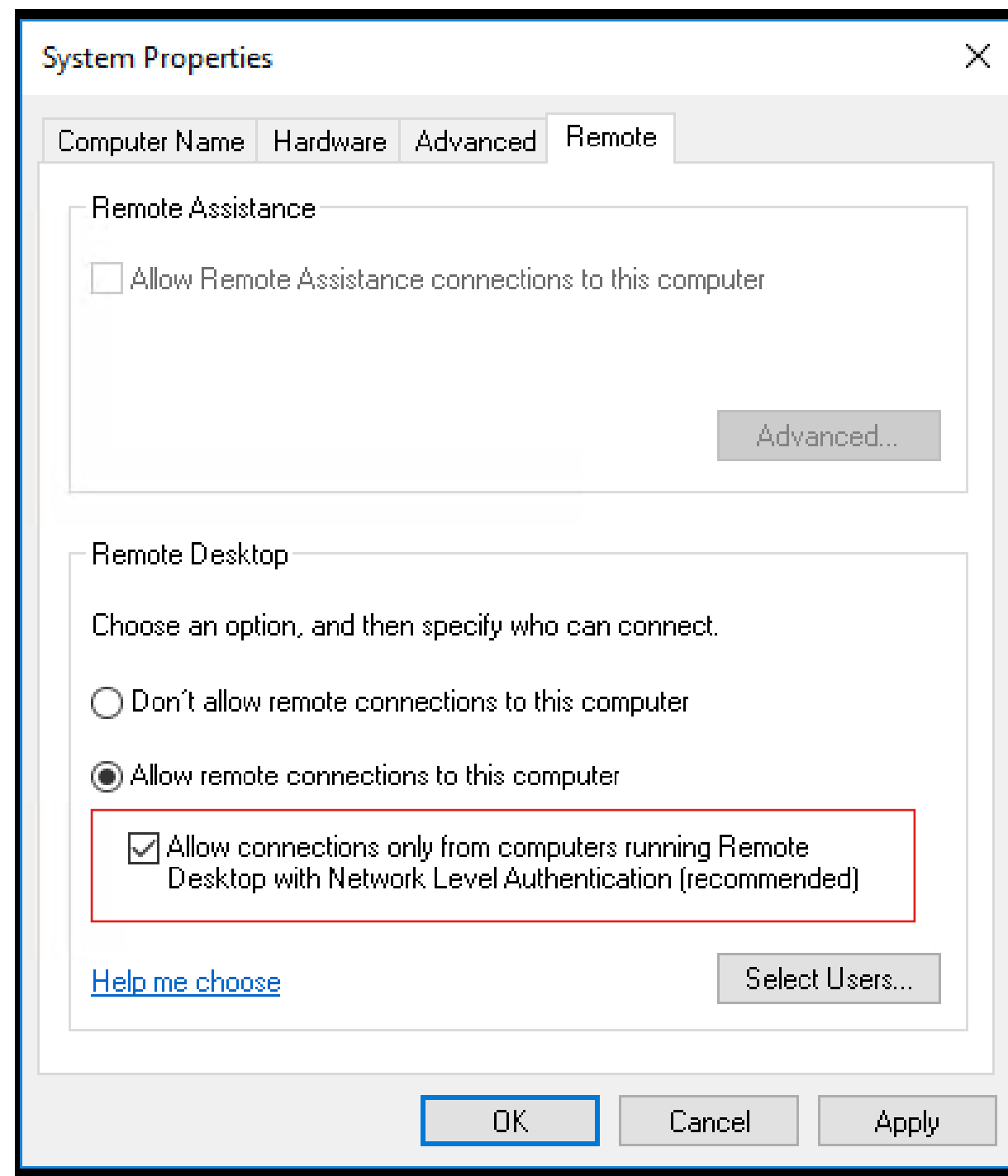
ENG

both secure and functional.

