



# **AAD Joined Machines - The New Lateral Movement**

Mor Rubin

# Who am I?

- Mor Rubin ([@rubin\\_mor](https://twitter.com/rubin_mor))
- Senior security researcher at Microsoft
- Interested in networking, cloud and On-Prem attacks, mitigations and detections



# Agenda

- Introduction to key terms
- NegoEx protocol
- Attacks
- Demo
- Hunting
- Takeaways



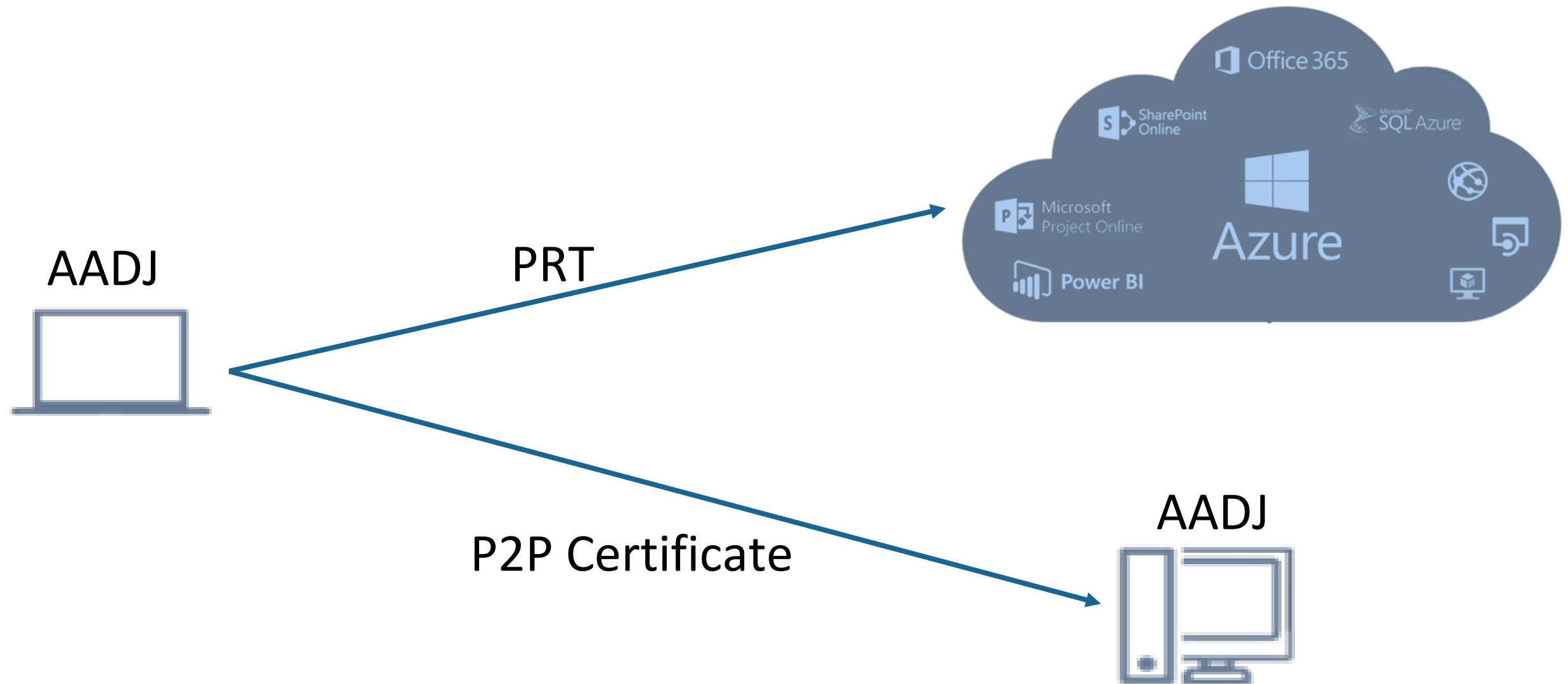
# Technical background

# Azure AD Joined device

(Windows Server) Active Directory	Azure Active Directory
LDAP	REST API's
NTLM/Kerberos	OAuth/SAML/OpenID/etc
Structured directory (OU tree)	Flat structure
GPO's	No GPO's
Super fine-tuned access controls	Predefined roles
Domain/forest	Tenant
Trusts	Guests

Ref: Dirk-Jan Mollema "I'm in your cloud... reading everyone's email"  
Troopers '19 <https://dirkjanm.io/assets/raw/TR19-Im%20in%20your%20cloud.pdf>

# AADJ Authenticated Connections

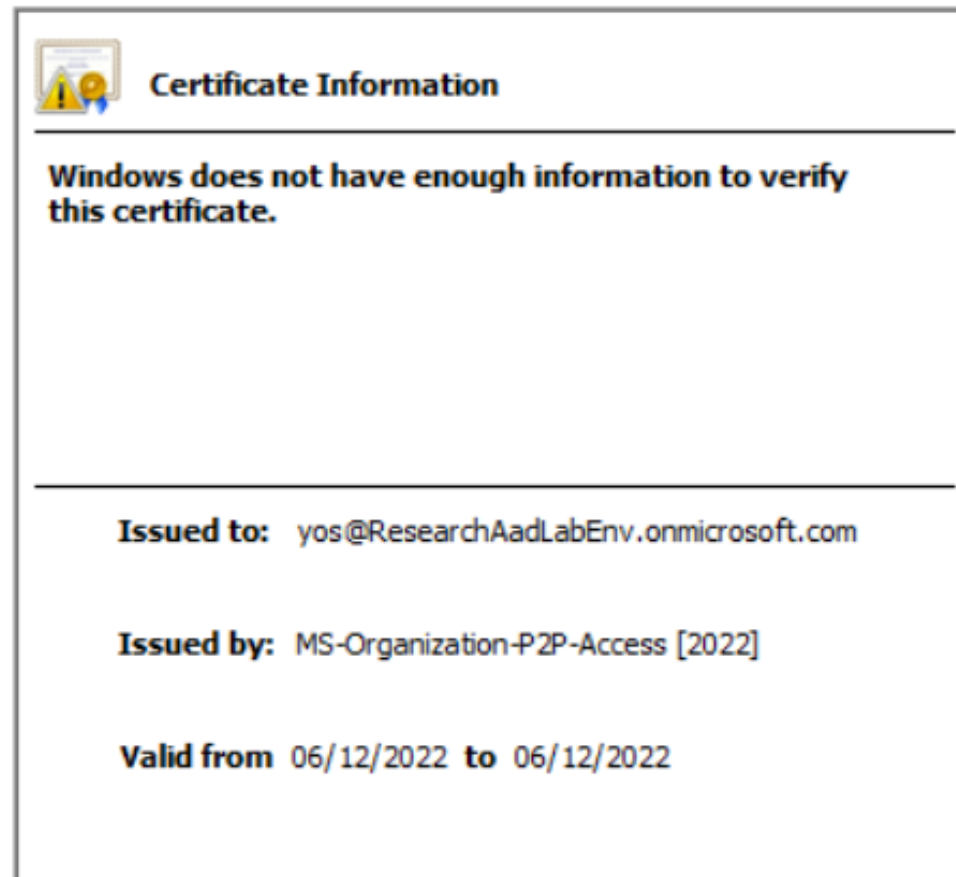


# Primary Refresh Token - PRT

- A JSON Web Token (JWT) for the user and the device it was issued for
- Can be compared to Ticket Granting Ticket (TGT)
- Can be used to authenticate to any application

