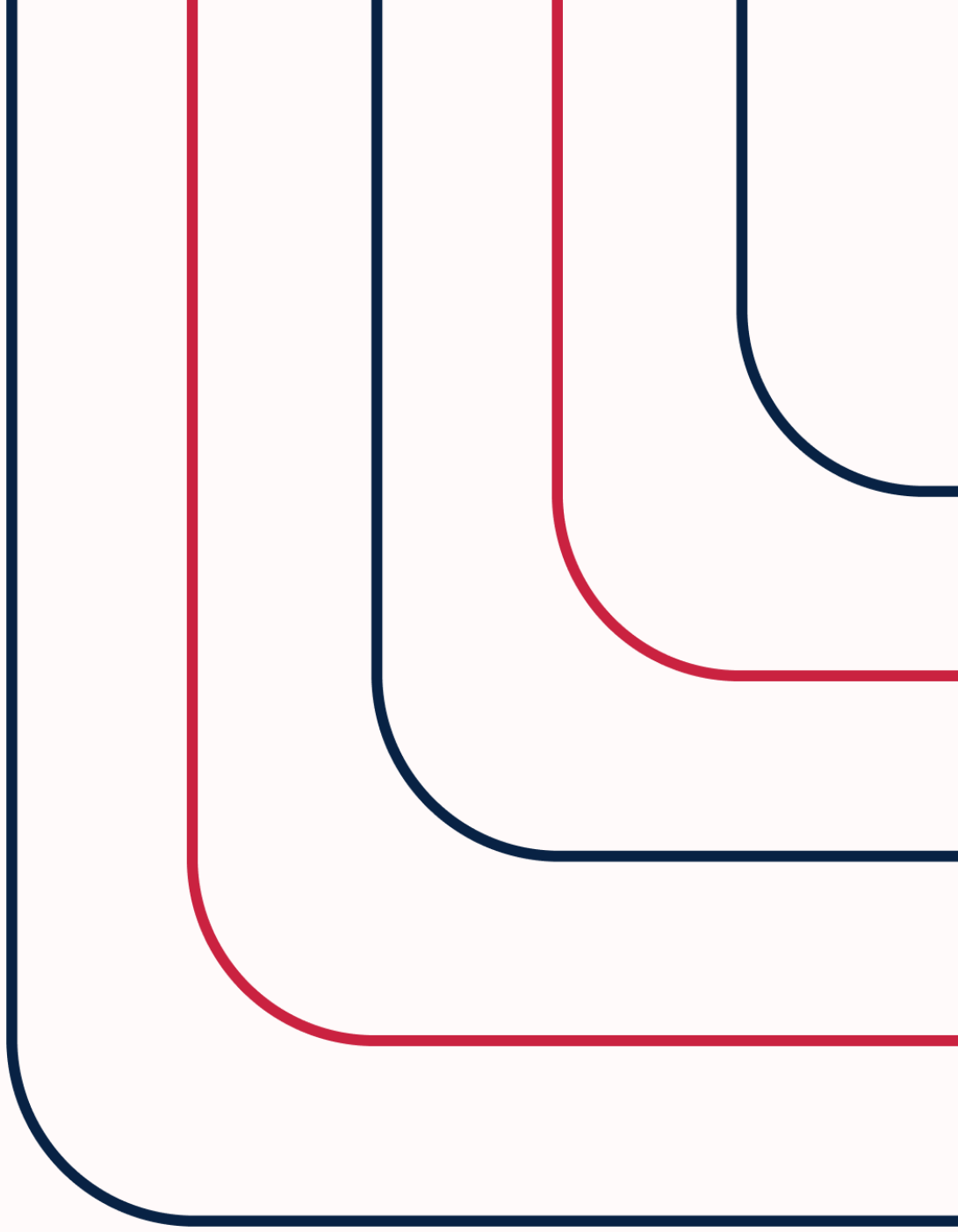
Wine RUMP

26 september 2025

It's RPC time!

Margaux DABERT
@Rauxam_

login by constellation

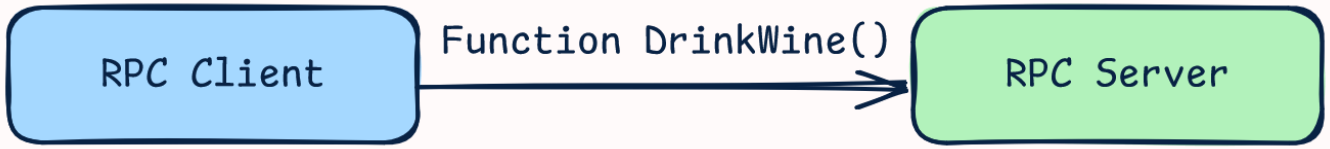


Introduction

What?

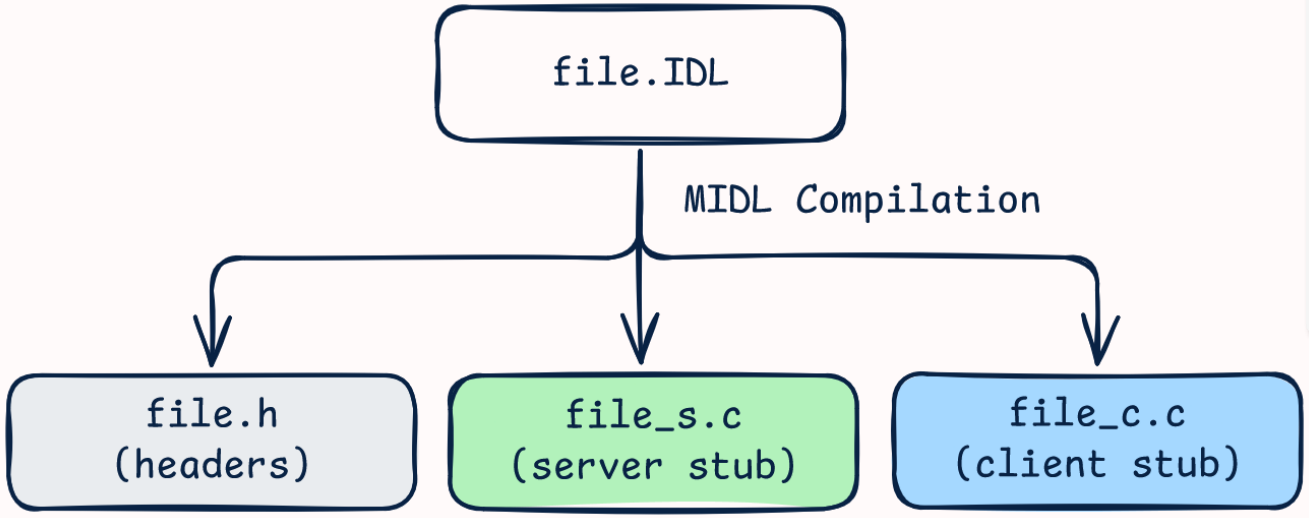
RPC/MSRPC

Offensive axis



How?

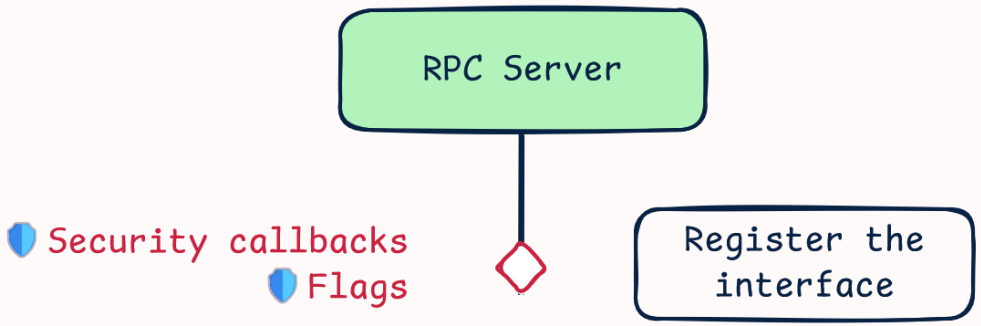
It begins with IDL (Interface Definition Language) file



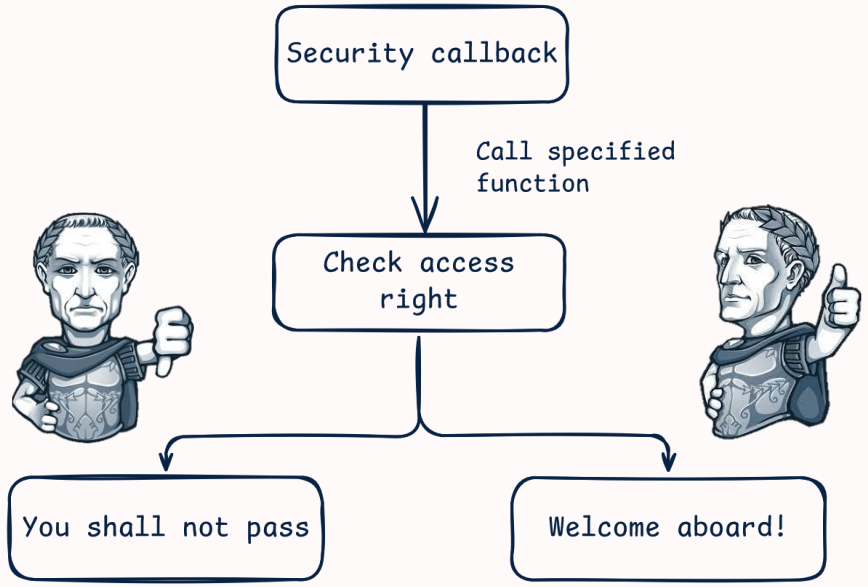
file.IDL

```
[
    uuid(d6b1ad2b-b550-4729-b6c2-1651f58480c3),
        version(1.0),
]

interface WineRumpInt
{
    int Proc0_DrinkWine(
        [in] handle_t hBinding,
        [in, string] const char* pszOutput);

    void Proc1_GrapeHarvest(
        [in] handle_t  hBinding);
}
```

1 – Server setup



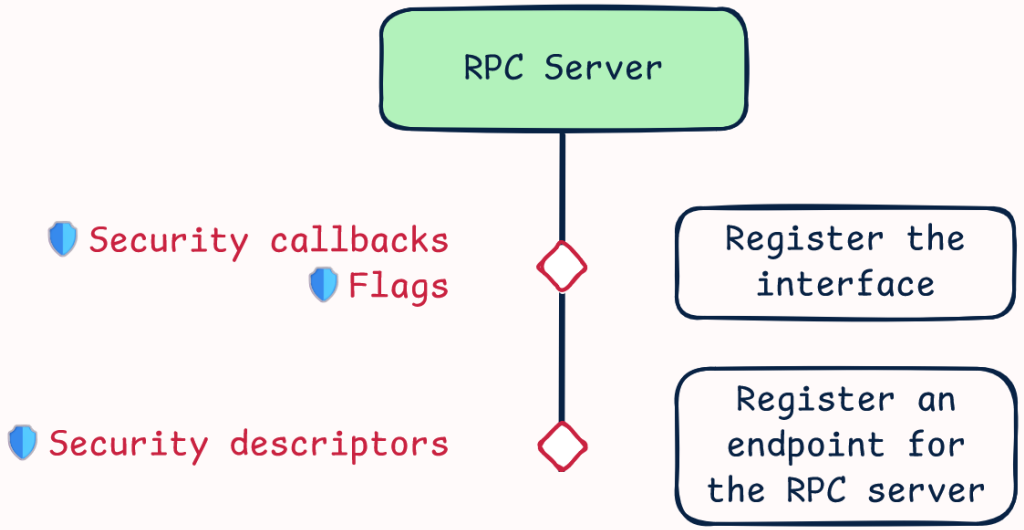

```
RpcServerRegisterIf2(
        WineRumptInt1_v1_0_s_ifspec,           // Interface to register.
        NULL,                                  // Nil-type UUID
        NULL,                                  // Use the MIDL generated entry-point vector.
        RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH, // Forces use of security callback.
        RPC_C_LISTEN_MAX_CALLS_DEFAULT,        // Use default number of concurrent calls.
        (unsigned)-1,                          // Infinite max size of incoming data blocks.
        SecurityCallback);                     // Security callback function.
```



