



CertifiedDCOM

The Privilege Escalation Journey to Domain Admin with DCOM

Tianze Ding (@D1iv3)

Tencent Security Xuanwu Lab

Whoami

Tianze Ding (@D1iv3)

- Senior Security Researcher, Tencent Security Xuanwu Lab
- Focusing on Active Directory Security / Cloud Security / Web Security
- 2022 MSRC Most Valuable Researchers
- Black Hat / DEFCON / HITB Speaker

Tencent 腾讯



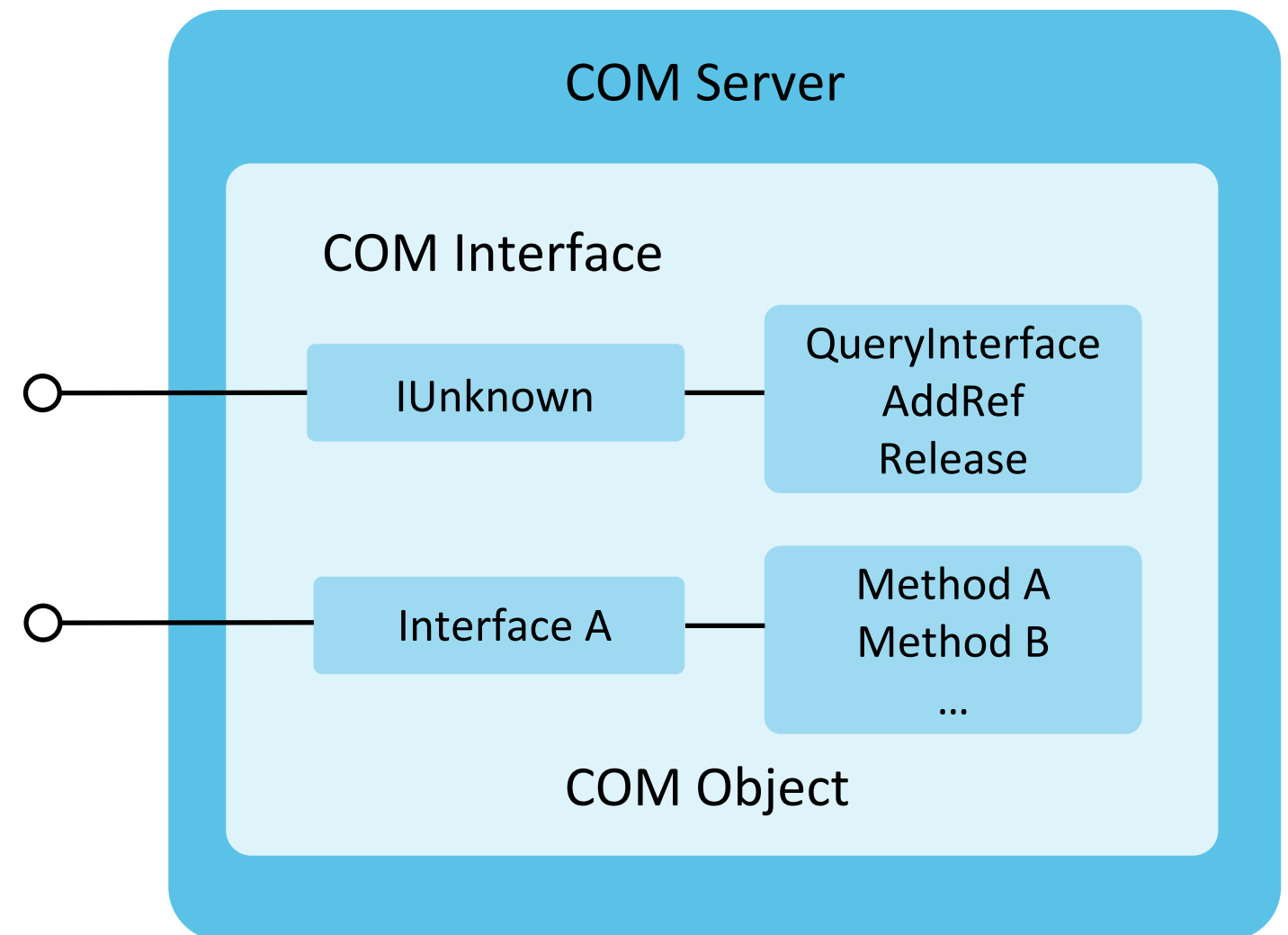
腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Agenda

- COM/DCOM Basics
- Previous Research
- COM Attack Surface from Local to Remote
- CertifiedDCOM: Privilege Escalation to Domain Admin
- Patches & Mitigations
- Conclusions & Takeaways

What is COM?

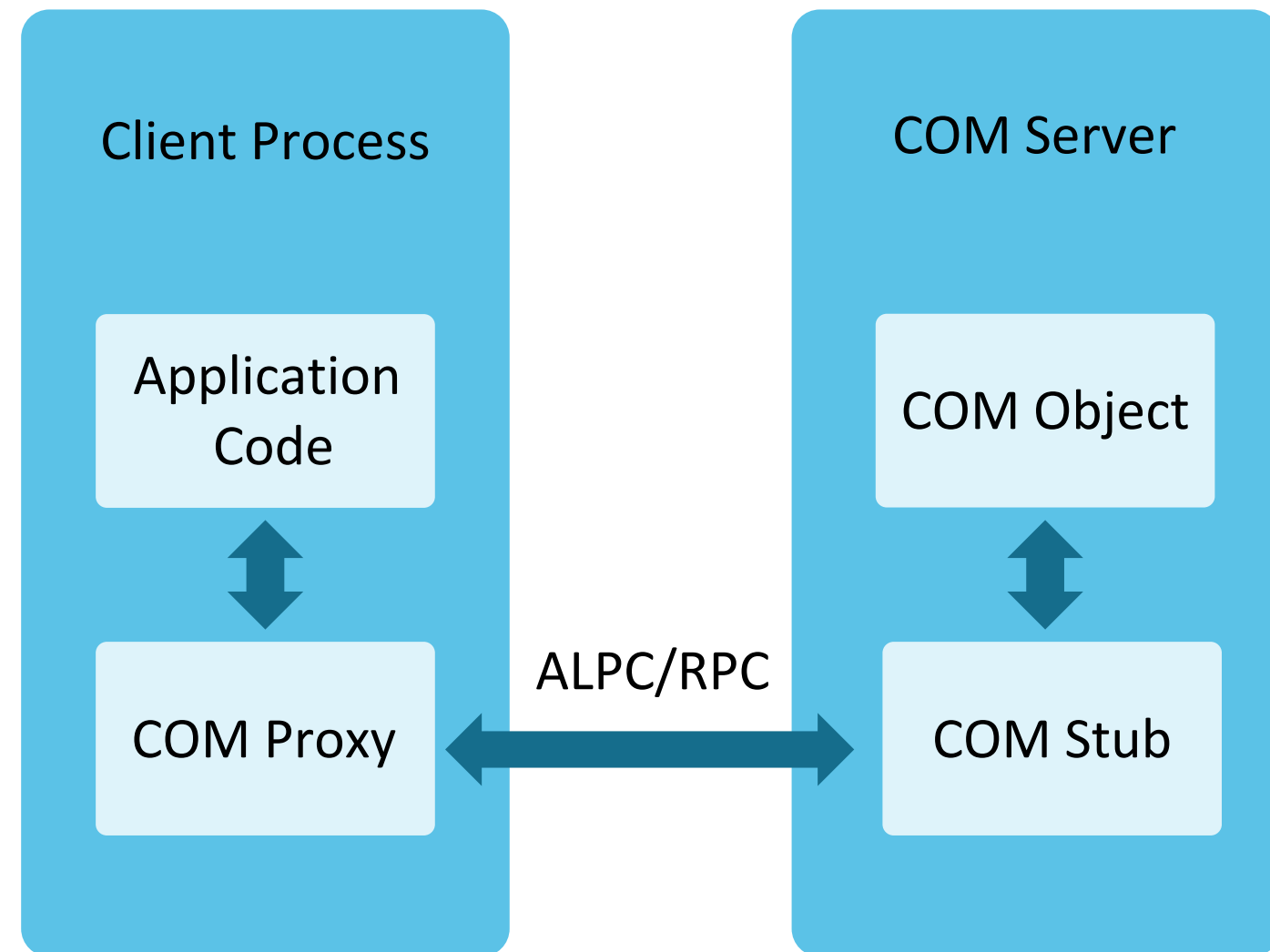
- Component Object Model (COM)
- COM is everywhere, OLE, ActiveX, DirectX, Windows Runtime, WMI, etc.
- COM Server
 - DLL/EXE files with one or more COM classes
- COM Object
 - An instance of a COM class which implements one or more interfaces
- COM Interface
 - A set of methods that can be invoked by clients



