Its Just Kerberos Delegation, Trust me.....

Darryl G. Baker, CISSP, CEH

@DFIRDeferred

Security Consultant @ Trimarc Security

Spec Ops Army Veteran

Microsoft Identity Specialist

Team Purple

Creator of Identity Security Village

Ham Radio Extra

Agenda

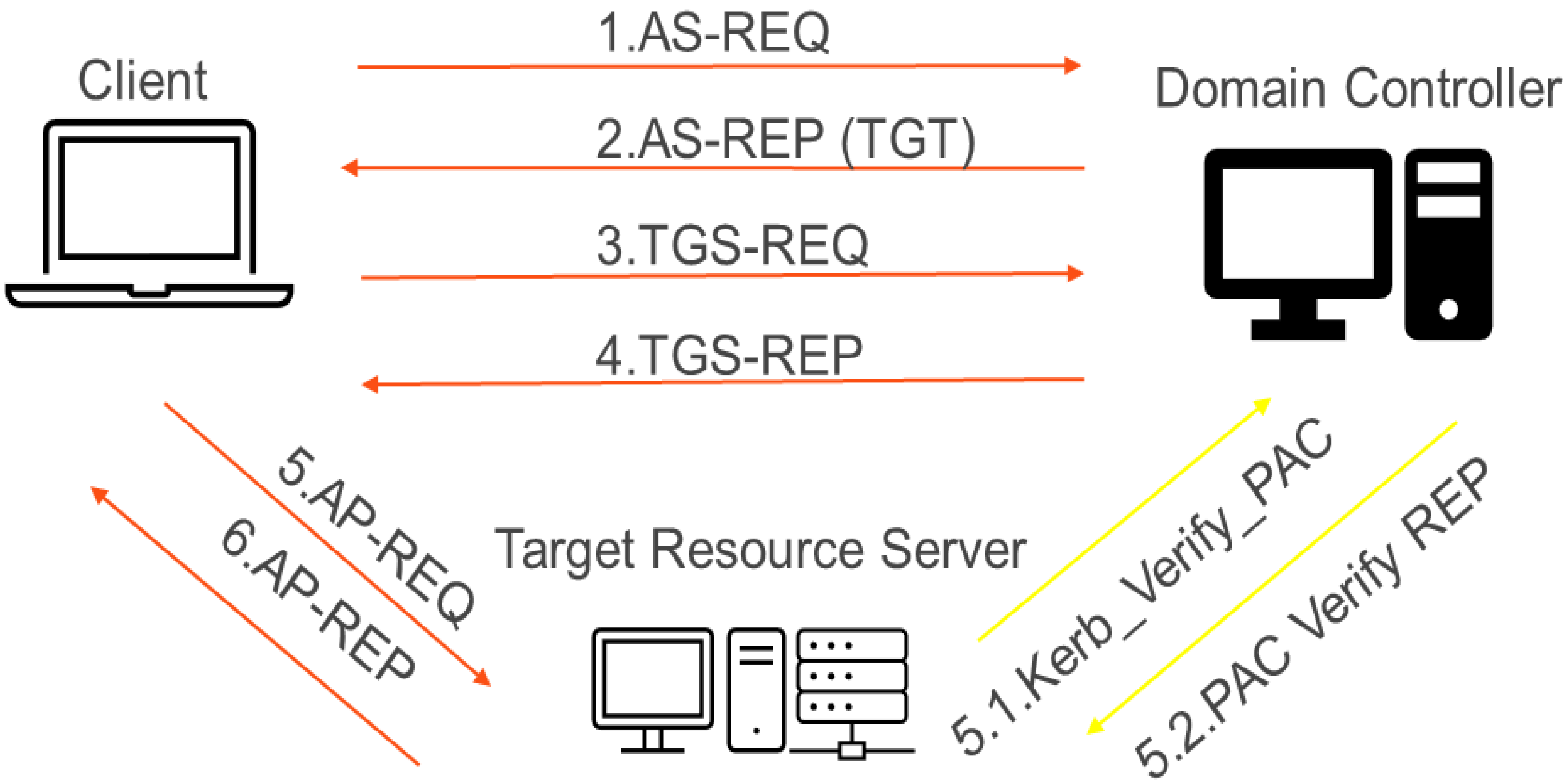
- Kerberos Authentication
- Types of Kerberos Delegation
- “Trending” Kerberos Delegation Attacks
- KrbRelayUp
- Delegation Behavior Across AD Trusts
- Attack Vectors for Delegation in Hybrid AD
- Mitigations

What is Kerberos?

