

RELAYING CREDENTIALS HAS NEVER BEEN EASIER:

HOW TO EASILY BYPASS THE LATEST NTLM RELAY MITIGATIONS

preempt

Marina Simakov
Yaron Zinar

DEFCON

ABOUT US

Marina Simakov (@simakov_marina)

- Senior Security Researcher @Preempt
- M.Sc. in computer science, with several published articles, with a main area of expertise in graph theory
- Previously worked as a Security Researcher @Microsoft
- Spoke at various security conferences such as Black Hat, Blue Hat IL and DefCon

Yaron Zinar (@YaronZi)

- Senior Security Researcher Lead @Preempt
- M.Sc. in Computer Science with a focus on statistical analysis
- Spent over 12 years at leading companies such as Google and Microsoft
- Among his team latest finding are CVE-2017-8563, CVE-2018-0886, CVE-2019-1040 and CVE-2019-1019

AGENDA

1. Introduction:
   - Common attacks on Active Directory
   - NTLM
     - Design weaknesses
     - NTLM Relay
     - Offered mitigations
2. Known Vulnerabilities
   - LDAPS Relay
   - CVE-2015-0005
3. New vulnerabilities
   - Your session key is my session key
   - Drop the MIC
   - EPA bypass
   - Attacking AD FS
     - External lockout bypass
     - Reverse-Kerberoasting
4. Takeaways

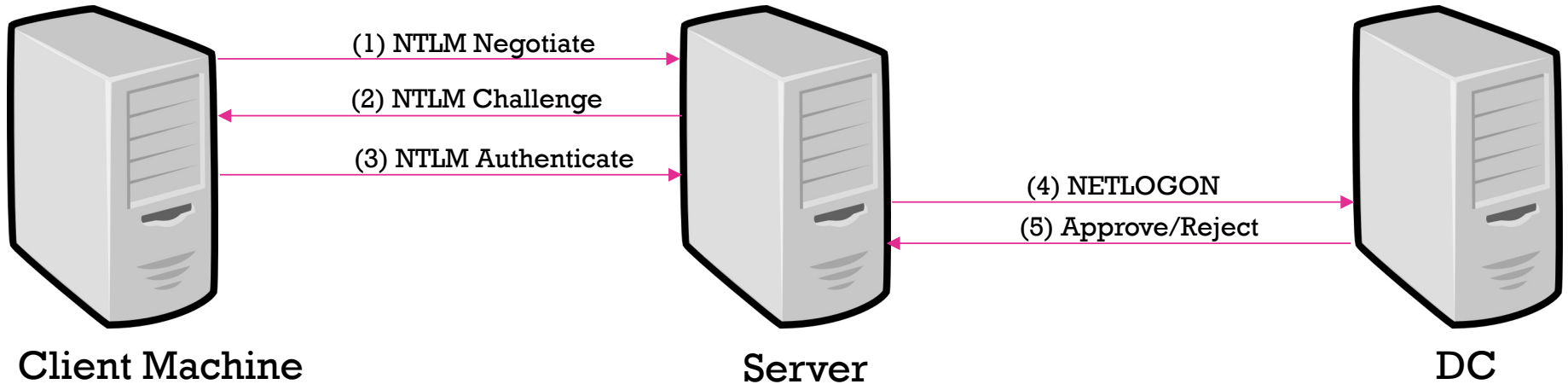


INTRODUCTION: ACTIVE DIRECTORY

- Main secrets storage of the domain
  - Stores password hashes of all accounts
  - In charge of authenticating accounts against domain resources
- Authentication protocols
  - LDAP
  - NTLM
  - Kerberos
- Common attacks
  - Golden & Silver Ticket
  - Forged PAC
  - PTT
  - PTH
  - NTLM Relay

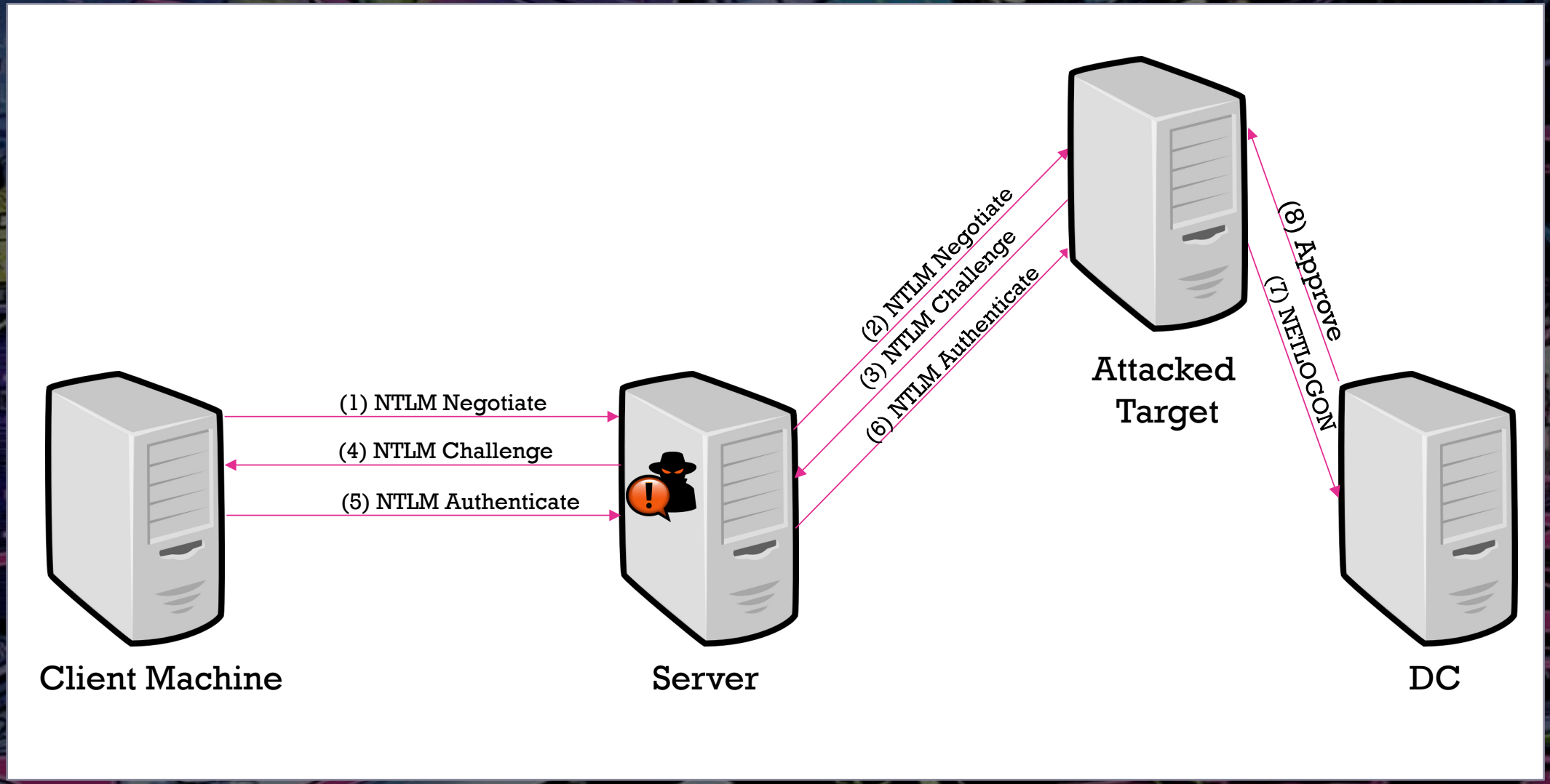
<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM



Authentication is *not* bound to the session!

NTLM RELAY



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>



NTLM RELAY: MITIGATIONS

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM RELAY: MITIGATIONS

- Mitigations:
  - SMB Signing
  - LDAP Signing
  - EPA (Enhanced Protection for Authentication)
  - LDAPS channel binding
  - Server SPN target name validation
  - Hardened UNC Paths