Prevent NLA Downgrade Attacks



- Enforce NLA at the Server Side
 - This is the **default**



Prevent NLA Downgrade Attacks



For Reference

PowerShell/Registry

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v  
UserAuthentication /t REG_DWORD /d 0 /f;
```

Group policy

Under

Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Settings/Remote
Desktop Session Host/Security

Set

Require user authentication for remote connections by using Network Level Authentication

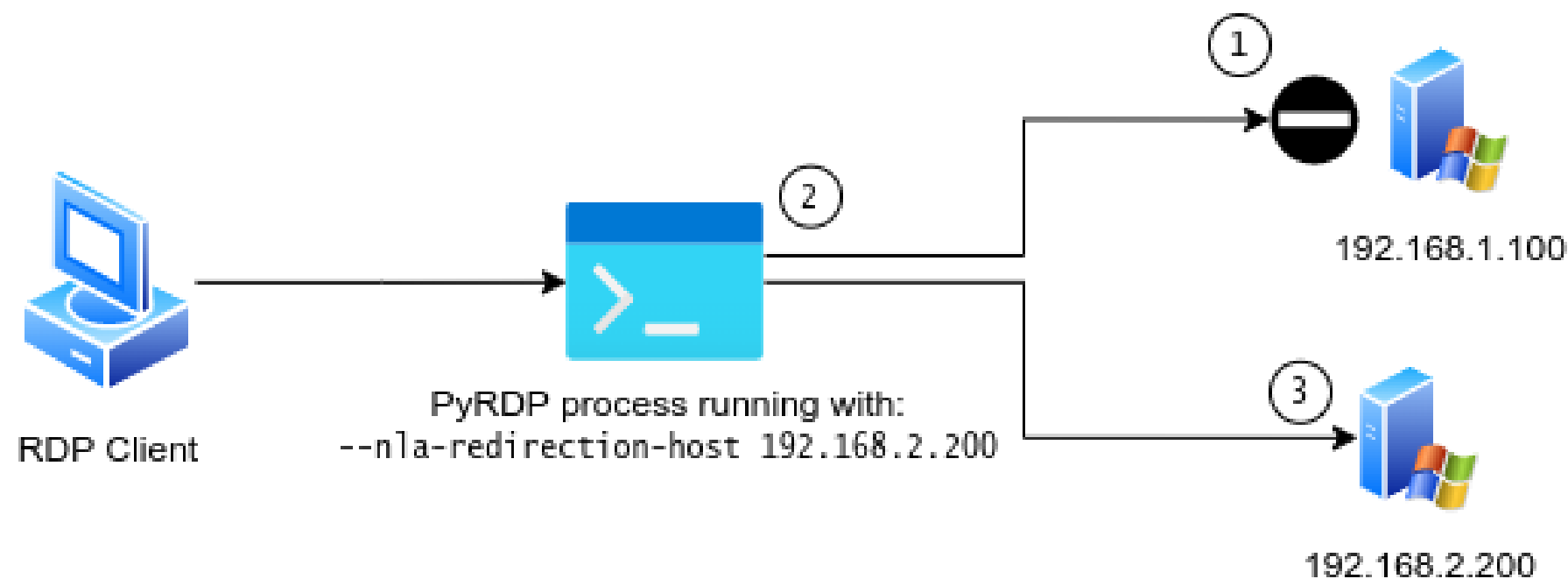
To **Enable**

Can't be disabled by users afterwards 

NLA Attack #2: Redirection to Non-NLA



1. Detects NLA enforcement
2. Transparently redirects
3. To an attacker controlled non-NLA system



Prevent Redirection to Non-NLA

Bad News

No specific way to enforce NLA on the client side