Kerberos Authentication

- Kerberos is a computer-network authentication protocol. It uses a ticket paradigm based on secret-key cryptography and a trusted third party. This allows for trusted hosts authenticate securely over insecure networks.
- Preferred Authentication method for Windows Domains.
- Before Windows, Microsoft used NTLM for authentication. NTLM is still used for authentication when either sever or client is not domain joined (although Kerberos and be strictly configured).

Kerberos Authentication and Delegation



Privileged Attribute Certificate

- **When a user requests a TGT, the PAC is included with it (containing the user’s security information). The PAC is signed by Key Distribution Center (KDC) on the DC so it cant be tampered with. When the user requests a Service Ticket, the KDC validates the signature of the PAC in the user's TGT and copies it into the Service Ticket that is then sent to the user. When the user authenticates to a service, the service validates the signature of the PAC and uses the data in the PAC to create a logon token for the user.**

- **[HKLMSYSTEMCurrentControlSetControlLsaKerberosParameters]**
  - 0- Disabled — Reverts the update
  - **1- (default)Deployment — Adds the new PAC. If an authenticating user has the new PAC structure, the authentication is validated.**
  - 2- Enforcement — Adds the new PAC. Old PAC structures will be denied

What is Kerberos Delegation in AD??

Delegation == Impersonation

ATTACK VECTORS
ATTACK VECTORS EVERYWHERE
imgflip.com

Types Kerberos Delegation

- **Unconstrained Delegation**
  - Enables an object to impersonate ANY other object when requesting access to ANY target resource
  - TGT from impersonated user is forwarded
- Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties trustedfordelegation,serviceprincipalname,description
- If an attacker can get admin access to this computer, they can use tools like Mimikatz to dump all TGT’s in the computer memory hoping to find one belonging to a user with elevated domain permission. The attacker then “Passes the Ticket” of the elevated user and requests service tickets on the user’s behalf to any other resource in the domain.