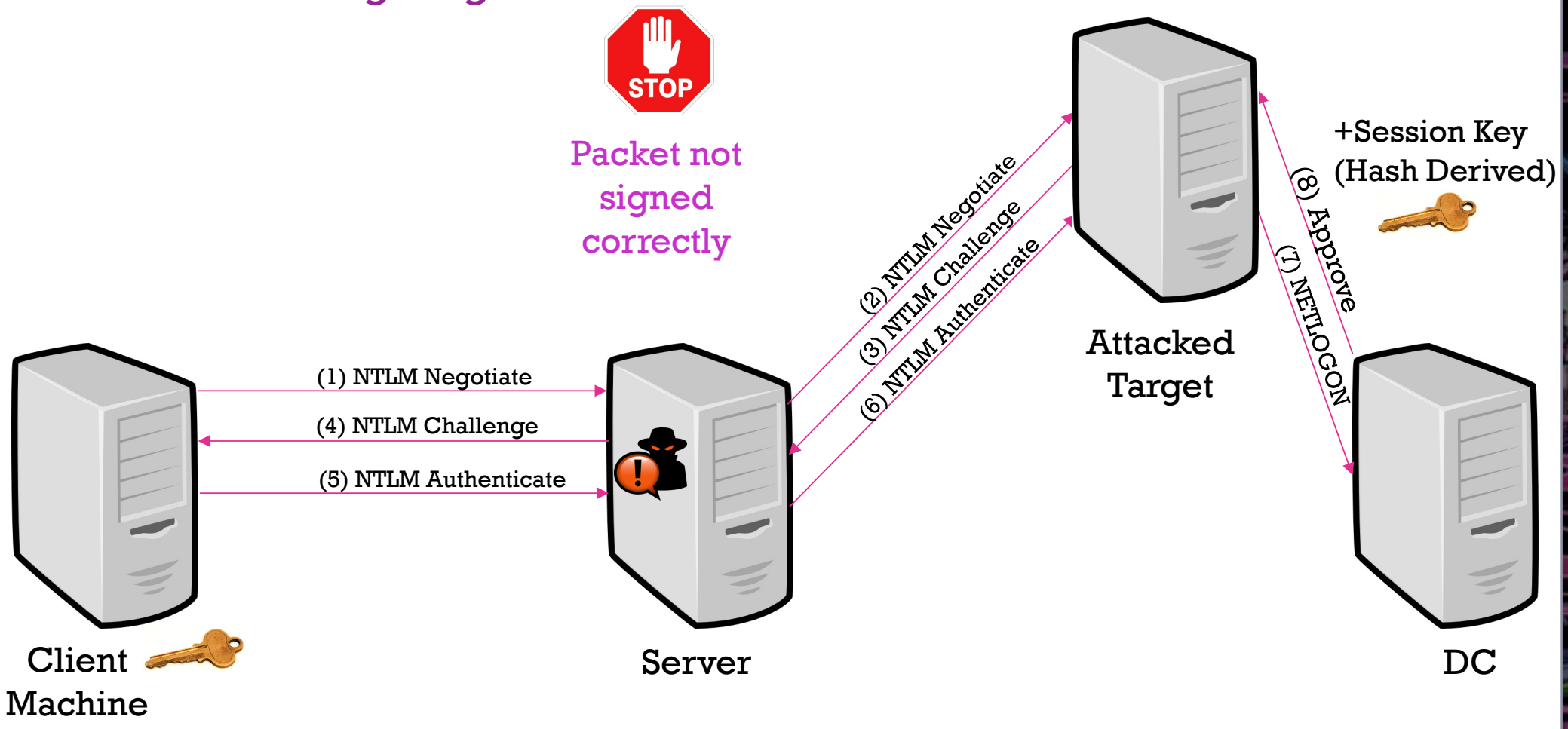
NTLM RELAY: MITIGATIONS

- SMB & LDAP signing
  - After the authentication, all communication between client and server will be signed
  - The signing key is derived from the authenticating account's password hash
  - The client calculates the session key by itself
  - The server receives the session key from the DC in the NETLOGON response
  - An attacker with relay capabilities has no way of retrieving the session key

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM RELAY: MITIGATIONS

- SMB & LDAP signing



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

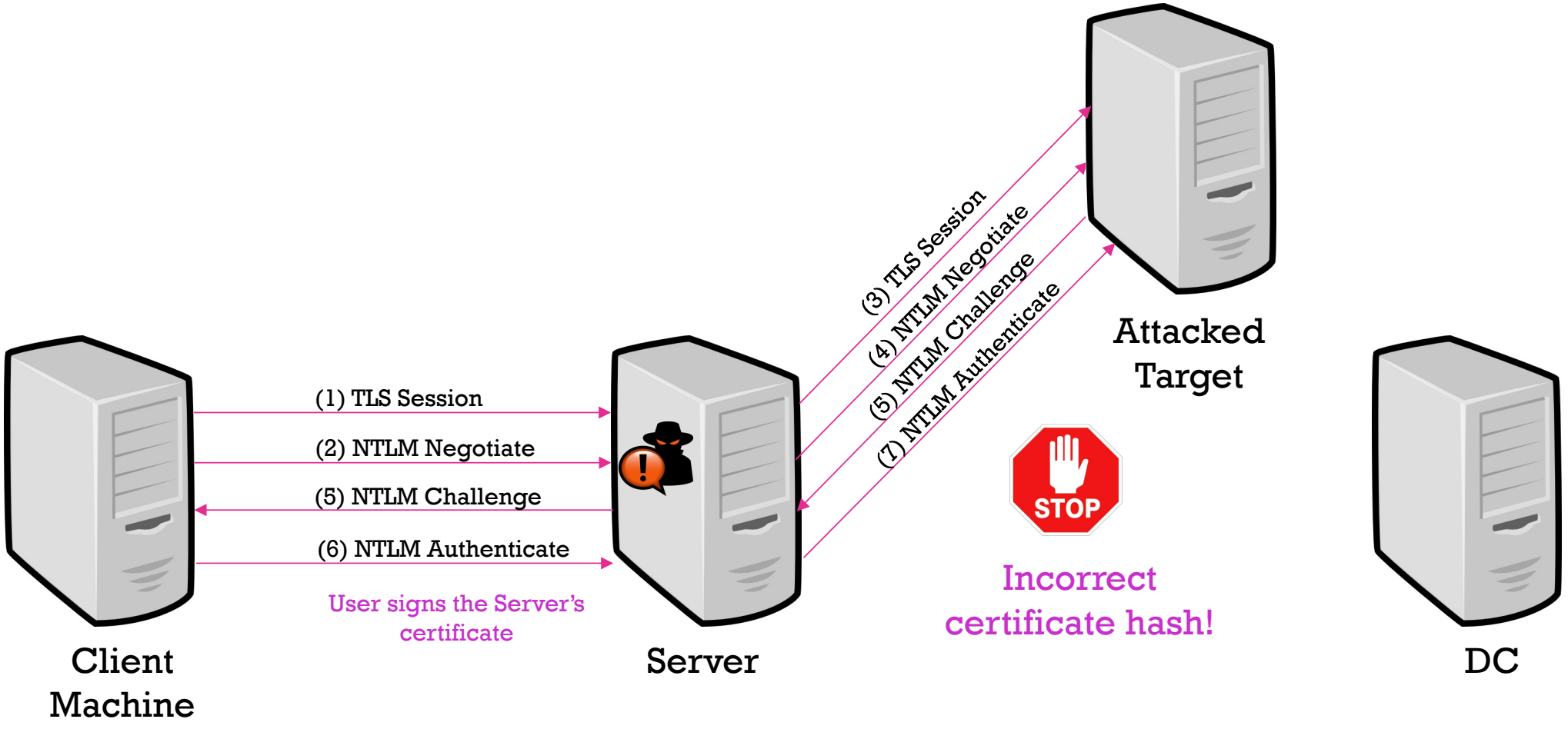
NTLM RELAY: MITIGATIONS

- EPA (Enhanced Protection for Authentication)
  - RFC 5056
  - Binds the NTLM authentication to the secure channel over which the authentication occurs
  - The final NTLM authentication packet contains a hash of the target service's certificate, signed with the user's password hash
  - An attacker with relay capabilities is using a different certificate than the attacked target, hence the client will respond with an incompatible certificate hash value

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM RELAY: MITIGATIONS

- EPA (Enhanced Protection for Authentication)





NTLM RELAY: KNOWN VULNERABILITIES

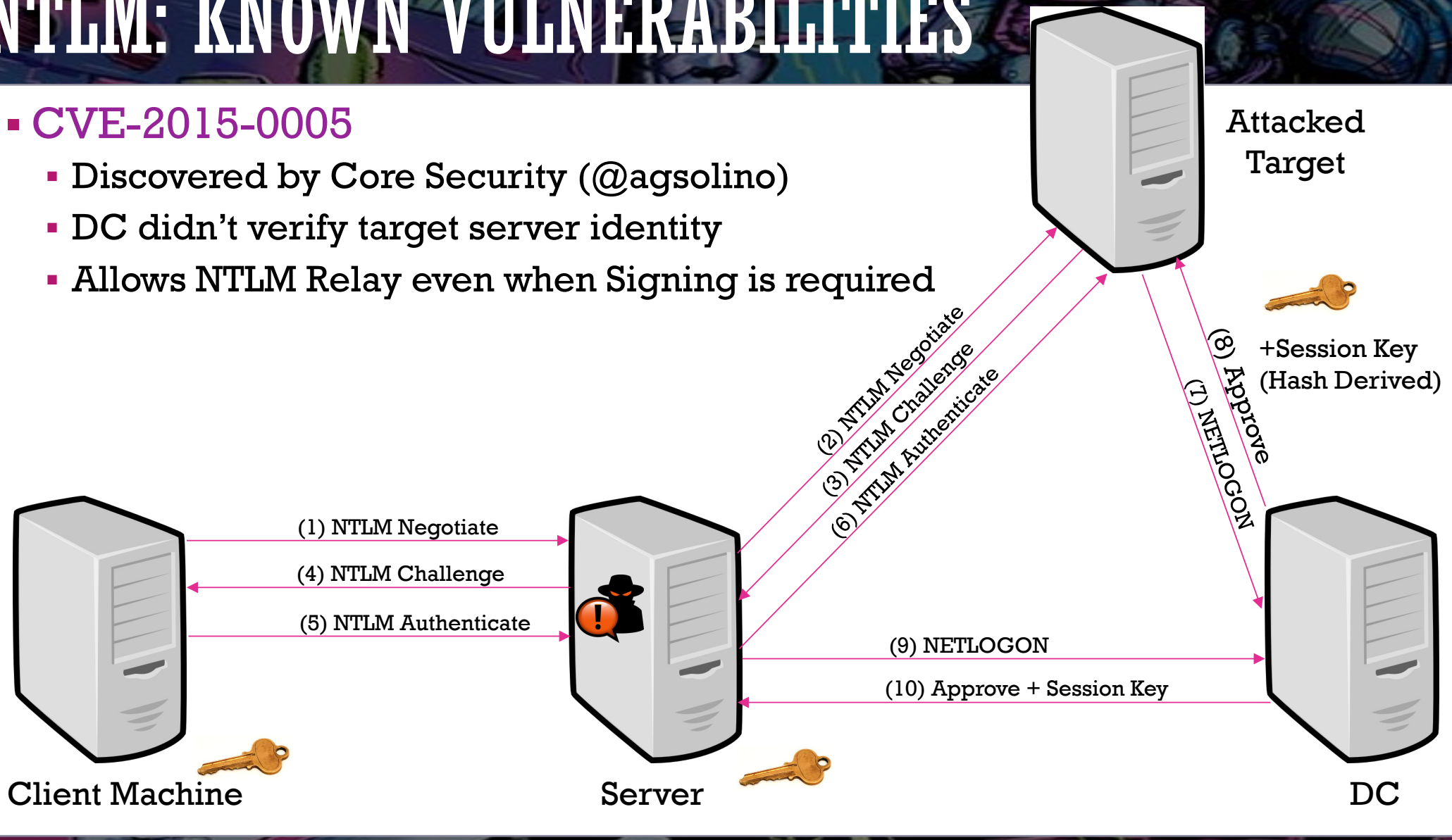
<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: KNOWN VULNERABILITIES

- LDAPS Relay (CVE-2017-8563)
  - Discovered by Preempt in 2017
    https://blog.preempt.com/new-ldap-rdp-relay-vulnerabilities-in-ntlm
  - Group Policy Object (GPO) - *"Domain Controller: LDAP server signing requirements"*
    - Requires LDAP sessions to be signed **OR**
    - Requires session to be encrypted via TLS (LDAPS)
  - TLS does not protect from credential forwarding!