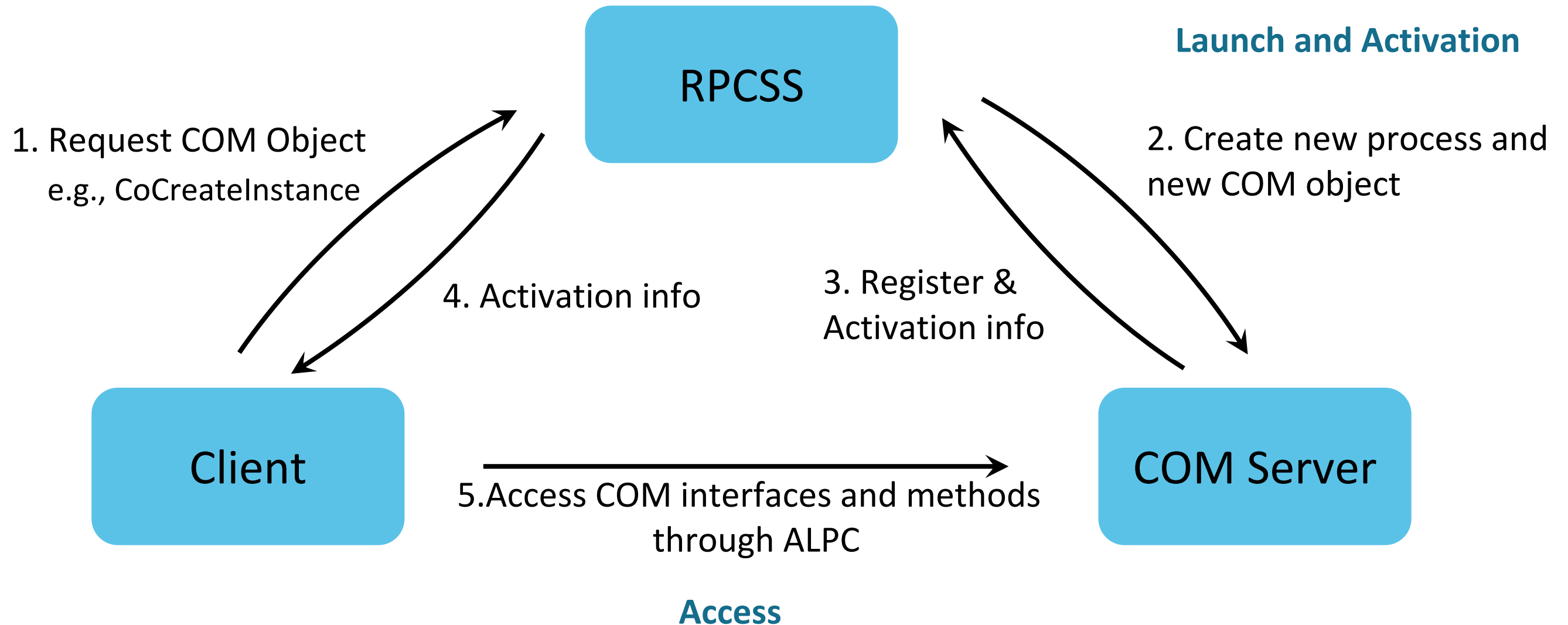
COM/DCOM

COM Server

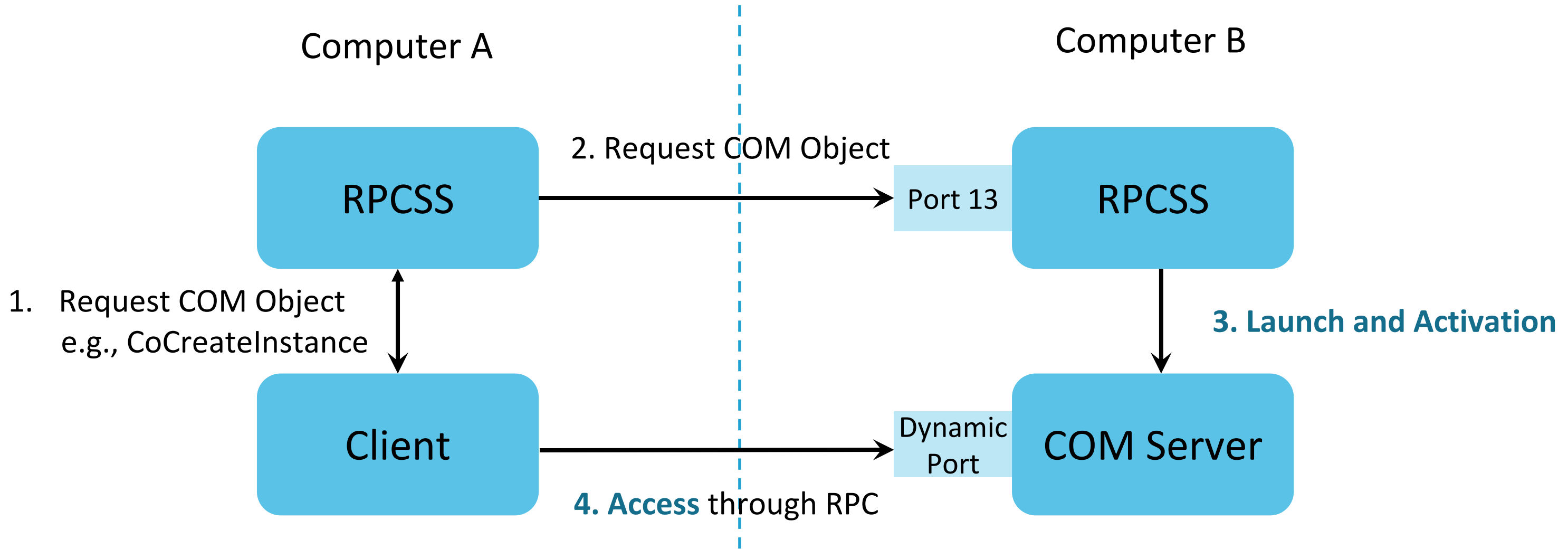
- In-Process Server
 - Runs in the same process of the client
- Out-of-Process Server
 - Runs in a separate process
 - Interact through ALPC
- Remote Server (DCOM)
 - Runs in a remote computer
 - Interact through RPC



Out-of-process COM

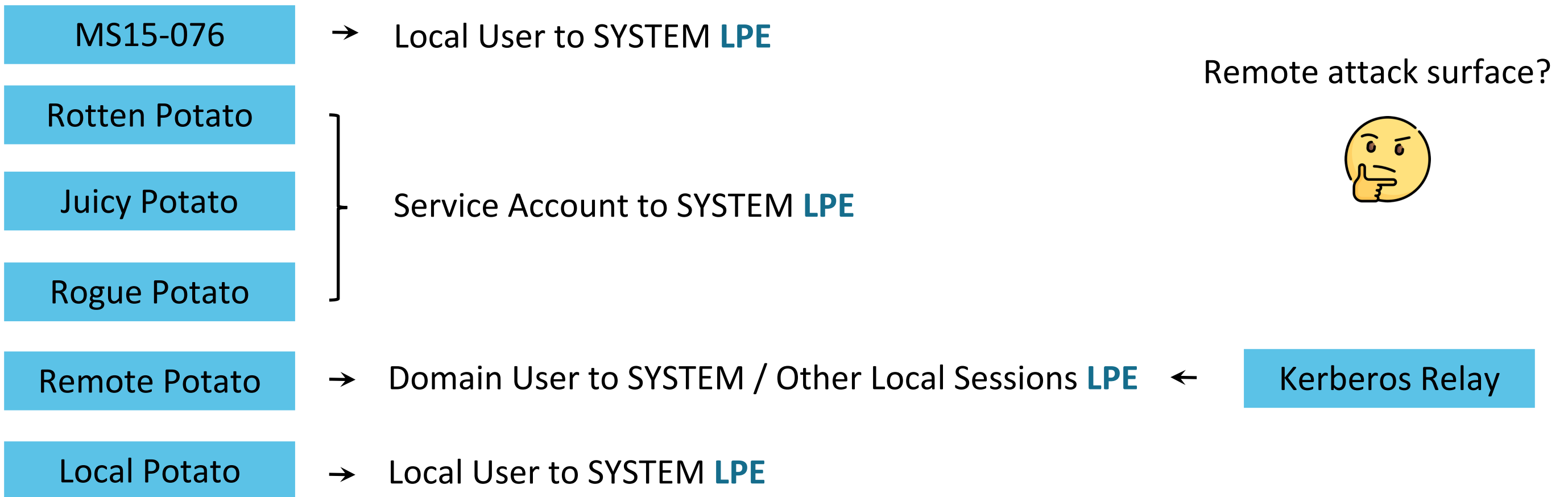


DCOM



Potato Attacks and Kerberos Relay

Potato attacks and Kerberos Relay abuse COM activation for **LPE**



The beginning of the story: [CoGetInstanceFromStorage](#)

CoGetInstanceFromIStorage

Windows APIs to create COM objects

- CoGetObject
- CoCreateInstance(Ex)
- CoCreateInstanceFromApp
- CoGetInstanceFromFile
- **CoGetInstanceFromIStorage**

Create a new COM object and **initializes it from a storage object**

```
HRESULT CoGetInstanceFromIStorage(  
    [in, optional] COSERVERINFO *pServerInfo,  
    [in, optional] CLSID *pClsid,  
    [in, optional] IUnknown *punkOuter,  
    [in] DWORD dwClsCtx,  
    [in] IStorage *pstg,  
    [in] DWORD dwCount,  
    [in, out] MULTI_QI *pResults  
);
```

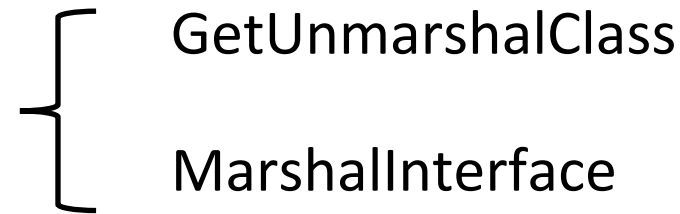
The **pstg** parameter is an **interface pointer** to the storage object

COM Marshaling/Unmarshaling

Interface pointers must be marshalled into OBJREF structures in crossing apartment/process/computer communication.

COM Client

IStorage IMarshal



EvilStroage *pstg

marshal

OBJREF_CUSTOM

COM Server

OBJREF_CUSTOM

unmarshal

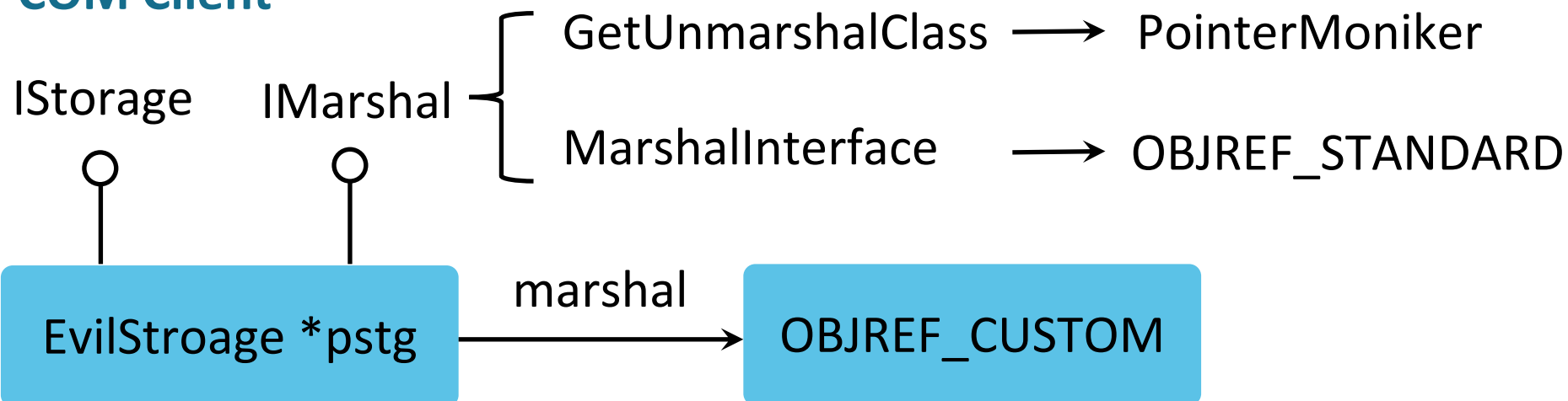
Create object and get interface pointer

OBJREF_CUSTOM

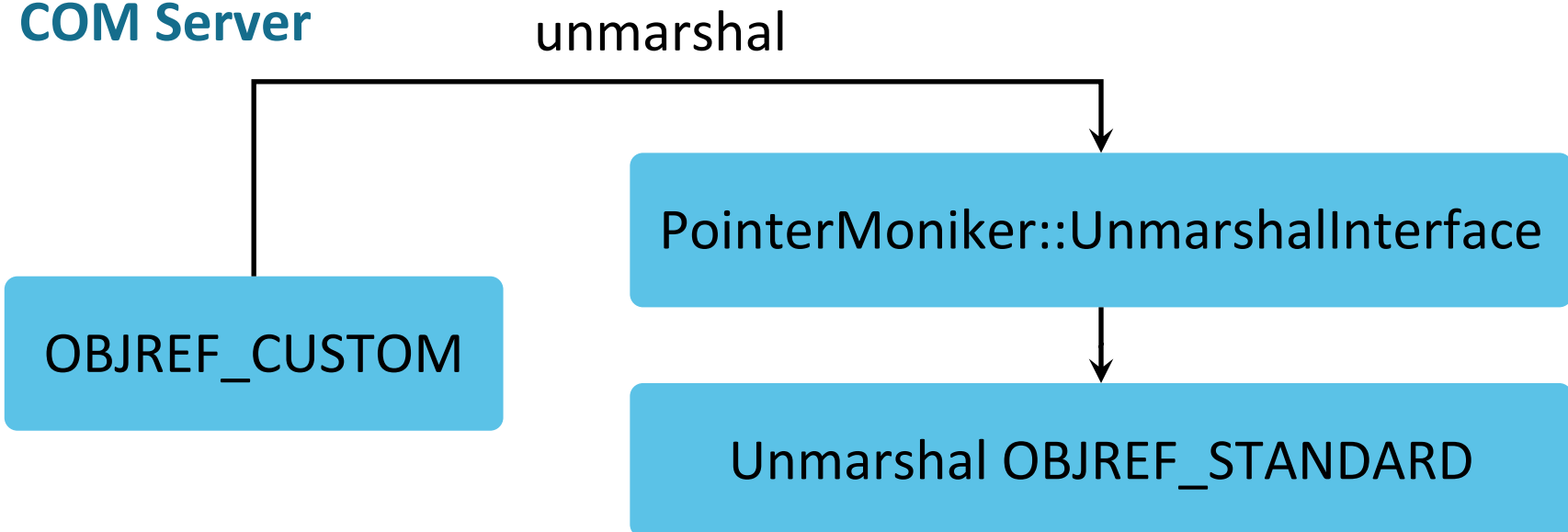
MEOW	OBJREF Type
IID	
CLSID	
cbExtension	Data Size
Data	

COM Marshaling/Unmarshaling

COM Client



COM Server



OBJREF_STANDARD

MEOW	OBJREF Type
IID	
Flags	cPublicRefs
OXID (Object Explorer ID)	
OID	
IPID	
StringBindings	
SecurityBindings	