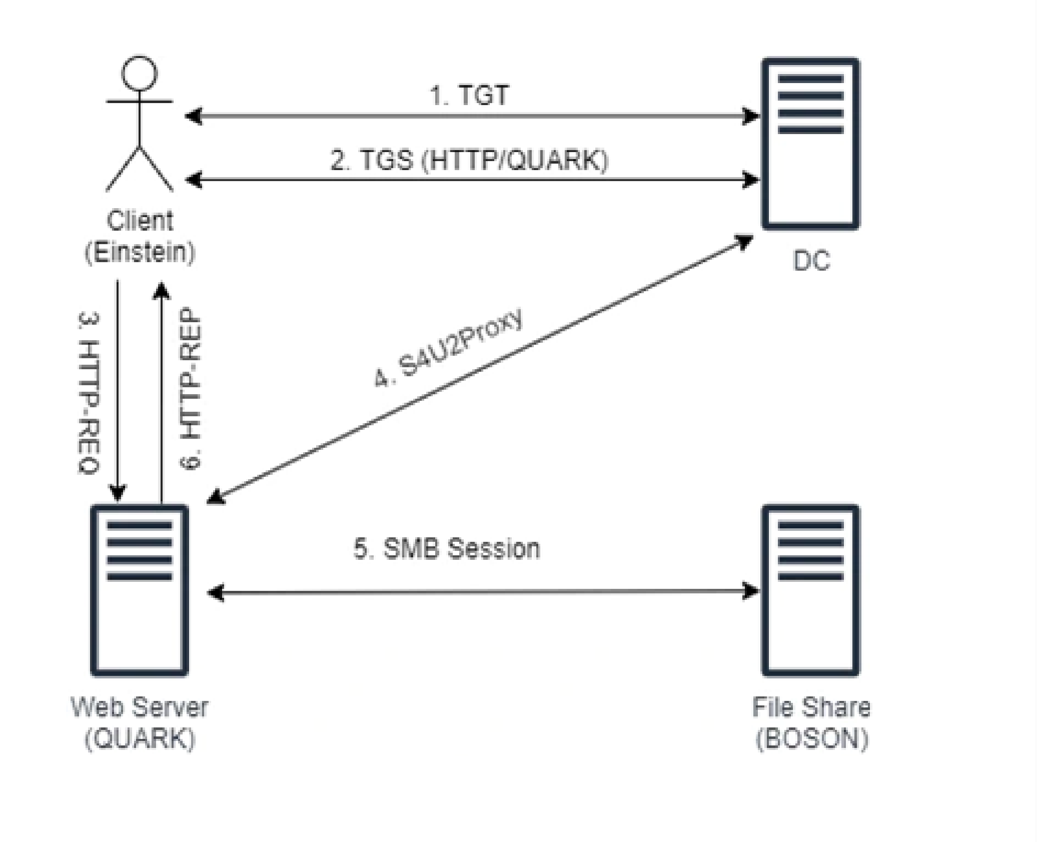
Kerberos Constrained Delegation

- Called for the Service-For-User Extensions
  - TGT’s are not forwarded. TGS plus S4U extensions are forwarded to request service tickets. These two extensions are S4U2Proxy and S4U2Self.

- Constrained Delegation falls into 3 subtypes
  - Kerberos Constrained Delegation (KCD)
  - Kerberos Constrained Delegation with Protocol Transition
  - Resource Based Constrained Delegation (RBCD)