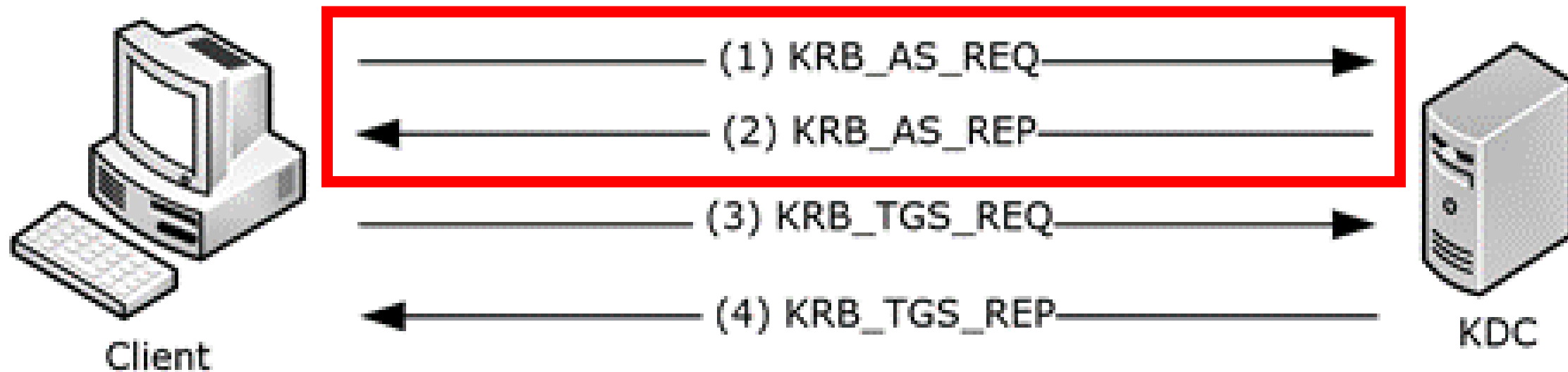
# P2P Azure AD certificate

- Certificate that is used for peer-to-peer authentication between Azure AD joined devices
- Issued by Azure AD upon request and valid only for 1 hour



# Kerberos PKINIT

Kerberos extension allows certificate authentication over Kerberos instead of hash (password)



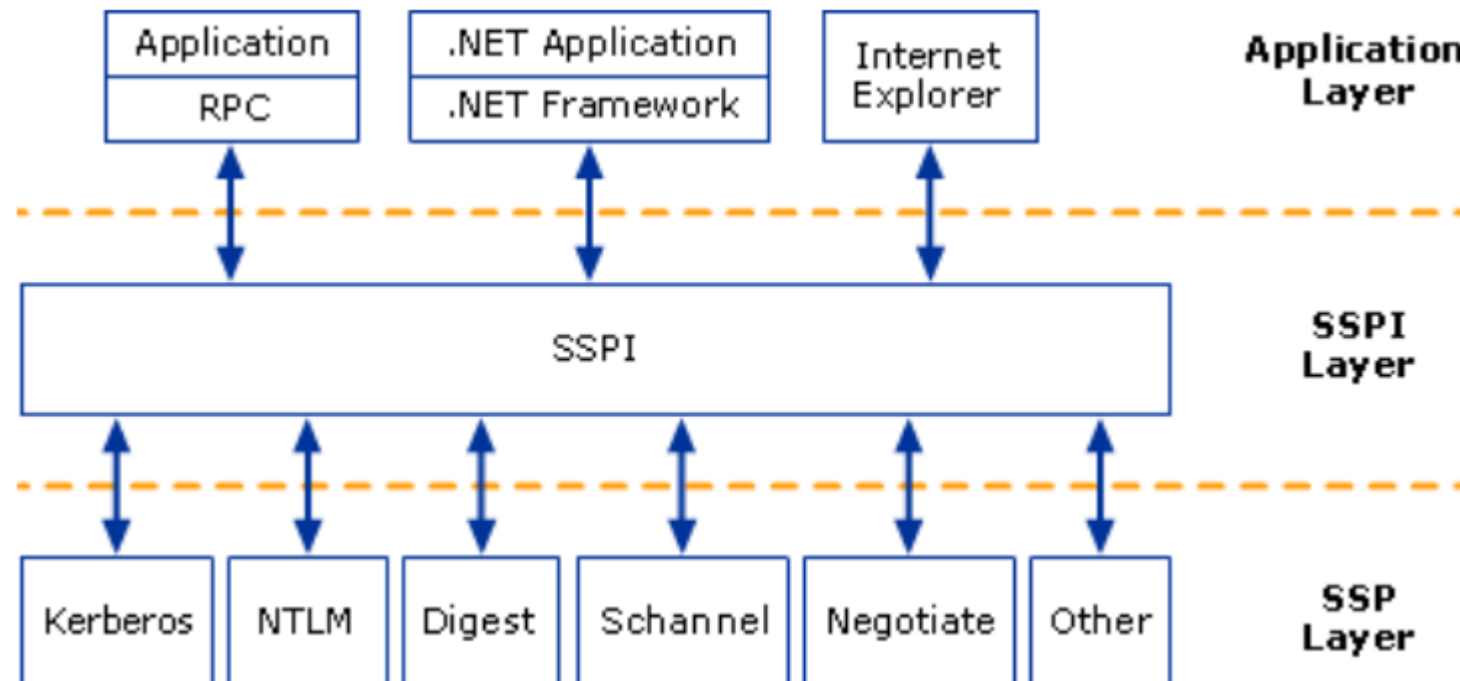
Ref: [https://docs.microsoft.com/en-us/openspecs/windows\\_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13](https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13)

# PKU2U

- Based on Kerberos version 5 messages and the Kerberos GSS-API mechanism.
- Implemented as a Security Support Provider (SSP) enables peer-to-peer authentication
- Used for authentication in NegoEx when no KDC exists