COM Marshaling/Unmarshaling

StringBinding

TowerId	NetworkAddress
---------	----------------

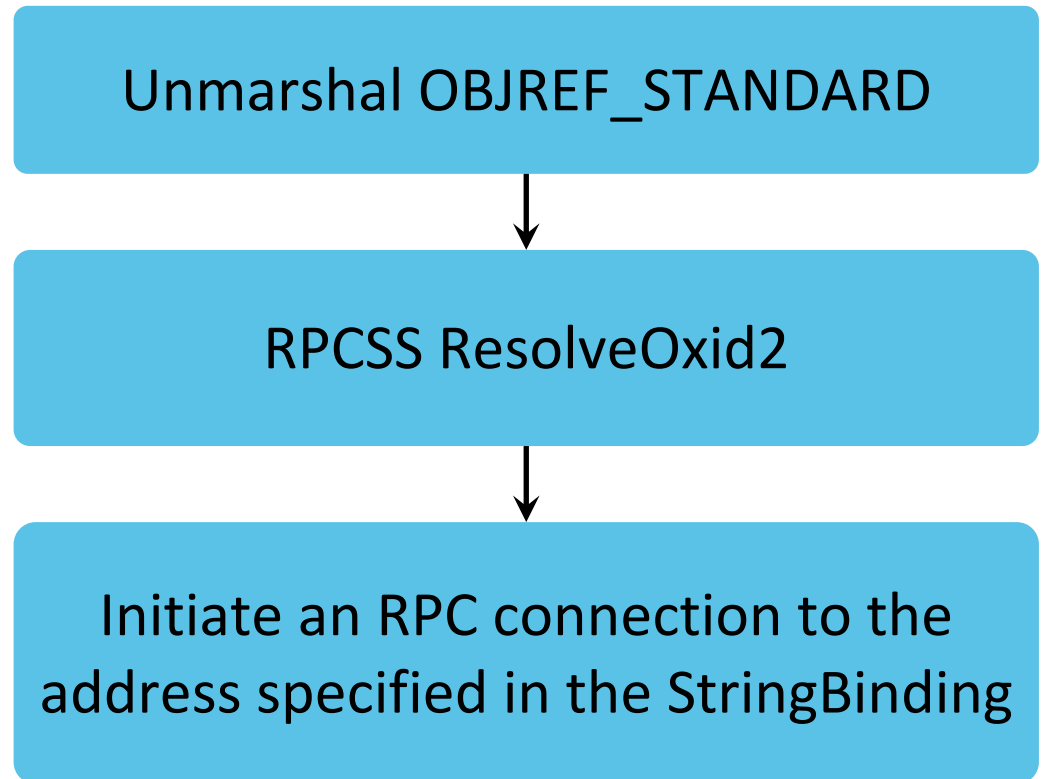
SecurityBinding

AuthnSvc	Reserved
Service Principal Name	

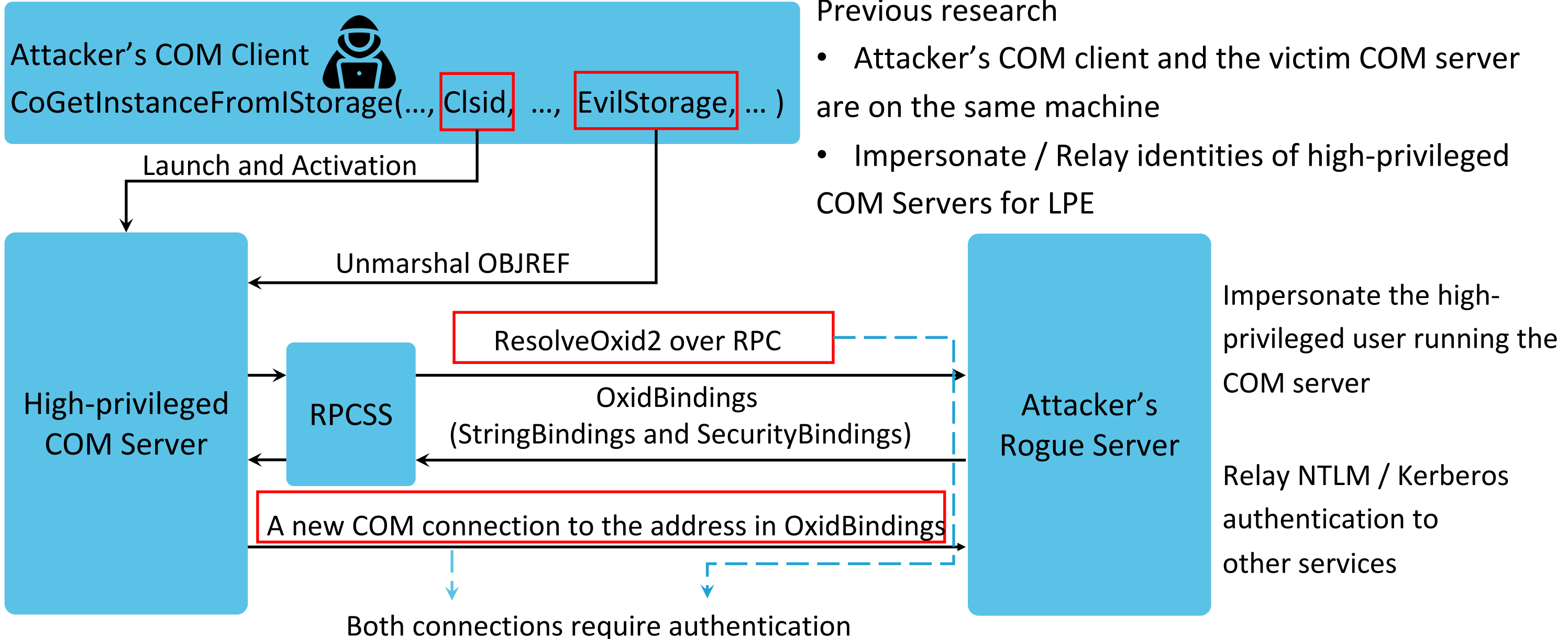
```
StringBinding[1]: TowerId=NCACN_IP_TCP, NetworkAddr="192.168.2.1"  
TowerId: NCACN_IP_TCP (0x0007)  
NetworkAddr: 192.168.2.1
```

```
SecurityBinding[1]: AuthnSvc=0x0010, AuthzSvc=0xffff, PrincName="rpcss/desktop-win10.demo.lab"  
AuthnSvc: RPC_C_AUTHN_GSS_KERBEROS (0x0010)  
AuthzSvc: Default (0xffff)  
PrincName: rpcss/desktop-win10.demo.lab
```

COM Server



CoGetInstanceFromStorage



Previous research

- Attacker's COM client and the victim COM server are on the same machine
- Impersonate / Relay identities of high-privileged COM Servers for LPE

Remote CoGetInstanceFromIStorage

```
HRESULT CoGetInstanceFromIStorage(  
  [in, optional] COSERVERINFO *pServerInfo,  
  [in, optional] CLSID *pClsid,  
  [in, optional] IUnknown *punkOuter,  
  [in] DWORD dwClsCtx,  
  [in] IStorage *pstg,  
  [in] DWORD dwCount,  
  [in, out] MULTI_QI *pResults  
);
```

```
typedef struct _COSERVERINFO {  
  DWORD dwReserved1;  
  LPWSTR pwszName;  
  COAUTHINFO *pAuthInfo;  
  DWORD dwReserved2;  
} COSERVERINFO;
```

```
typedef enum tagCLSCTX {  
  ...  
  CLSCTX_REMOTE_SERVER  
  ...  
}
```

Remote Computer Name

Remote Auth Info

Remote Activation

CoGetInstanceFromIStorage also supports **remote COM activation**

Can we use CoGetInstanceFromIStorage to coerce **a remote computer** connect to us over RPC/DCOM and exploit it for a NTLM/Kerberos Relay attack ?

Remote CoGetInstanceFromIStorage

- Suppose an attacker has **Domain User / Domain Computer** privileges
- Use CoGetInstanceFromIStorage to activate a COM object on a remote domain computer

```
PS C:\Users\attacker\Desktop> .\RemoteCoGetInstanceFromIStorage.exe -target 192.168.2.100 -oxidresolver 192.168.2.1
[*] Use default CLSID: 90f18417-f0f1-484e-9d3c-59dceee5dbd8
[*] Attacked Target: 192.168.2.100
[*] Rogue OxidResolver: 192.168.2.1
objref:TUVPVwEAAAAAAAAAAAAAAAAAMAAAAAAAAABGgQIAAAAAAAAAAD1ELk+k81cP77FdBmhrf5dAmwAABwF///hJptuVP0T0xIADgAHADEAOQAYAC4AMQA2AD
gALgAyAC4AMQAAAAAACgD//wAAAAA=:

[*] Forcing SYSTEM authentication
[*] Using CLSID: 90f18417-f0f1-484e-9d3c-59dceee5dbd8
System.UnauthorizedAccessException: Access is denied.

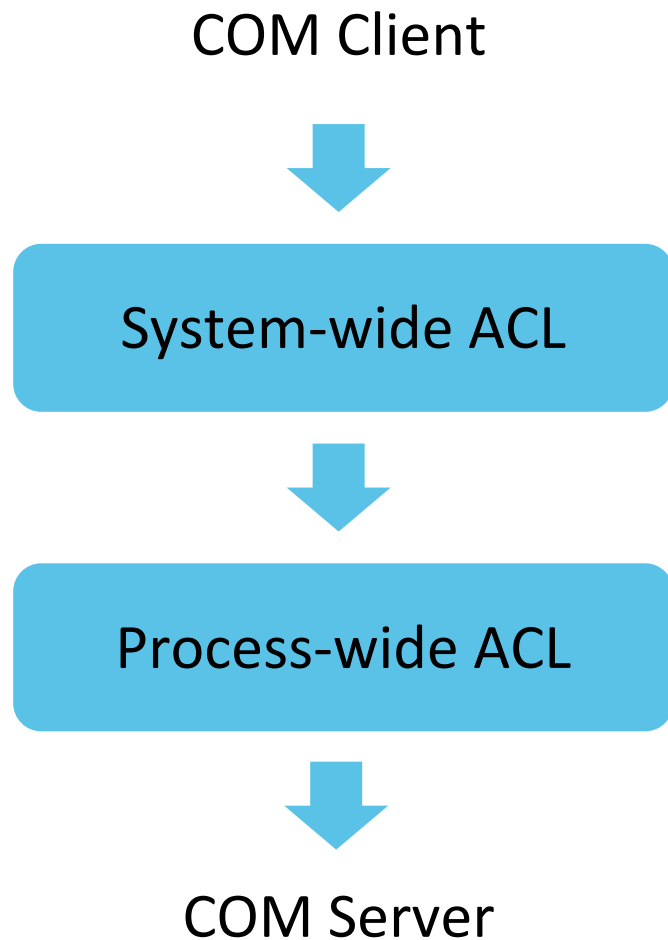
Access is denied.

at Exploit.Ole32.CoGetInstanceFromIStorage(COSERVERINFO pServerInfo, Guid& pclsid, Object pUnkOuter, CLSCTX dwClsC
tx, IStorage pstg, UInt32 cmq, MULTI_QI[] rgmqResults)
at Trigger.Program.Main(String[] args)
```

→ **Access is Denied**

COM Security

COM Launch / Activation / Access



System-wide Launch and Activation Limits

- Defined in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole

Launch and Activation Permission

Security Limits

Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- S-1-15-3-1024-2405443489-874036122-4286035555-1823
- Administrators (DESKTOP-WIN10\Administrators)
- Performance Log Users (DESKTOP-WIN10\Performance L...

Permissions for Everyone

	Allow	Deny
Local Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Launch	<input type="checkbox"/>	<input type="checkbox"/>
Local Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Activation	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

Launch and Activation Permission

Security Limits

Group or user names:

- S-1-15-3-1024-2405443489-874036122-4286035555-1823
- Administrators (DESKTOP-WIN10\Administrators)
- Performance Log Users (DESKTOP-WIN10\Performance L...
- Distributed COM Users (DESKTOP-WIN10\Distributed COM...

Permissions for Administrators

	Allow	Deny
Local Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Local Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>

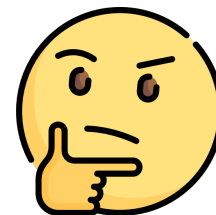
OK Cancel

By default, only users in **specify high-privileged local groups** are allowed to perform Remote Launch and Remote Activation

Remote Attack Surface?

Low-privileged accounts (e.g., Domain Users, Domain Computers) are not allowed to activate any COM object on a remote computer in Windows default COM security configuration

Where is the remote attack surface ?




Remote Attack Surface in Active Directory

Windows

- Windows default COM Security configuration
- Preinstalled COM classes in Windows



Active Directory

- Widely used services in Active Directory 
- COM classes introduced by these services
- Special COM security configuration introduced by these services

Add Roles and Features Wizard

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select one or more roles to install on the selected server.

