Delegate or Escalate?

The Dangers of Kerberos Delegation

Jared Yeo

CISA, CISM, OSCP, CRTE, Crest (CRT)

Disclaimer

The views, thoughts and opinions expressed in this presentation are my own and do not express the views or opinions of my employer, organization, committee or other group of individual.

Do not implement any suggestions without doing your own due diligence and getting organizational buy in. You know your network better than me.

Acknowledgements

Elad Shamir (@elad_shamir) for the research on Kerberos Delegation
shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html

Benjamin Delpy (@gentilkiwi) for Mimikatz and Kekeo
github.com/gentilkiwi/mimikatz
github.com/gentilkiwi/kekeo

Will Schroeder (@harmj0y) for Rubeus
github.com/GhostPack/Rubeus
www.harmj0y.net/blog/

Lee Christensen (@tifkin_) for discovering “the printer bug” and providing a POC
github.com/leechristensen/SpoolSample

Kevin Robertson (@NetSPI) for Powermad and research on MachineAccountQuota
github.com/Kevin-Robertson/Powermad
blog.netspi.com/machineaccountquota-is-useful-sometimes/

Matan Hart (@machosec) for “Delegate to the Top” whitepaper
blackhat.com/docs/asia-17/materials/asia-17-Hart-Delegate-To-The-Top-Abusing-Kerberos-For-Arbitrary-Impersonations-And-RCE.pdf

MIT and Microsoft for Kerberos
docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-kerberos
web.mit.edu/kerberos/

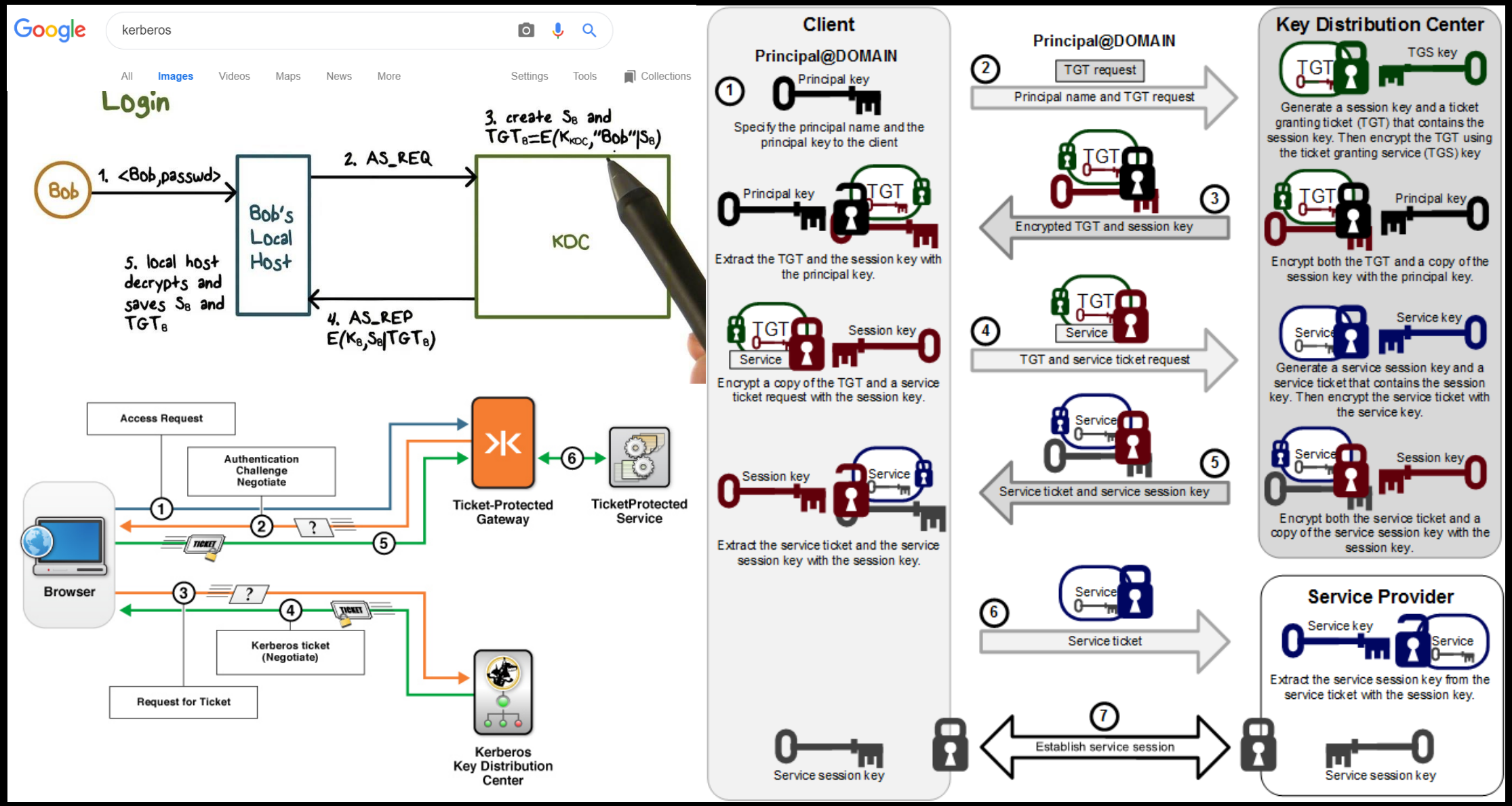
Matt Bush (@3xocyte)
Alberto Solino (@agsolino)
Danyal Drew (@danyaldrew)
Andy Robbins (@_wald0)
Sean Metcalf (@PyroTek3)
Vincent Le Toux (@mysmartlogon)
Many others…

Kerberos Authentication

What?