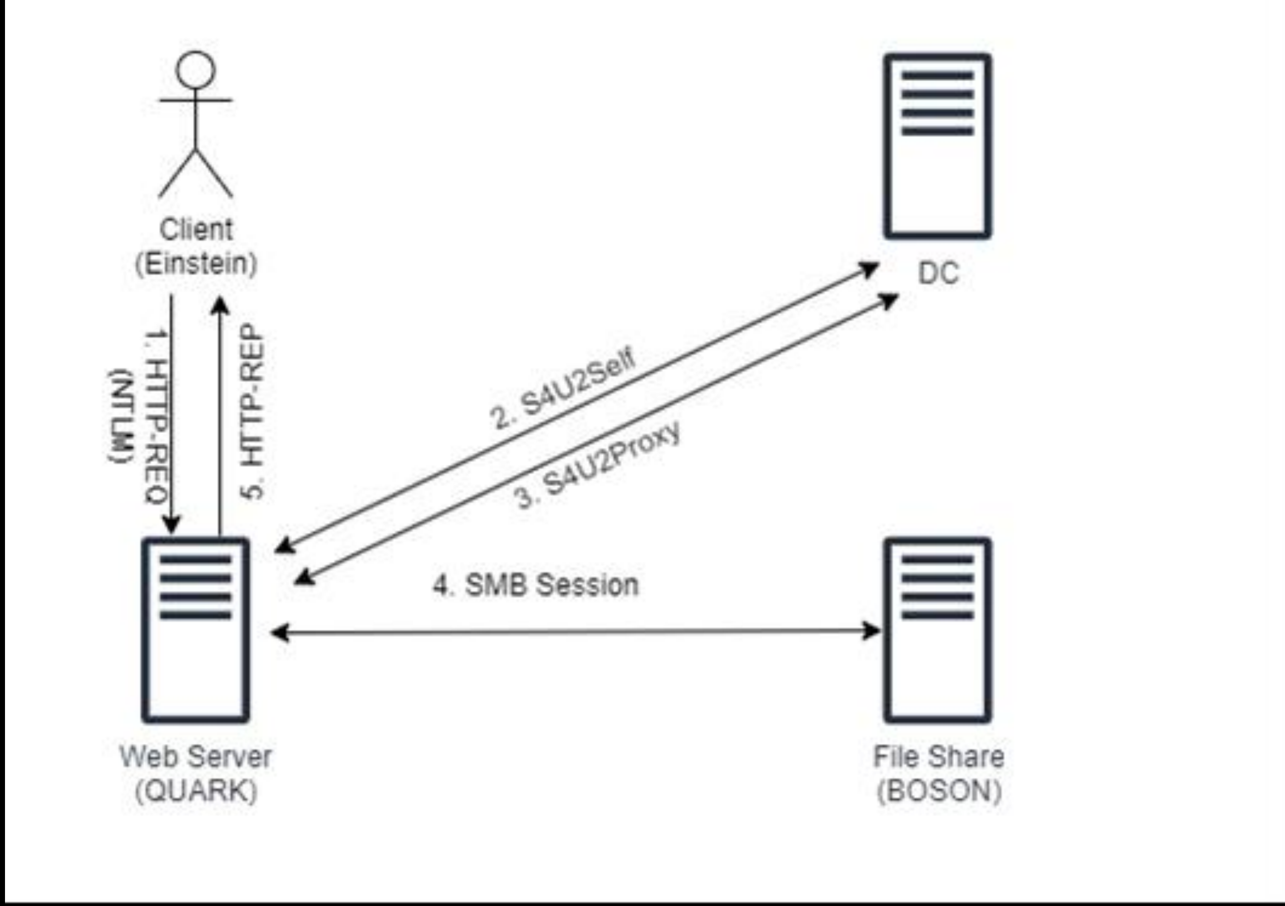
Constrained Delegation

- Considered the most secure type of Delegation due to control of constraints
- **Msds-allowedtodelegateto** attribute
- **S4U2Proxy**
  - Allows a service to send a valid TGS to KDC and request TGS to another service



Constrained Delegation w/ Protocol Transition

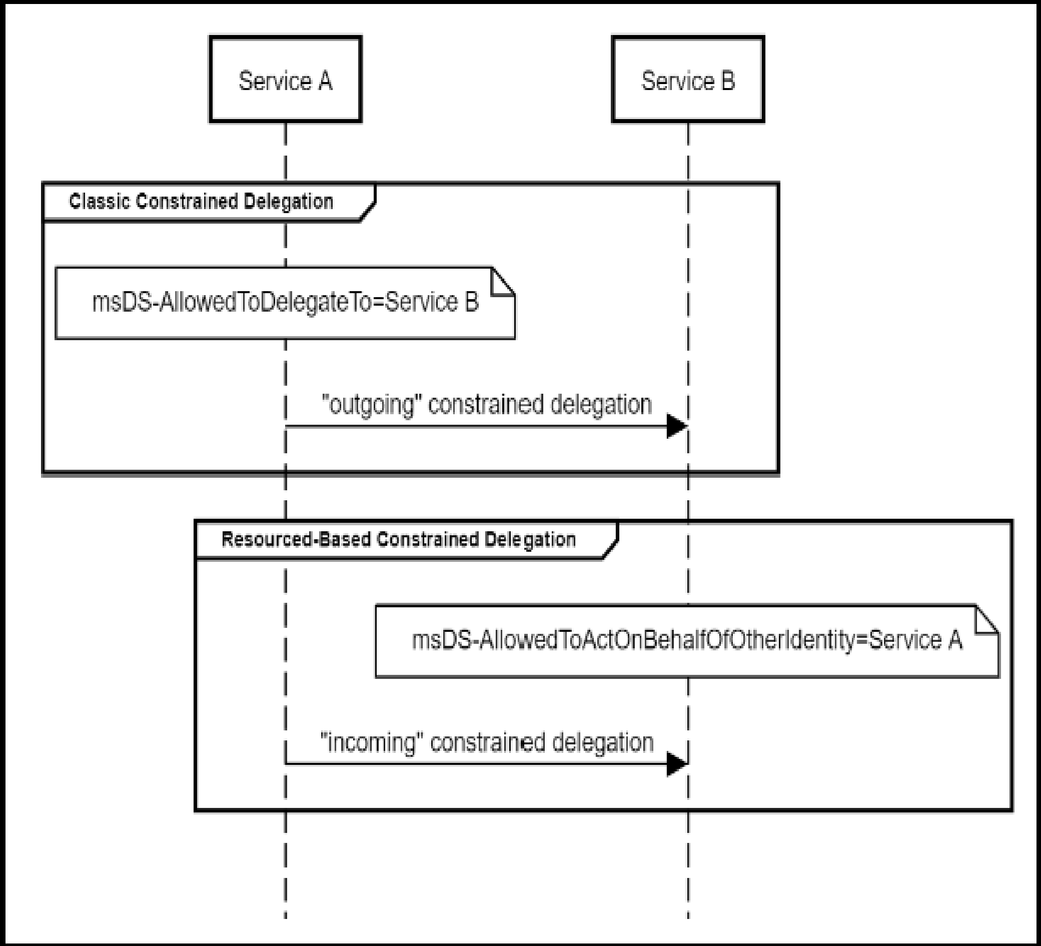
- Used when initial authentication is not Kerberos; NTLM for example.
- **TRUSTED_TO_AUTH_FOR_DELEGATION**
- **S4U2Self**
  - S4U2Self allows a service to request a TGS to itself. Then use this TGS with S4U2Proxy to request TGS to another service.