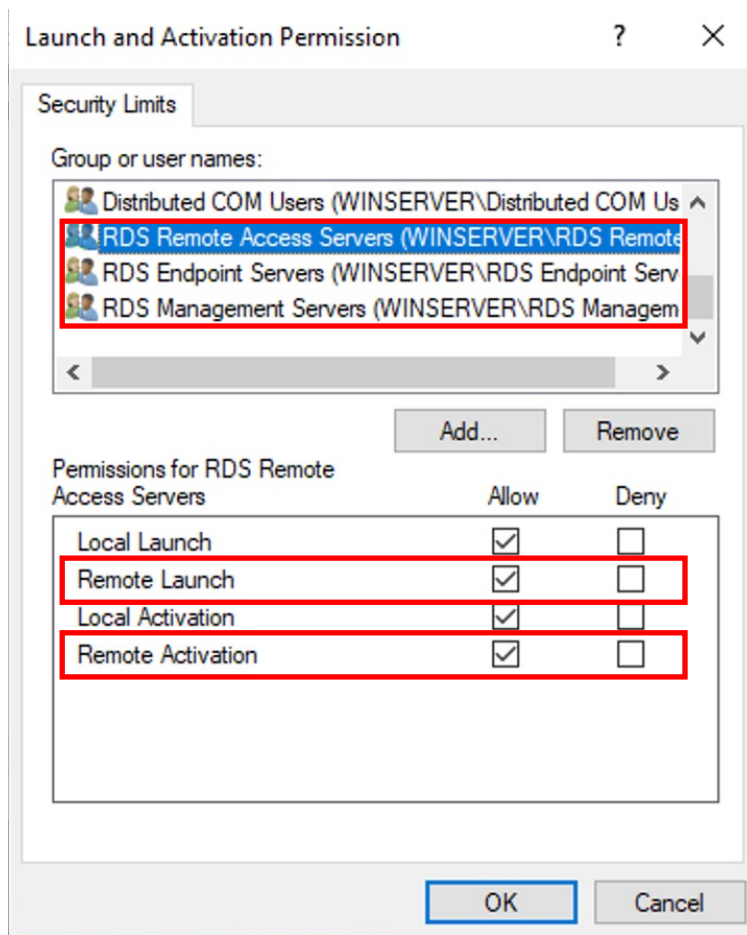
Roles

- Active Directory Certificate Services
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Controller
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

Special COM Security Configuration

RDS (Remote Desktop Service)

- Widely used by enterprise virtual application/desktop solutions, e.g., Citrix, VMware Horizon



```
C:\Users\administrator.DEMO>net localgroup "RDS Endpoint Servers"
Alias name      RDS Endpoint Servers
Comment        Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal
virtual desktops run. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS
and RD Virtualization Host servers use...
Members
-----
DEMO\WINSERVER$
NT AUTHORITY\NETWORK SERVICE
The command completed successfully.

C:\Users\administrator.DEMO>net localgroup "RDS Management Servers"
Alias name      RDS Management Servers
Comment        Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS
Central Management service must be included in this group.
Members
-----
NT SERVICE\RDMS
NT SERVICE\TSCPubRPC
NT SERVICE\tssdis
```

RDS Remote Access Servers, RDS Endpoint Servers and RDS Management Servers have Remote Launch and Remote Activation privileges.

In the RDS default configuration, no low-privilege domain accounts in these groups.

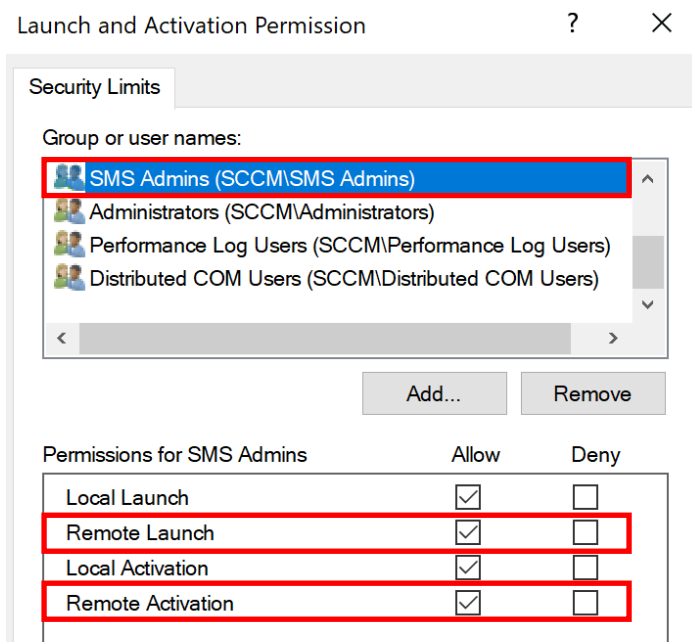
Special COM Security Configuration

SCCM (System Center Configuration Manager)

SMS Admins group has Remote Launch and Remote Activation privileges.

By default, each administrative user in a hierarchy and the site server computer account are members of the SMS Admins group.

No low-privilege domain accounts in the SMS Admins group.



Permissions for SMS Admins

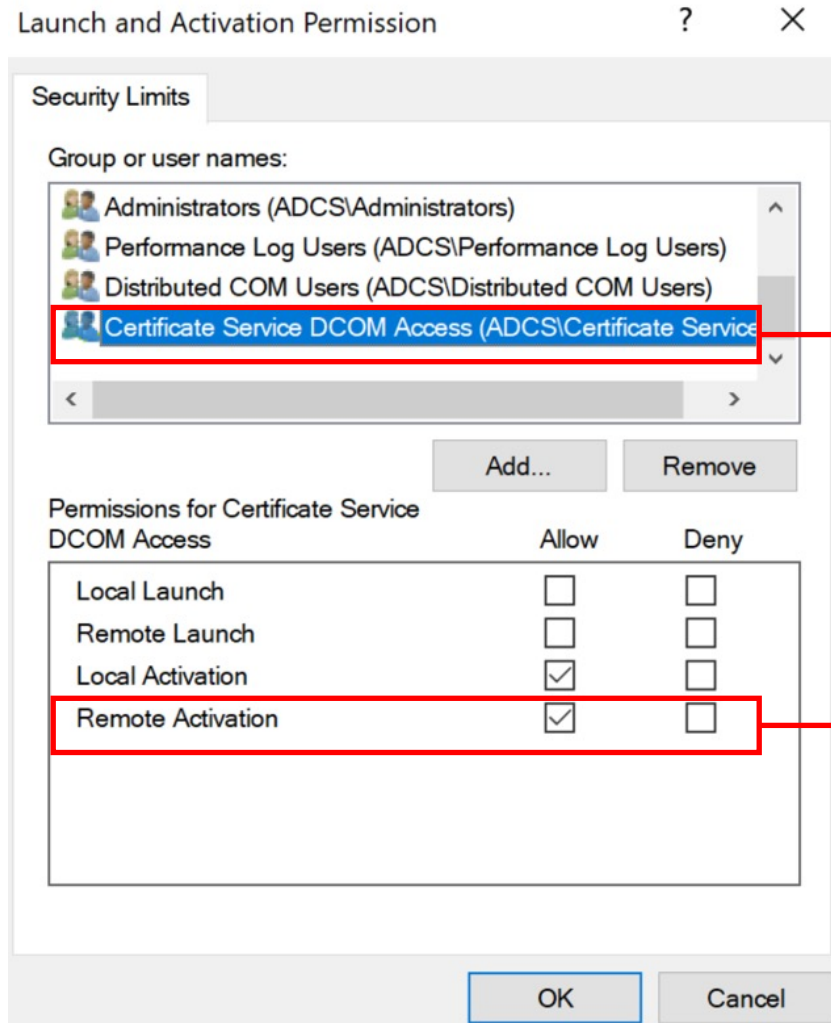
You can view the rights and permissions for the SMS Admins group in the WMI Control M group is granted **Enable Account** and **Remote Enable** on the `Root\SMS` WMI namespace. **Execute Methods, Provider Write, and Enable Account.**

```
C:\Users\administrator.DEMO>net localgroup "SMS Admins"  
Alias name      SMS Admins  
Comment        Members have access to the SMS Provider.  
  
Members  
  
DEMO\administrator  
DEMO\sccm$
```

When you use a remote Configuration Manager console, configure **Remote Activation** DCOM permissions on both the site server computer and the SMS Provider. Grant these rights to the **SMS Admins** group. This action simplifies administration instead of granting these rights directly to users or groups. For more information, see [Configure DCOM permissions for remote Configuration Manager consoles.](#)

Special COM Security Configuration

AD CS (Active Directory Certificate Service)



Certificate Service DCOM Access group has Remote Activation privilege

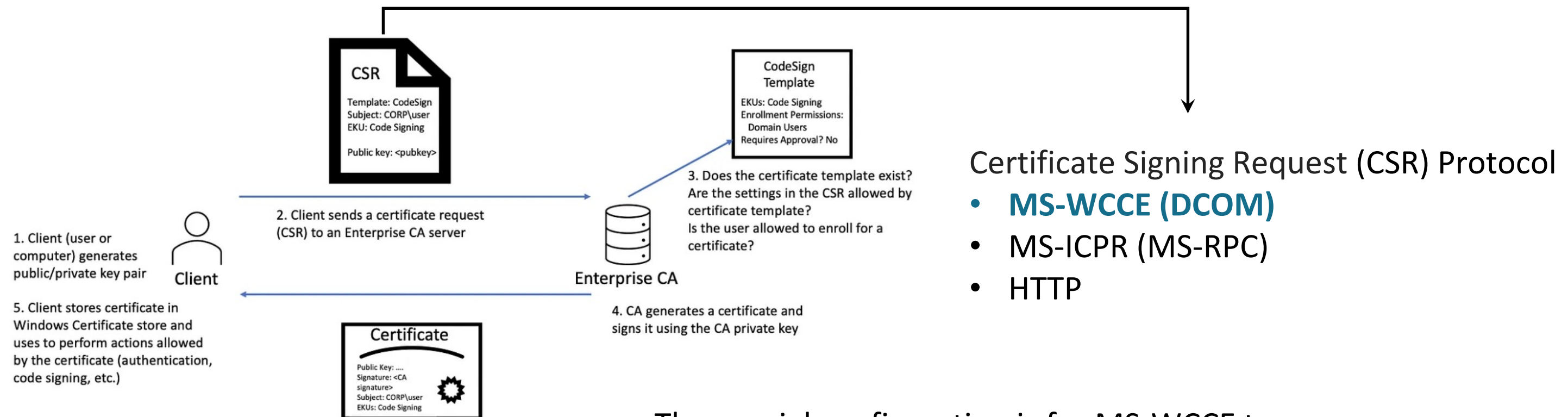
```
C:\Users\administrator.DEMO>net localgroup "Certificate Service DCOM Access"  
Alias name      Certificate Service DCOM Access  
Comment        Members of this group are allowed to connect to Certification Authorities in the enterprise  
Members  
-----  
NT AUTHORITY\Authenticated Users  
The command completed successfully.
```

The **Authenticated Users** group is in the Certificate Service DCOM Access group

By default , **any domain account can pass the system-wide ACL check** and are allowed to activate COM objects remotely on AD CS

Special COM Security Configuration

AD CS (Active Directory Certificate Service)



The special configuration is for MS-WCCE to allow any domain account to send a CSR to AD CS with DCOM

<https://posts.specterops.io/certified-pre-owned-d95910965cd2>

Find Exploitable COM Classes on ADCS

Process-wide Security

- Process-wide ACL
- Identity
- Authentication Level
- Impersonation Level

- Registry
 - Defined in `HKEY_CLASSES_ROOT\AppID\{AppID_GUID}`
- CoInitializeSecurity API
 - COM server can call it explicitly to override the configuration in the registry

The image shows three overlapping dialog boxes from the Windows operating system, all titled "CertSrv Request Properties".

- The top-left dialog is in the "General" tab. It shows "Application Name: CertSrv Request", "Application ID: {D99E6E74-FC88-11D0-B498-00A0C90312F3}", "Application Type: Local Service", "Authentication Level: Default" (highlighted with a red box), and "Service Name: CertSvc".
- The top-right dialog is in the "Security" tab. It shows "Launch and Activation Permissions" set to "Customize". Below it, the "Access Permissions" section is visible, leading to a "Launch and Activation Permission" dialog.
- The bottom-right dialog is the "Launch and Activation Permission" dialog, in the "Security" tab. It shows "Group or user names:" with "Everyone" selected. Below, the "Permissions for Everyone" table is shown:

Permissions for Everyone	Allow	Deny
Local Launch	<input type="checkbox"/>	<input type="checkbox"/>
Remote Launch	<input type="checkbox"/>	<input type="checkbox"/>
Local Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The bottom dialog is the "Which user account do you want to use to run this application?" dialog. It has three radio button options: "The interactive user.", "The launching user.", and "This user." (all unselected). Below these are fields for "User:", "Password:", and "Confirm password:". At the bottom, "The system account (services only)." is selected (highlighted with a red box).