Good News

More general mitigation advice coming up



Marc-André Moreau
@awakecoding



@fdwl is there a GPO, registry key or .RDP file option that can be used to enforce RDP NLA *in the client*? @obilodeau just asked me, and it totally makes sense to get a client-side configuration, since he's working on attacks involving a malicious RDP server

[Traduire le Tweet](#)

5:32 PM · 5 avr. 2022 · Twitter Web App



Tweetez votre réponse.

Répondre



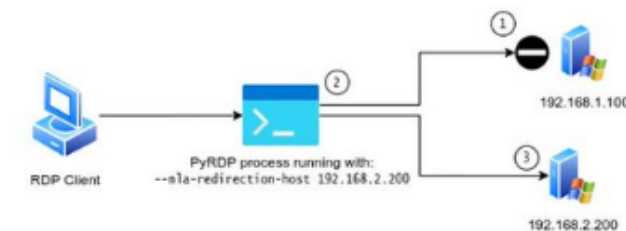
Olivier Bilodeau @obilodeau · 8 min
En réponse à @awakecoding et @fdwl
Trying to defend against this scenario



NLA Attack #2: Redirection to Non-NLA

Click to add subtitle

1. Detects NLA enforcement
2. Transparently redirects
3. To an attacker controlled non-NLA system



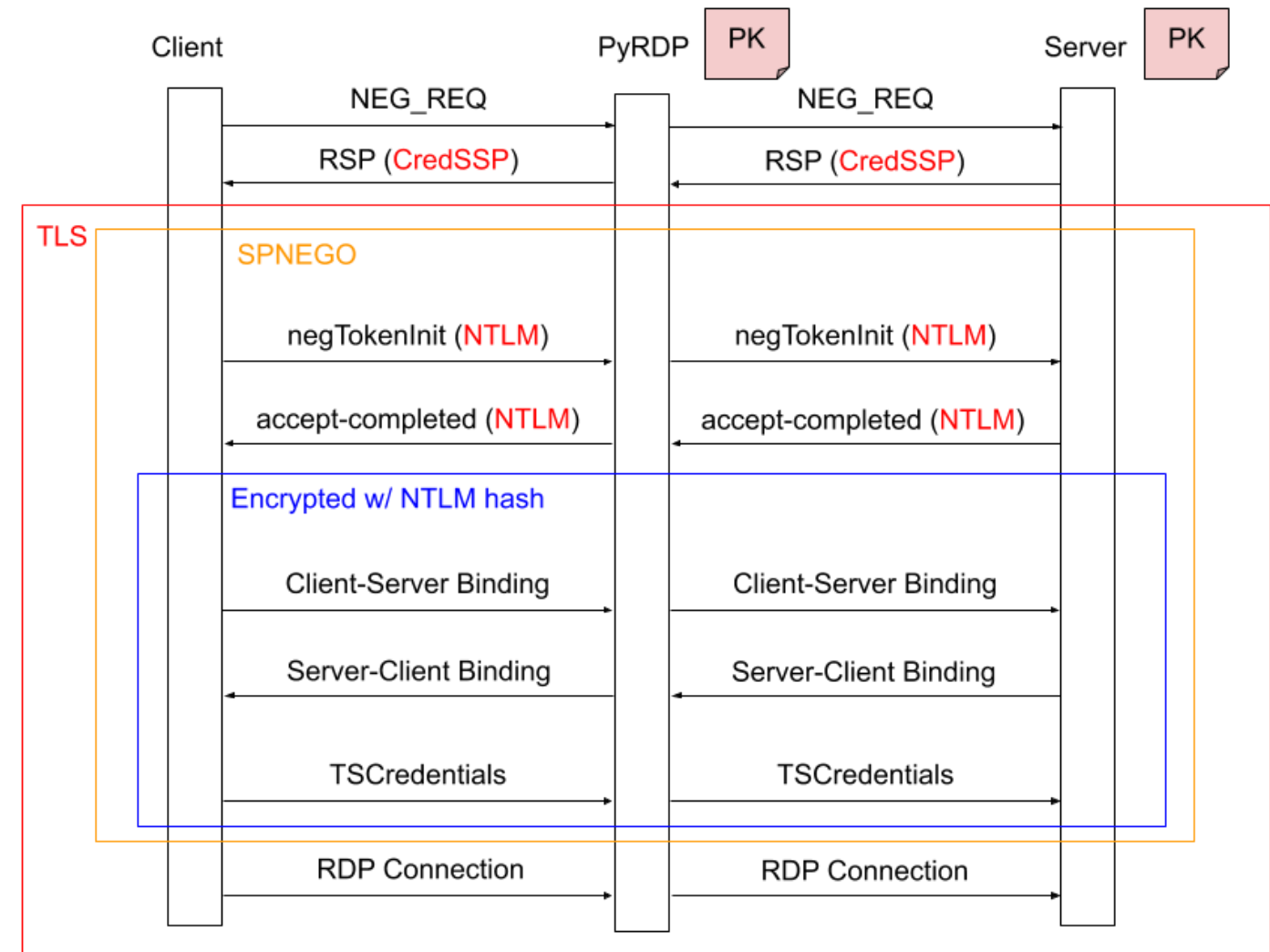