Note: the initial authentication of the client is not verified by the KDC

Resource Based Constrained Delegation

- **msDS-allowedToActoOnBehalfOfOtherIdentity**
- Does not require the TrustedToAuthForDelegation
- Transfers the ability to configure constrained delegation for the service from the domain administrator to the service administrator.
- Configured directly on the target resource object.
- Any user with write access to a computer object can configure RBCD on that object.


Service A
Service B
Classic Constrained Delegation
msDS-AllowedToDelegateTo=Service B
"outgoing" constrained delegation
Resourced-Based Constrained Delegation
msDS-AllowedToActOnBehalfOfOtherIdentity=Service A
"incoming" constrained delegation

THEY TOLD ME I COULD BE ANYTHING I WANTED
SO I BECAME A DOMAIN CONTROLLER
imgflip.com

Interesting Trends in KCD Attacks

- SPN Modification
  - Kerberos uses SPNs to identify the security principal of a service or application. An SPN consists of either two parts or three parts. The first part is the service class, the second part is the host name, and the third part (if present) is the domain name
  - The target service can validate inbound service tickets because they are encrypted with the hash of the service account's password. The SPN is not validated in this process and the SPN is part of the unencrypted part of the ticket.
  - This means an attacker who has compromised a system with KCD configured, can modify the service portion of the SPN to authenticate to another service on the resource. For instance:
  - **Cifs**/targetmachine.domain.corp

Can be replaced with:

https/targetmachine.domain.corp

With intentions to RCE via WinRM

Trending RBCD Attacks

- Why RBCD?
  - Write privileges to a computer object are all that is needed to configure RBCD
  - Default Machine Account Quota Settings allow for users to create 10 domain computer objects (with write access).
  - Privilege Escalation is typically the goal of this attack.