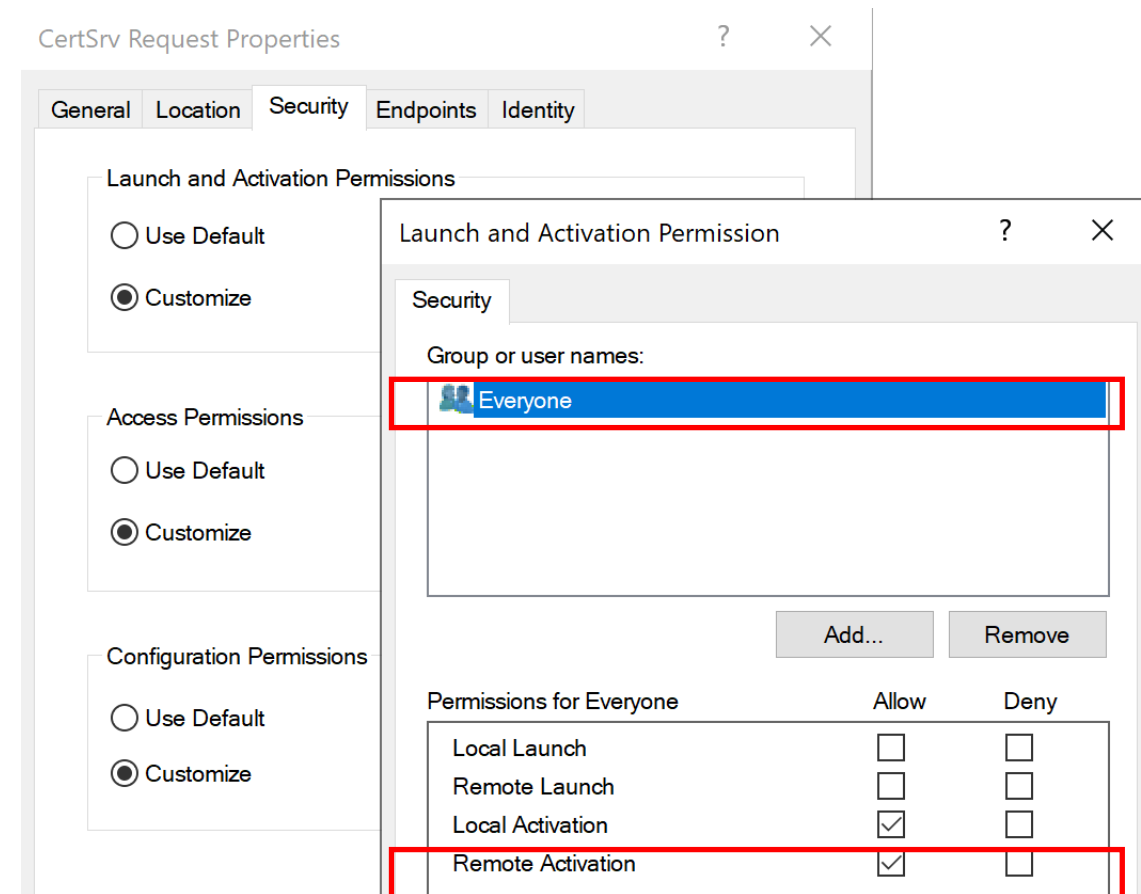
Find Exploitable COM Classes on ADCS

Process-wide ACL for Launch / Activation / Access

- Defined in the LaunchPermission and AccessPermission registry values

What kind of exploitable COM do we need?

- COM servers that are already launched
 - Certificate Service DCOM Access group does not have Remote Launch privilege in the ADCS system-wide ACL
- Process-wide ACL allows remote activation by low-privileged domain accounts



Find Exploitable COM Classes on ADCS

Identity

- Defined in the RunAs registry value
- The user identity the COM server runs as

The Interactive user

- Use the user that is currently logged on to the computer for authentication

The system account

- Use the domain computer account for authentication

What kind of exploitable COM do we need?

- COM servers with the identity set to any user can perform network authentication except
 - Local Service, which use the anonymous user for network authentication

The screenshot shows the 'CertSrv Request Properties' dialog box with the 'Identity' tab selected. The question 'Which user account do you want to use to run this application?' is displayed. There are three radio button options: 'The interactive user.', 'The launching user.', and 'This user.'. Below these are input fields for 'User:', 'Password:', and 'Confirm password:', with a 'Browse...' button next to the 'User:' field. The 'The system account (services only)' option is selected and highlighted with a red box.

Find Exploitable COM Classes on ADCS

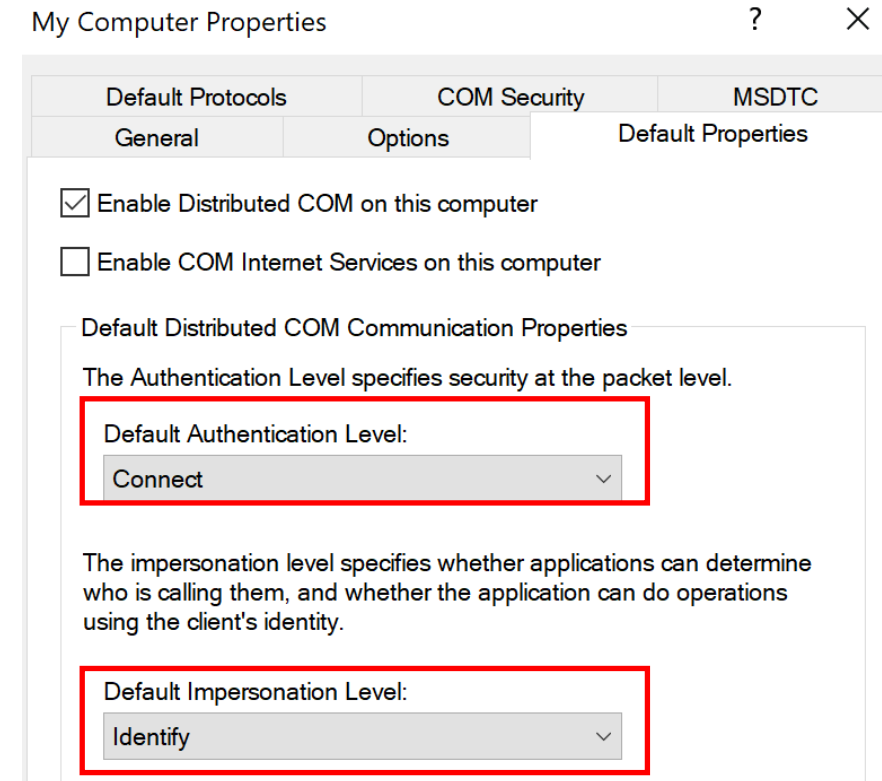
Authentication Level

- Defined in the AuthenticationLevel registry value
- The default value is `RPC_C_AUTHN_LEVEL_CONNECT`, which means no signing and sealing in DCOM connections

Impersonation Level

- The default value is `RPC_C_IMP_LEVEL_IDENTIFY`, which means the server cannot impersonate the client

What kind of exploitable COM do we need?



Target of Relay Attack

Authentication Level

Impersonation Level

LDAP/LDAPS

`RPC_C_AUTHN_LEVEL_CONNECT`

`>= RPC_C_IMP_LEVEL_IDENTIFY`

SMB

`>= RPC_C_AUTHN_LEVEL_CONNECT`

`RPC_C_IMP_LEVEL_IMPERSONATE`

ADCS HTTP(S)

`>= RPC_C_AUTHN_LEVEL_CONNECT`

`RPC_C_IMP_LEVEL_IMPERSONATE`

ADCS MS-ICPR

`>= RPC_C_AUTHN_LEVEL_CONNECT`

`RPC_C_IMP_LEVEL_IMPERSONATE`

Exploitable COM Classes on ADCS

Exploitable COM classes on ADCS

Name	CLSID	Identity	Authentication Level	Impersonation Level
CertSrv Request	d99e6e74-fc88-11d0-b498-00a0c90312f3	SYSTEM	CONNECT	IDENTIFY
CertSrv Admin	d99e6e73-fc88-11d0-b498-00a0c90312f3	SYSTEM	CONNECT	IDENTIFY
OCSPRequestD	3ab092c4-de6a-4dc4-be9e-fdacbb05759c	SYSTEM	CONNECT	IDENTIFY
OCSPAdminD	6d5ad135-1730-4f19-a4eb-3f78e7c976bb	SYSTEM	CONNECT	IDENTIFY

CertSrv Request and CertSrv Admin

- installed in ADCS by default for MS-WCCE

OCSPRequestD and OCSPAdminD

- introduced by the ADCS Online Responder role



Use the ADCS\$ computer account for network authentication

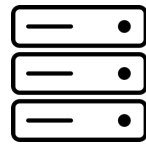


Relay ADCS\$'s authentication messages to LDAP(S)

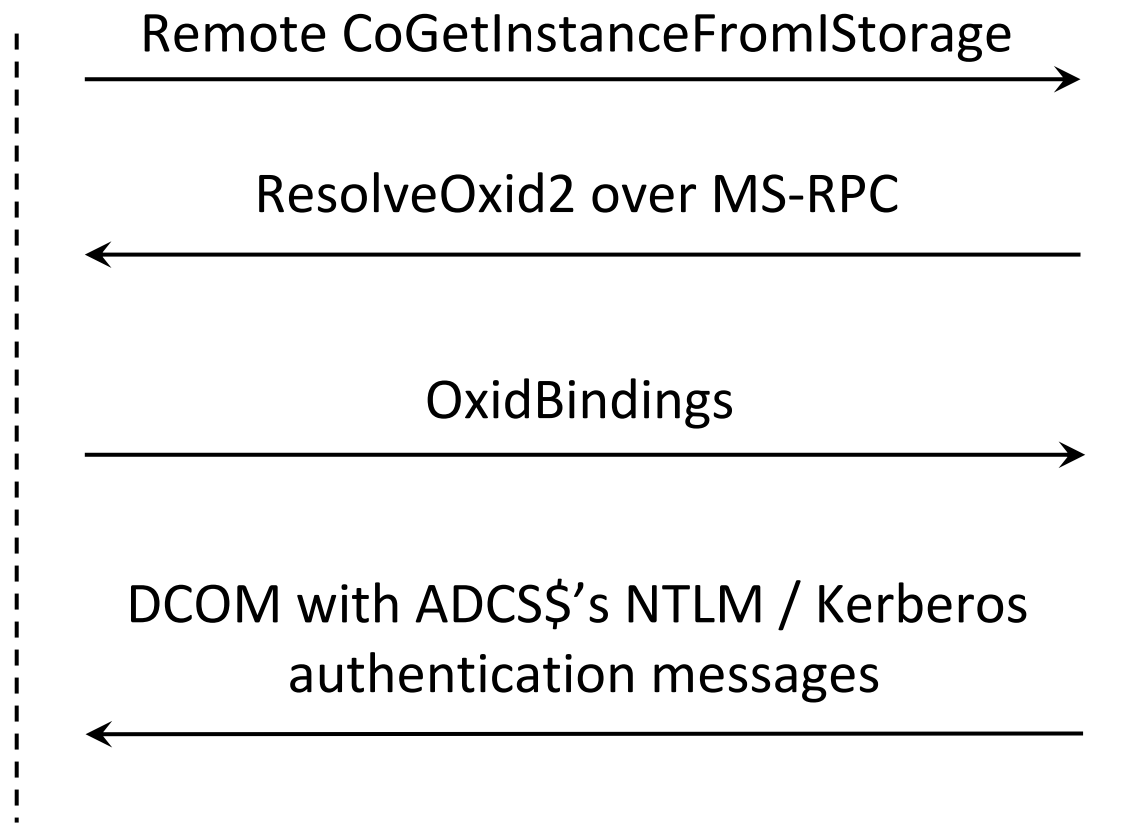
NTLM Relay / Remote Kerberos Relay



Attacker



ADCS



An attacker can use CoGetInstanceFromIStorage to activate an exploitable COM object on ADCS remotely

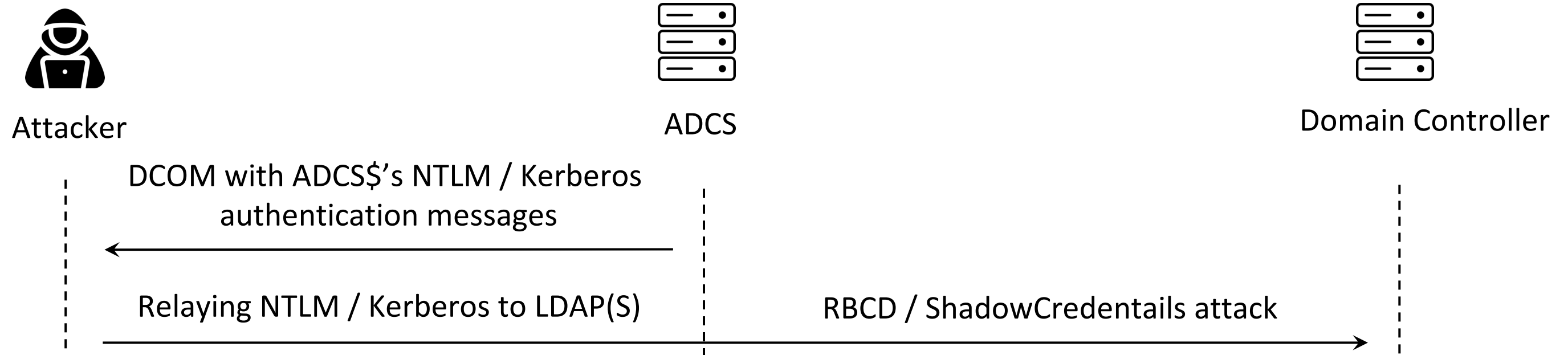
```
DCOM OXID Resolver, ResolveOxid2
Operation: ResolveOxid2 (4)
[Request in frame: 60]
OxidBindings: STRINGBINDINGS=2, SECURITYBINDINGS=1
  NumEntries: 65
  SecurityOffset: 45
  StringBinding[1]: TowerId=NCACN_IP_TCP, NetworkAddr="DESKTOP-WIN10[23456]"
  StringBinding[2]: TowerId=NCACN_IP_TCP, NetworkAddr="192.168.2.142[23456]"
  SecurityBinding[1]: AuthnSvc=0x0010, AuthzSvc=0xffff, PrincName="ldap/dc.demo.lab"
    AuthnSvc: RPC_C_AUTHN_GSS_KERBEROS (0x0010)
    AuthzSvc: Default (0xffff)
    PrincName: ldap/dc.demo.lab
```