NTLM: KNOWN VULNERABILITIES

- CVE-2015-0005
  - Discovered by Core Security (@agsolino)
  - DC didn't verify target server identity
  - Allows NTLM Relay even when Signing is required



NTLM: KNOWN VULNERABILITIES

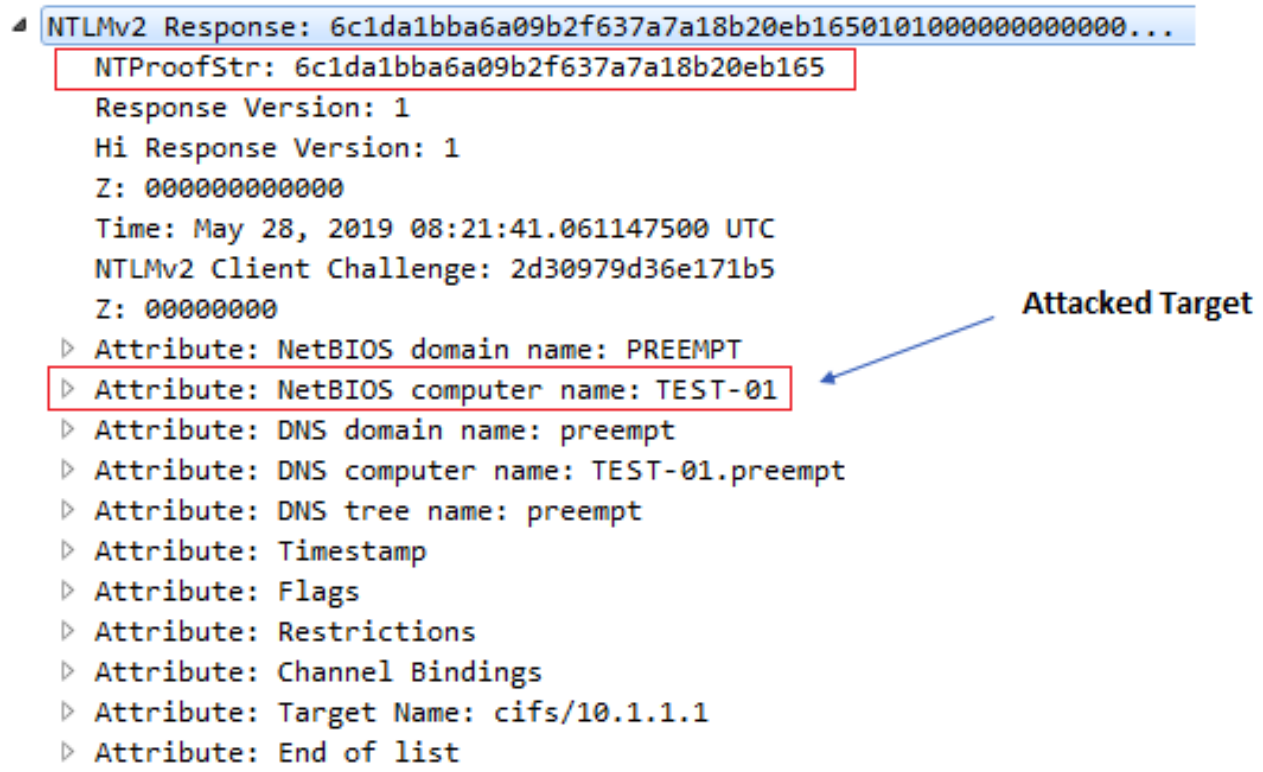
- CVE-2015-0005
  - NTLM Challenge message:
    - Contains identifying information about the target computer

```
▲ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  ▷ Target Name: PREEMPT
  ▷ Negotiate Flags: 0x02898205, Negotiate Version, Negotiate Target Info,
    NTLM Server Challenge: 5254321a3ca3b35b
    Reserved: 0000000000000000
  ▲ Target Info
      Length: 164
      Maxlen: 164
      Offset: 76
    ▷ Attribute: NetBIOS domain name: PREEMPT
    ▷ Attribute: NetBIOS computer name: TEST-01
    ▷ Attribute: DNS domain name: preempt
    ▷ Attribute: DNS computer name: TEST-01.preempt
    ▷ Attribute: DNS tree name: preempt
    ▷ Attribute: Timestamp
    ▷ Attribute: End of list
  ▷ Version 6.3 (Build 9600); NTLM Current Revision 15
```

Attacked Target

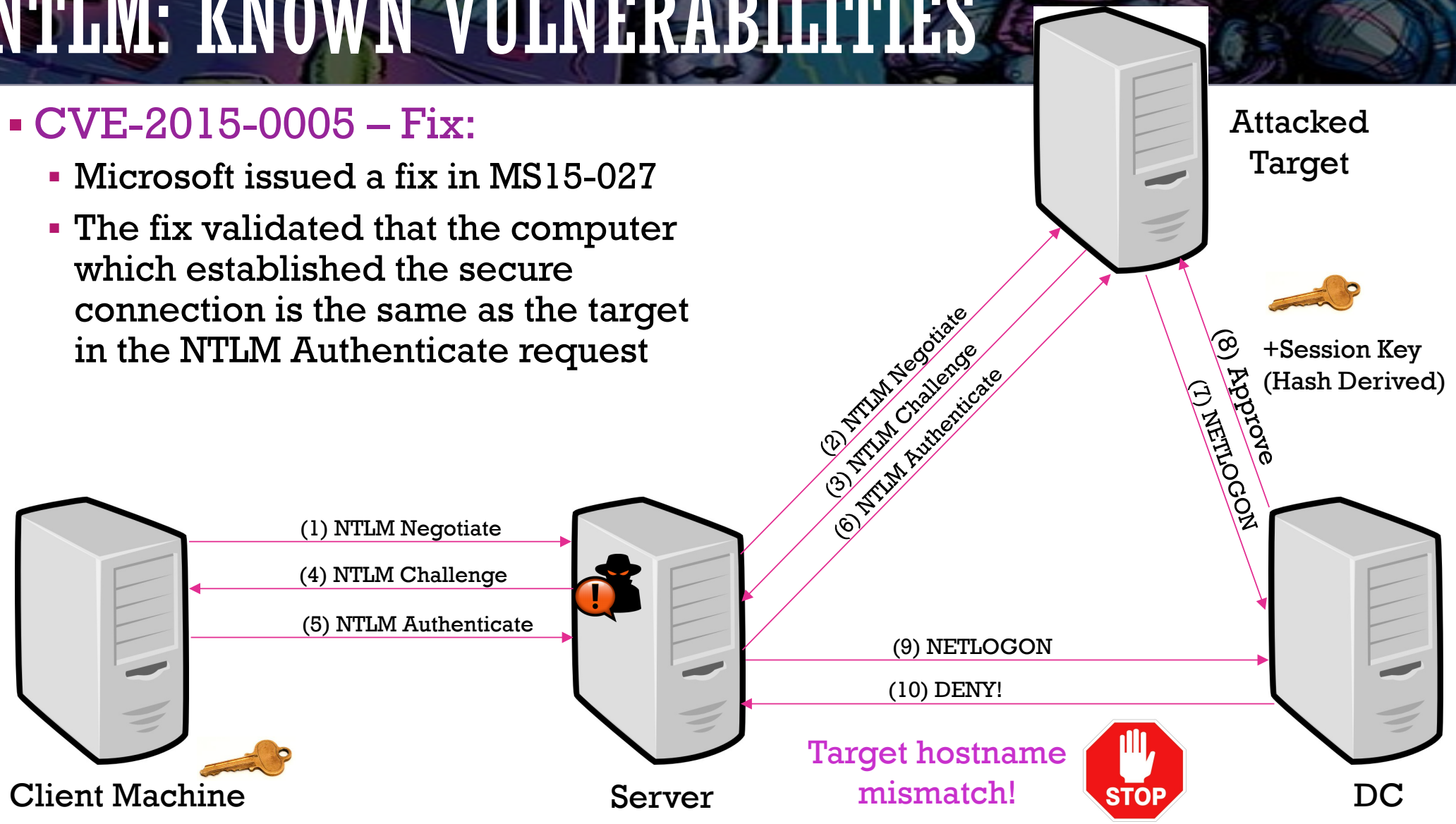
NTLM: KNOWN VULNERABILITIES

- CVE-2015-0005
  - NTLM Authenticate message:
    - User calculates HMAC_MD5 based on the challenge message using his NT Hash



NTLM: KNOWN VULNERABILITIES

- CVE-2015-0005 – Fix:
  - Microsoft issued a fix in MS15-027
  - The fix validated that the computer which established the secure connection is the same as the target in the NTLM Authenticate request





NTLM RELAY: NEW VULNERABILITIES

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: NEW VULNERABILITIES

- Your session key is my session key
  - Retrieve the session key for any NTLM authentication
  - Bypasses the MS15-027 fix
- Drop the MIC
  - Modify session requirements (such as signing)
  - Overcome the MIC protection
- EPA bypass
  - Relay authentication to servers which require EPA
  - Modify packets to bypass the EPA protection
- Attacking AD-FS
  - External lockout policy bypass
  - Reverse-Kerberoasting

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>



YOUR SESSION KEY IS MY SESSION KEY

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: NEW VULNERABILITIES

- Your session key is my session key
  - MS15-027 fix validates target NetBIOS name
  - But what is the target NetBIOS name field is missing?