# GSSAPI \ SSPI

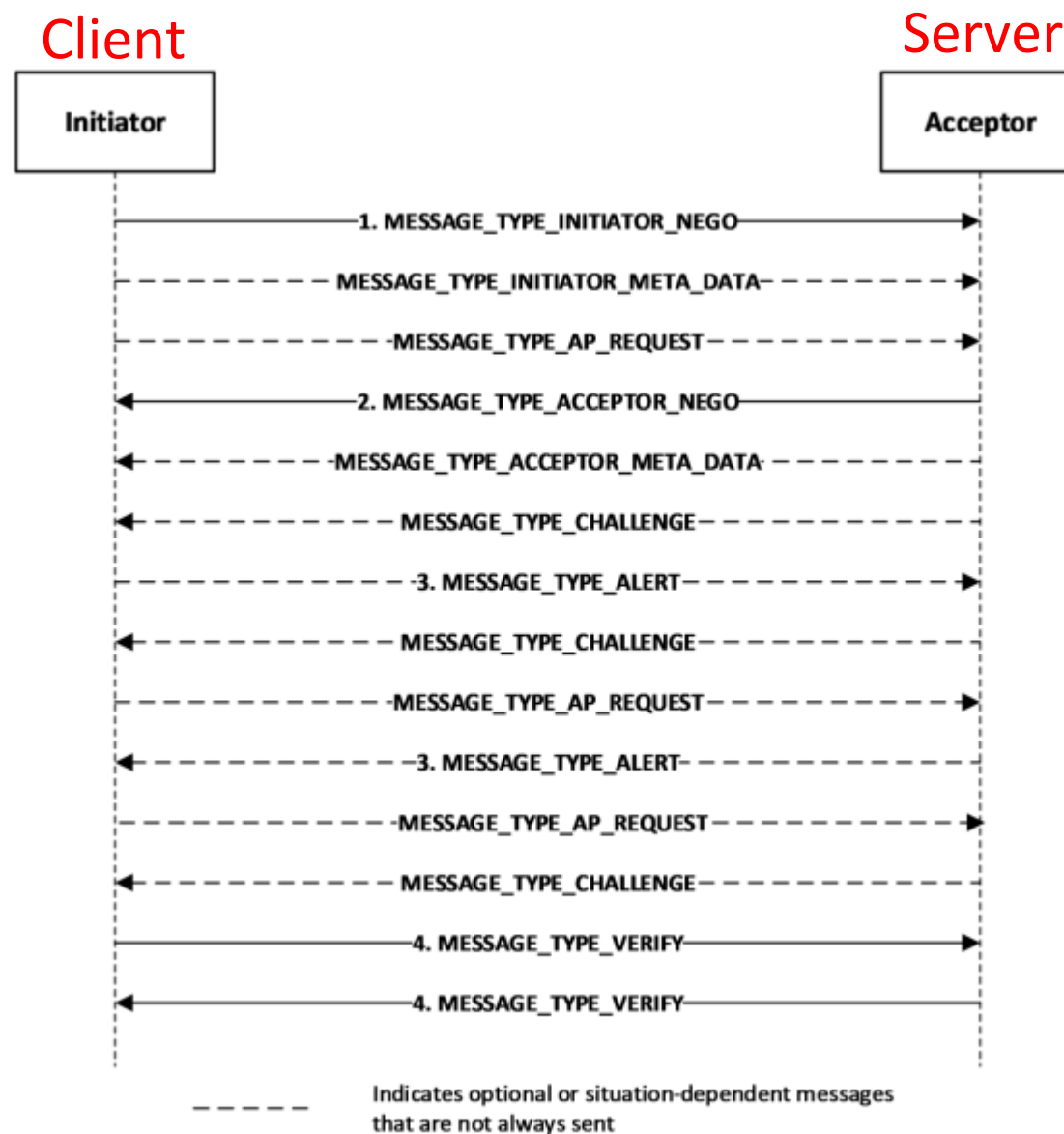
- SSPI is an API that allows application to add authenticity and privacy layer
- It is applicable to any application that allows 'Windows Authentication'





# NegoEx protocol

# NegoEx



# Initiator nego

- Contains a random identifies the session

```
▼ NEGOEX INITATOR_NEGO
  ▼ Header
    Signature: NEGOEXTS
    MessageType: INITATOR_NEGO (0x00000000)
    SequenceNum: 0
    cbHeaderLength: 96
    cbMessageLength: 112
    ConversationID: 9d83f81e-56dd-b01b-6b63-f950144f90ec
    Random: d5fc77674ebacb87d03413f29894a59dc4895bc5712d421140a89ce12802e9f5
    ProtocolVersion: 0
  > AuthSchemes: 1 at 96
  > Extensions: 0 at 0
```

\* Similar for the server side in Acceptor nego

# Initiator metadata

Generated by GSS\_Query\_meta\_data()

```

0150 00 ae 00 00 00 30 81 ab a0 81 a8 30 81 a5 30 51
0160 80 4f 30 4d 31 4b 30 49 06 03 55 04 03 1e 42 00
0170 4d 00 53 00 2d 00 4f 00 72 00 67 00 61 00 6e 00
0180 69 00 7a 00 61 00 74 00 69 00 6f 00 6e 00 2d 00
0190 50 00 32 00 50 00 2d 00 41 00 63 00 63 00 65 00
01a0 73 00 73 00 20 00 5b 00 32 00 30 00 32 00 32 00
01b0 5d 30 27 80 25 30 23 31 21 30 1f 06 03 55 04 03
01c0 13 18 54 6f 6b 65 6e 20 53 69 67 6e 69 6e 67 20
01d0 50 75 62 6c 69 63 20 4b 65 79 30 27 80 25 30 23
01e0 31 21 30 1f 06 03 55 04 03 13 18 54 6f 6b 65 6e
01f0 20 53 69 67 6e 69 6e 67 20 50 75 62 6c 69 63 20
0200 4b 65 79

```

```

.....0...0...00
.O0M1K0I ..U...B.
M.S...0. r.g.a.n.
i.z.a.t. i.o.n...
P.2.P... A.c.c.e.
s.s. [. 2.0.2.2.
]0'·%0#1 !0...U..
..Token Signing
Public Key0'·%0#
1!0...U. ...Token
Signing Public
Key

```

\* Similar for the server side in Acceptor metadata

# AP\_REQUEST

## PKU2U part

```

▼ NEGOEX AP_REQUEST
  ▼ Header
    Signature: NEGOEXTS
    MessageType: AP_REQUEST (0x00000005)
    SequencNum: 4
    cbHeaderLength: 64
    cbMessageLength: 2449
    ConversationID: 8fbe4731-61c7-bcda-7766-cc10
    AuthScheme: 0d53335c-f9ea-4d0d-b2ec-4ae3786e25f1
  ▼ Exchange: 2385 bytes at 64
    ExchangeOffset: 64
    ExchangeByteCount: 2385
    ExchangePad: 0000
    ▼ PKU2U
      ▼ as-req
        pvno: 5
        msg-type: krb-as-req (10)
        ▼ padata: 1 item
          ▼ PA-DATA pA-PK-AS-REQ
            ▼ padata-type: pA-PK-AS-REQ (16)
              ▼ padata-value: 308208128082080e3082080a020103310b300906052b0e03021a05003082021f06072b06...
                ▼ signedAuthPack
  ▼ PKU2U
    ▼ as-req
      pvno: 5
      msg-type: krb-as-req (10)
      ▼ padata: 1 item
        ▼ PA-DATA pA-PK-AS-REQ
          ▼ padata-type: pA-PK-AS-REQ (16)
            ▼ padata-value: 308208128082080
              ▼ signedAuthPack