OxidBindings

SecurityBinding

- AuthnSvc can be set to NTLM / Kerberos
- PrincName can be set to any SPN

NTLM Relay / Remote Kerberos Relay



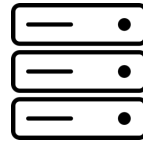
The authentication in this DCOM connection will adhere to the process-wide security configurations of the exploitable COM

The attacker can then relay ADCS\$'s authentication messages to LDAP(S) to perform RBCD / ShadowCredentials attack

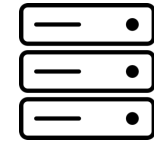
NTLM Relay / Remote Kerberos Relay



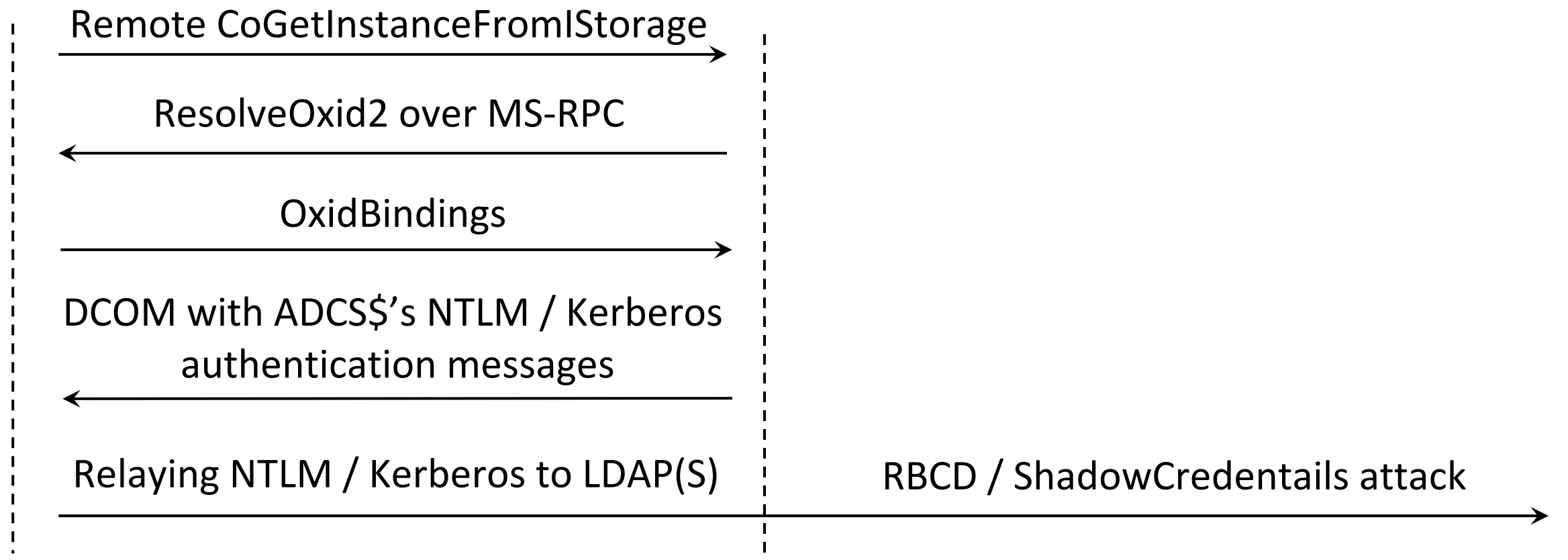
Attacker



ADCS



Domain Controller



Privilege Escalation to Domain Admin

Attack Path #1

- Use S4U2Self/S4U2Proxy to request a domain admin's ST to access the ADCS
- RCE on the ADCS with PSEXEC, WMIEXEC, WINRM ... to dump the private key
- Escalate to Domain Admin with the Golden Certificate attack

Attack Path #2

- Use S4U2Self/S4U2Proxy to request a domain admin's ST to access the ADCS
- Use the domain admin's ST to request a certificate with MS-WCCE/MS-ICPR/...
- Use the domain admin's certificate to request a TGT with PKINIT
- Escalate to Domain Admin with the TGT

Demo

<https://youtu.be/OHwjeGUSM4w>

Patch and Mitigation

Patch - CVE-2022-37976

- Released on October 11, 2022
- The patch raised the authentication level to `RPC_C_AUTHN_LEVEL_PKT_PRIVACY` in the Certificate Service.

DCOM Authentication Hardening

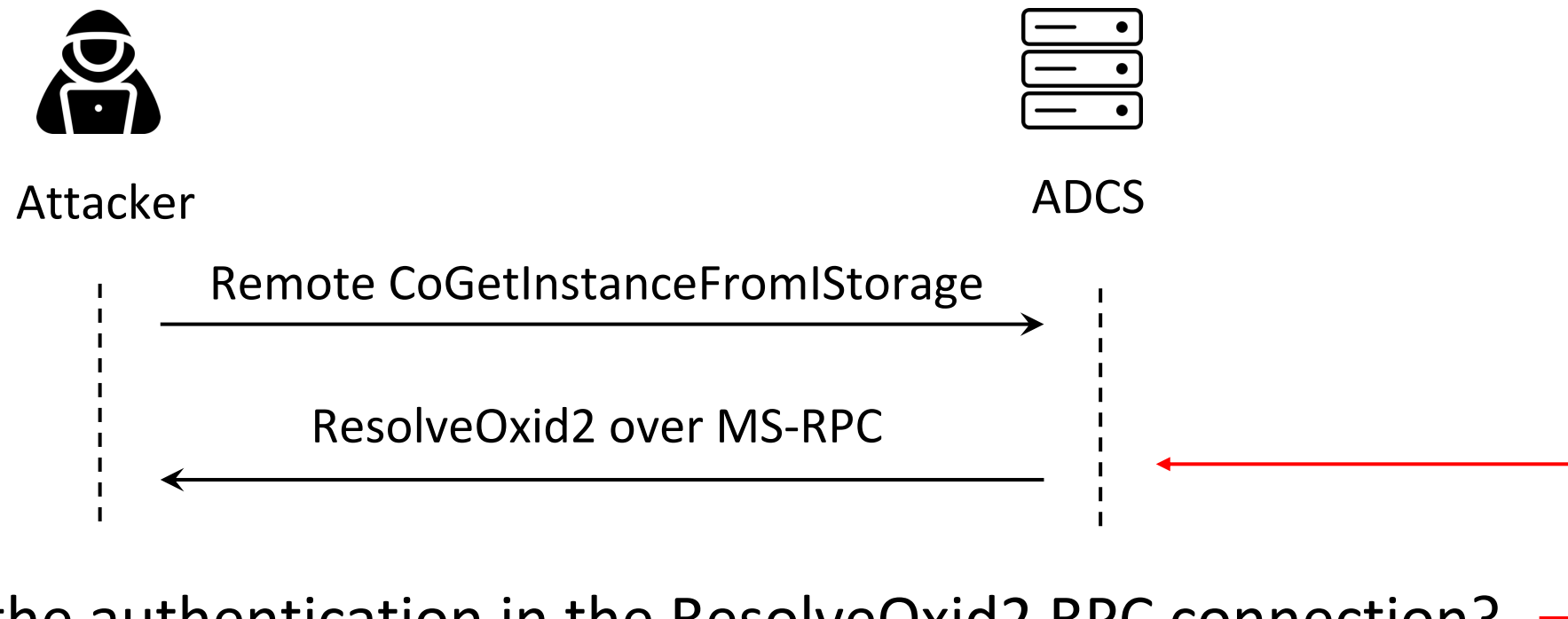
- Released on November 8, 2022
- The update automatically raised authentication level for all non-anonymous activation requests from DCOM clients to `RPC_C_AUTHN_LEVEL_PKT_INTEGRITY` if it's below Packet Integrity.

Enable Protection for Relay Attacks

- LDAP Signing and Channel Binding

Can We Relay to Other Services?

- Relaying to ADCS HTTP(S) / SMB / MS-ICPR requires the impersonation level of authentication set to `RPC_C_IMP_LEVEL_IMPERSONATE`
- No remotely activatable COM class on ADCS satisfies this requirement



- Can we relay the authentication in the ResolveOxid2 RPC connection?

Can We Relay to Other Services?

rpcss.dll!ResolveClientOXID

```
QoS.Version = v86;  
QoS.Capabilities = v86;  
QoS.IdentityTracking = v86;  
QoS.ImpersonationType = 3; // RPC_C_IMP_LEVEL_IMPERSONATE  
  
v110 = RpcBindingSetAuthInfoExW(  
    Binding,  
    pSPN,  
    2 - ((*((_DWORD *)v20 + 11) & 2) != 0),  
    v108,  
    AuthzSvc,  
    (unsigned int)AuthzSvc,  
    &QoS);
```

The impersonation level of the ResolveOxid2 RPC authentication is RPC_C_IMP_LEVEL_IMPERSONATE

NTLM Relay

- We can relay ADCS\$'s NTLM authentication messages in the ResolveOxid2 RPC to another ADCS Server's HTTP / MS-ICPR (without IF_ENFORCEENCRYPTICERTREQUEST flag)
- Requires two ADCS server in the domain, because we can't relay NTLM back to the same machine

Kerberos Relay ?

SecurityBinding

AuthnSvc	Reserved
Service Principal Name	

Can we set arbitrary SPN in the forged OBJREF's SecurityBinding?

rpcss.dll!ResolveClientOXID

```
else
{
    rpcssSPN = (char *)L"RPCSS/" - (char *)ServerPrincName;
    v100 = length;
    ServerPrincName_ = ServerPrincName;
    do
    {
        if ( !(0x7FFFFFFE - length + v100) )
            break;
        v102 = *(RPC_WSTR)((char *)ServerPrincName_ + rpcssSPN);
        if ( !v102 )
            break;
        *ServerPrincName_++ = v102;           // Copy RPCSS/ to ServerPrincName
        --v100;
    }
    while ( v100 );
    v103 = ServerPrincName_ - 1;
    if ( v100 )
        v103 = ServerPrincName_;
    *v103 = 0;
}
StringCchCatW(_ServicePrincName, length, _MachineNameFromStringBinding); // RPCSS/ + MachineName from StringBinding
```

The SPN in the ResolveOxid2 RPC authentication is forced to **RPCSS/MachineNameFromStringBinding**

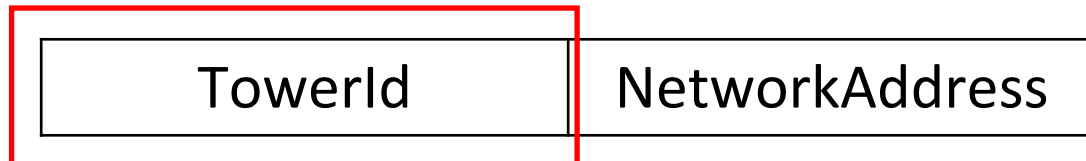
Kerberos Relay

- Unable to trigger Kerberos Relay with the SecurityBinding



RPC Protocol Sequence

StringBinding



RPC sequence type

- identifies the protocol to be used in RPC calls

TCP, UDP, SMB, NetBIOS, HTTP, MQ ...

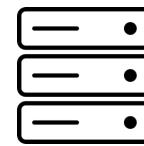
Can these protocols be abused for NTLM/Kerberos Relay?