1. An attacker configure RBCD on a machine 1 which they have write access to.

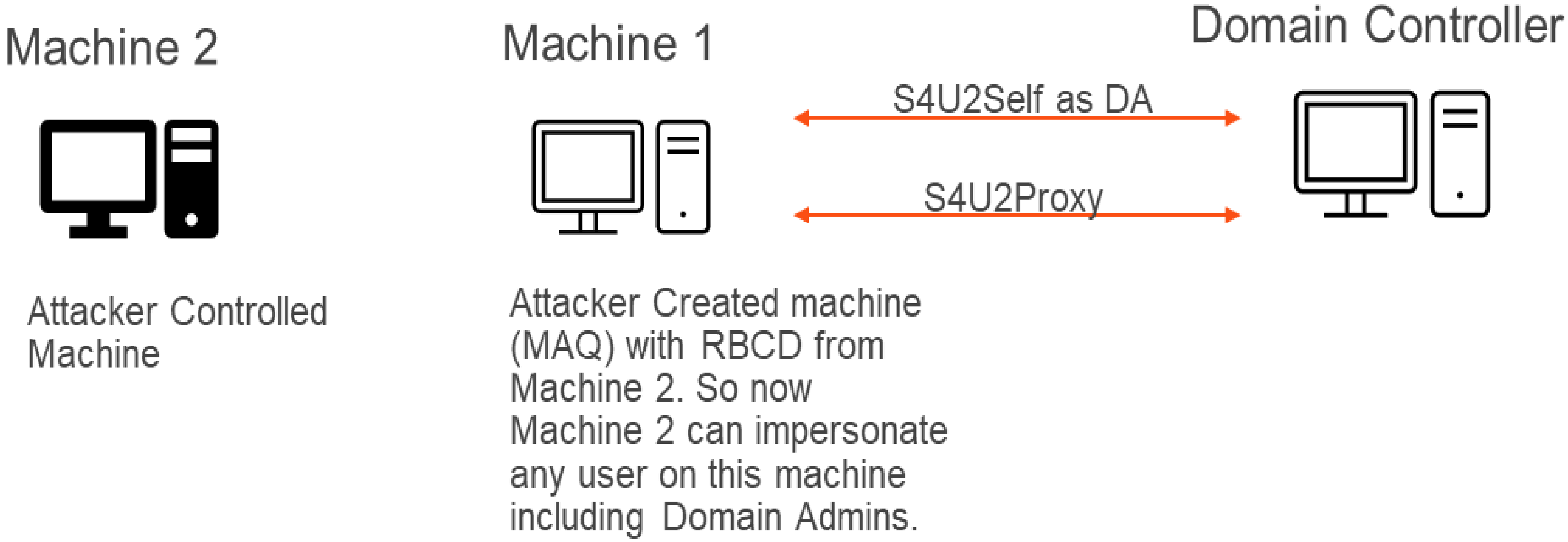
2. Another attacker-controlled machine, machine 2, is added to the machine 1’s msDS-AllowedToActOnBehalfOfOtherIdentity attribute, meaning that machine 2 can impersonate any user (including domain admins) on machine 1.

3. Using a tool like Rubeus the attacker can request an S4U2Self on behalf of machine two impersonating a domain admin.

4. Then, the S4U2Self would be used to request an S4U2Proxy back to itself as an elevated user

PWN.

Example of a RBCD PrivEsc Attack



Machine 2

Machine 1

Domain Controller

S4U2Self as DA

S4U2Proxy

Attacker Controlled Machine

Attacker Created machine (MAQ) with RBCD from Machine 2. So now Machine 2 can impersonate any user on this machine including Domain Admins.

KrbRelayUp

YOU GOT THE RIGHT STUFF
KrbRelay
PowerMad
Rubeus
ADCSPwn
Whisker
NEW KID ON THE BLOCK
memegenerator.net

KrbRelayUp

- KrbRelayUp- enables attackers to gain SYSTEM privileges on Windows systems with default configurations.
- An LDAP relay is part of this attack in environments when LDAP signing is not configured.
- The lack of LDAP signing is not required for environments where Extended Protection for Authentication (EPA) for Active Directory Certificate Services (AD CS) is not enabled.

0. (Optional) New machine account creation (New-MachineAccount)

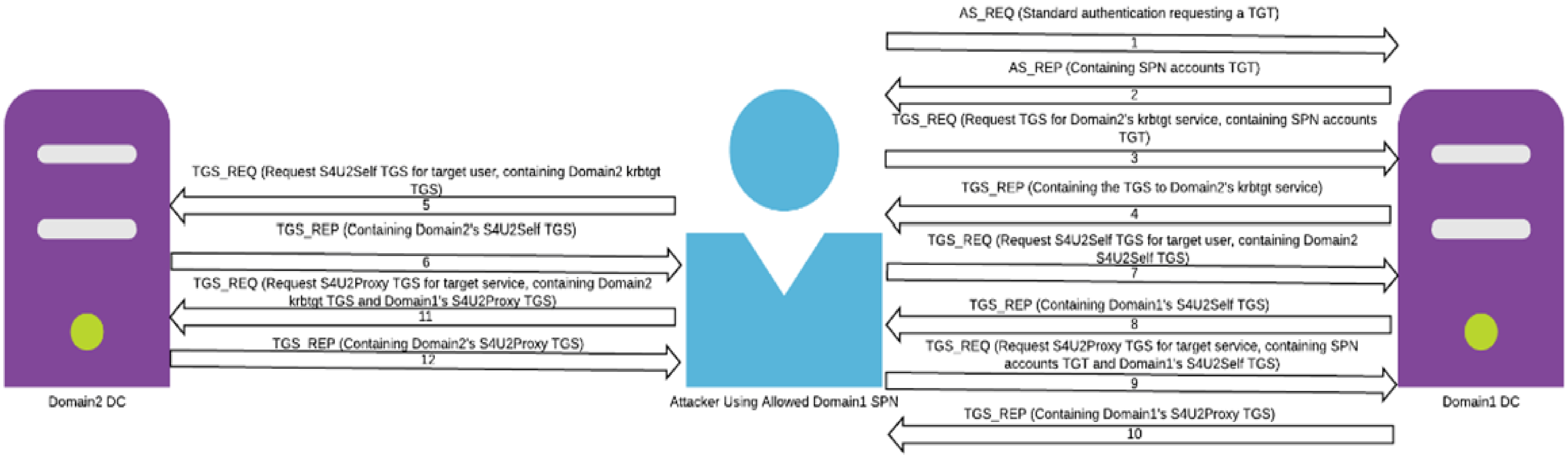
1. Local machine account auth coercion (KrbRelay)