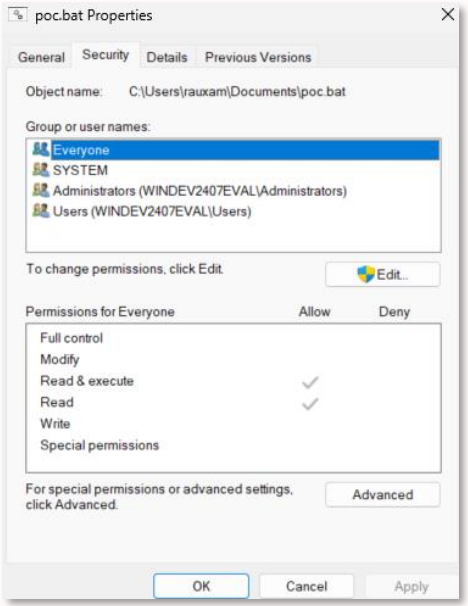

```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] Registering server interface {d6b1ad2b-b550-4729-b6c2-1651f58480c3} (WineRumpInt)
    -> Flag "RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH" & Security callback set.
```

Code based on CSandker project InterProcessCommunication-Samples

1 – Server setup

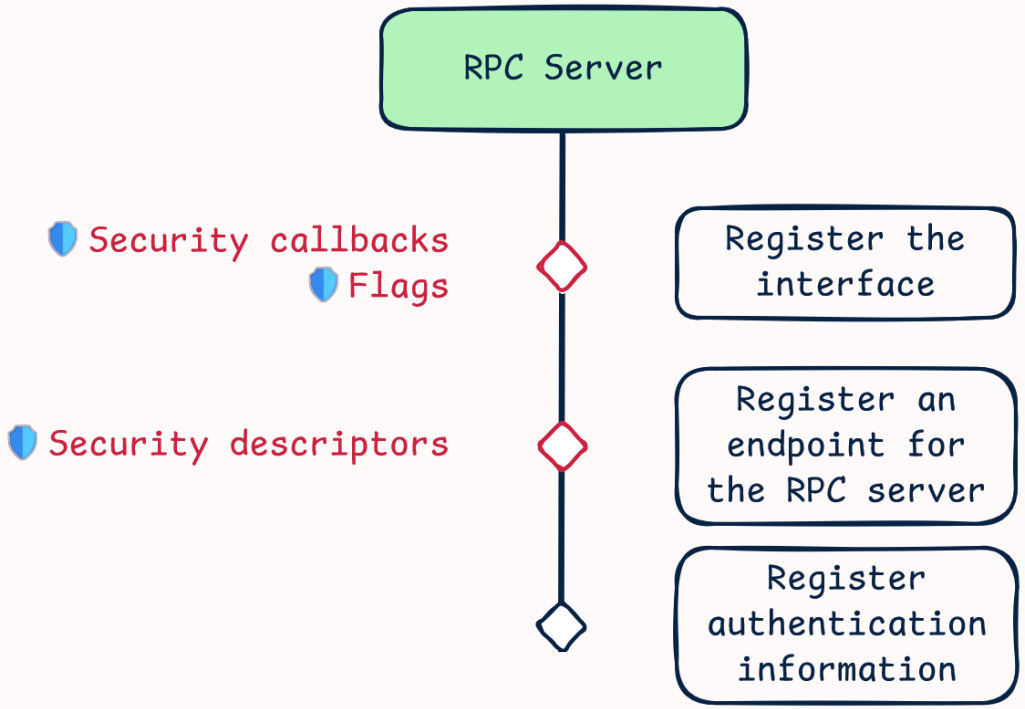



```
RpcServerUseProtseqEp(
        pszProtSeq,                     // Protocol to use.
        RPC_C_PROTSEQ_MAX_REQS_DEFAULT, // Backlog queue length for TCP/IP.
        pszTCPPort,                     // TCP/IP port or named pipe for example to use.
        NULL                            // No Security Descriptor
    );
```




```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] Registering server interface {d6b1ad2b-b550-4729-b6c2-1651f58480c3} (WineRumpInt)
    -> Flag "RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH" & Security callback set.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump-Admin'.
    -> Security descriptor defined on endpoint: only Admin user is able to access this endpoint.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump'.
    -> Default security descriptor defined on endpoint.
```

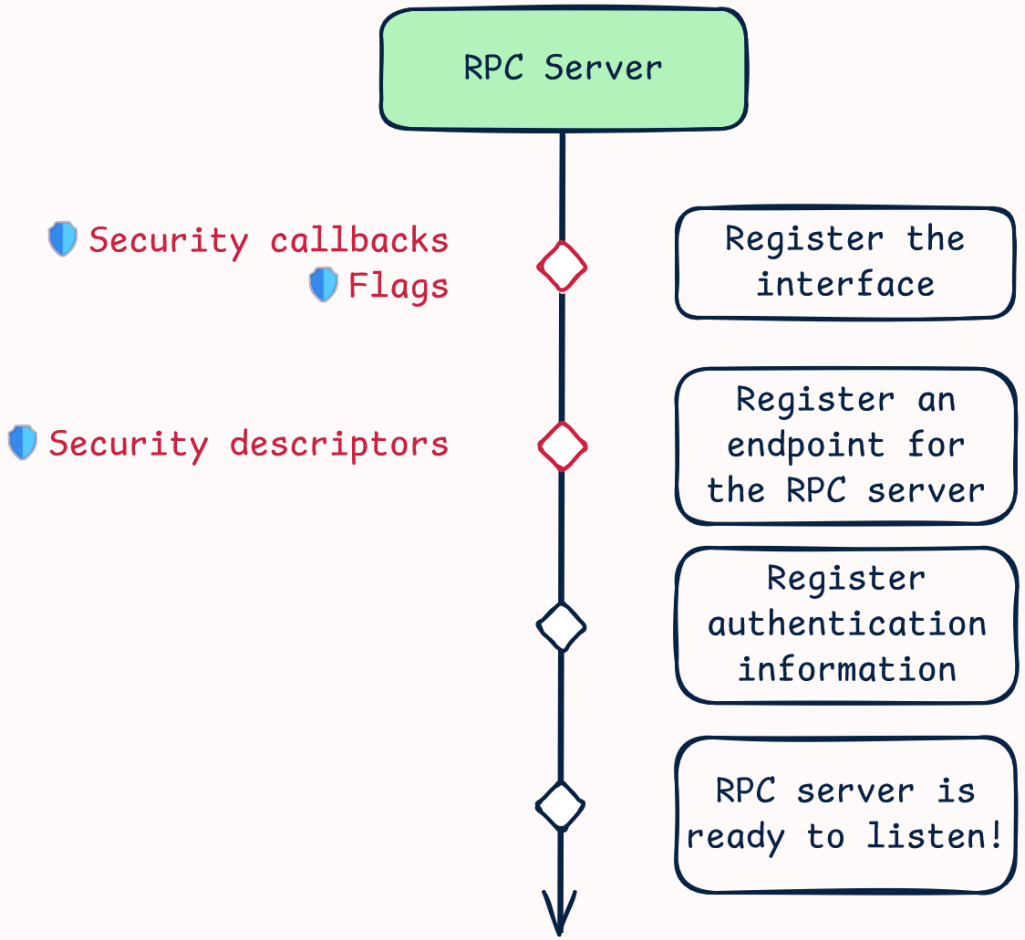
1 – Server setup




```
RpcServerRegisterAuthInfo(
        pszSpn,                 // Server principal name
        RPC_C_AUTHN_WINNT,       // using NTLM as authentication service provider
        NULL,                   // Use default key function, is ignored for NTLM SSP
        NULL);                  // No arg for key function
```

```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] Registering server interface {d6b1ad2b-b550-4729-b6c2-1651f58480c3} (WineRumpInt)
    -> Flag "RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH" & Security callback set.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump-Admin'.
    -> Security descriptor defined on endpoint: only Admin user is able to access this endpoint.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump'.
    -> Default security descriptor defined on endpoint.
[*] Register authentication information.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
```

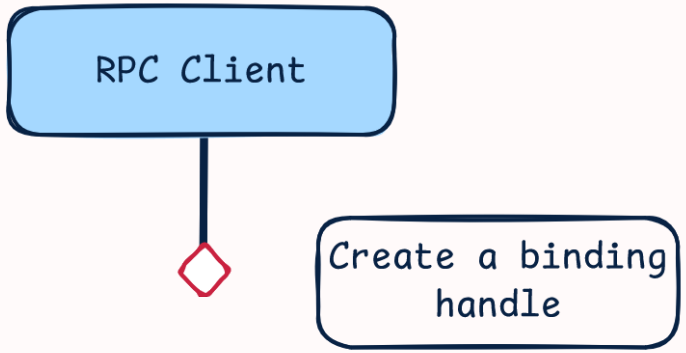
1 – Server setup




```
RpcServerListen(
        1,                                  // Recommended minimum number of threads.
        RPC_C_LISTEN_MAX_CALLS_DEFAULT,     // Recommended maximum number of threads.
        FALSE);
```

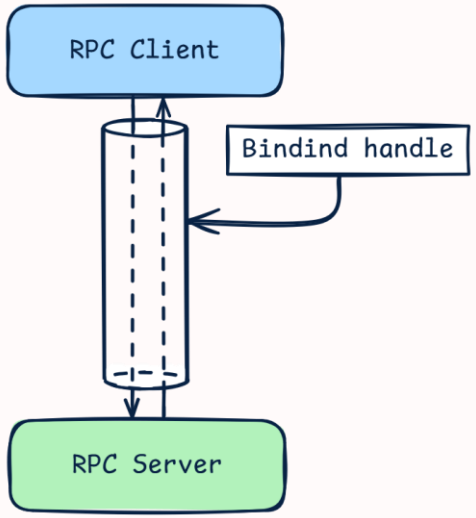
```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] Registering server interface {d6b1ad2b-b550-4729-b6c2-1651f58480c3} (WineRumpInt)
    -> Flag "RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH" & Security callback set.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump-Admin'.
    -> Security descriptor defined on endpoint: only Admin user is able to access this endpoint.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump'.
    -> Default security descriptor defined on endpoint.
[*] Register authentication information.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
[*] RPC Server is ready!

Listening for client order. Who wants a glass of wine?
```

2 – Client side



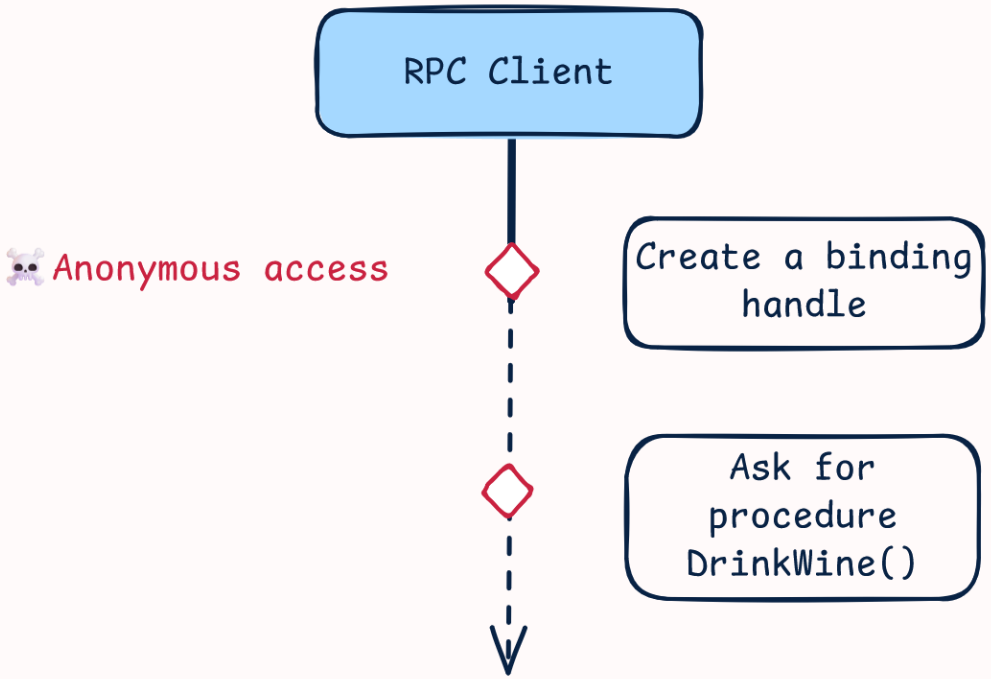

```
RpcStringBindingCompose(
        NULL,                   // UUID to bind to.
        pszProtSeq,             // Protocol to use.
        pszTCPHost,             // Network address to use.
        pszTCPPort,             // TCP/IP port or named pipe to use.
        NULL,                   // Protocol dependent network options to use.
        &szStringBinding);      // String binding output.
```