Tower Id	RPC Transport
0x04	ncacn_dnet_nsp
0x07	ncacn_ip_tcp
0x08	ncadg_ip_udp
0x09	ncacn_nb_tcp
0x0C	ncacn_spx
0x0D	ncacn_nb_ipx
0x0E	ncadg_ipx
0x0F	ncacn_np
0x10	ncalrpc
0x13	ncacn_nb_nb
0x16	ncacn_at_dsp
0x17	ncadg_at_ddp
0x1A	ncacn_vns_spp
0x1D	ncadg_mq
0x1F	ncacn_http
0x21	ncacn_hvsocket

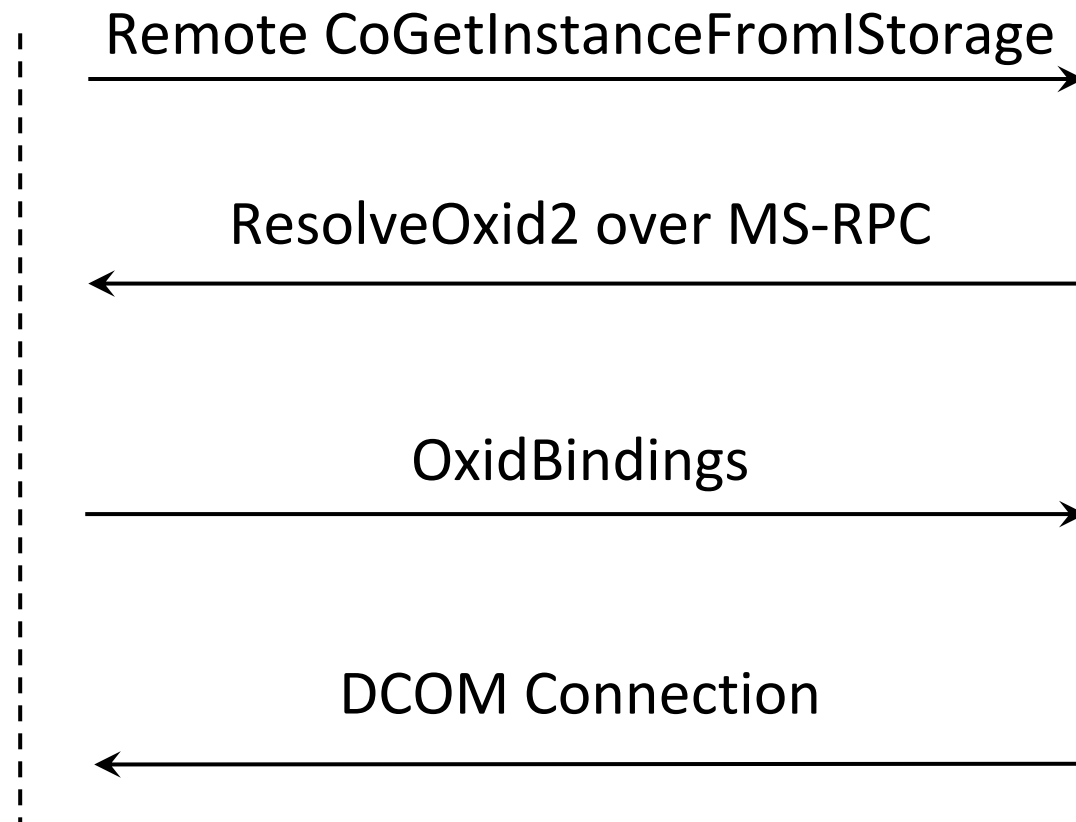
RPC Protocol Sequence



Attacker



ADCS



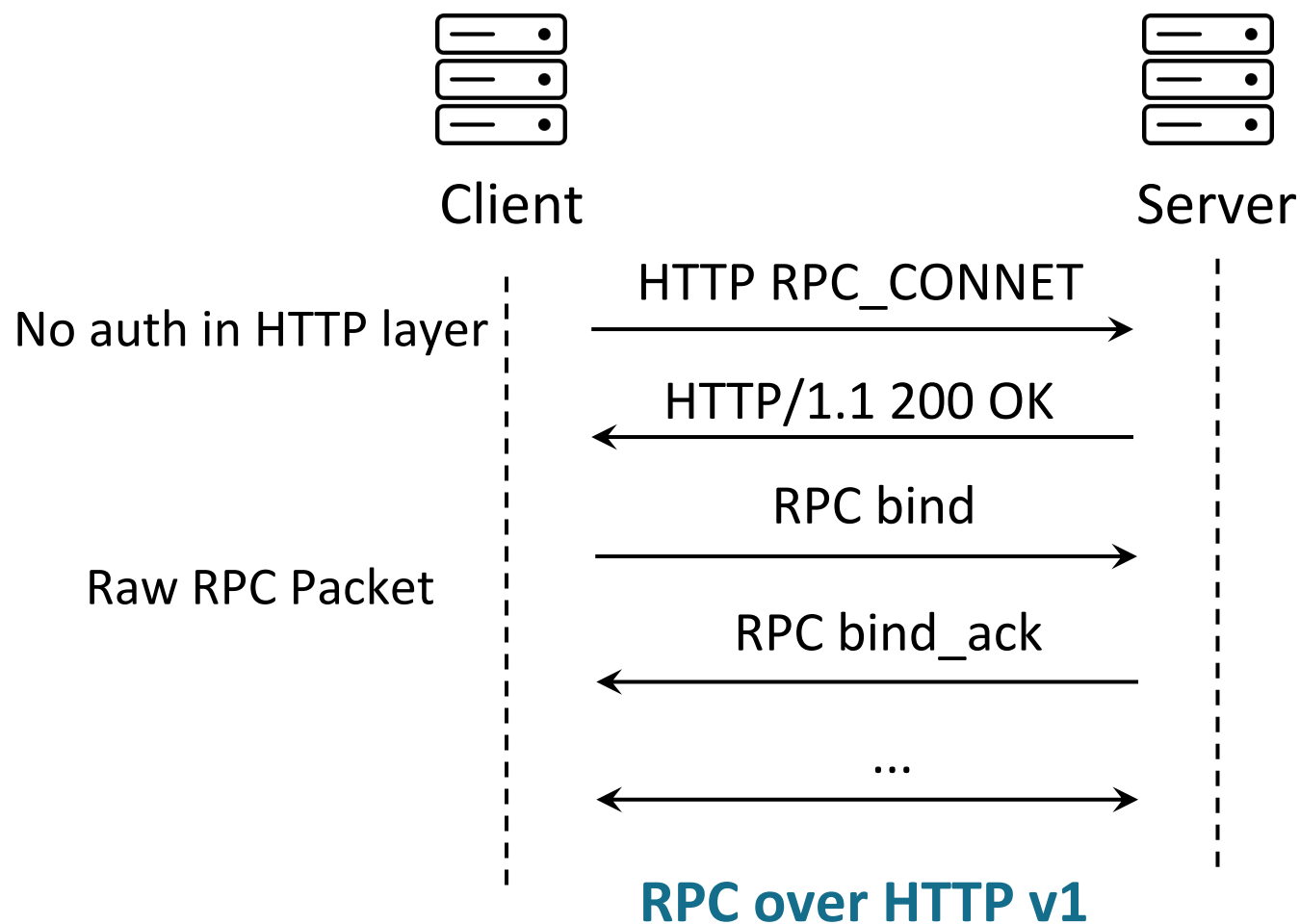
- ncacn_ip_tcp
- ncacn_http



- ncacn_ip_tcp
- ncacn_http
- ncacn_np

RPC over HTTP (ncacn_http)

- Support both RPC over HTTP v1 and RPC over HTTP v2
- Use the RPC over HTTP v2 first; if that fails, the client will fall back to the RPC over HTTP v1



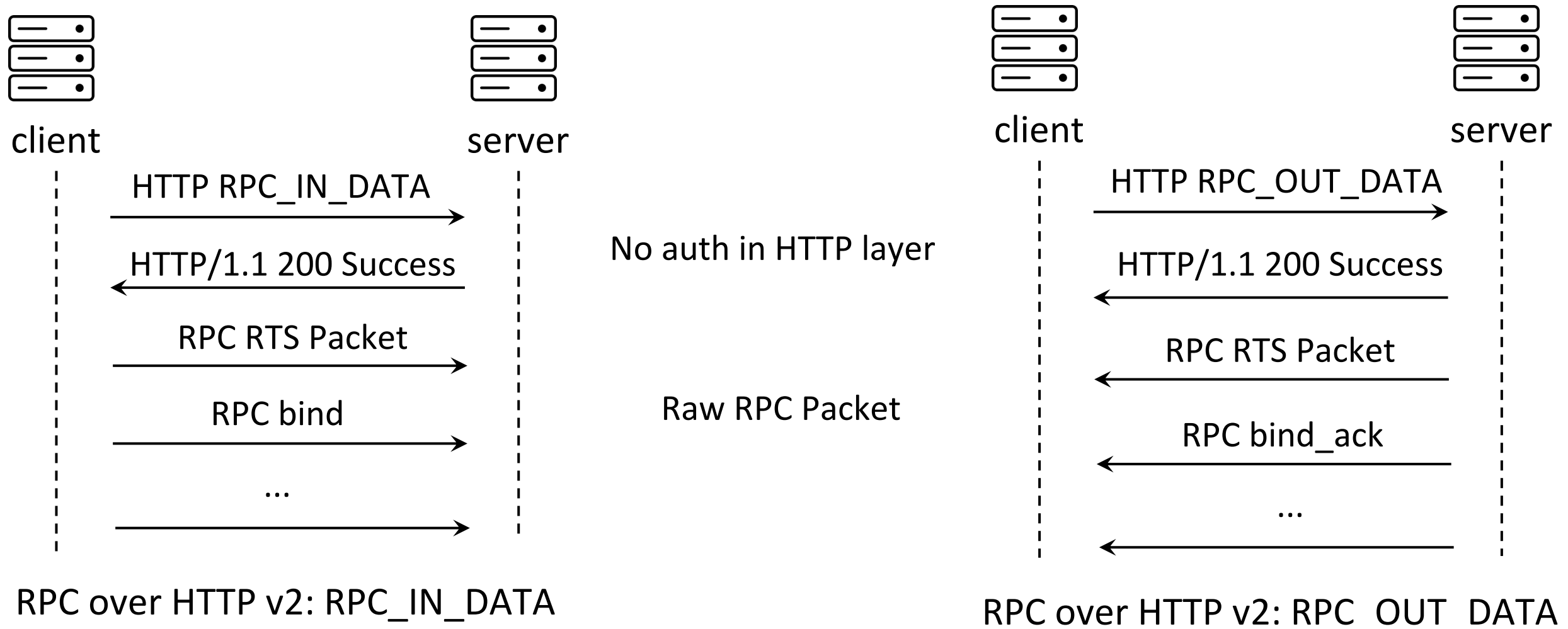
Authentication messages in the RPC packet

192.168.2.1...	192.168.2.1	HTTP	RPC_CONNECT 192.168.2.1:593 HTTP/1.1
192.168.2.1	192.168.2.101	HTTP	HTTP/1.1 200 OK
192.168.2.1...	192.168.2.1	HTTP	Continuation
192.168.2.1	192.168.2.101	HTTP	Continuation
192.168.2.1...	192.168.2.1	HTTP	Continuation

> Frame 84: 288 bytes on wire (234 bytes captured)	0000	00 0c 29 7d b8 e8 3e 22 fb 79 13 65 08 00 45 02	..)}..>" ..y.e..E..
> Ethernet II, Src: 3e:22:fb:79:1c:29, Dst: 02:00:00:00:00:00	0010	01 12 00 00 40 00 40 06 00 00 c0 a8 02 01 c0 a8	...@.@...
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.101	0020	02 65 00 50 cc db 46 c2 45 5a da 49 e5 f2 50 18	...e.P..F..EZ.I..P..
> Transmission Control Protocol, Src Port: 593, Dst Port: 80	0030	10 00 86 bb 00 00 05 00 0c 07 10 00 00 00 ea 00xV4...
> Hypertext Transfer Protocol	0040	a6 00 03 00 00 00 f8 0f f8 0f 78 56 34 12 05 009999....]
File Data: 234 bytes	0050	39 39 39 39 00 00 01 00 00 00 00 00 00 04 5d+H`...
Data (234 bytes)	0060	88 8a eb 1c c9 11 9f e8 08 00 2b 10 48 60 02 00NTLMSS...
Data [truncated]: 05000c07	0070	00 00 0a 05 00 00 00 00 00 00 4e 54 4c 4d 53 53	P.....8.....
[Length: 234]	0080	50 00 02 00 00 00 08 00 08 00 38 00 00 00 15 82	...V.../ kJ.....
	0090	89 e2 8a 56 94 e9 7f 2f 6b 4a 00 00 00 00 00 00	...f.f.@...cE..
	00a0	00 00 66 00 66 00 40 00 00 00 0a 00 63 45 00 00	...D.E.M. 0...D..
	00b0	00 0f 44 00 45 00 4d 00 4f 00 02 00 08 00 44 00	E.M.O...D.C...
	00c0	45 00 4d 00 4f 00 01 00 04 00 44 00 43 00 04 00	...d.e.m.o...l.a...
	00d0	10 00 64 00 65 00 6d 00 6f 00 2e 00 6c 00 61 00	o...d.c...d.e...
	00e0	62 00 03 00 16 00 64 00 63 00 2e 00 64 00 65 00	m.o...l.a.b....
	00f0	6d 00 6f 00 2e 00 6c 00 61 00 62 00 05 00 10 00	d.e.m.o...l.a.b...
	0100	64 00 65 00 6d 00 6f 00 2e 00 6c 00 61 00 62 00	...~2j
	0110	07 00 08 00 7e 02 32 6a a5 8d da 01 00 00 00 00	


RPC over HTTP (ncacn_http)

RPC over HTTP v2



RPC over HTTP (ncacn_http)

RPC over HTTP (ncacn_http)

- No authentication in the HTTP layer 
- The RPC authentication in **ncacn_http** works the same as it is in **ncacn_ip_tcp**

NTLM Relay / Kerberos Relay

- We can perform NTLM Relay / Kerberos Relay with RPC packets in HTTP connections the same as RPC over **ncacn_ip_tcp**
- RPC over HTTP traffic may bypass some network restrictions or NDR devices

RPC over Named Pipe (ncacn_np)

- The DCOM connection also support RPC over Named Pipe (ncacn_np)
- The ncacn_np uses the identity of RPCSS (NETWORK SERVICE) for network authentication in the SMB layer

192.168.2.1...	192.168.2.1	SMB	Negotiate Protocol Request
192.168.2.1	192.168.2.101	SMB2	Negotiate Protocol Response
192.168.2.1...	192.168.2.1	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
192.168.2.1	192.168.2.101	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_RE
192.168.2.1...	192.168.2.1	SMB2	Session Setup Request, NTLMSSP_AUTH, User: DEMO\ADCS\$
192.168.2.1	192.168.2.101	SMB2	Session Setup Response
192.168.2.1...	192.168.2.1	SMB2	Tree Connect Request Tree: \\192.168.2.1\IPC\$
192.168.2.1	192.168.2.101	SMB2	Tree Connect Response, Error: STATUS_NETWORK_SESSION_EXF
192.168.2.1...	192.168.2.1	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
192.168.2.1	192.168.2.101	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_RE
192.168.2.1...	192.168.2.1	SMB2	Session Setup Request, NTLMSSP_AUTH, User: DEMO\ADCS\$

The ADCS machine account ←

RPC over Named Pipe (ncacn_np)

The impersonation level of the authentication is SECURITY IMPERSONATION, which means the client can be impersonated by the server.