2. Kerberos relay to LDAP (KrbRelay)

3. Add RBCD privs and obtain privileged ST to local machine (Rubeus)

4. Using said ST to authenticate to local Service Manager and create a new service as NT/SYSTEM. (SCMUACBypass)

Delegation Behavior Across AD Trusts



1 AS_REQ (Standard authentication requesting a TGT)

2 AS_REP (Containing SPN accounts TGT)

3 TGS_REQ (Request TGS for Domain2's krbtgt service, containing SPN accounts TGT)

4 TGS_REP (Containing the TGS to Domain2's krbtgt service)

5 TGS_REQ (Request S4U2Self TGS for target user, containing Domain2 krbtgt TGS)

6 TGS_REP (Containing Domain2's S4U2Self TGS)

7 TGS_REQ (Request S4U2Self TGS for target user, containing Domain2 S4U2Self TGS)

8 TGS_REP (Containing Domain1's S4U2Self TGS)

9 TGS_REQ (Request S4U2Proxy TGS for target service, containing SPN accounts TGT and Domain1's S4U2Self TGS)

10 TGS_REP (Containing Domain1's S4U2Proxy TGS)

11 TGS_REQ (Request S4U2Proxy TGS for target service, containing Domain2 krbtgt TGS and Domain1's S4U2Proxy TGS)

12 TGS_REP (Containing Domain2's S4U2Proxy TGS)

The Work of Charlie Clark (exploit.ph)

Steps Of Cross-Trust KCD

1. The first step is still the same, a standard Kerberos authentication with the **local** domain controller. (1 and 2)
2. A service ticket is requested for the **foreign** domains krbtgt service from the **local** domain controller. (3 and 4)
3. A service ticket for *yourself* as the target user you want to impersonate is requested from the **foreign** domain controller. (5 and 6)
4. A service ticket for *yourself* as the user you want to impersonate is now requested from the **local** domain controller. (7 and 8)
5. A service ticket for the target service (on the **foreign** domain) is requested from the **local** domain controller. (9 and 10)
6. A service ticket for the target service is requested from the **foreign** domain controller. (11 and 12)

Full proof of concept here: https://exploit.ph/crossing-trusts-4-delegation.html

Summary Of Cross-Trust KCD Vulnerabilities

In a domain that has taken steps to make attacking Kerberos delegation harder, such as setting the machine account quota to 0, if a trust is in place with another, less secure domain, constrained delegation attacks could still be possible.