```

# CHALLENGE

## PKU2U part

```
▼ NEGOEX CHALLENGE
  > Header
    AuthScheme: 0d53335c-f9ea-4d0d-b2ec-4ae3786ec308
  ▼ Exchange: 3143 bytes at 64
    ExchangeOffset: 64
    ExchangeByteCount: 3143
    ExchangePad: 0000
  ▼ PKU2U
    ▼ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      ▼ padata: 1 item
        ▼ PA-DATA pA-PK-AS-REP
          ▼ padata-type: pA-PK-AS-REP (17)
            ▼ padata-value: a08206ab308206a78082067f308:
              > dhSignedData
            crealm: WELLKNOWN:PKU2U
          > cname
        ▼ ticket
          tkt-vno: 5
          realm: WELLKNOWN:PKU2U
```

```
PKU2U
▼ as-rep
  pvno: 5
  msg-type: krb-as-rep (11)
  ▼ padata: 1 item
    ▼ PA-DATA pA-PK-AS-REP
      ▼ padata-type: pA-PK-AS-REP (17)
        ▼ padata-value: a08206ab308206a78082067f308:
          > dhSignedData
        crealm: WELLKNOWN:PKU2U
      > cname
    ▼ ticket
      tkt-vno: 5
      realm: WELLKNOWN:PKU2U
```

# VERIFY

- NegoEx validator
- Checksum all previous messages

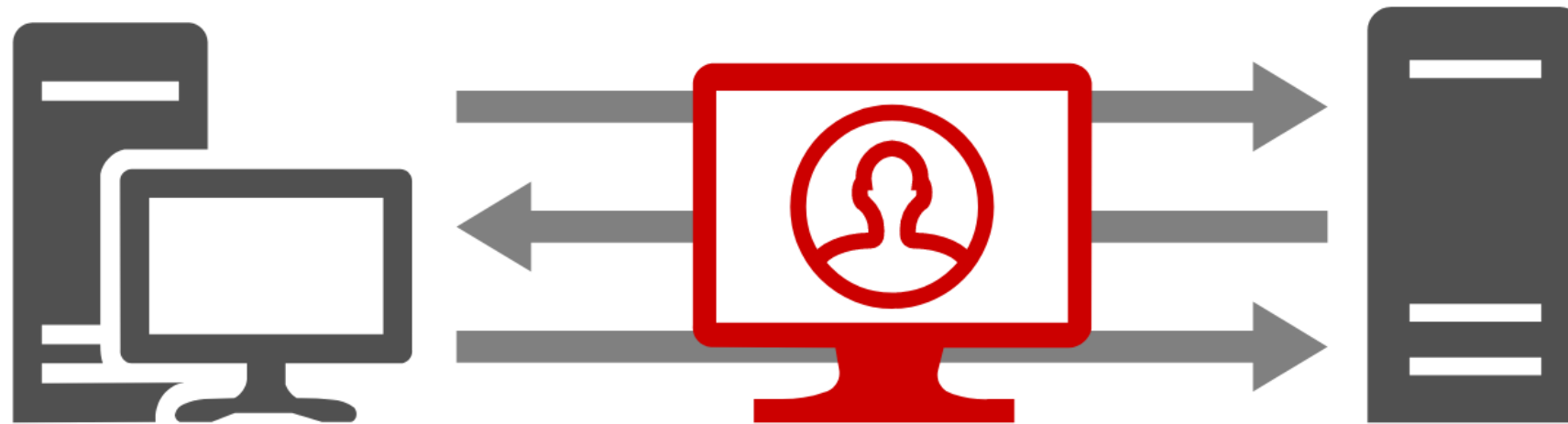
```
▼ NEGOEX VERIFY
  ▼ Header
    Signature: NEGOEXTS
    MessageType: VERIFY (0x00000006)
    SequencNum: 7
    cbHeaderLength: 80
    cbMessageLength: 92
    ConversationID: 8fbe4731-61c7-bcda-7766-cc10e83bb9b2
    AuthScheme: 0d53335c-f9ea-4d0d-b2ec-4ae3786ec308
  ▼ Checksum
    cbHeaderLength: 20
    ChecksumScheme: rfc3961 (1)
    ChecksumType: 16
  ▼ Checksum Vector: 12 at 80
    ChecksumOffset: 80
    ChecksumCount: 12
    ChecksumPad: 0000
    Checksum: bcf15036e12a6754e3a0fb50
```