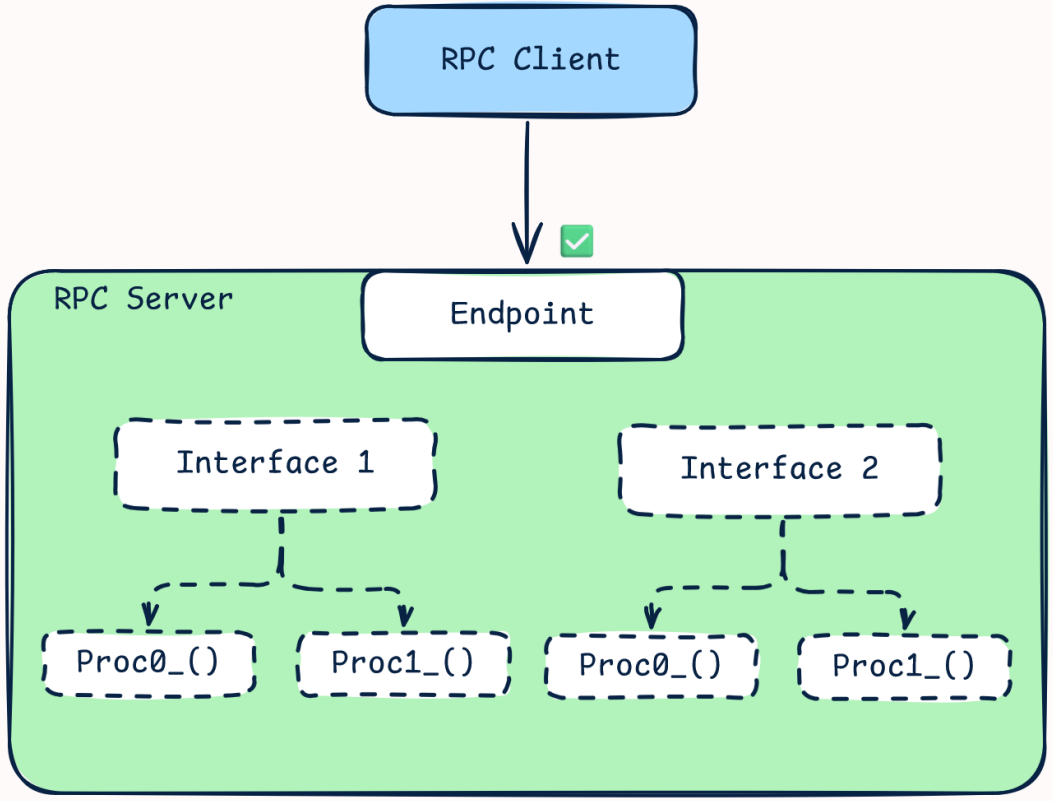
```
RpcBindingFromStringBinding(
        szStringBinding,    // The string binding to validate.
        &hExplicitBinding   // Put the result in the implicit binding
    );                      // handle defined in the IDL file.
```



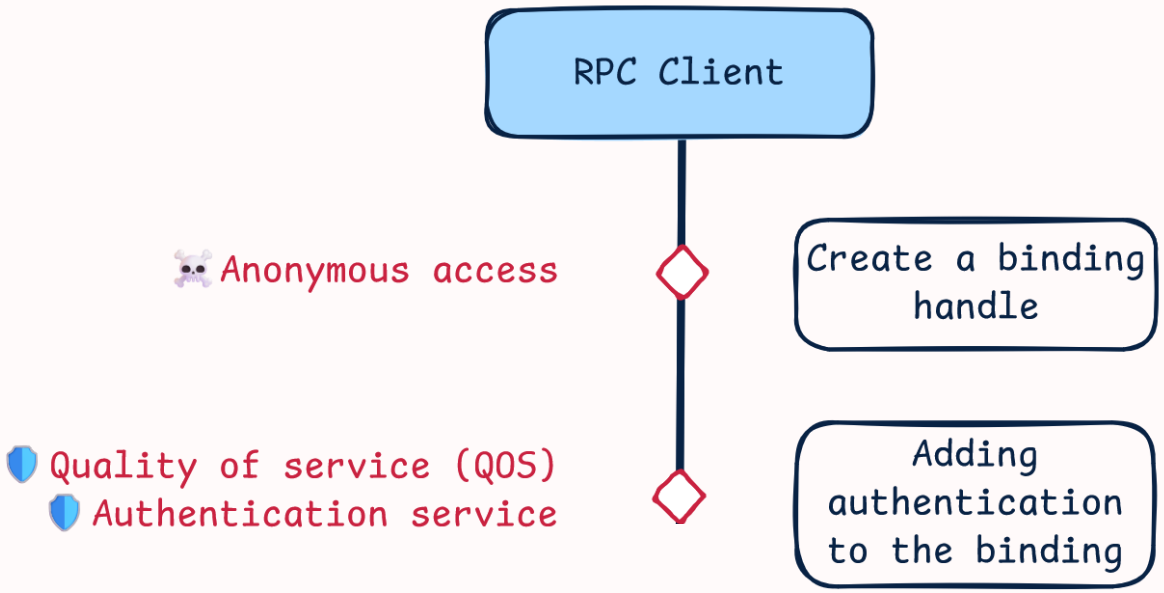

```
> whoami
windev2407eval\rauxam
> .\RPCClient.exe
[*] Starting RPC Client!

[*] FIRST TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump-Admin' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
```

2 – Client side

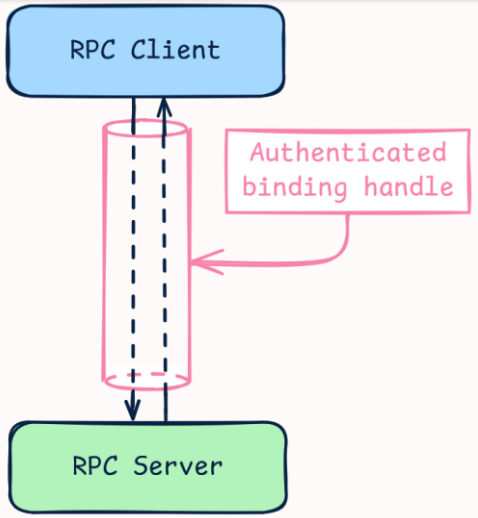




2 – Client side

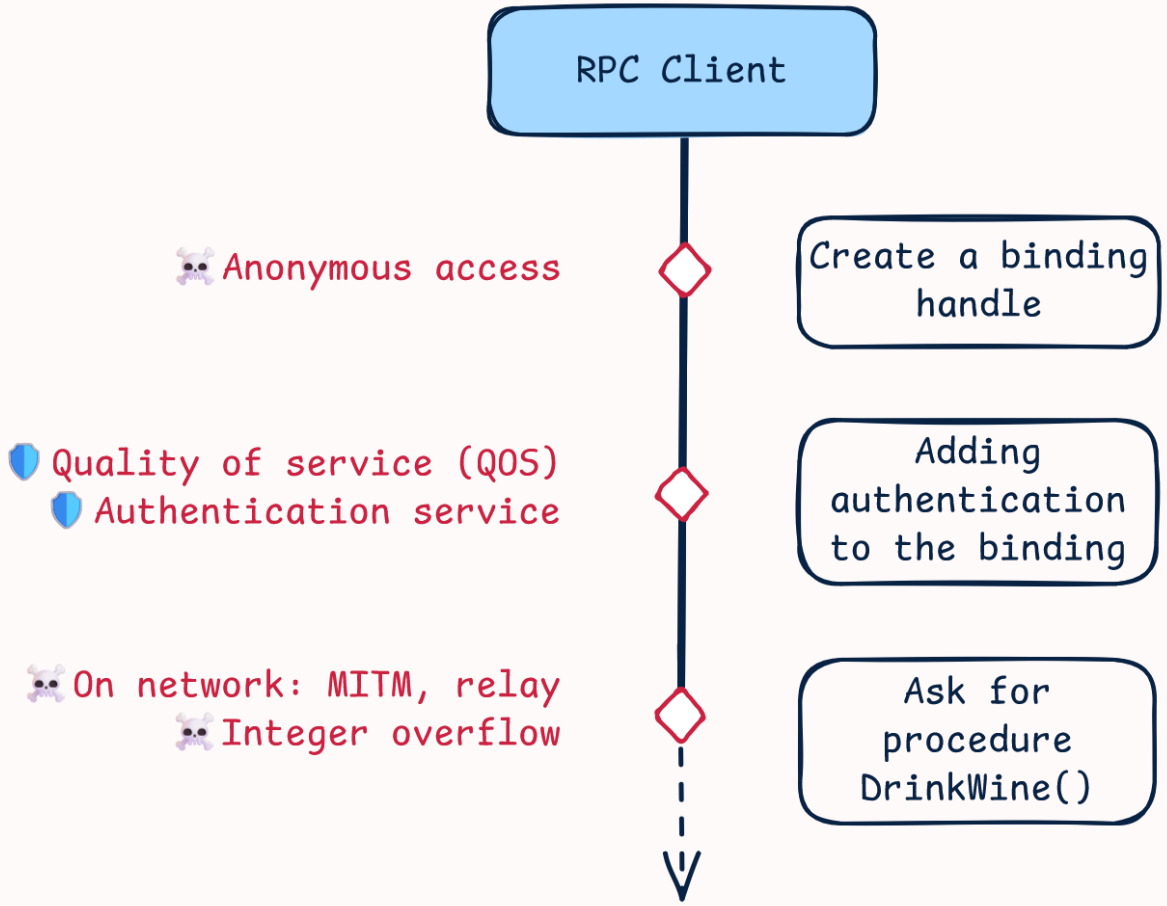



```
RpcBindingSetAuthInfoEx(
            hExplicitBinding,        // the client's binding handle
            pszHostSPN,              // the server's service principale name (SPN)
            RPC_C_AUTHN_LEVEL_PKT,   // authentication level
            RPC_C_AUTHN_WINNT,       // using NTLM as authentication service provider
            NULL,                    // use current thread credentials
            RPC_C_AUTHZ_NAME,        // authorization based on the provided SPN
            &secQos                  // Quality of Service structure
        );
```




```
> whoami
windev2407eval\rauxam
> .\RPCClient.exe
[*] Starting RPC Client!

[*] FIRST TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump-Admin' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
[*] Set Binding authentication with current thread credentials.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
    -> QOS: Impersonation type set to RPC_C_IMP_LEVEL_IMPERSONATE (server can impersonate client locally).
```

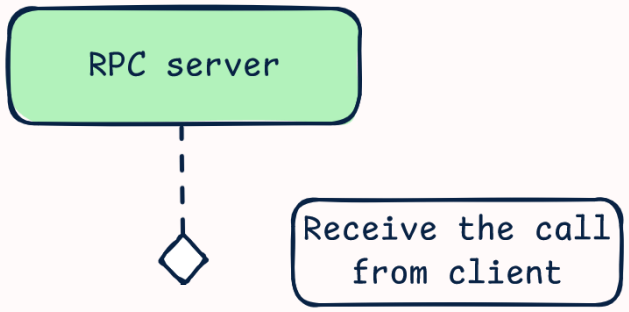
2 – Client side




```
CLIENT_CALL_RETURN RPC_VAR_ENTRY NdrClientCall3(
  MIDL_STUBLESS_PROXY_INFO *pProxyInfo,              //information about proxy
  unsigned long            nProcNum,                 //Procedure number
  void                     *pReturnValue,
  ...
);
```

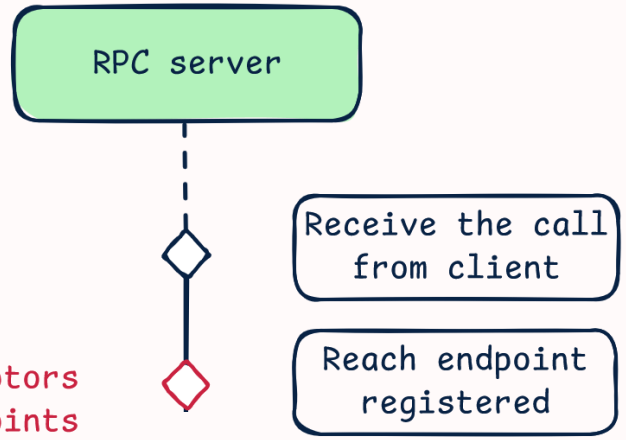
```
> whoami
windev2407eval\rauxam
> .\RPCClient.exe
[*] Starting RPC Client!

[*] FIRST TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump-Admin' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
[*] Set Binding authentication with current thread credentials.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
    -> QOS: Impersonation type set to RPC_C_IMP_LEVEL_IMPERSONATE (server can impersonate client
locally).
[*] Call procedure DrinkWine().
```