Original challenge:

```
▲ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  ▷ Target Name: PREEMPT
  ▷ Negotiate Flags: 0x02898205, Negotiate Version, Negotiate
    NTLM Server Challenge: 5254321a3ca3b35b
    Reserved: 0000000000000000
  ▲ Target Info
      Length: 164
      Maxlen: 164
      Offset: 76
    ▷ Attribute: NetBIOS domain name: PREEMPT
    ▷ Attribute: NetBIOS computer name: TEST-01
    ▷ Attribute: DNS domain name: preempt
    ▷ Attribute: DNS computer name: TEST-01.preempt
    ▷ Attribute: DNS tree name: preempt
    ▷ Attribute: Timestamp
    ▷ Attribute: End of list
  ▷ Version 6.3 (Build 9600); NTLM Current Revision 15
```

Modified challenge:

```
▲ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  ▷ Target Name: PREEMPT
  ▷ Negotiate Flags: 0x02898205, Negotiate Version, Negotiate
    NTLM Server Challenge: 5254321a3ca3b35b
    Reserved: 0000000000000000
  ▲ Target Info
      Length: 164
      Maxlen: 164
      Offset: 76
    ▷ Attribute: NetBIOS domain name: PREEMPT
    ▷ Attribute: DNS domain name: preempt
    ▷ Attribute: DNS computer name: TEST-01.preempt
    ▷ Attribute: DNS tree name: preempt
    ▷ Attribute: Timestamp
    ▷ Attribute: End of list
  ▷ Version 6.3 (Build 9600); NTLM Current Revision 15
```

NTLM: NEW VULNERABILITIES

- Your session key is my session key
  - The client responds with an NTLM_AUTHENTICATE message with target NetBIOS field missing
  - The NETLOGON message is sent without this field
  - The domain controller responds with a session key!

NTLM: NEW VULNERABILITIES

- Your session key is my session key
  - But what if the NTLM AUTHENTICATE message includes a **MIC**?
  - MIC: Message integrity for the NTLM NEGOTIATE, NTLM CHALLENGE, and NTLM AUTHENTICATE
  - MIC = HMAC_MD5(SessionKey, ConcatenationOf(NTLM_NEGOTIATE, NTLM_CHALLENGE, NTLM_AUTHENTICATE))

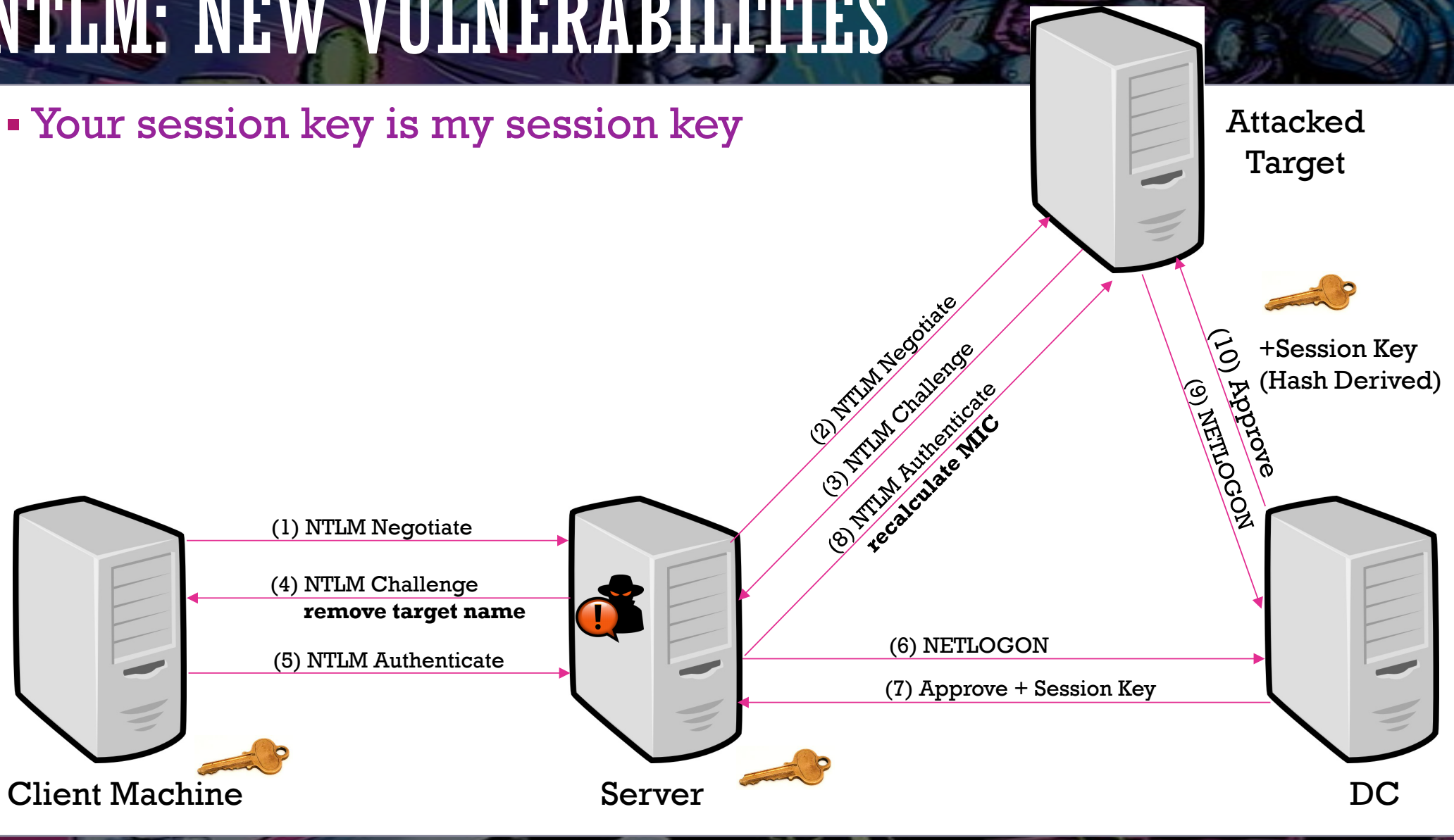
```
▾ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  › Lan Manager Response: 000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 0000000000000000
  › NTLM Response: 1336da946b1e967178af213a953bc69b0101000000000000...
  › Domain name: PREEMPT
  › User name: user01
  › Host name: TEST-01
  › Session Key: b694a2f88063a2fc0e8f122d33b90523
  › Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128,
  › Version 10.0 (Build 17134); NTLM Current Revision 15
    MIC: 7b7f086333cdd6d48a694c3c0cd2aa8d
```

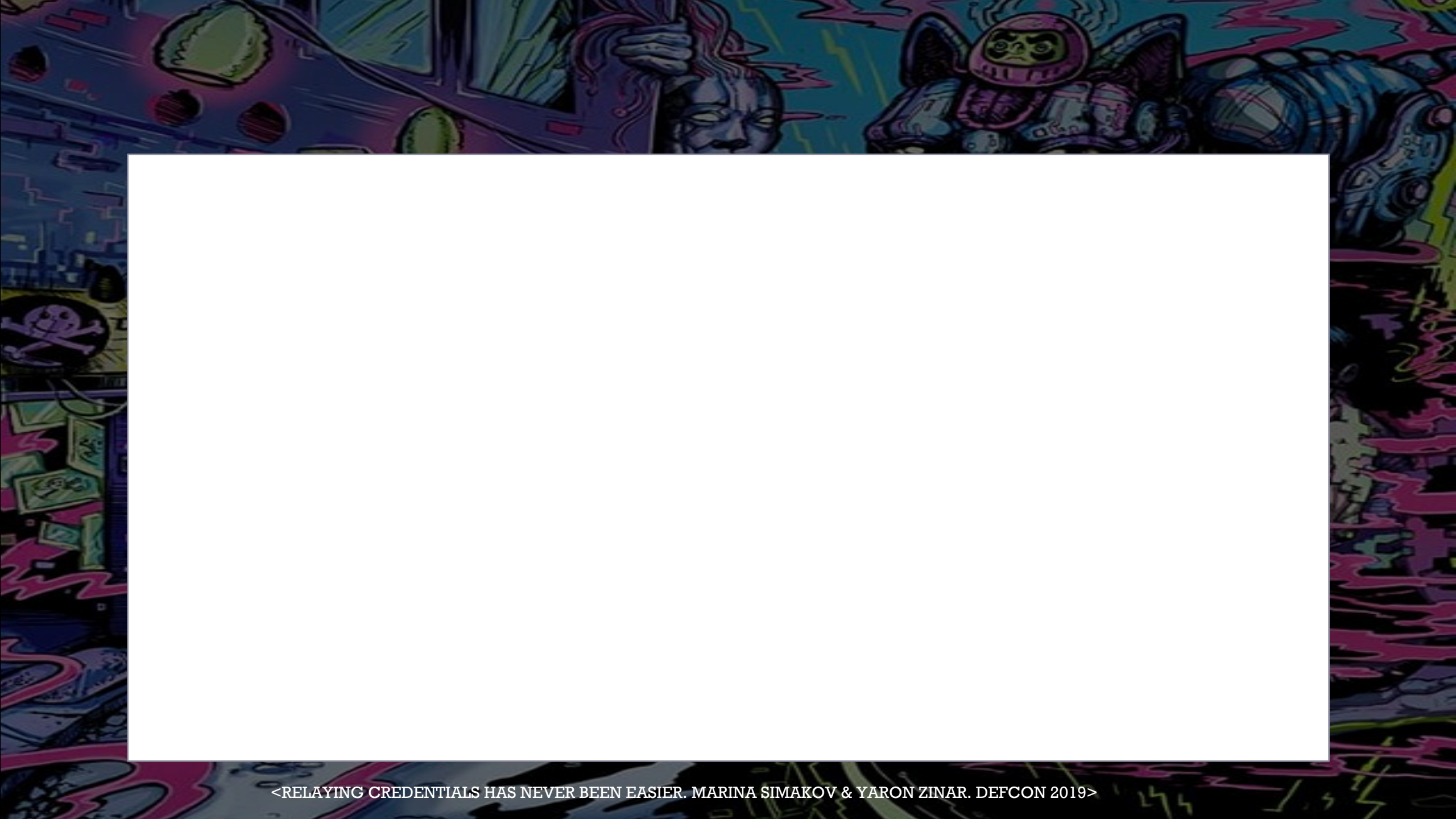
NTLM: NEW VULNERABILITIES

- Your session key is my session key
  - Overcoming the MIC problem:
    - By removing the target hostname we are able to retrieve the session key
    - We have all 3 NTLM messages
    - The client provides a MIC which is based on the modified NTLM_CHALLENGE message
    - We recalculate the MIC based on the original NTLM_CHALLENGE message