1





NLA Attack #3: NLA MITM

- No tampering at the SPNEGO layer
- But the crypto said?
 - $E(H(PK | Challenge), NTLM-Hash)$
- Requires substantial setup
 - Server certificate and private key*



*: <https://github.com/GoSecure/pyrdp/blob/master/docs/cert-extraction.md>

Attack Video Demo

NLA Bypass, Legit Certificates (lets encrypt), as bad as it can get..
([link to video](#))

NetNTLMv2 Hash Capture

NetNTLMv2 Hash Capture



- On an NLA authentication



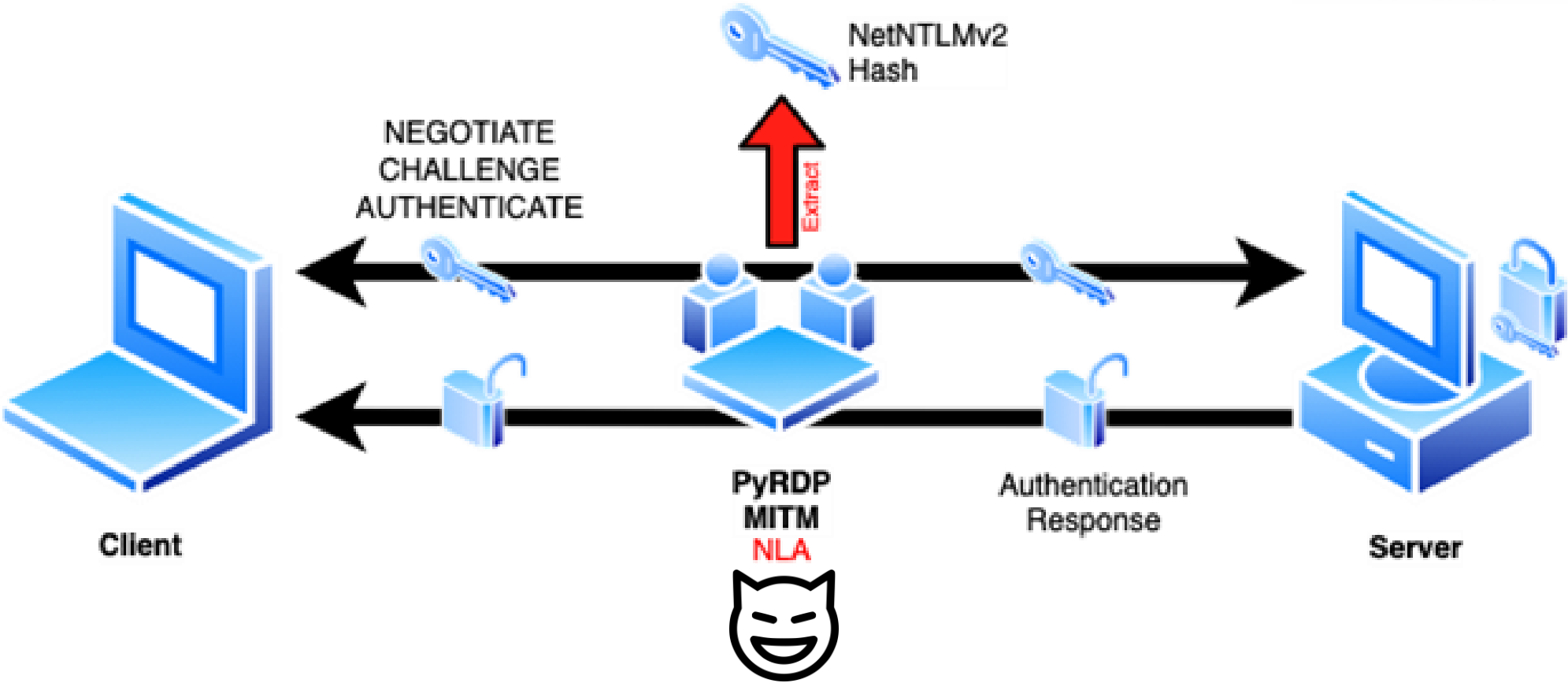
- Victim is tricked into connecting to rogue RDP
- The NTLM hash capture is done on-the-fly
- Hashes can be cracked using password cracking tools

NetNTLMv2 Hash Capture

(cont.)



HASHCAT



NetNTLMv2 Hash Capture



Example of captured hash

User

Server
Challenge

Net-NTLMv2 Hash