3 – In the [uuid] family, I would like the procedure [opnum]

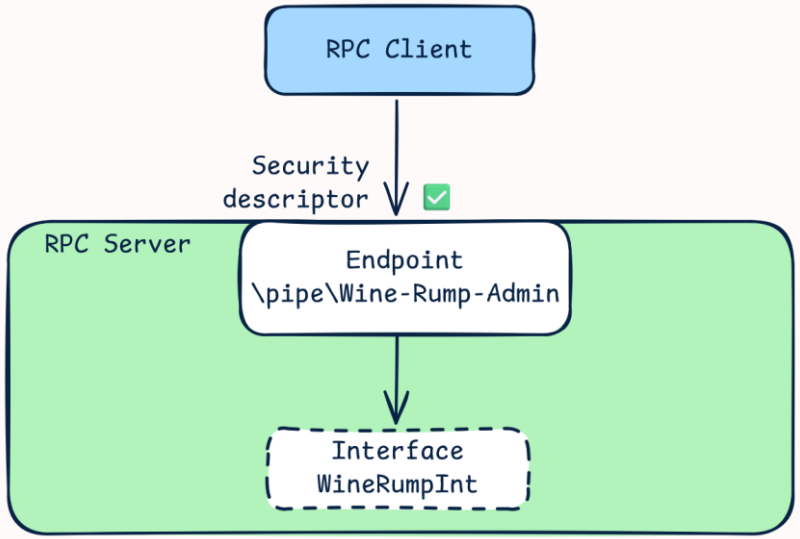



```
NdrServerCallAll(          // wrapper used by runtime for invoking server-side functions
  PRPC_MESSAGE pRpcMsg
);
```

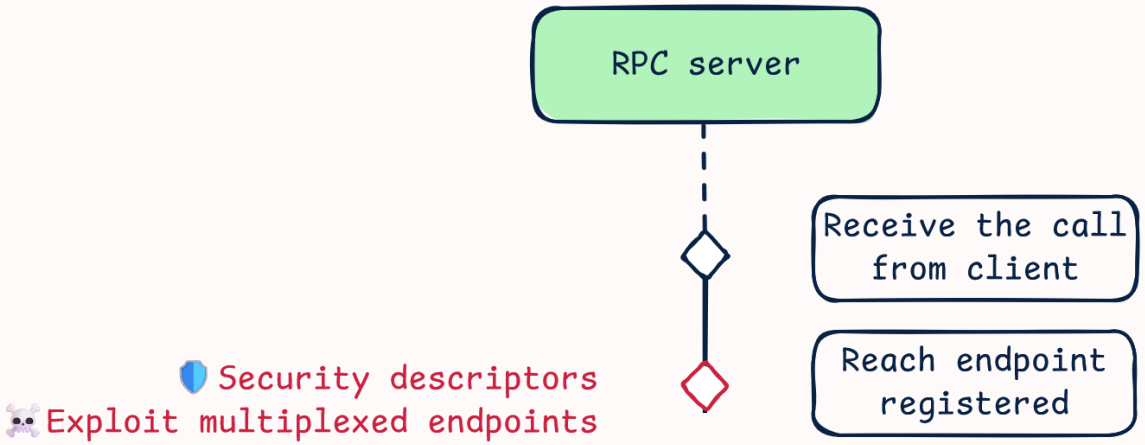
3 – In the [uuid] family, I would like the procedure [opnum]

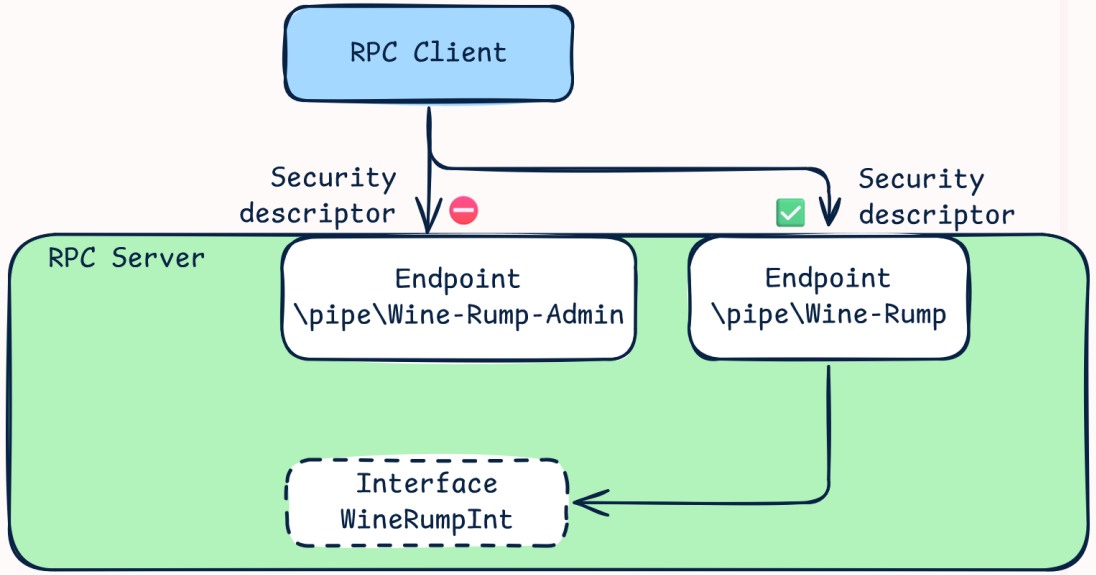


🛡️ Security descriptors
☠️ Exploit multiplexed endpoints

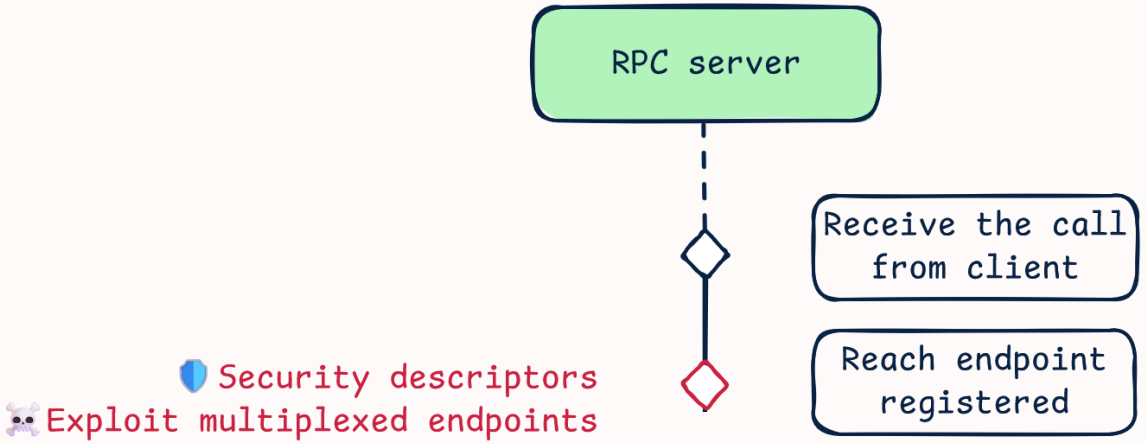


3 – In the [uuid] family, I would like the procedure [opnum]





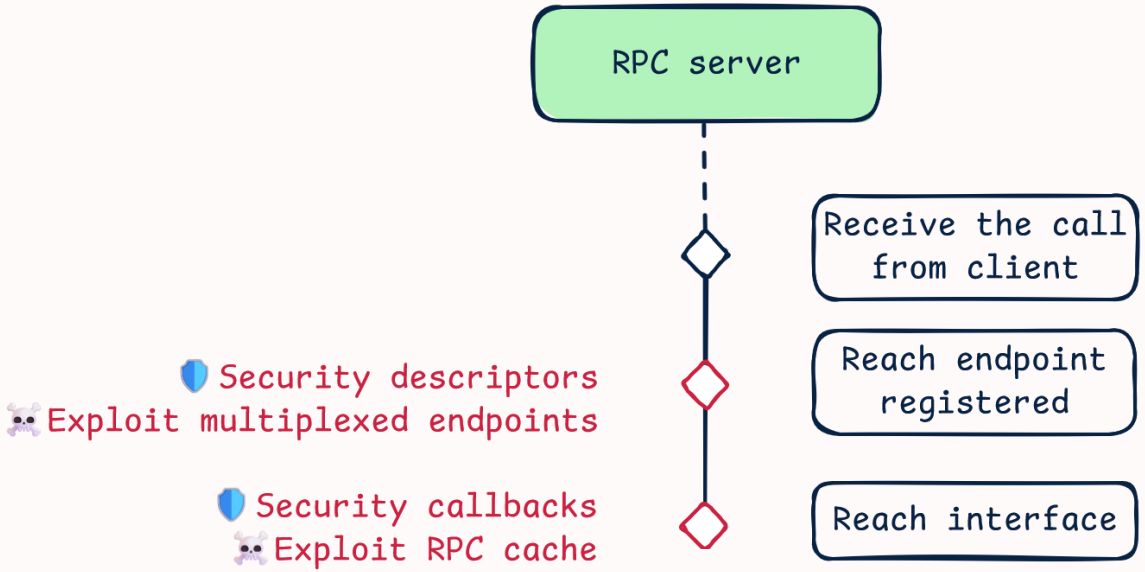
3 – In the [uuid] family, I would like the procedure [opnum]

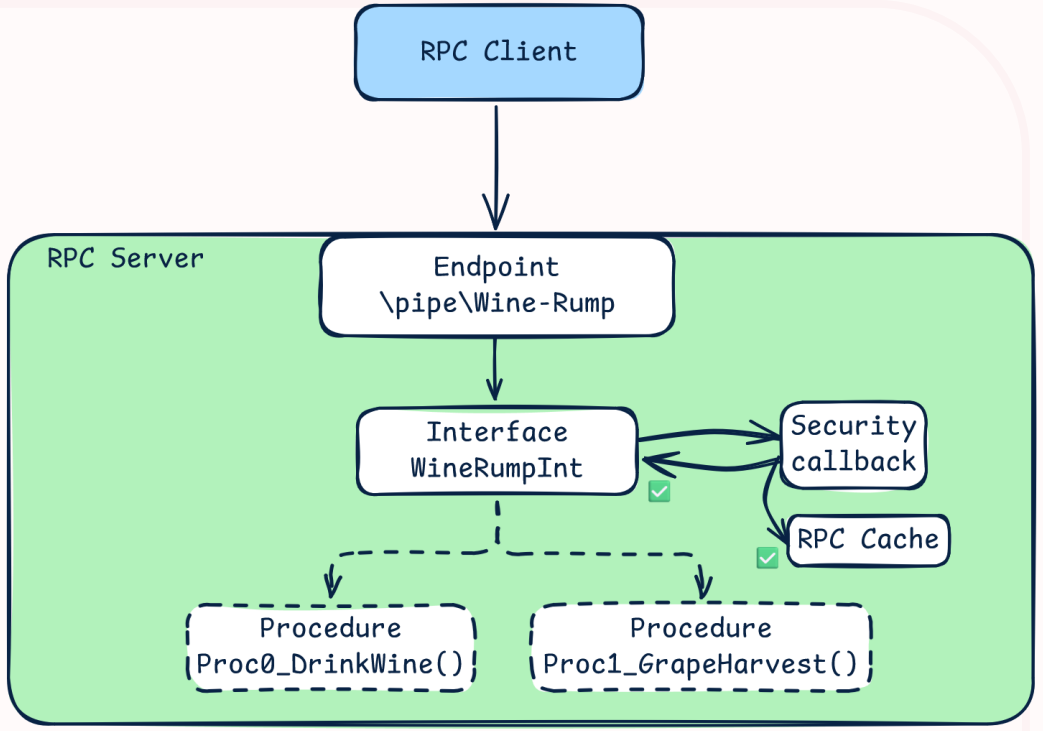



```
> whoami
windev2407eval\rauxam
> .\RPCClient.exe
[*] Starting RPC Client!

[*] FIRST TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump-Admin' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
[*] Set Binding authentication with current thread credentials.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
    -> QOS: Impersonation type set to RPC_C_IMP_LEVEL_IMPERSONATE (server can impersonate client
locally).
[*] Call procedure DrinkWine().
[->] Server response is: sorry, you're not Admin you can't use entrance \pipe\Wine-Rump-Admin. Ru
ntime reported exception: 5.

[*] SECOND TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
[*] Set Binding authentication with current thread credentials (once again).
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
    -> QOS: Impersonation type set to RPC_C_IMP_LEVEL_IMPERSONATE (server can impersonate client
locally).
[*] Call procedure DrinkWine().
```

```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] RPC Server is ready!

Listening for client order. Who wants a glass of wine?

[*] Entrance \pipeWine-Rump: Welcome!
```