# Attacks

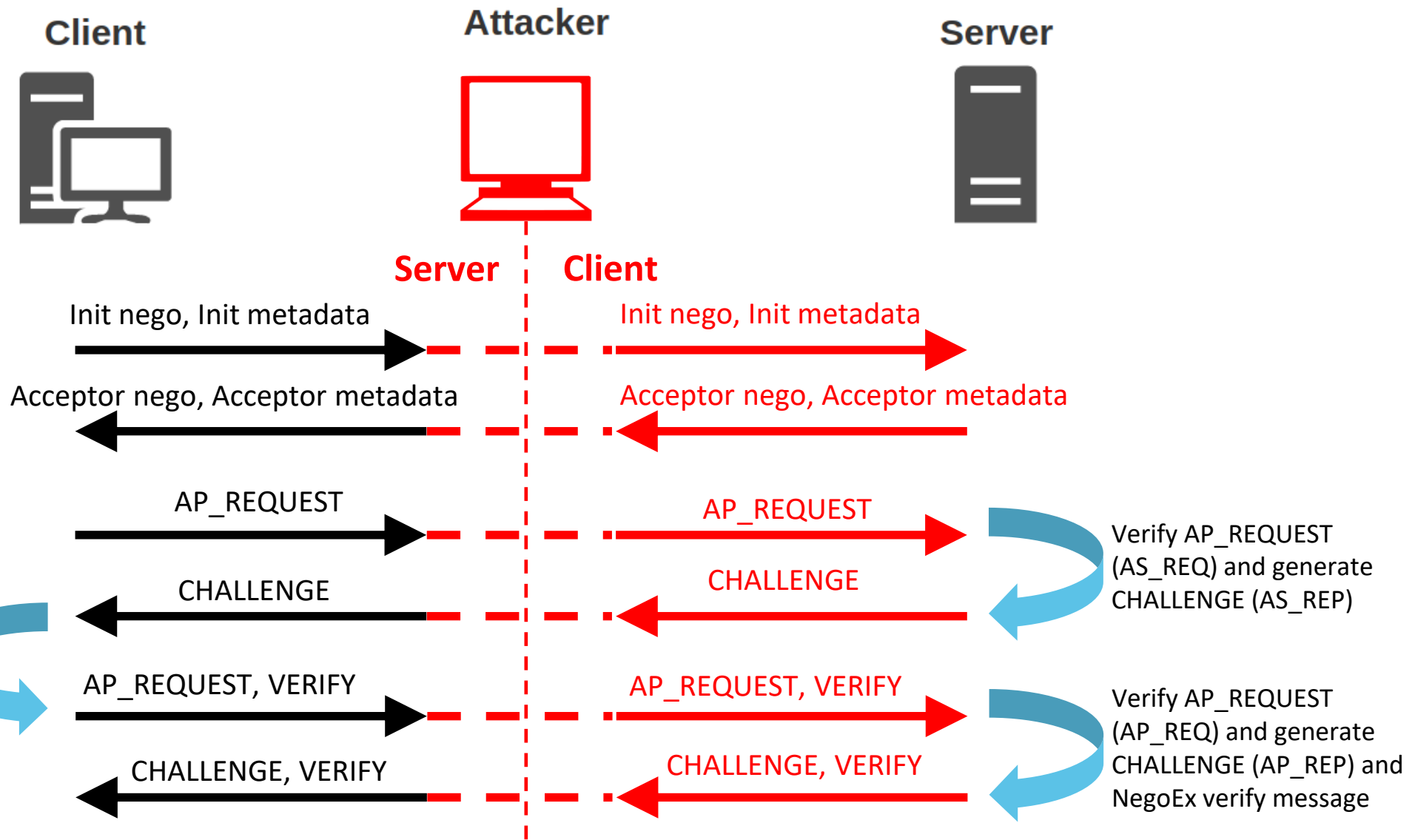
# NegoEx Relay

- Data is not shared between computers to find the “real” source
- Authentication process is easily relayed when not signed