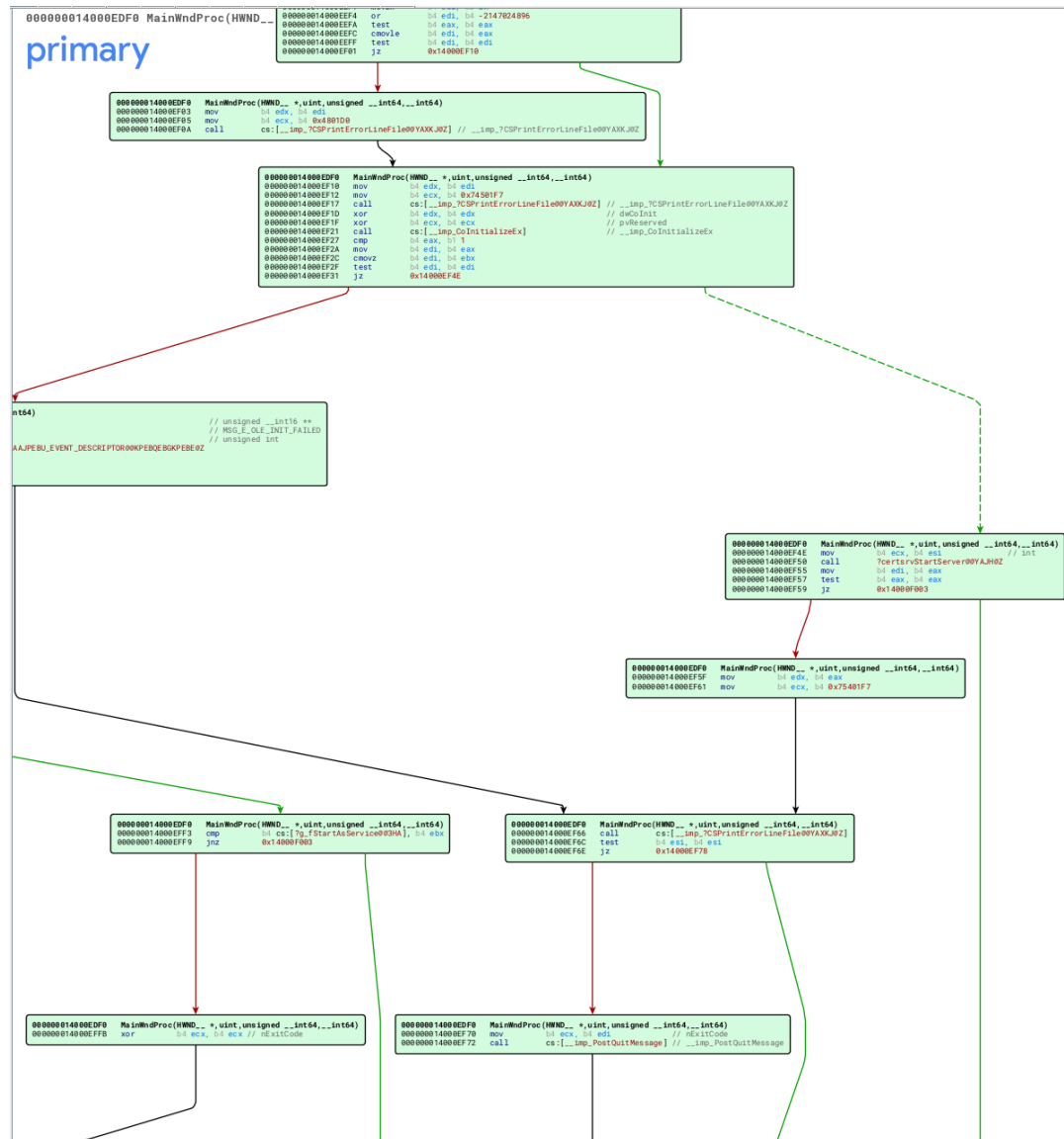
NTLM Relay

- We can relay ADCS's NTLM authentication messages in the SMB to another ADCS Server's HTTP / MS-ICPR (without IF_ENFORCEENCRYPTICERTREQUEST flag)
- Requires two ADCS server in the domain

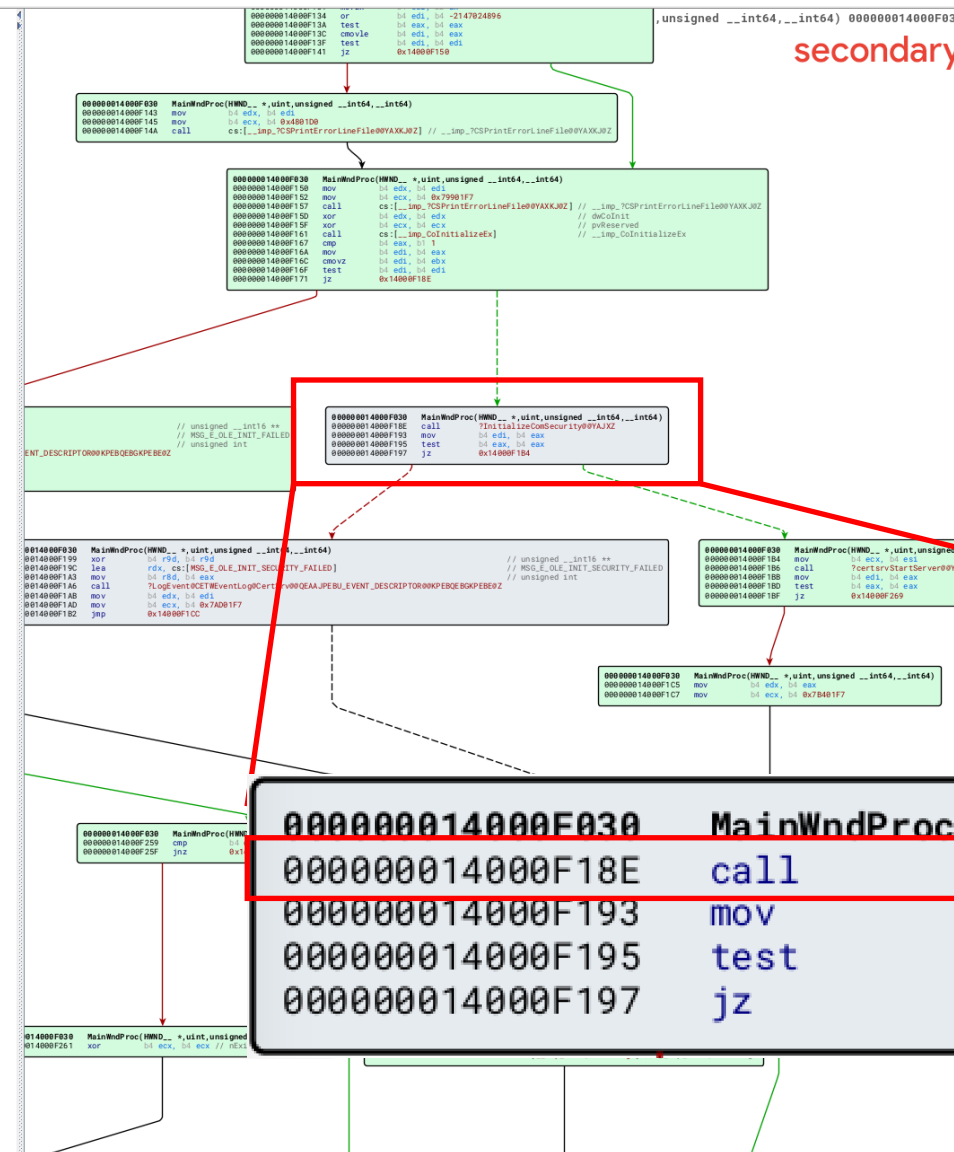
Kerberos Relay

- The SPN in the authentication is forced to be **CIFS/MachineNameFromStringBinding**
- Unable to trigger Kerberos Relay

CVE-2022-37976 Patch Analysis



certsrv.exe before patch



```

000000014000F030 MainWndProc(HWND_ *, uint, unsigned __int64, __int64)
000000014000F18E call    ?InitializeComSecurity@YAJXJZ
000000014000F193 mov     b4 edi, b4 eax
000000014000F195 test    b4 eax, b4 eax
000000014000F197 jz     0x14000F1B4
  
```

certsrv.exe after patch

CVE-2022-37976 Patch Analysis

MainWndProc

- InitializeComSecurity → This function is introduced by the patch
- CoInitializeSecurity

```
loc_14000CE2D:          ; pReserved3
mov     [rsp+78h+lpdwOwnerSize], r13
xor     r9d, r9d          ; pReserved1
mov     dword ptr [rsp+78h+pOwner], r13d ; dwCapabilities
xor     r8d, r8d          ; asAuthSvc
mov     [rsp+78h+lpdwSaclSize], r13 ; pAuthList
or      edx, 0FFFFFFFFh ; cAuthSvc
mov     dword ptr [rsp+78h+pSacl], 3 ; dwImpLevel
mov     rcx, r12          ; pSecDesc
mov     dword ptr [rsp+78h+lpdwDaclSize], 6 ; dwAuthnLevel
call    cs:___imp_CoInitializeSecurity
mov     ebx, eax
test   eax, eax
jz     short loc_14000CE7F
```

Impersonation Level is set to

RPC_C_IMP_LEVEL_IMPERSONATE

Authentication Level is set to

RPC_C_AUTHN_LEVEL_PKT_PRIVACY

Kerberos Reflection

The patch for CVE-2022-37976 changed the impersonation level of the Certificate Service (CertSrv Request and CertSrv Admin) to **RPC_C_IMP_LEVEL_IMPERSONATE**

NTLM Relay

With the patch, we can relay DCOM to ADCS HTTP / MS-ICPR running on a different machine

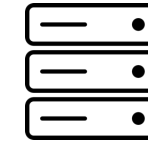
Kerberos Reflection

Kerberos Reflection is not restricted, we can **relay Kerberos back to the same ADCS server**

Kerberos Reflection



Attacker



ADCS

Remote CoGetInstanceFromIStorage with the CertSrv Request COM

ResolveOxid2 over MS-RPC

OxidBindings StringBinding : attacker's machine
SecurityBinding : http/adcs.domain.local

DCOM with ADCS's Kerberos AP-REQ messages

Relaying Kerberos AP-REQ to ADCS HTTP

Request a certificate of ADCS\$

ncacn_ip_tcp
or
ncacn_http

Mitigations

ADCS HTTP Endpoints

- Follow [Microsoft's guide](#) to enable EPA (Extended Protection for Authentication) on your ADCS HTTP endpoints
- EPA can protect your ADCS HTTP endpoints from both NTLM Relay and Kerberos Relay

MS-ICPR

- Keep the default settings of the MS-ICPR, don't remove the IF_ENFORCEENCRYPTICERTREQUEST flag

Black Hat Sounds Bytes

CertifiedDCOM

- A remote attack surface of DCOM and AD CS
- Privilege escalation from Domain Users to Domain Admin
- Take Kerberos Relay to the next level, make it a remote attack vector
- Attacks may also work against customized DCOM with misconfigurations

Mitigations

- Update your AD CS to install the patch for CVE-2022-37976
- Update all your machines to enable DCOM Authentication Hardening
- Enable LDAP Signing and Channel Binding & Enable EPA for ADCS HTTP
- Check your customized system-wide and process-wide COM security configurations

Acknowledgments

Standing on the shoulders of giants !

- James Forshaw (@tiraniddo)
- Andrea Pierini (@decoder_it)
- Antonio Cocomazzi (@splinter_code)
- @cube0x0



Thank You !

Tianze Ding (@D1iv3)
Tencent Security Xuanwu Lab