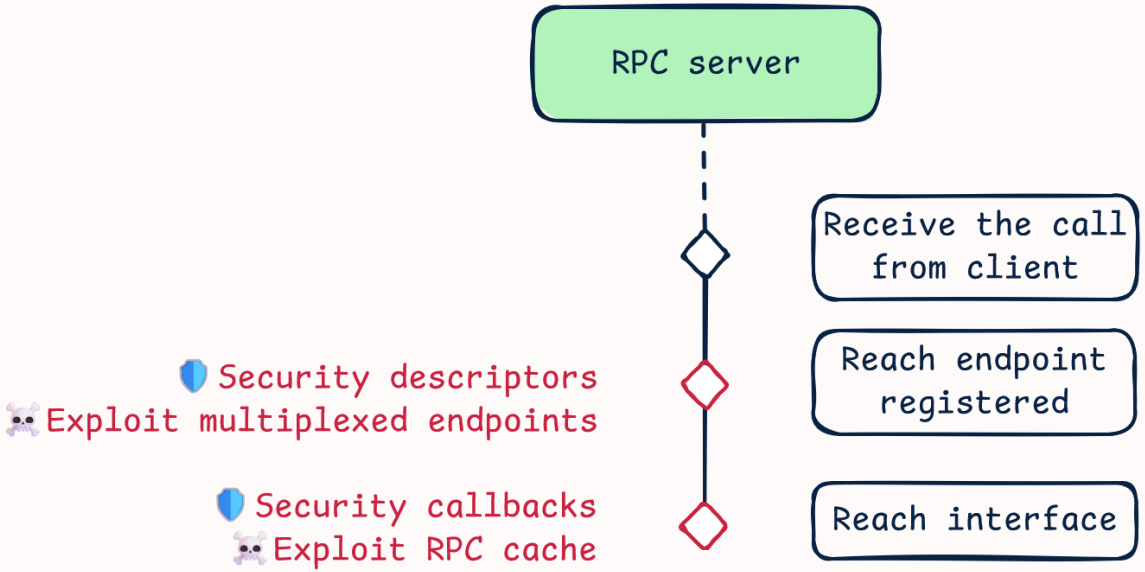
3 – In the [uuid] family, I would like the procedure [opnum]

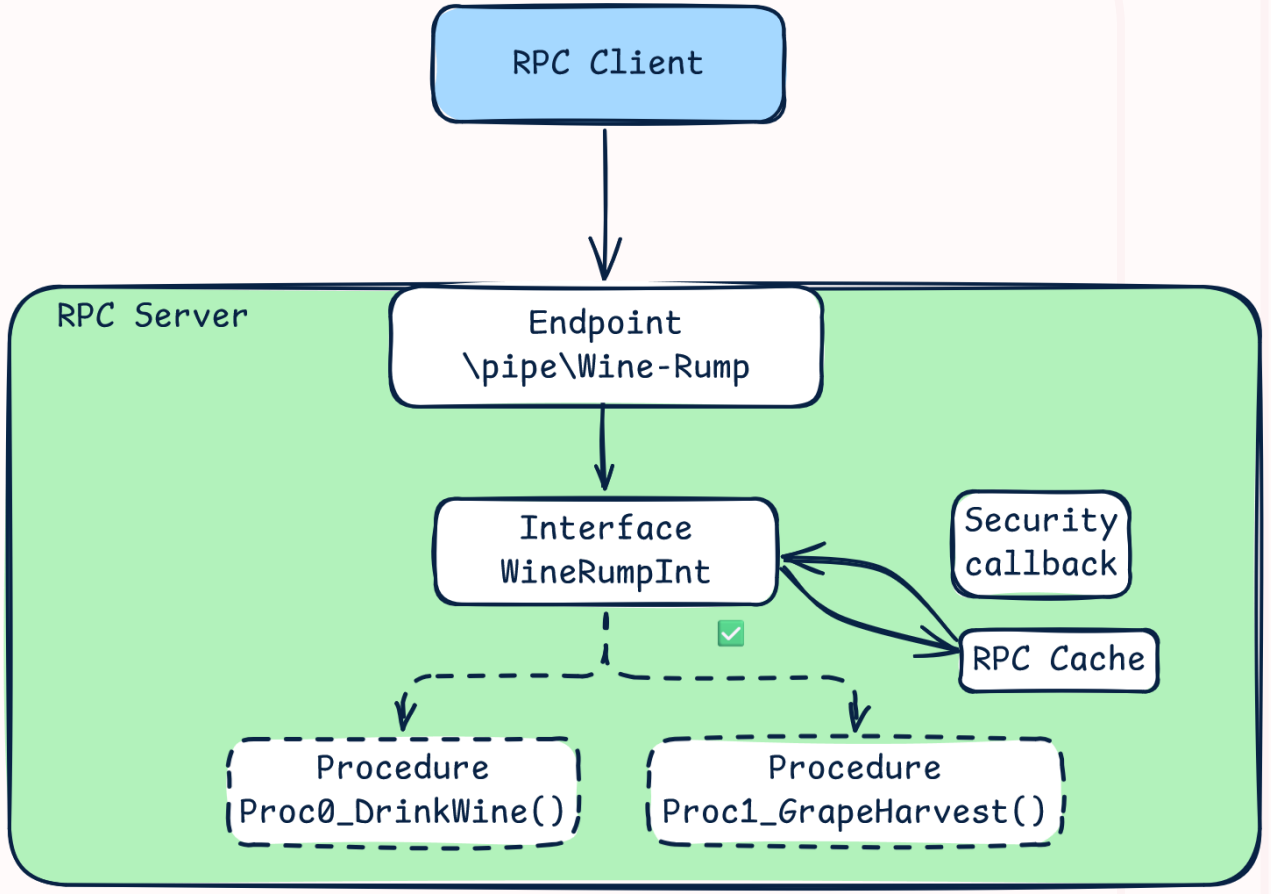




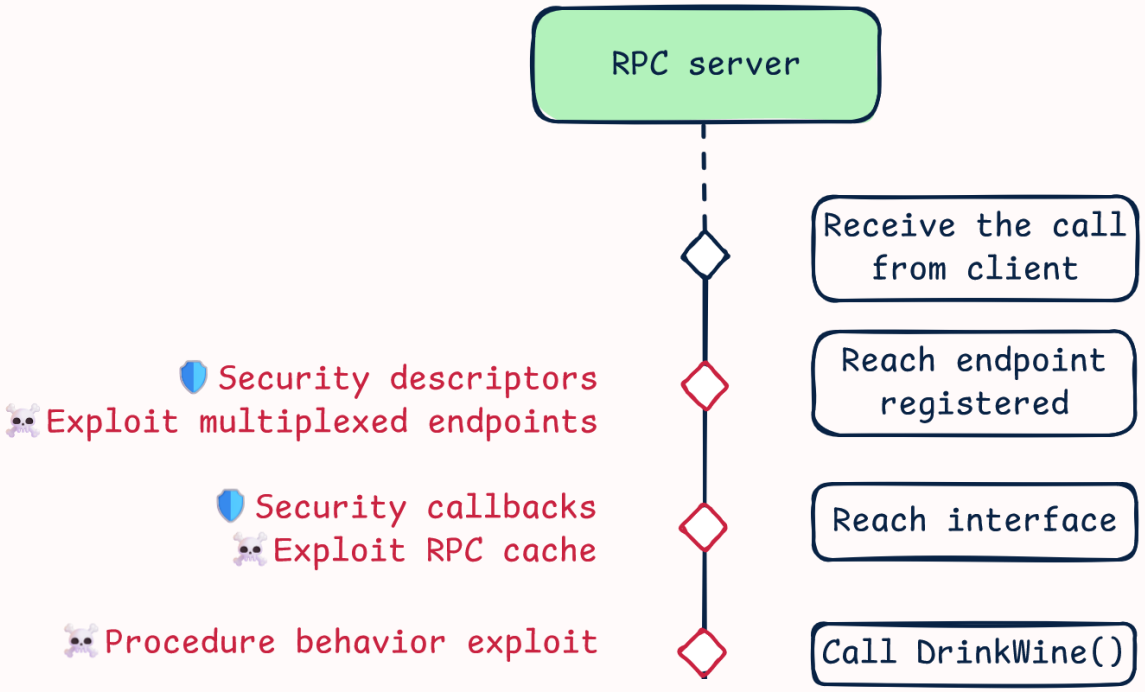

```
> .\RPCServer.exe
[*] Starting RPC Server!
[*] RPC Server is ready!

Listening for client order. Who wants a glass of wine?

[*] Entrance \pipeWine-Rump: Welcome!
[*] Security check: ID card checked. The customer can order.
```

3 – In the [uuid] family, I would like the procedure [opnum]