“a chain is no stronger than its weakest link”

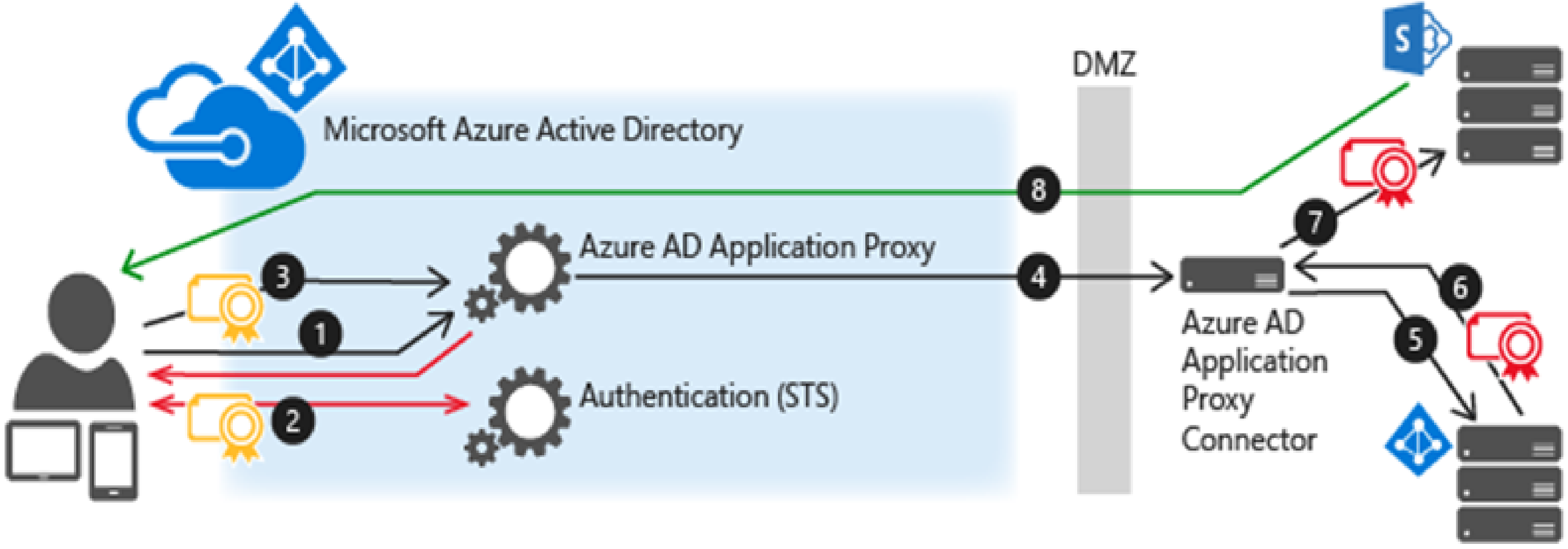
-Thomas Reid

Attack Vectors for Delegation in Hybrid AD

- Azure AD VMs joined to on-premise Domain Controllers
  - Vulnerable to KrbRelup, and other KCD attack methods
- Synchronized Accounts configured for Azure Global Administrator or Intune Administrator (or any other Azure Admin Role)
  - These Azure Roles have the ability to run scripts as SYSTEM on all Azure AD and hybrid joined devices.

- Application Proxy
  - Azure Application Proxies are connected directly to on-premise Application Proxy connectors which can be configured with KCD.

Attack Vectors for Delegation in Hybrid AD



Microsoft Azure Active Directory
DMZ
Azure AD Application Proxy
Authentication (STS)
Azure AD Application Proxy Connector
S
1
2
3
4
5
6
7
8

Application Proxy Connectors- On-premises applications that use integrated Windows authentication (IWA) that are published through an Azure Application Proxy require a Kerberos ticket for access. Application Proxy uses Kerberos Constrained Delegation to support these applications, by impersonating users to send and receive tokens on their behalf.

Mitigations

- Enable LDAP Signing and Channel Binding
- Enable Extended Protection for Authenticaiton (EPA)
- Set Machine Account Quota to 0
- MS Defender for Endpoint
  - Defender for Endpoint leverages these network signals and looks for suspicious LDAP and Kerberos requests to Active Directory domain controllers to accurately detect attacks using KrbRelayUp
- MS Defender for Identity
  - Suspicious Kerberos delegation attempt by a newly created computer.
  - Suspicious edit of the Resource Based Constrained Delegation Attribute by a machine account (KrbRelayUp).
- Use a SIEM or SOAR to monitor for these activities.

Special Thanks to the hard work and research by:

Charlie Clark

Will Schroeder

Elad Shamir

Benjamin Delpy

Sean Metcalf

Andy Robbins

Mor Davidovich

Thank You!

Questions?