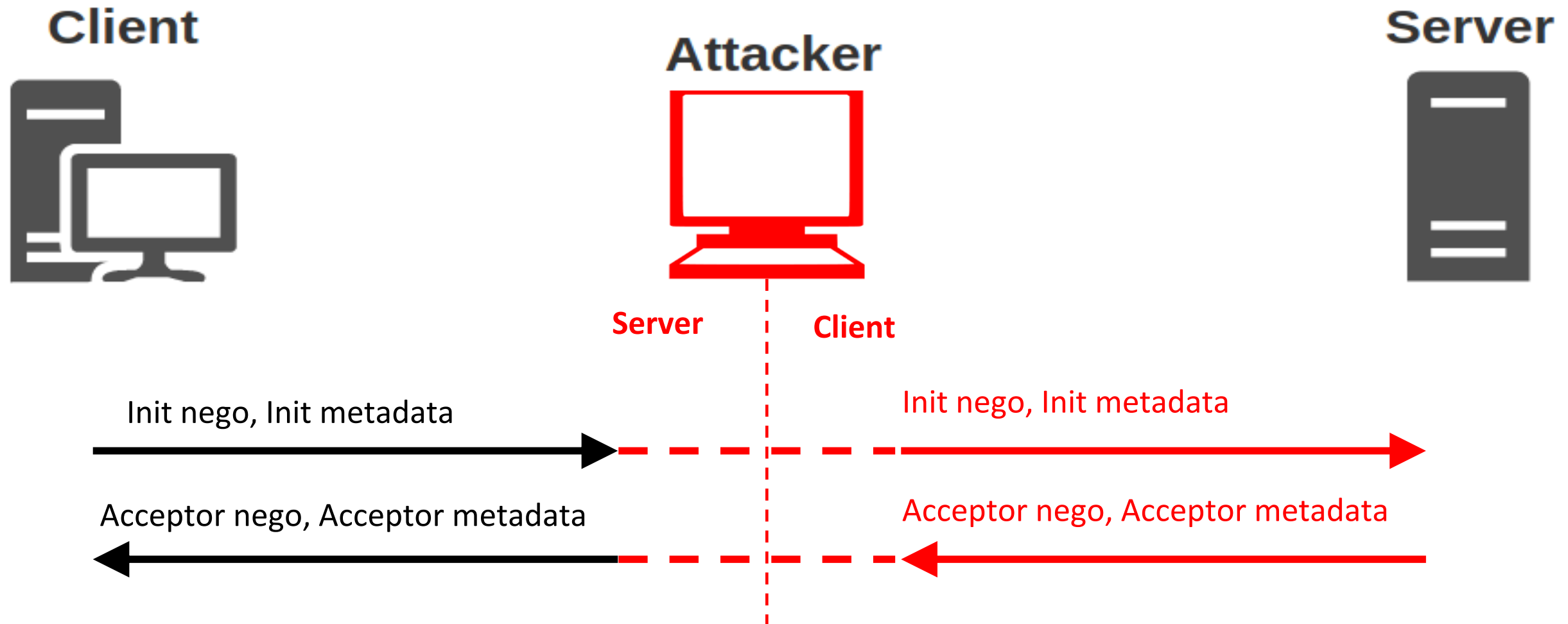


\* Relaying back to victim does not work

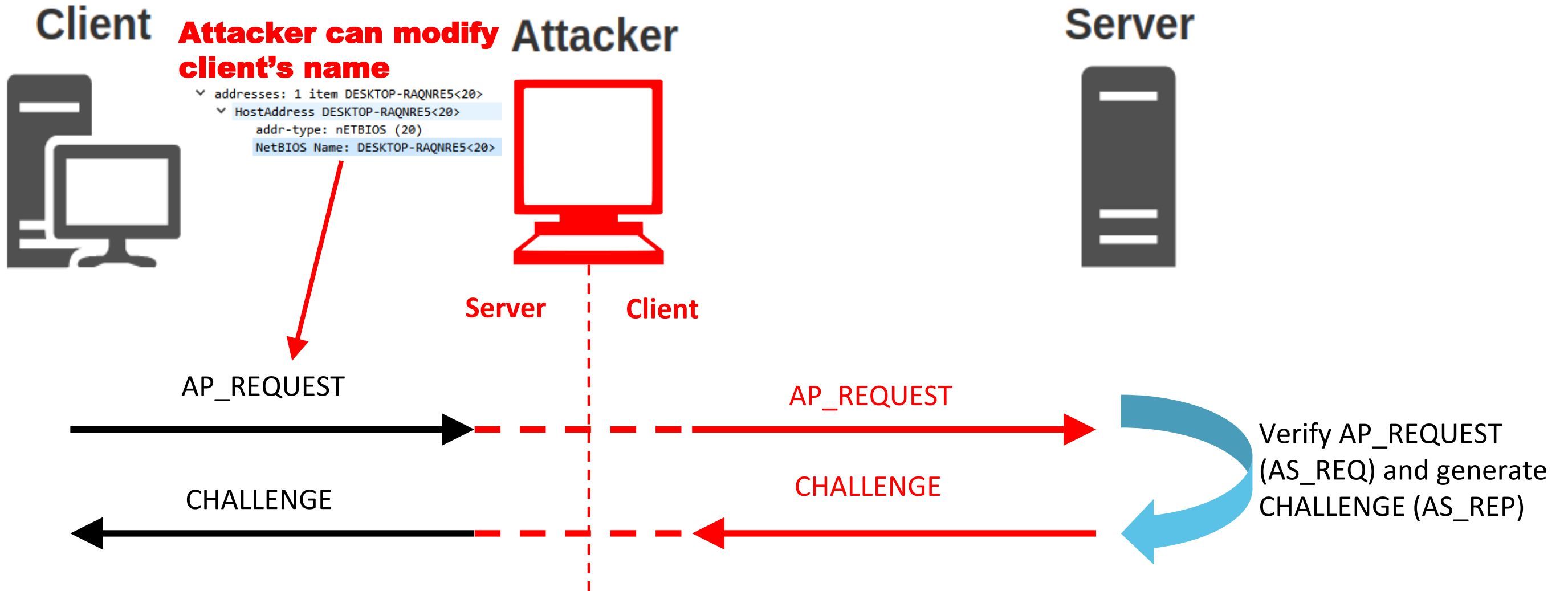
# NegoEx Relay



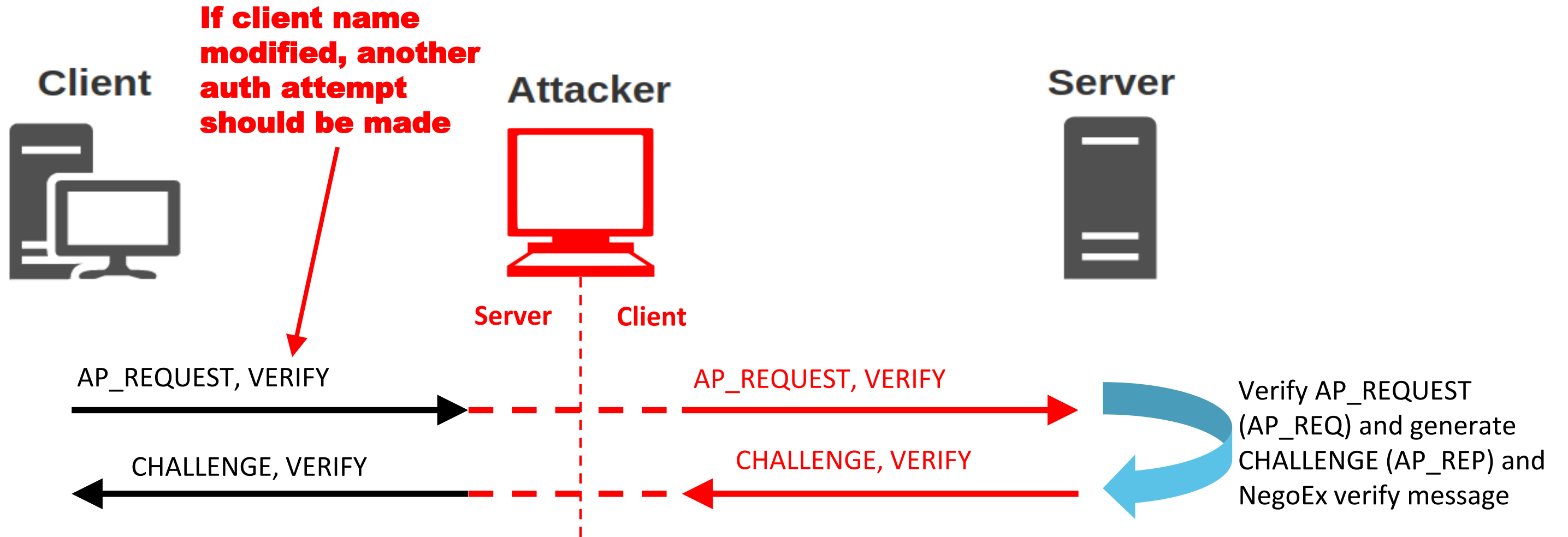
# NegoEx Relay



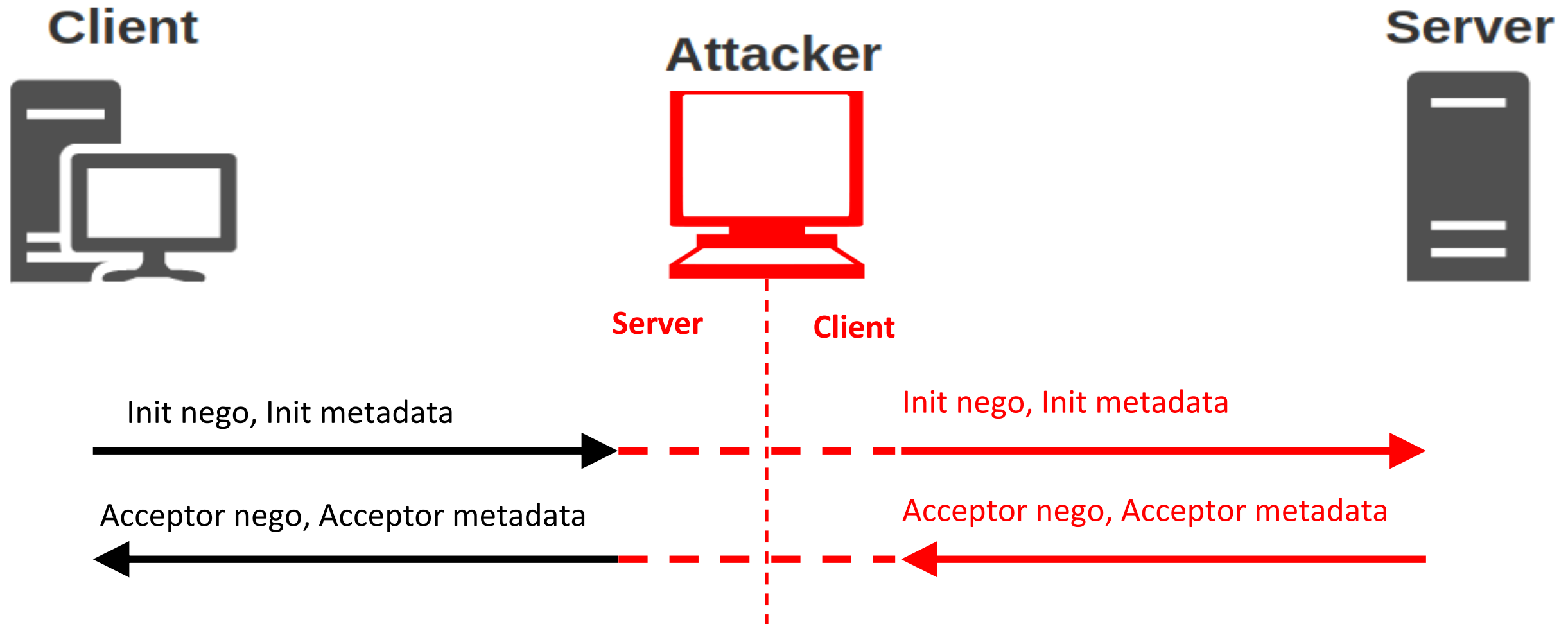
# NegoEx Relay



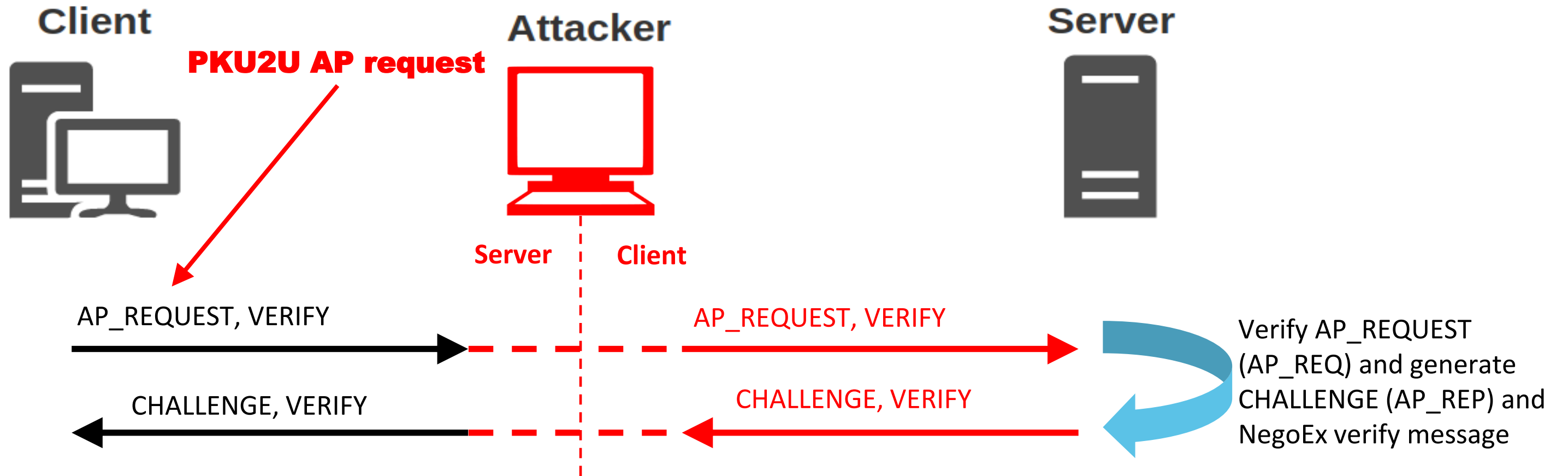
# NegoEx Relay



# NegoEx Relay – Changed client name



# NegoEx Relay - Changed client name





**Demo**

# PRT To Cert

```
{
  "alg": "HS256",
  "ctx": "XLYoL3j04fP8CzB6940G2L1KEgYuhRZ6"
}.{
  "aud": "login.microsoftonline.com",
  "cert_token_use": "user_cert",
  "client_id": "38aa3b87-a06d-4817-b275-7a316988d93b",
  "csr":
  "MIICdTCCAQAwMDEuMCwGA1UEAwldGplZmZvcnRzQGF0cHJlc2VhcmNoLm9ubWljcm9zb2Z0LmNvbTCCAS
  HePQC83gOD5JZzbdtr1riGWi6X1CUUnmmt8/e5Vf3N7HE2xqz4mJzZlqMeGhy50ZaAIOLaB0uzw7FfS5coLPO2r
  Ig3MoEXbWCclipp7y4rwPpNg4vhLdrshaM3EoTXHsagr5MitGF0AU5nHyNrvPFnYxS/gcaP9HQRSQbTBIHFpU4c
  RY0RbDWzkUSqYbCBwpgnsndGdrF73K1mLPTThu9r1IuqRmMcfIzelqRkiGwVA0pTEo8CAwEAAaAAMA0GCSqGSIsbE
  7UfQSM9AFK0GsT+FxdIH0H08Pc/d5pYHSsVH5AISyJw7gvLWhZy1BbNZHwe1GusfGFCaq7BI2y3dZgw3UY+hSFJ
  UsQu+bNu0j45GGcXbYa3kGjuFfgiLCTkmyFyxwpCSRhn37kNd0RUTZuGZAdxLhu3XIBBBGEbSoIZGFYT7CCQO4Gc
  KH90+Xrv+R+v5sqvKp/25rYJIgHKCBukyseyM+KGb",
  "csr_type": "http://schemas.microsoft.com/windows/pki/2009/01/enrollment#PKCS10",