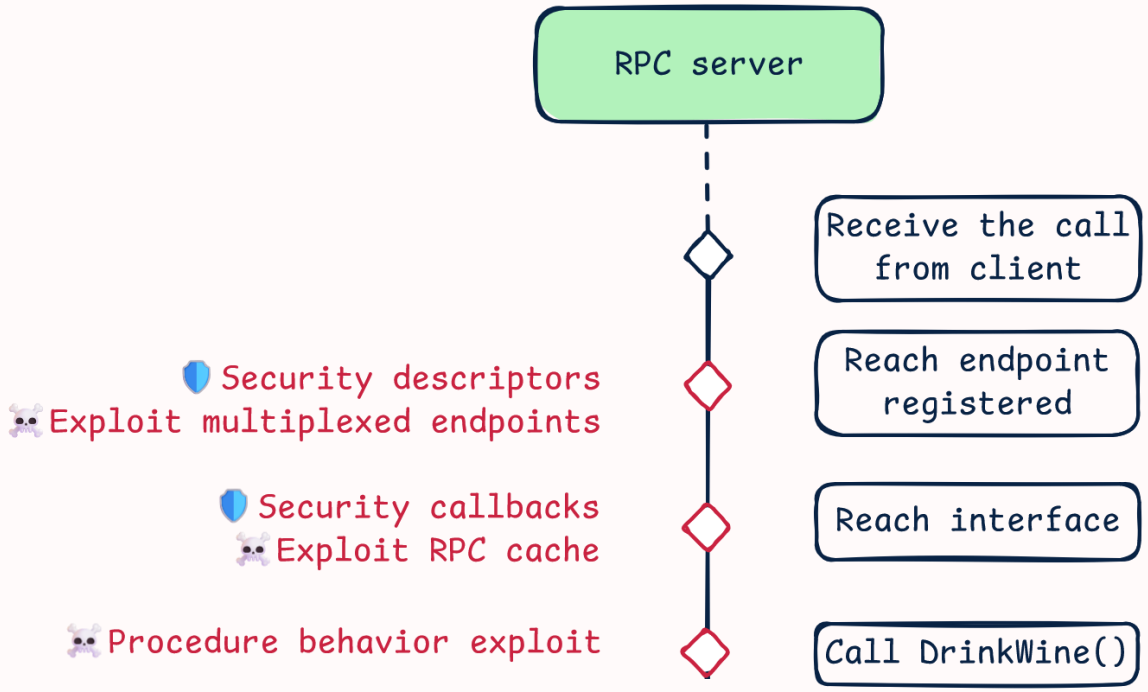


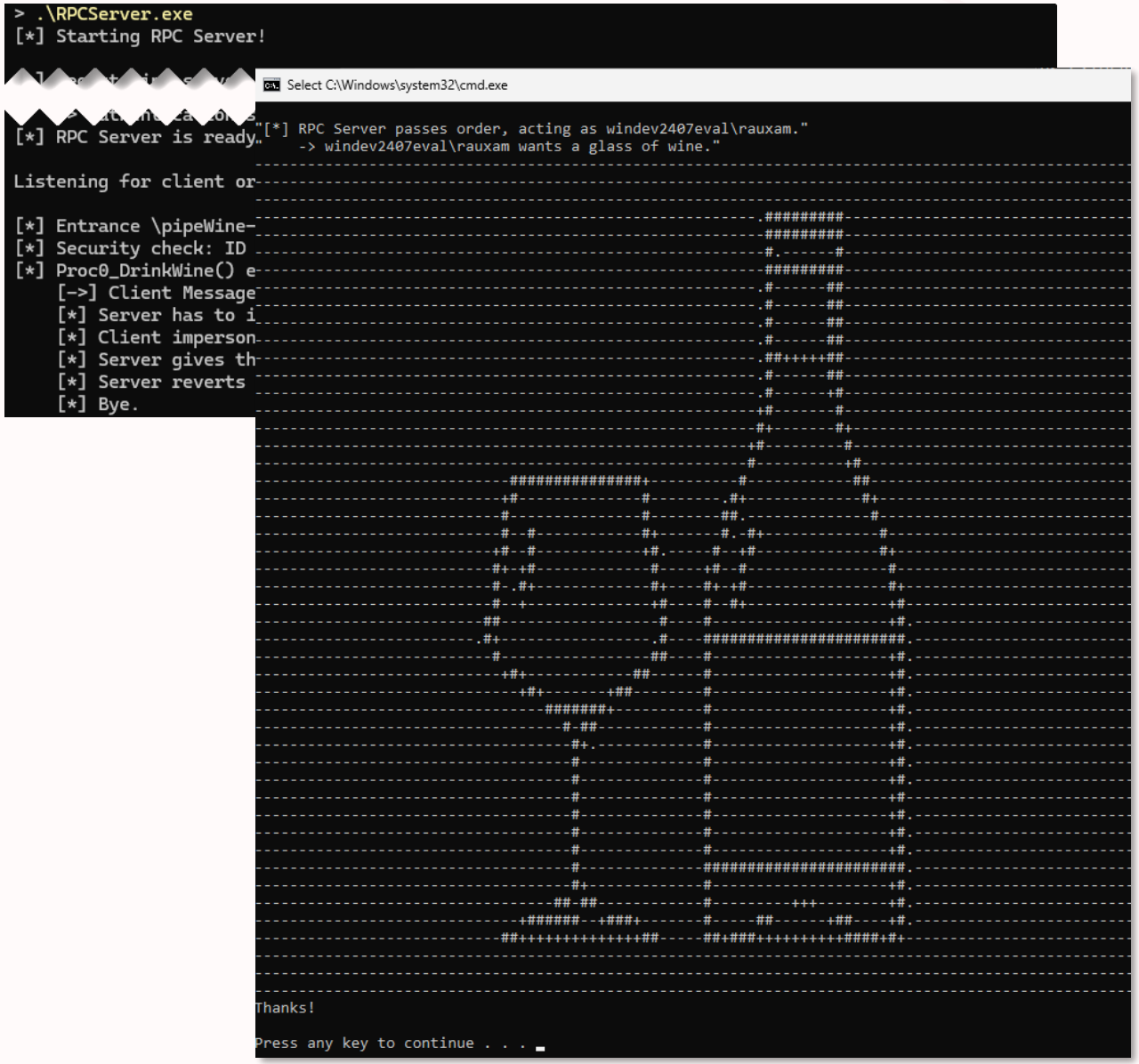
3 – In the [uuid] family, I would like the procedure [opnum]



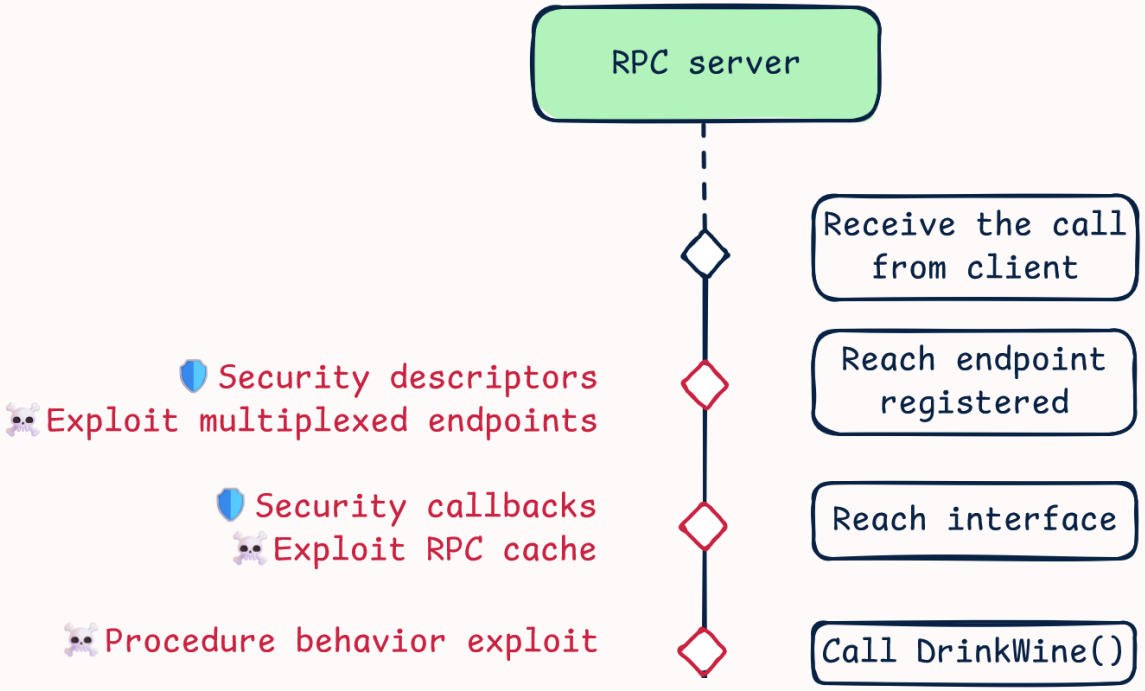

```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] RPC Server is ready!

Listening for client order. Who wants a glass of wine?

[*] Entrance \pipeWine-Rump: Welcome!
[*] Security check: ID card checked. The customer can order.
[*] Proc0_DrinkWine() execution.
    [->] Client Message: Hello from client using \pipe\Wine-Rump! I would like a glass of wine.
    [*] Server has to impersonate client to place order.
    [*] Client impersonation successful.
    [*] Server gives the glass of wine to the client.
    [*] Server reverts to its identity.
    [*] Bye.
```

3 – In the [uuid] family, I would like the procedure [opnum]



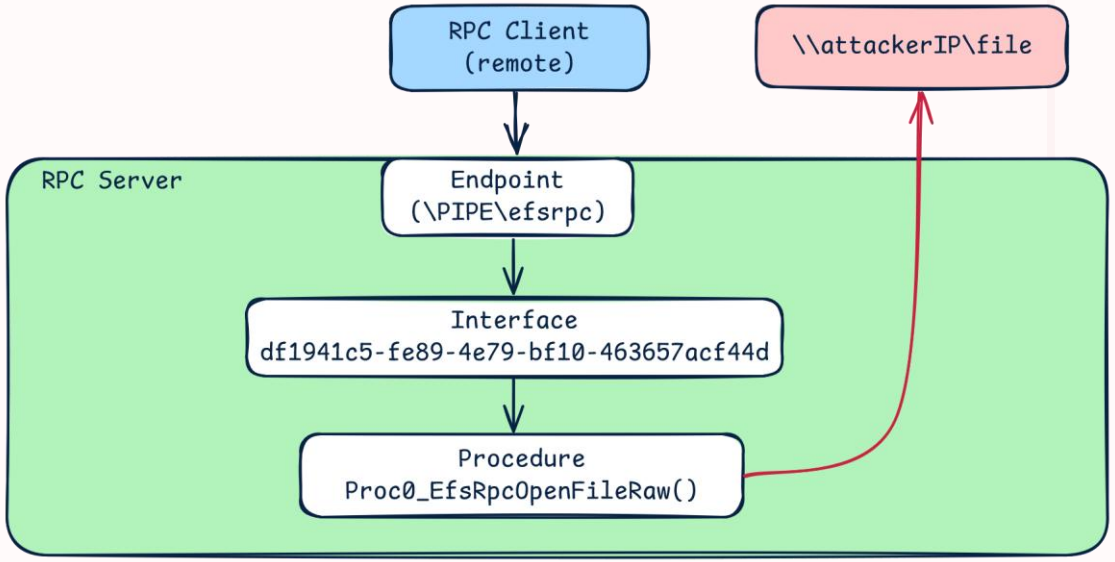


3 – In the [uuid] family, I would like the procedure [opnum]

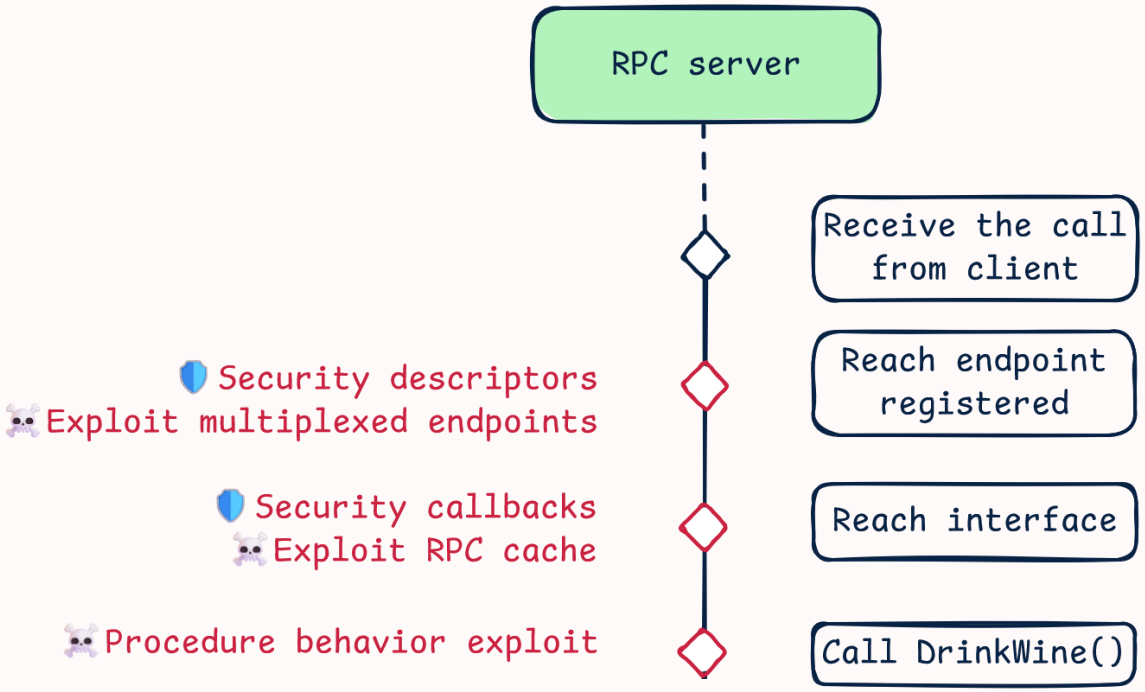



```
[
uuid(df1941c5-fe89-4e79-bf10-463657acf44d),    // RPC interface for EFSR
version(1.0),
]


interface efsrpc
{

long Proc0_EfsRpcOpenFileRaw(
  [in] handle_t binding_h,
  [out] PEXIMPORT_CONTEXT_HANDLE* hContext,
  [in, string] wchar_t* FileName,            // Path (local or remote) of ressource to open
  [in] long Flags
);

[...]
}
```