```
[2021-11-10 22:52:28.343] - INFO - Karen105427 - pyrdp.mitm.connections.ntlmssp - [!] NTLMSSP Hash:
admin::937f60a48cea8943:f298d601927699c77aab319e7de5b9ac:01010000000000000000debca285d6d7015f3d313dc29e3
80c0000000002000a00570049004e004e00540001000a00570049004e004e00540004000a00570049004e004e00540003000a00
570049004e004e00540005000a00570049004e004e00540006000400020000000a0010000000000000000000000000000000
0090022005400450052004d005300520056002f006c006f00630061006c0068006f0073007400000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

Net-NTLMv2 Response

NetNTLMv2 Hash Cracking



With john (hashcat works too)

```
$ john --format=netntlmv2 --wordlist=~/.wordlist/rockyou.txt hashes.txt
```

```
Using default input encoding: UTF-8
```

```
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
```

```
Will run 8 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
purple (admin)
```

```
1g 0:00:00:00 DONE (2022-04-07 14:44) 14.28g/s 58514p/s 58514c/s 58514C/s  
123456..000000
```

```
Session completed
```

Preventing Hash Capture



- Verify connection to RDP server
 - Server address
 - Domain name
- Always look for valid certificates
 - Attack tools will often use hardcoded certificate values
- But...

How Bad is it Really?

Demo!

[\(link to video\)](#)



Preventing Hash Capture

After what we found...

- Never use RDP on untrusted networks!
- Avoid NTLM => Use Kerberos
- Audit NTLM usage*

Wrapping Up

Recap of the Risks



Attacks on the Client

- Stealing files, clipboard, keystrokes
- Recording screen
- Stealing hashed or plaintext credentials
- Code exec via DLL Sideload^{*}
- RDP Phishing aka Rogue RDP^{*}

Attacks on the Server

- Credential Bruteforcing
- Session takeover
- Command injection



Defensive Side

- RD Gateway
- Require valid TLS with specific CA
- NTLM Restrictions
- Shadow Attack Framework (AutoRDPwn)
- Enterprise-scale mitigation
- Blog, blog, blog!

Offensive Side

- RestrictedAdmin with PyRDP
- Kerberos Downgrade
- Shadow Attack Framework (AutoRDPwn)
- RD Gateway



Red Team Take Aways

- **RDP is often misconfigured and under the radar**
- **You can do more than credential bruteforcing with it**
 - **Attack clients**
 - **Attack servers**
 - **Attack both!**
 - **No EDR/XDR coverage (that I'm aware of)**