NTLM: NEW VULNERABILITIES

- Your session key is my session key





<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: NEW VULNERABILITIES

- Your session key is my session key – Fix:
  - Windows servers deny requests which do not include a target

- Issues:
  - NTLMv1
    - messages do not have av_pairs -> no target field
    - Such authentication requests remain vulnerable to the attack
  - Non-Windows targets are still vulnerable
  - Patching is not enough



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: NEW VULNERABILITIES

- Drop the MIC
  - MIC = HMAC_MD5(SessionKey, ConcatenationOf(NTLM_NEGOTIATE, NTLM_CHALLENGE, NTLM_AUTHENTICATE))
  - If client & server negotiate session privacy/integrity, attackers cannot take over the session

```
▾ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
  ▾ Negotiate Flags: 0xe2088297, Negotiate 56, Negotiate Key Exchange,
                     ....
      .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
                     ....
    Calling workstation domain: NULL
    Calling workstation name: NULL
  ▸ Version 10.0 (Build 17134); NTLM Current Revision 15
```

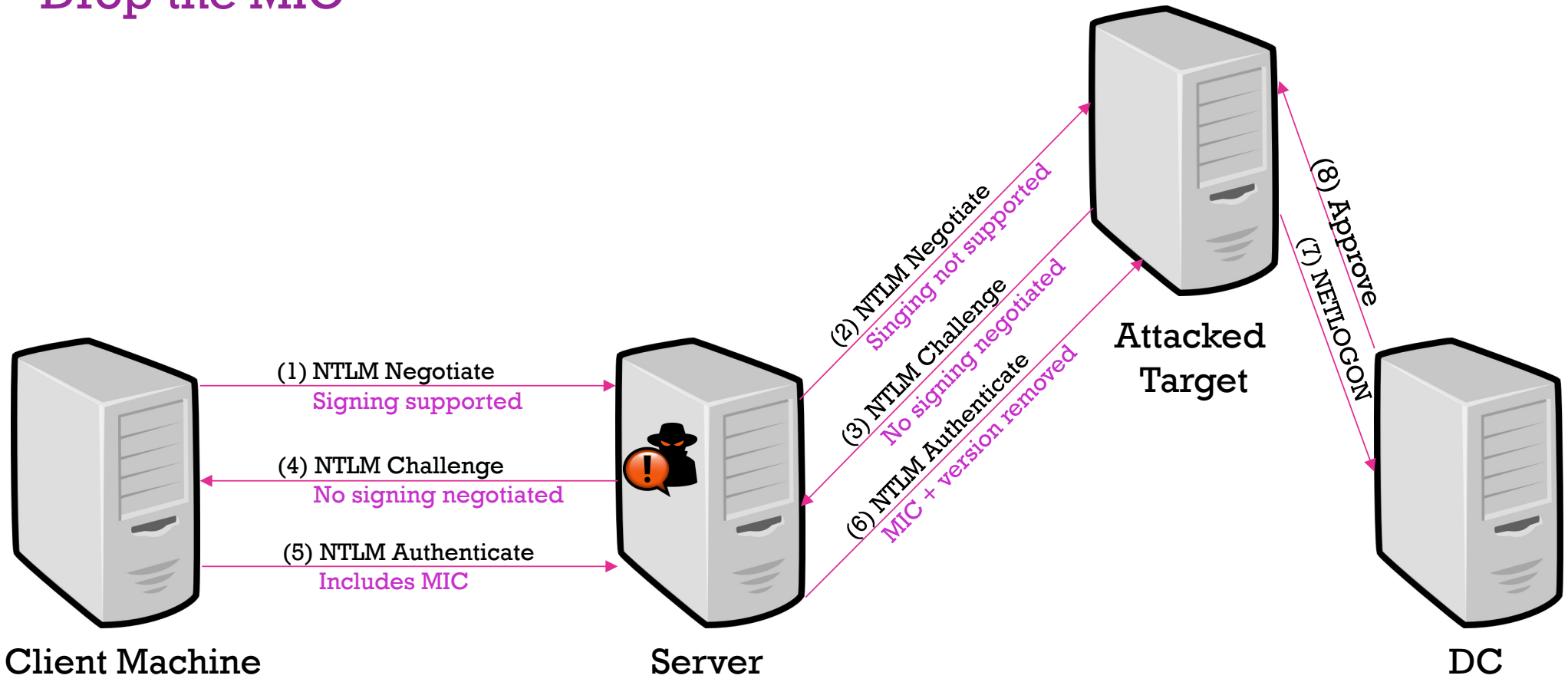
  - The MIC protects the NTLM negotiation from tampering

NTLM: NEW VULNERABILITIES

- Drop the MIC
  - SMB clients turn on the signing negotiation flag by default & use a MIC
  - It is not possible (or at least, not trivial) to relay SMB to another protocol which relies on this negotiation flag (in contrast to other protocols such as HTTP)
  - How can we overcome this obstacle?
    - MIC can be modified only if the session key is known
    - Otherwise, it can be simply removed ☺
    - [In order to remove the MIC, the version needs to be removed as well, as well as some negotiation flags]
  - Result: It is possible to tamper with any stage of the NTLM authentication flow when removing the MIC

NTLM: NEW VULNERABILITIES

- Drop the MIC



NTLM: NEW VULNERABILITIES

- Drop the MIC - Problem
  - The MIC presence is notified in the msvAvFlags attribute in the NTLM authentication message
  - msvAvFlags is signed with the user's password hash

MsvAvFlags 0x0006	A 32-bit value indicating server or client configuration. 0x00000001: Indicates to the client that the account authentication is constrained. 0x00000002: Indicates that the client is providing message integrity in the MIC field (section 2.2.1.3) in the AUTHENTICATE_MESSAGE.<14> 0x00000004: Indicates that the client is providing a target SPN generated from an untrusted source.<15>

```
▷ Attribute: Timestamp
◢ Attribute: Flags
    NTLMV2 Response Item Type: Flags (0x0006)
    NTLMV2 Response Item Length: 4
    Flags: 0x00000002
▷ Attribute: Restrictions
▷ Attribute: Channel Bindings
▷ Attribute: Target Name: cifs/10.1.0.107
▷ Attribute: End of list
```

  - Even if the corresponding bit is set, the target server does not verify that the MIC is indeed present



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

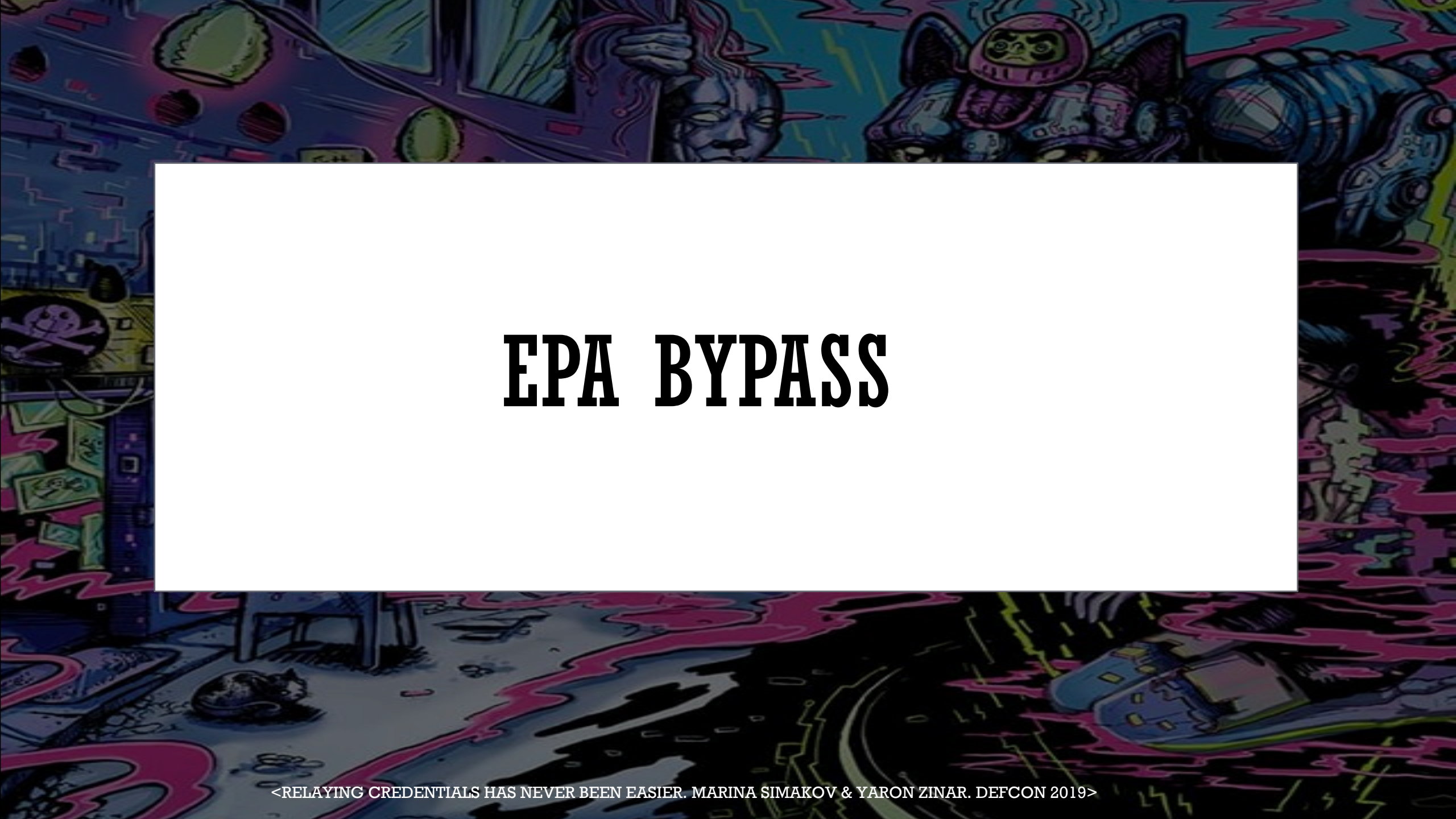
NTLM: NEW VULNERABILITIES

- MIC bypass - Fix:
  - If msvAvFlags indicate that a MIC is present, verify its presence.