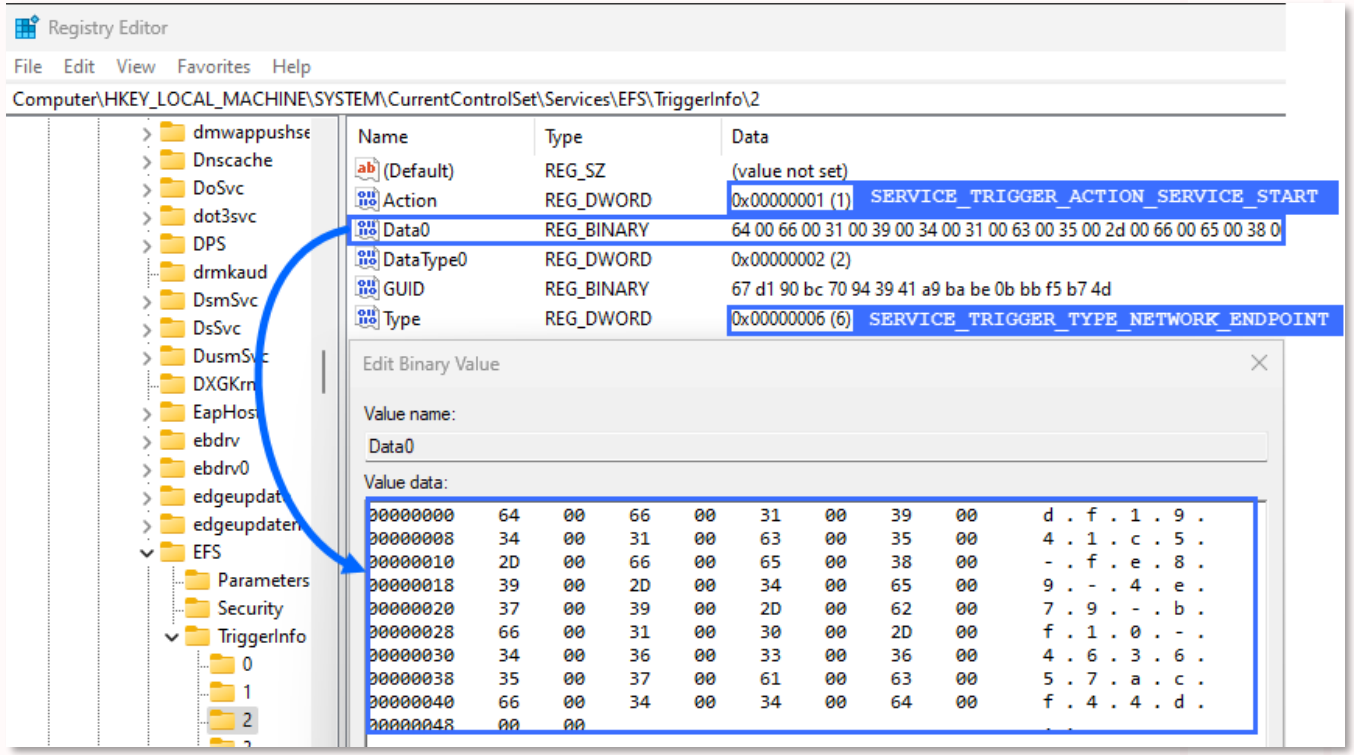
Coercion - Petit Potam case (Encrypting File System)



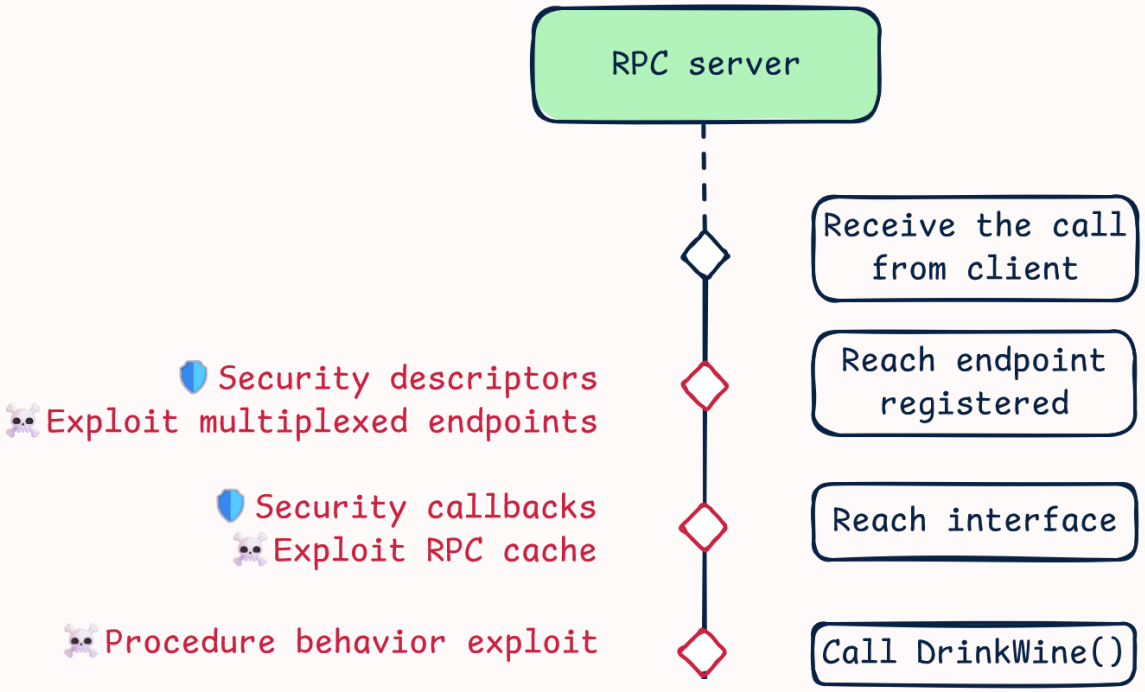
3 – In the [uuid] family, I would like the procedure [opnum]



Petit Potam case with Windows 11 since SpectorOps article 19/08/2025



3 – In the [uuid] family, I would like the procedure [opnum]

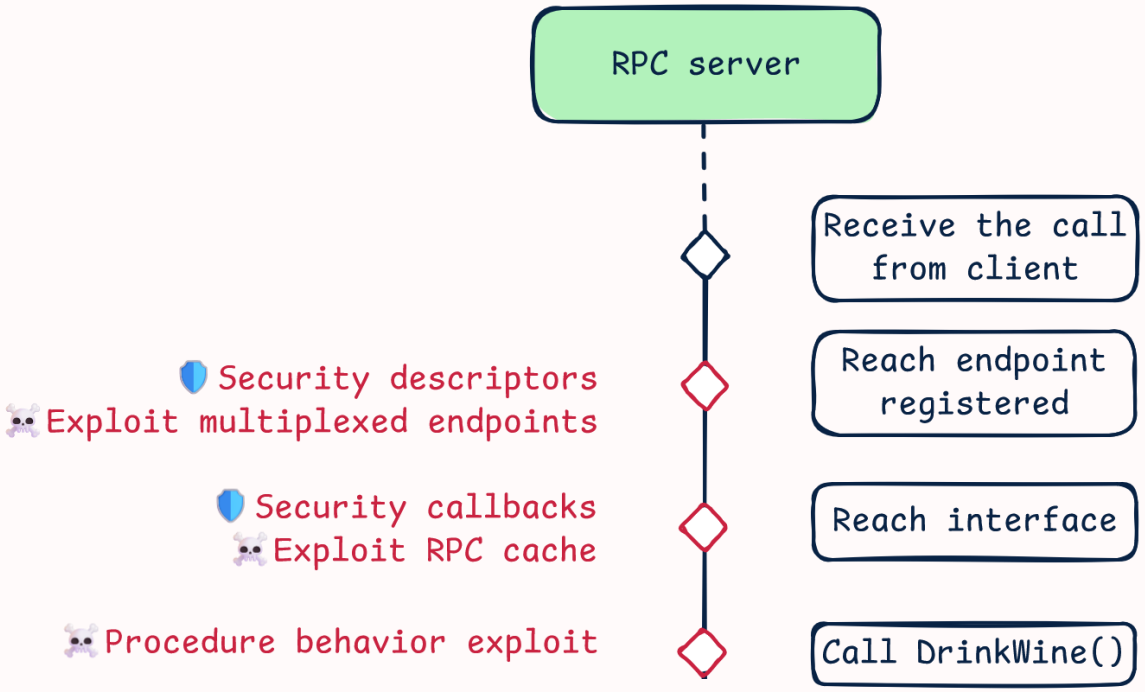


Petit Potam case with Windows 11 since SpectorOps article 19/08/2025

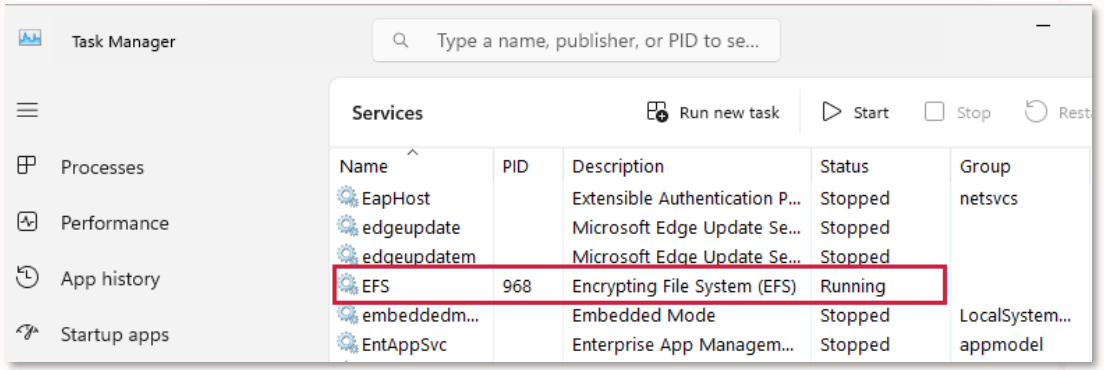
```
PS> RpcPing.exe  /t ncacn_np /s 192.168.1.190 /f df1941c5-fe89-4e79-bf10-463657acf44d /u NTLM
/a connect /I "USER,DOMAIN,*"

Enter password for server:

Exception 1717 (0x000006B5)
Number of records is: 1
ProcessID is 6260
System Time is: 9/19/2025 21:9:52:276
Generating component is 2
Status is 0x6B5, 1717
Detection location is 1750
Flags is 0
NumberOfParameters is 1
Long val: 0x1c010003
```

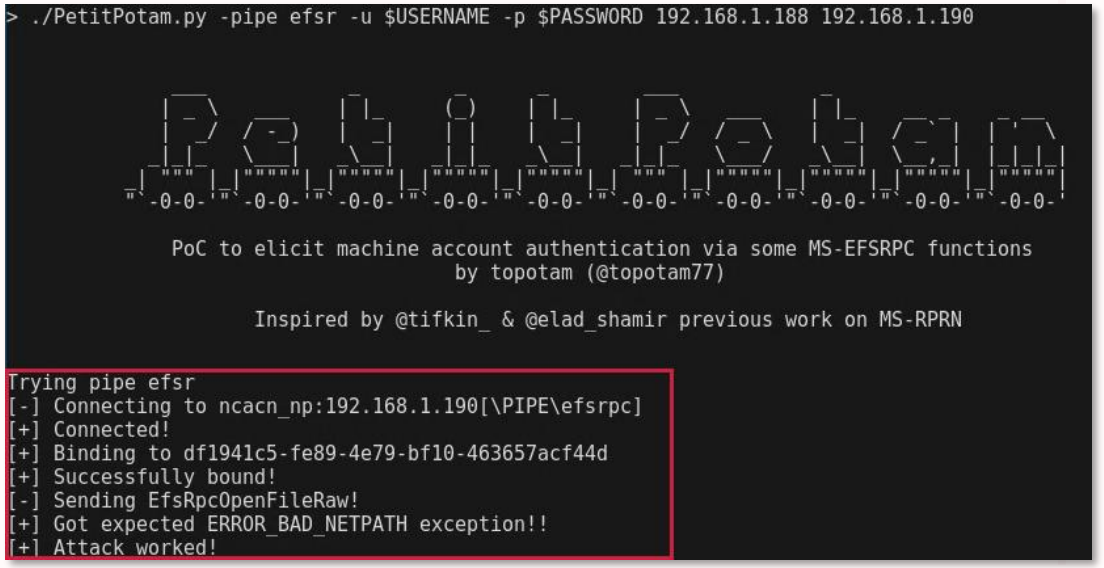
```
$ nxc smb 192.168.1.190 -u $USER -p $PASS -d $DOMAIN -M coerce_plus
SMB         192.168.1.190   445    WINDEV2407EVAL   [*] Windows 11 Build 22621 x64
(name:WINDEV2407EVAL) (domain:WinDev2407Eval) (signing:False) (SMBv1:False)
SMB         192.168.1.190   445    WINDEV2407EVAL   [+] WinDev2407Eval\USER:PASS
COERCE_PLUS 192.168.1.190   445    WINDEV2407EVAL   VULNERABLE, PetitPotam
COERCE_PLUS 192.168.1.190   445    WINDEV2407EVAL   VULNERABLE, PrinterBug
COERCE_PLUS 192.168.1.190   445    WINDEV2407EVAL   VULNERABLE, MSEven
```