Blue Team Take Aways

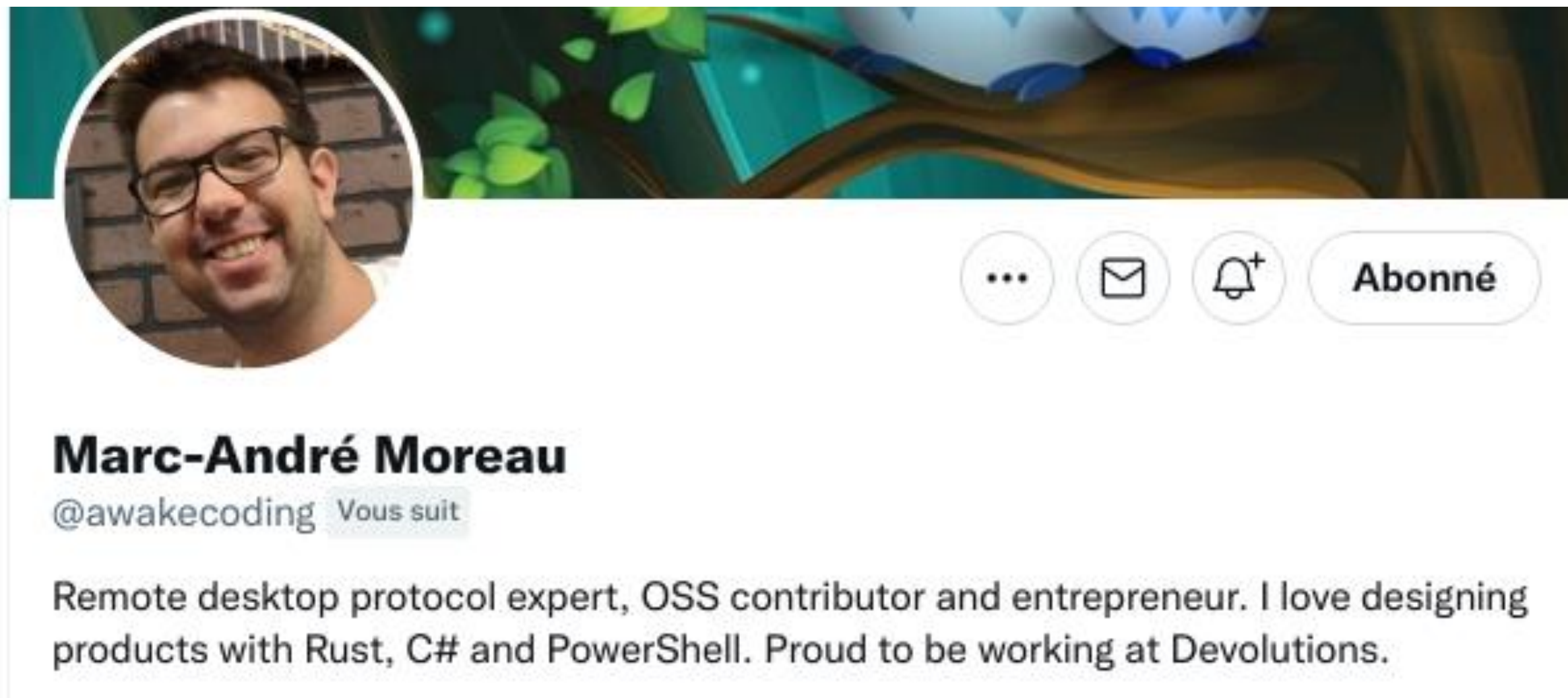


- **Today: Never use RDP on unprotected networks!**
- **Today: Train users to not click through certificate errors!**
- **Soon: Make sure NLA is enforced on all RDP servers (default, often deactivated)**
- **Long-term: Carefully roll-out Remote Credential Guard or Restricted Admin client-side enforcement**

Special Shoutout!



Big shout out to Marc-André Moreau (@awakecoding)!



Thank You!

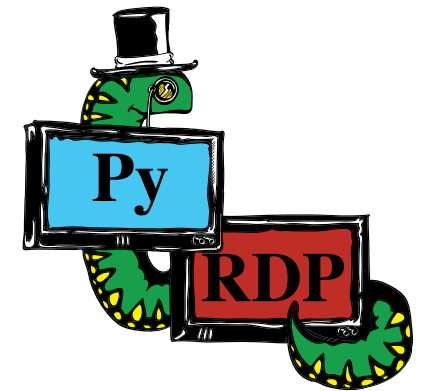
And Resources



Special Thanks to those that made PyRDP possible!

- Citronneur, Emilio Gonzalez, Francis Labelle, Maxime Carbonneau, Alexandre Beaulieu and coolacid

Questions? See you at the panel!



References

- <https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-terminalservices-rdp-winstationextensions>
- <https://www.gosecure.net/blog/2020/10/20/announcing-pyrdp-1-0/>
- <https://www.gosecure.net/blog/2022/01/17/capturing-rdp-netntlmv2-hashes-attack-details-and-a-technical-how-to-guide/>
- <https://www.darkoperator.com/blog/2012/3/17/configuring-network-level-authentication-for-rdp.html>
- <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/rdp-files>