  "grant_type": "refresh_token",
  "iss": "aad:brokerplugin",
  "refresh_token": "0.ATkAY9dbAZUjoUiJxnig3rfk0Ic7qjhtoBdIsnV6MwmI2Ts5ABo.AgABAAAAAAD--
  5ArU_aSiX8965g2mjzvDPK44gV406v3dz_7iAlmCKHNptk2dMtum7U8j7FT99Bz_3K6tPpE0tkT_29vrobffibn
  qFIXYw_2uLiGrmJHjS4cJQ-1R7VY136fZ33Qe-G8tP_ePpk9wmCEG1BB6Ld9y9JhHYF8v5-
  R9KmvW5WggRoBvmTCuTNs5Lqm18B71IxFW1Wv4ZAhyi7Nkb1gg6AbQ2NO_6UoMs8KcZvx49BqF3WF3NvhDbf2yk
  umZ7sm_spLZb4sqI15bvFr4L3_5Kw59JUy8hHEBTAnaR3J3FNuVfEa1eP36PKTWWSqioDBa0zM1TF-
  33IQbSwFyvIqfy4mcFQU3sA0mQQ8t99GB6A1fPXcqdSor2uBKAp13HAYyKnX_QaFW4AXEDHVsL2761v4abzwrh4
  _Lj11TI1mDY1WG5cuu5xbI92uLRw1Cx713IjrPFEmKmwMran7qnTMGVtaSKUoW0Ybc7K6L0yePihKXsuJjSmDUS
  zXb2EfdT_C4yZDRuwYr0SaD54B1yORcsdkYcsq0z80uPHxHitfYhxRDKsXWRwWDSRG0Ns4bUbd1cJhliDGZ8_jv
  Bei2bR0aoZZ0pdcIixVZSsndCYyhUas2tfGc_xyUTmNZyzdNKOpgTiNj9-dHPze0VFzcKNokYm1kQD17PETMwn
  QL9HnsGsOEC_85JMTQt0pFnVn2hbf0NNmB8PJF7nZp3R_BQyrtg2e1pe8VCac3ds-
  3BDN0h9hj200kdXz4izdP98hfUJ5dF501y1BkXDHQaGDv0IzPk7Pn0s9LIy_1g6iehIB3gI7D35z9IXUvGDHbHLv
  guYDtL0GwLd5ZwEymRj8yIU",
  "request_nonce": "AwABAAAAAACA0z_BAD0_zOQzto8WLOcV1XqAjnuuHhAoRyff_t5sEhPPU10MU2x1Kv
  "scope": "openid aza ugs"
}.[Signature]
```



# Pass the certificate

- Possible by requesting new certificate from PRT or by stealing a certificate from the certificate store on computer