3 – In the [uuid] family, I would like the procedure [opnum]

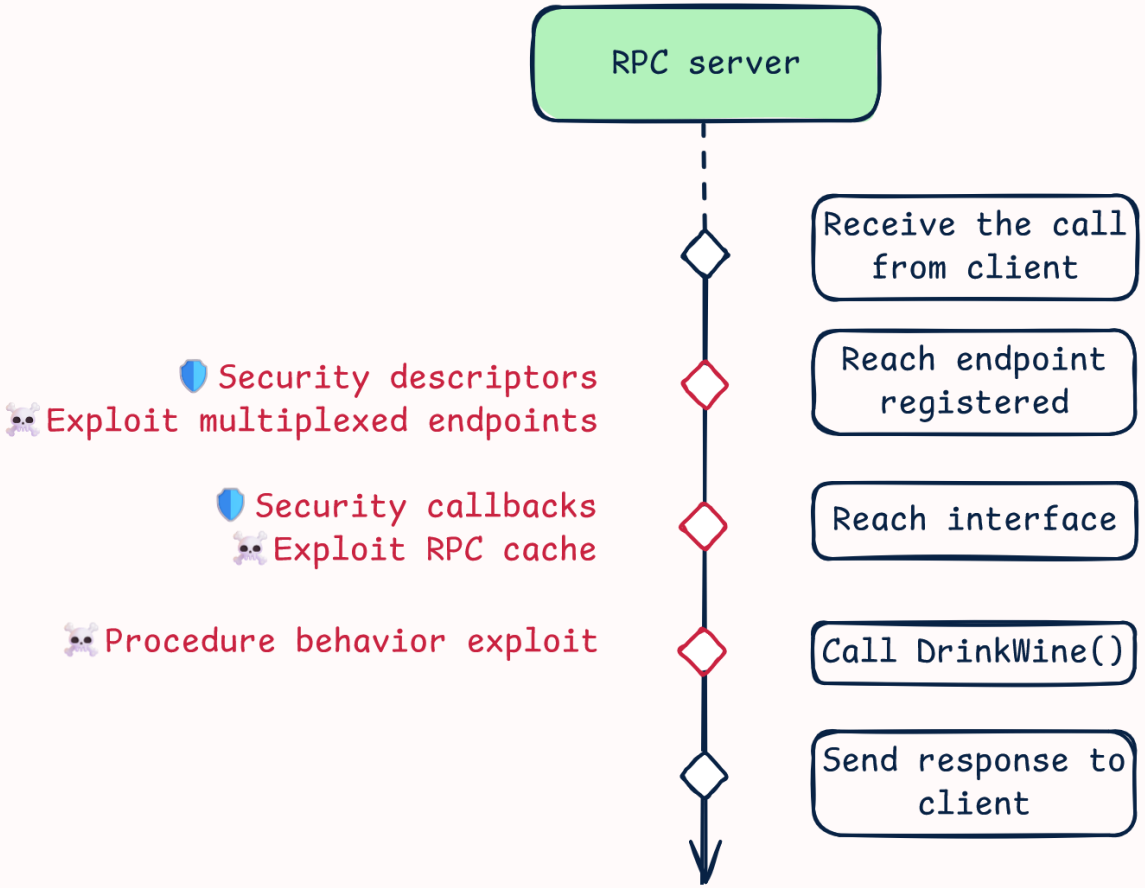


Petit Potam case with Windows 11 since SpectorOps article 19/08/2025



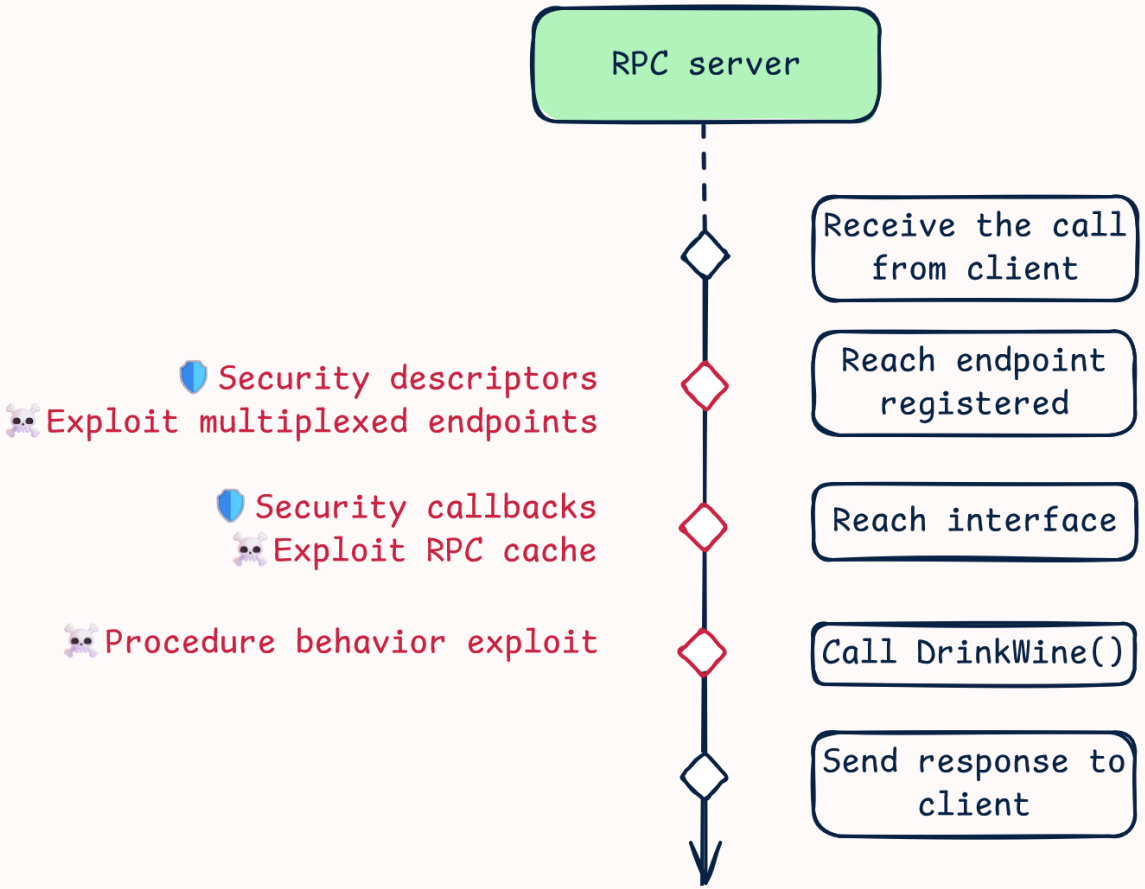


3 – In the [uuid] family, I would like the procedure [opnum]




```
> .\RPCServer.exe
[*] Starting RPC Server!

[*] Registering server interface {d6b1ad2b-b550-4729-b6c2-1651f58480c3} (WineRumpInt)
    -> Flag "RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH" & Security callback set.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump-Admin'.
    -> Security descriptor defined on endpoint: only Admin user is able to access this endpoint.
[*] Register endpoint using protocol 'ncacn_np' at '\pipe\Wine-Rump'.
    -> Default security descriptor defined on endpoint.
[*] Register authentication information.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
[*] RPC Server is ready!

Listening for client order. Who wants a glass of wine?

[*] Entrance \pipeWine-Rump: Welcome!
[*] Security check: ID card checked. Client can order.
[*] Proc0_DrinkWine() execution.
    [->] Client Message: Hello from client using \pipe\Wine-Rump! I would like a glass of wine.
    [*] Server has to impersonate client to place order.
    [*] Client impersonation successful.
    [*] Server gives the glass of wine to the client.
    [*] Server reverts to its identity.
    [*] Bye.
[*] RPC Server has finished his order and is ready again!

Listening for client order. Who wants a glass of wine?
```

3 – In the [uuid] family, I would like the procedure [opnum]



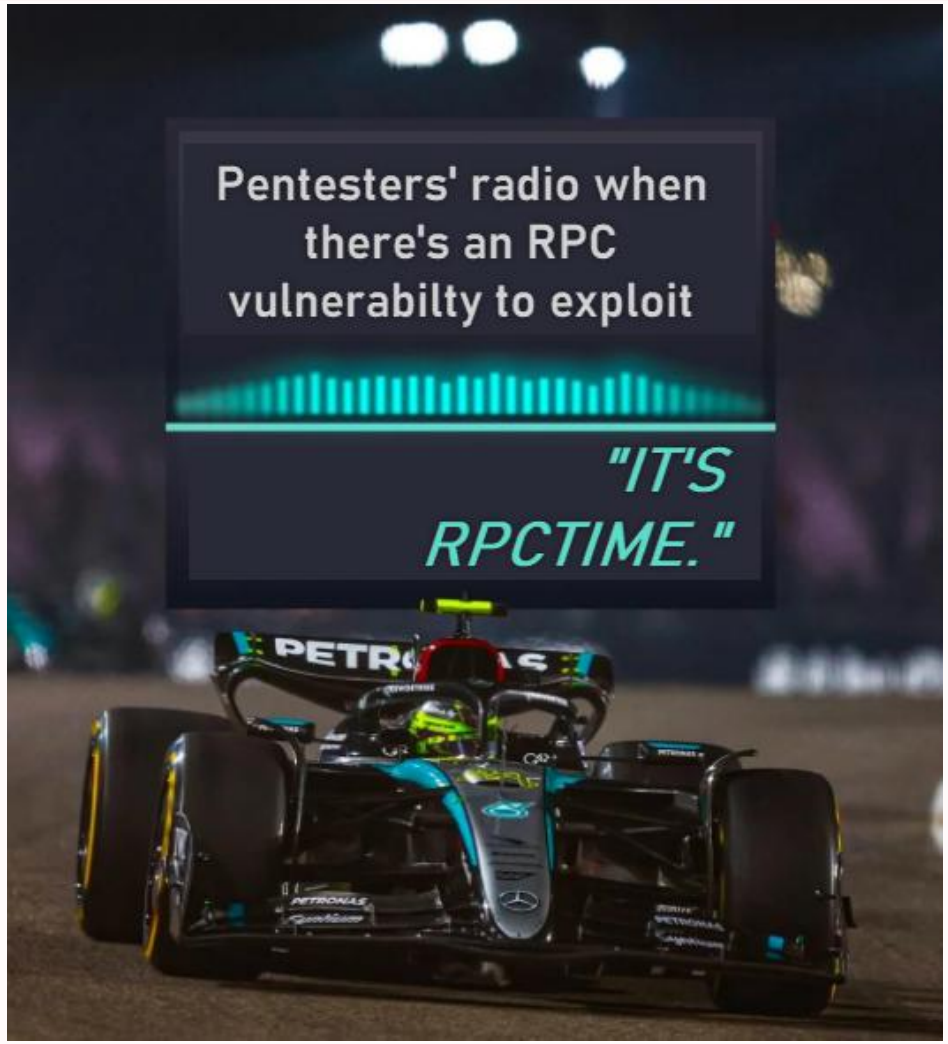

```
> whoami
windev2407eval\rauxam
> .\RPCClient.exe
[*] Starting RPC Client!

[*] FIRST TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump-Admin' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
[*] Set Binding authentication with current thread credentials.
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
    -> QOS: Impersonation type set to RPC_C_IMP_LEVEL_IMPERSONATE (server can impersonate client
locally).
[*] Call procedure DrinkWine().
[->] Server response is: sorry, you're not Admin you can't use entrance \pipe\Wine-Rump-Admin. Ru
ntime reported exception: 5.

[*] SECOND TRY
[*] Create binding handle to 'WINDEV2407EVAL:\pipe\Wine-Rump' using protocol 'ncacn_np'.
    -> RpcStringBindingCompose: OK
    -> RpcBindingFromStringBinding: OK
[*] Set Binding authentication with current thread credentials (once again).
    -> Authentication service provider: RPC_C_AUTHN_WINNT (NTLM Authentication).
    -> QOS: Impersonation type set to RPC_C_IMP_LEVEL_IMPERSONATE (server can impersonate client
locally).
[*] Call procedure DrinkWine().
[->] Server response is: 1 glass.
```

Conclusion

→ Lot of security mechanisms involved

→ Current topic

Principal references: Akamai, CSandker, Itm4n



That’s all folks!

Thanks for your attention

login
by constellation