- Issues:
  - Some clients don't add a MIC by default (Firefox on Linux or MacOS)
  - These clients are still vulnerable to NTLM session tampering

  - More serious issue:
    CVE-2019-1166 –
    Drop The MIC 2 ☺



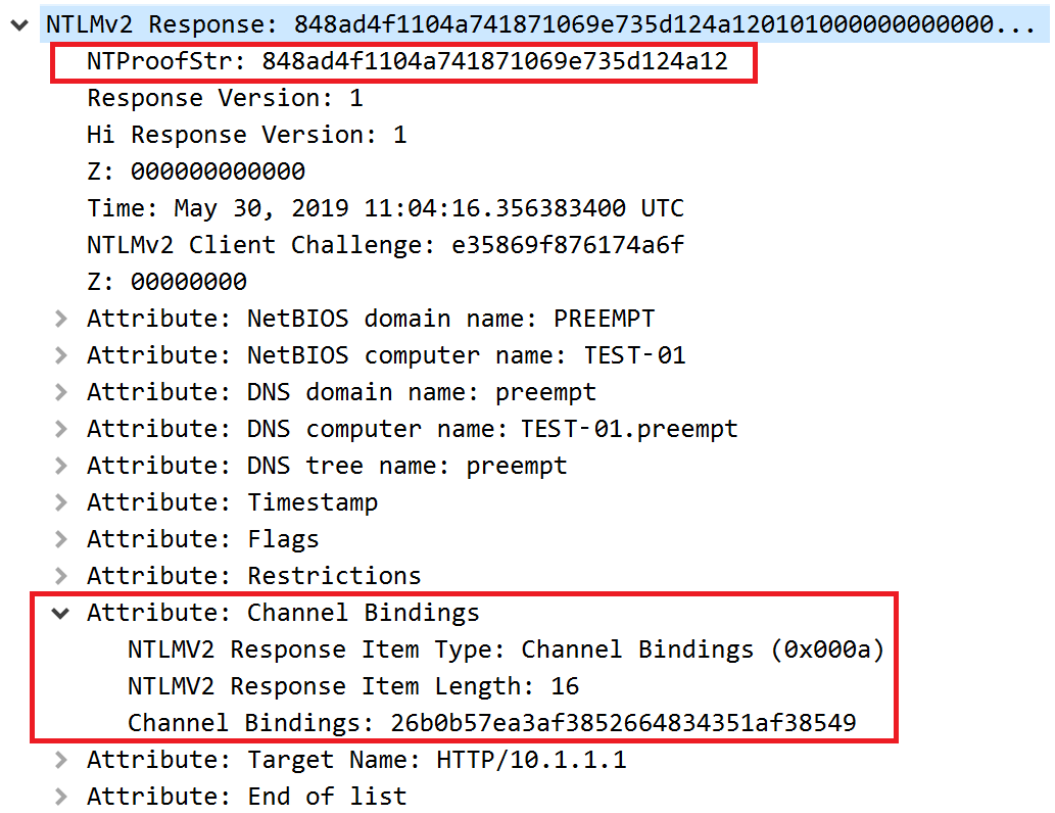


EPA BYPASS

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: NEW VULNERABILITIES

- EPA (Enhanced Protection for Authentication) bypass
  - EPA binds authentication packets to a secure TLS channel
  - Adds a Channel Bindings field to the NTLM_AUTHENTICATE message based on the target server certificate
  - Prevents attackers from relaying the authentication to another server
  - Modification requires knowledge of the user's NT HASH

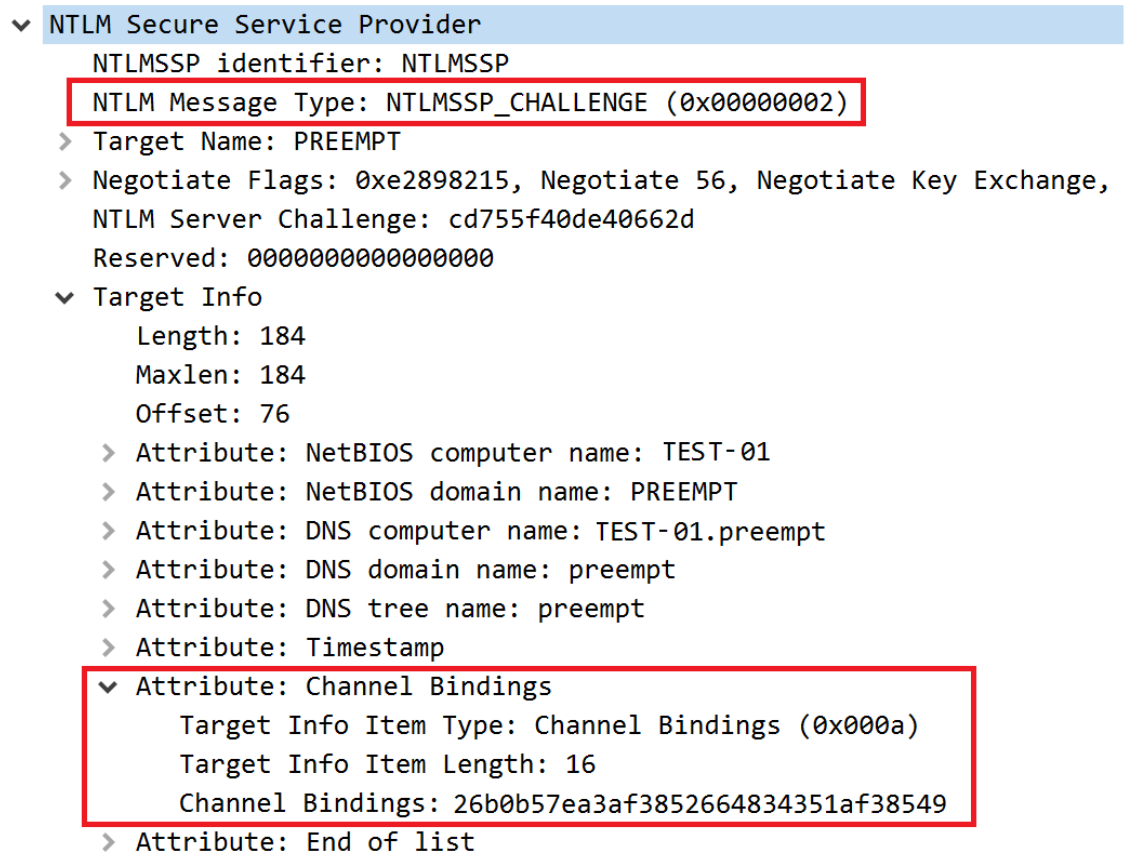


NTLM: NEW VULNERABILITIES

- EPA (Enhanced Protection for Authentication) bypass
  - Servers protected by EPA:
    - AD-FS
    - OWA
    - LDAPS
    - Other HTTP servers (e.g. Sharepoint)
  - Unfortunately by default, EPA is disabled on all of the above servers
  - In most cases, these servers are vulnerable to much simpler attack vectors

NTLM: NEW VULNERABILITIES

- EPA (Enhanced Protection for Authentication) bypass
  - Modifying the Channel Bindings in the NTLM_AUTHENTICATE message is not possible
  - But what if we add a Channel Bindings field to the NTLM_CHALLENGE message before we send it to the client?



NTLM: NEW VULNERABILITIES

- EPA (Enhanced Protection for Authentication) bypass
  - Client will add our crafted field to the NTLM_AUTHENTICATE message!
  - Additional fields would be added to the message, including a second Channel Binding
  - Server takes the first Channel Binding for verification

```
NTLMv2 Response: b0eea4395eea94869ae86aef3e7f72d10101000000000000...
    NTProofStr: b0eea4395eea94869ae86aef3e7f72d1
    Response Version: 1
    Hi Response Version: 1
    Z: 000000000000
    Time: Apr 18, 2019 14:17:09.242052800 UTC
    NTLMv2 Client Challenge: 26b00961558b7b4a
    Z: 00000000
  > Attribute: NetBIOS computer name: TEST-01
  > Attribute: NetBIOS domain name: PREEMPT
  > Attribute: DNS computer name: TEST-01.preempt
  > Attribute: DNS domain name: preempt
  > Attribute: DNS tree name: preempt
  > Attribute: Timestamp
  v Attribute: Channel Bindings
      NTLMV2 Response Item Type: Channel Bindings (0x000a)
      NTLMV2 Response Item Length: 16
      Channel Bindings: 26b0b57ea3af385ae64834351e5a2f49
  > Attribute: Flags
  > Attribute: Restrictions
  v Attribute: Channel Bindings
      NTLMV2 Response Item Type: Channel Bindings (0x000a)
      NTLMV2 Response Item Length: 16
      Channel Bindings: 00000000000000000000000000000000
  > Attribute: Target Name: HTTP/10.1.1.1
  > Attribute: End of list
```

NTLM: NEW VULNERABILITIES

- EPA (Enhanced Protection for Authentication) bypass
  - What if the NTLM_AUTHENTICATE message includes a MIC?
  - **DROP THE MIC!**

Original NTLM_AUTHENTICATE:

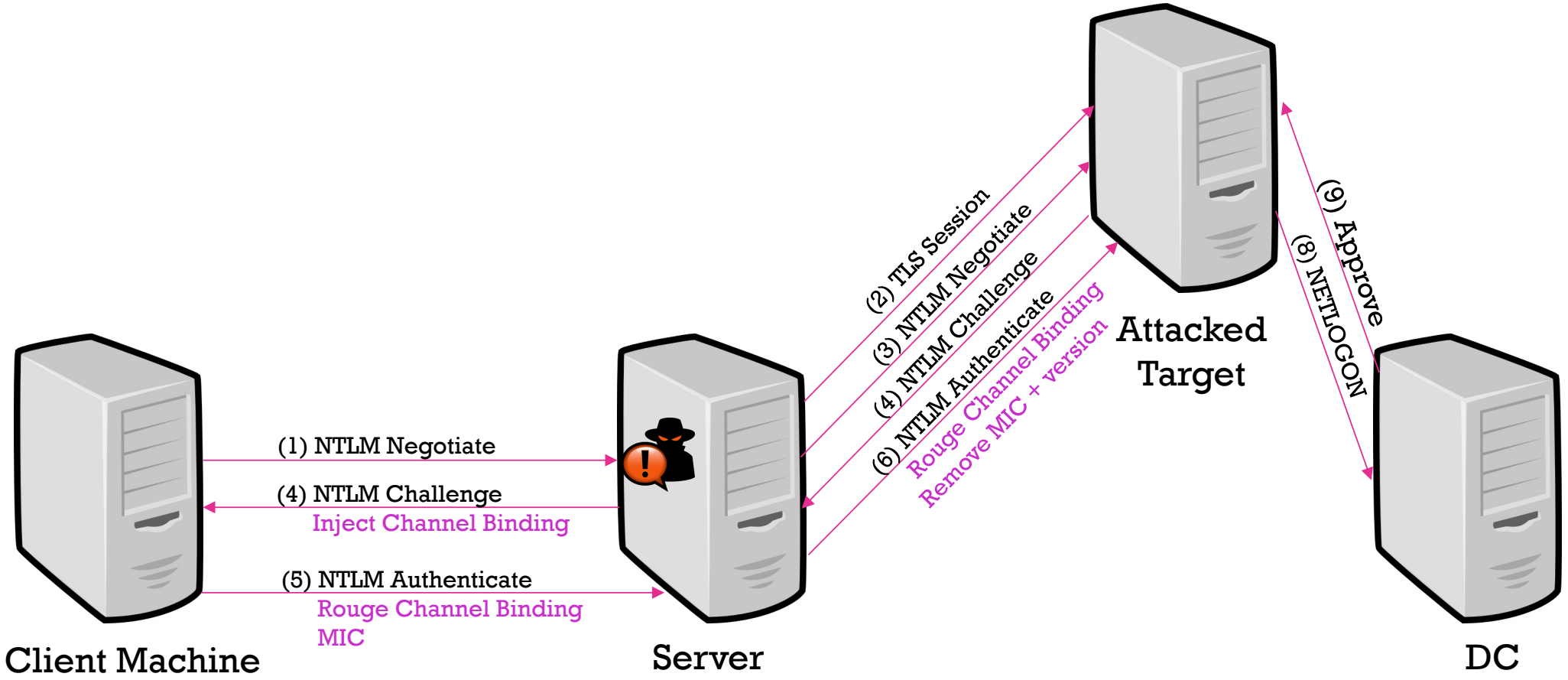
```
NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  > Lan Manager Response: 0000000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 0000000000000000
  > NTLM Response: b0eea4395eea94869ae86aef3e7f72d10101000000000000...
  > Domain name: PREEMPT
  > User name: user01
  > Host name: TEST-01
  > Session Key: f2ee625796ccac3fd657e015dd25454a
  > Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate
  > Version 6.1 (Build 7601); NTLM Current Revision 15
    MIC: e746de89e1e239ad880738eccfe687dc
```

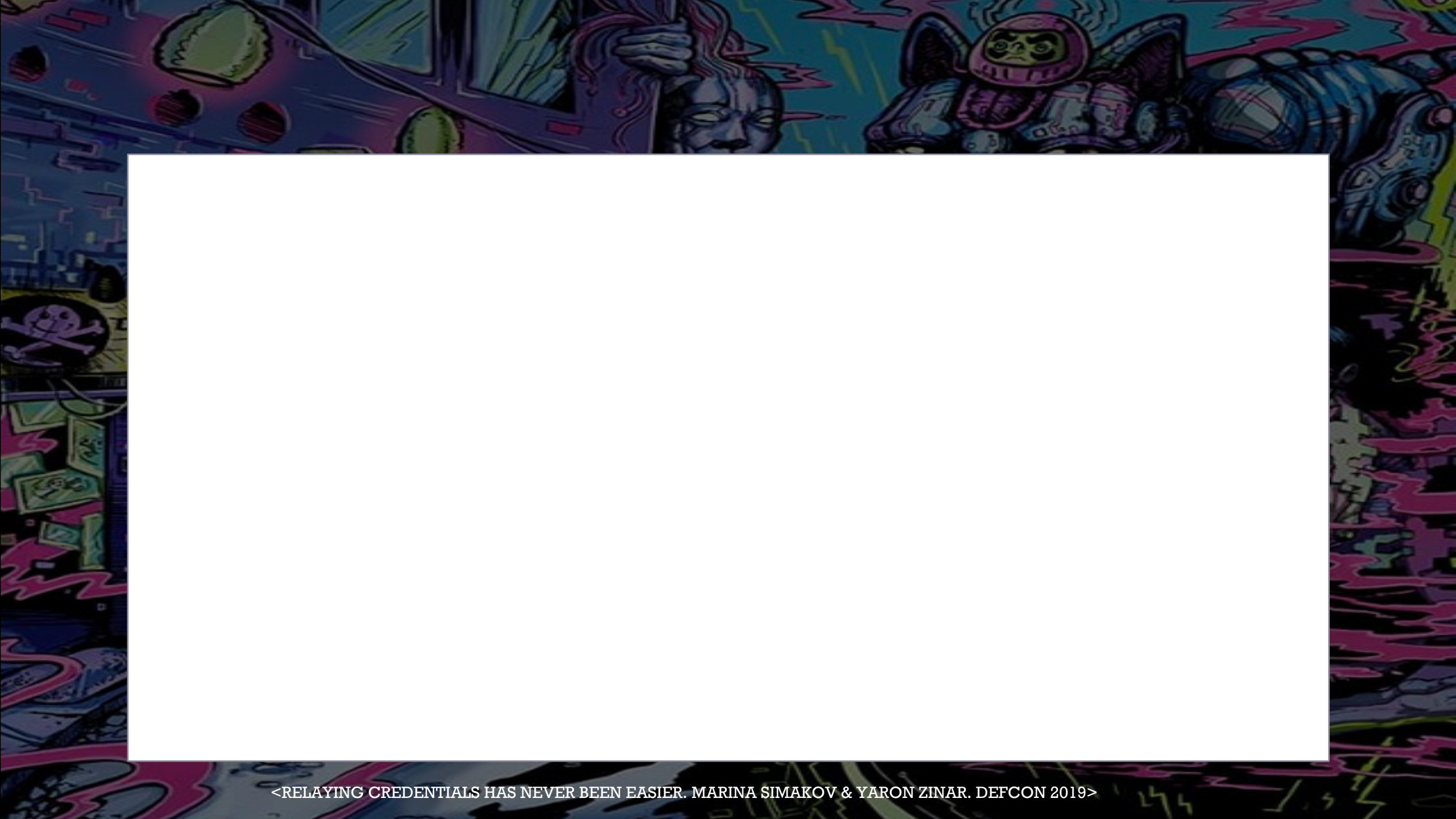
Modified NTLM_AUTHENTICATE:

```
NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  > Lan Manager Response: 0000000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 0000000000000000
  > NTLM Response: b0eea4395eea94869ae86aef3e7f72d10101000000000000...
  > Domain name: PREEMPT
  > User name: user01
  > Host name: TEST-01
  > Session Key: 30002e0030002e003300390000000000
  > Negotiate Flags: 0xa0880205, Negotiate 56, Negotiate 128, Negotiate Target
```

NTLM: NEW VULNERABILITIES

- EPA (Enhanced Protection for Authentication) bypass





<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

NTLM: NEW VULNERABILITIES

- EPA bypass - Fix:
  - Servers deny authentication requests which include more than one channel binding value
- Issues:
  - Some clients don't support EPA & don't add a MIC (Firefox on Linux or MacOS)
  - These clients are still vulnerable to the EPA bypass
  - One such client is enough to make the entire domain vulnerable