160	5.659343	172.23.1.176	172.23.1.63	TCP	1514 63006 → 445 [ACK] Seq=300 Ack=1163 Win=2100992 Len=1460 [TCP segment of
→	161	5.659343	172.23.1.176	SMB2	1502 Session Setup Request, INITATOR_NEGO, INITIATOR_META_DATA, AP_REQUEST
	162	5.659413	172.23.1.63	TCP	54 445 → 63006 [ACK] Seq=1163 Ack=3208 Win=2102272 Len=0
←	163	5.691521	172.23.1.63	SMB2	3372 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, CHALLENGE
	164	5.691868	172.23.1.176	TCP	54 63006 → 445 [ACK] Seq=3208 Ack=4481 Win=2102272 Len=0
	165	5.693763	172.23.1.176	TCP	1514 63006 → 445 [ACK] Seq=3208 Ack=4481 Win=2102272 Len=1460 [TCP segment of
	166	5.693763	172.23.1.176	SMB2	317 Session Setup Request, AP_REQUEST, VERIFY
	167	5.693802	172.23.1.63	TCP	54 445 → 63006 [ACK] Seq=4481 Ack=4931 Win=2102272 Len=0
	173	5.703085	172.23.1.63	SMB2	458 Session Setup Response, CHALLENGE, VERIFY
	174	5.703638	172.23.1.176	SMB2	158 Tree Connect Request Tree: \\client7\IPC\$



# Hunting

# Windows events

Windows event 4624 can be leveraged for hunting of NegoEx logins

## New Logon:

Security ID:	AzureAD\yos
Account Name:	AzureAD\yos@ResearchAadLabEnv.onmicrosoft.com
Account Domain:	-
Logon ID:	0x622EF72

## Network Information:

Workstation Name:	DESKTOP-RAQNRE5
Source Network Address:	172.18.255.51
Source Port:	57137

## Detailed Authentication Information:

Logon Process:	Pku2uSsp
Authentication Package:	NegoExtender
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

# Traffic analysis

Traffic analysis tools like Zeek can parse NegoEx and extract the relevant data

```
SMB2 1502 Session Setup Request, INITATOR_NEGO, INITIATOR_META_DATA, AP_REQ...
version: v3 (2)
serialNumber: 0x5c6cffa328ee476316b18f684136cc03
  signature (sha256WithRSAEncryption)
    Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
  issuer: rdnSequence (0)
    rdnSequence: 1 item (id-at-commonName=\000M\000S\000-\0000\000r\000g\000a\000n\000i\000)
      RDNSequence item: 1 item (id-at-commonName=\000M\000S\000-\0000\000r\000g\000a\000n\000i\000)
        RelativeDistinguishedName item (id-at-commonName=\000M\000S\000-\0000\000r\000g\000a\000n\000i\000)
          Id: 2.5.4.3 (id-at-commonName)
          DirectoryString: bmpString (3)
            bmpString: MS-Organization-P2P-Access [2022]
  validity
    > notBefore: utcTime (0)
    > notAfter: utcTime (0)
  subject: rdnSequence (0)
    rdnSequence: 3 items (id-at-commonName=yos@ResearchAadLabEnv.onmicrosoft.com,id-at-co
```

**Serial Number**

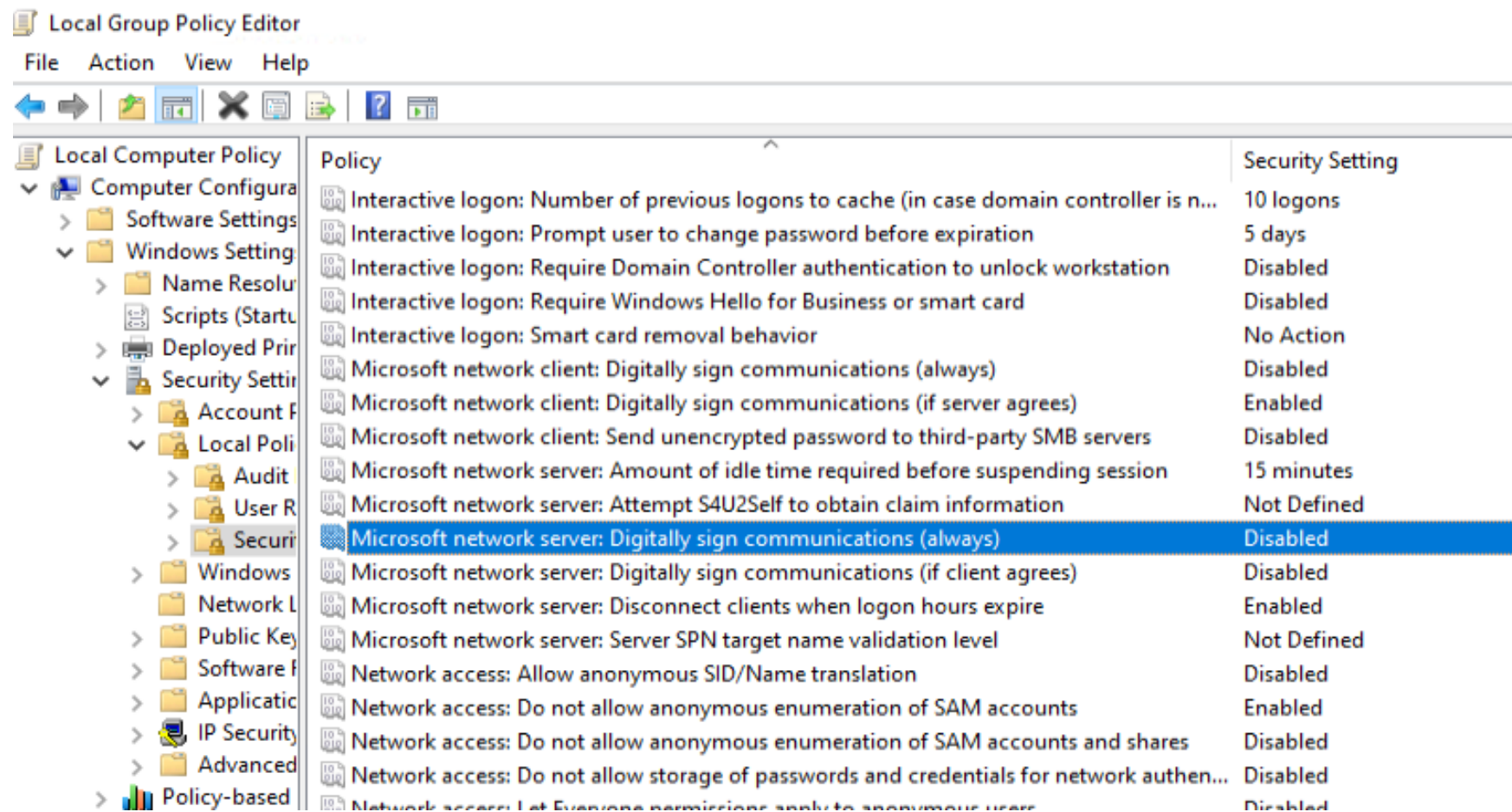
5C6CFFA328EE476316B18F684136CC03

**Subject**

CN=yos@ResearchAadLabEnv.onmicrosoft.com,CN=S-1-12-1-

# Mitigations

- SMB signing



# Tools

- NegoEx relay tool
- Azure AD certificate requestor
- Authentication tool with Azure AD certificate
- Wireshark dissector for NegoEx
- Zeek build that dissect NegoEx Kerberos packets

# Takeaways

- Patching is not enough
- Usage of SMB signing is a must
- Hunt hunt hunt

## Thank you Questions?



[@Rubin\\_mor](https://t.me/learningnets)