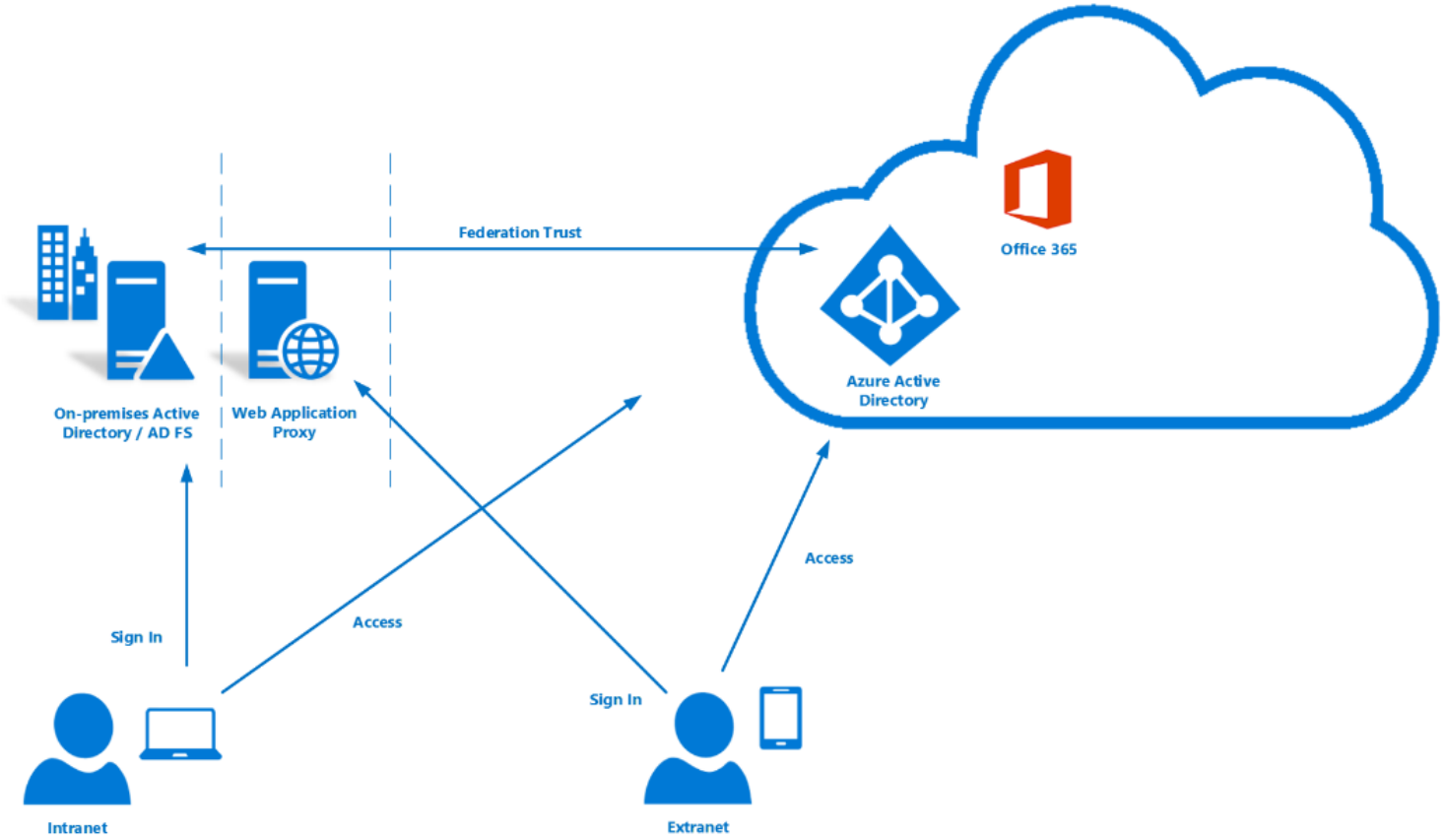


ATTACKING AD-FS

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

ATTACKING AD-FS

- AD-FS Architecture



https://www.sherweb.com/blog/office-365/active-directory-federation-services/

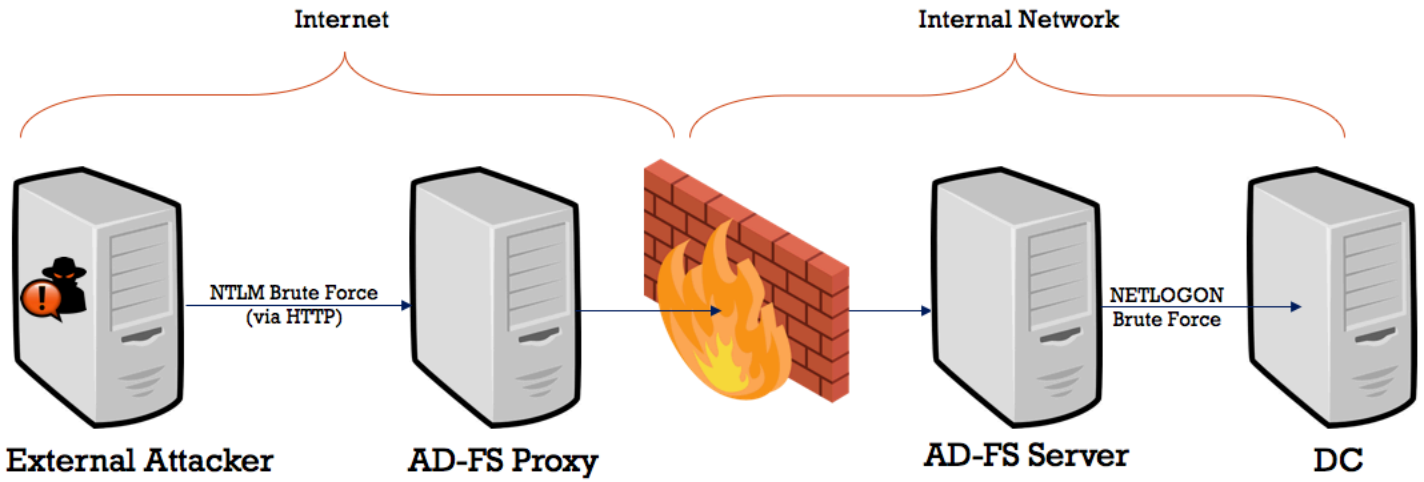
ATTACKING AD-FS

- AD-FS Proxy
  - Open to the internet
  - Easy target for brute-force/password spraying attacks

- External Lockout Policy
  - Locks the user coming from the external network after exceeding the **Extranet Lockout Threshold**
  - Has effect when: **Extranet Lockout Threshold < AD Lockout Threshold**
  - Prevents brute-force-attacks
  - Prevents malicious account lockouts

ATTACKING AD-FS

- WIA (Windows Integrated Authentication)
  - Use Kerberos or NTLM SSO capabilities to authenticate to AD-FS
  - WIA authentications were accepted by the AD-FS proxy
  - **NTLM relay** against the AD-FS proxy from the external network
  - **NTLM authentications** target at the AD FS proxy allowed attackers to bypass the external lockout policy (CVE-2019-1126)



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>

ATTACKING AD-FS

- WIA (Windows Integrated Authentication)
  - **Kerberos authentications** allowed attackers to brute-force the AD-FS service account's password
  - Generate service tickets using different passwords and send to AD-FS proxy
  - If password is successfully guessed -> log into cloud resources using any desired privileges
  - No logs generated for unsuccessful attempts
  - **Reverse-Kerberoasting!**

<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>



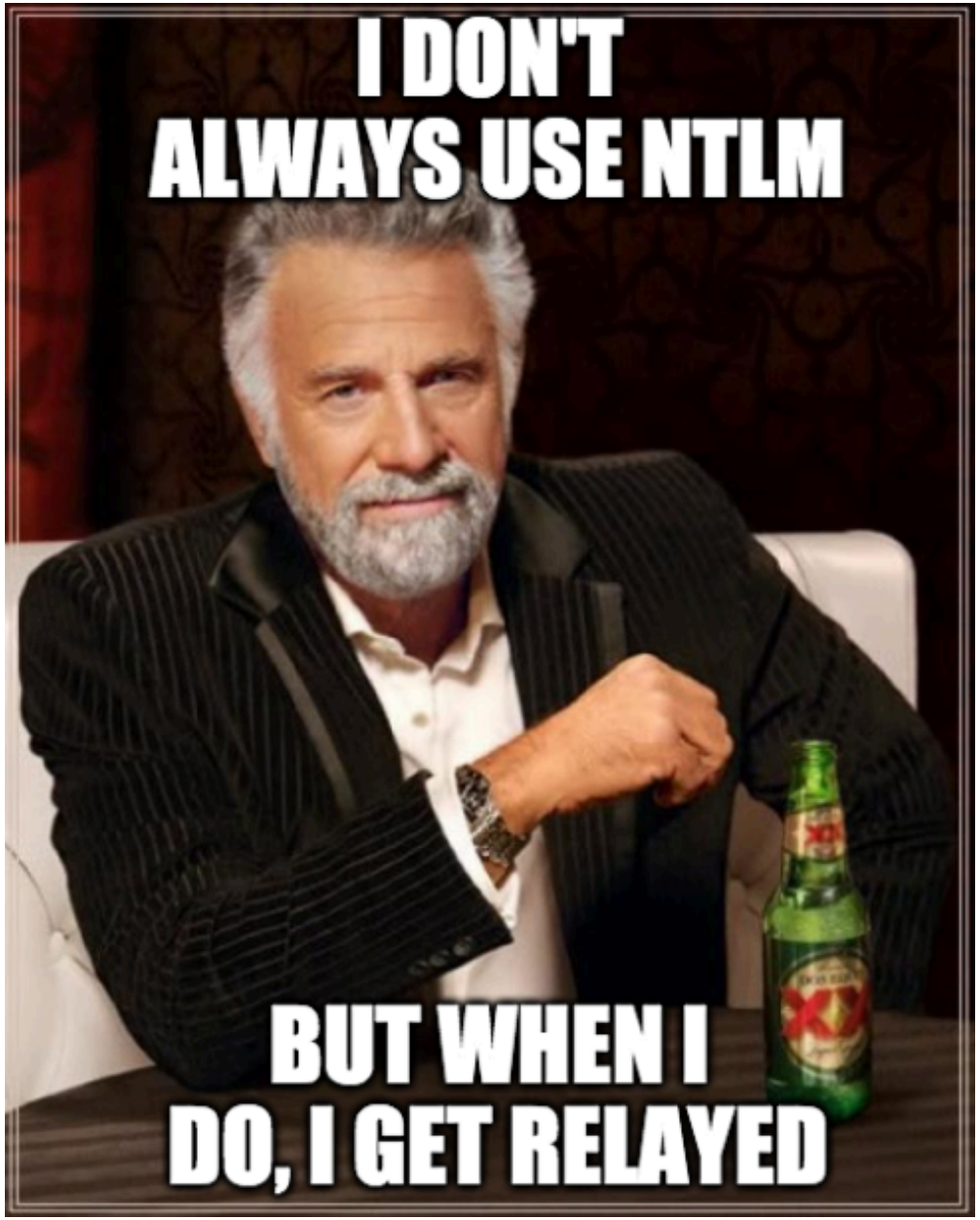
TAKEAWAYS

TAKEAWAYS

- Patch all vulnerable machines!
- Restrict NTLM usage as much as possible
  - NTLM authentication is susceptible to NTLM relay attacks
  - Always prefer Kerberos usage
- Disable NTLMv1 in your environment
  - Configure the GPO 'Network security: LAN Manager authentication level' to: 'Send NTLMv2 response only. Refuse LM & NTLM'
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level
- Incorporate NTLM relay mitigations:
  - SMB & LDAP signing
  - LDAP channel binding
  - EPA

CREDITS

- The Preempt Research Team
  - Eyal Karni (@eyal_karni)
  - Sagi Sheinfeld
- Alberto Solino (@agsolino)
  - Some of the vulnerabilities are merged into impacket!
  - https://github.com/SecureAuthCorp/impacket



<RELAYING CREDENTIALS HAS NEVER BEEN EASIER. MARINA SIMAKOV & YARON ZINAR. DEFCON 2019>


THANK YOU!