Kerberos Authentication

What?



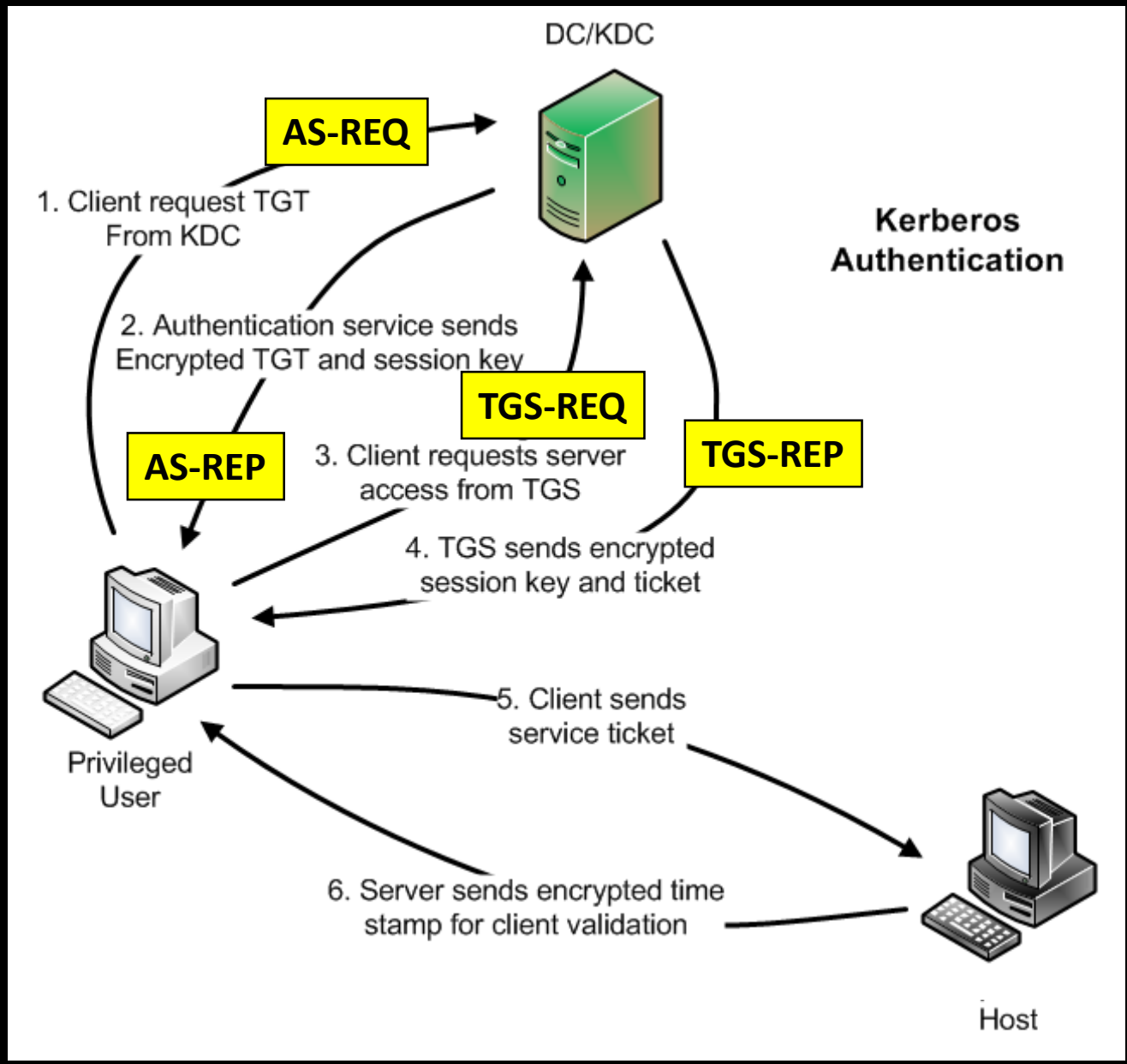
Kerberos Authentication
In a Nutshell

Kerberos comes down to just this

- A protocol for authentication
- Avoids storing passwords locally or sending them over network (uses tickets)
- Key Distribution Center (KDC) authenticates users
- Ticket Granting Server (TGS) provides service tickets to services
- Services are identified by Service Principal Names (**SPN**)
- Built on symmetric-key cryptography (service tickets encrypted)

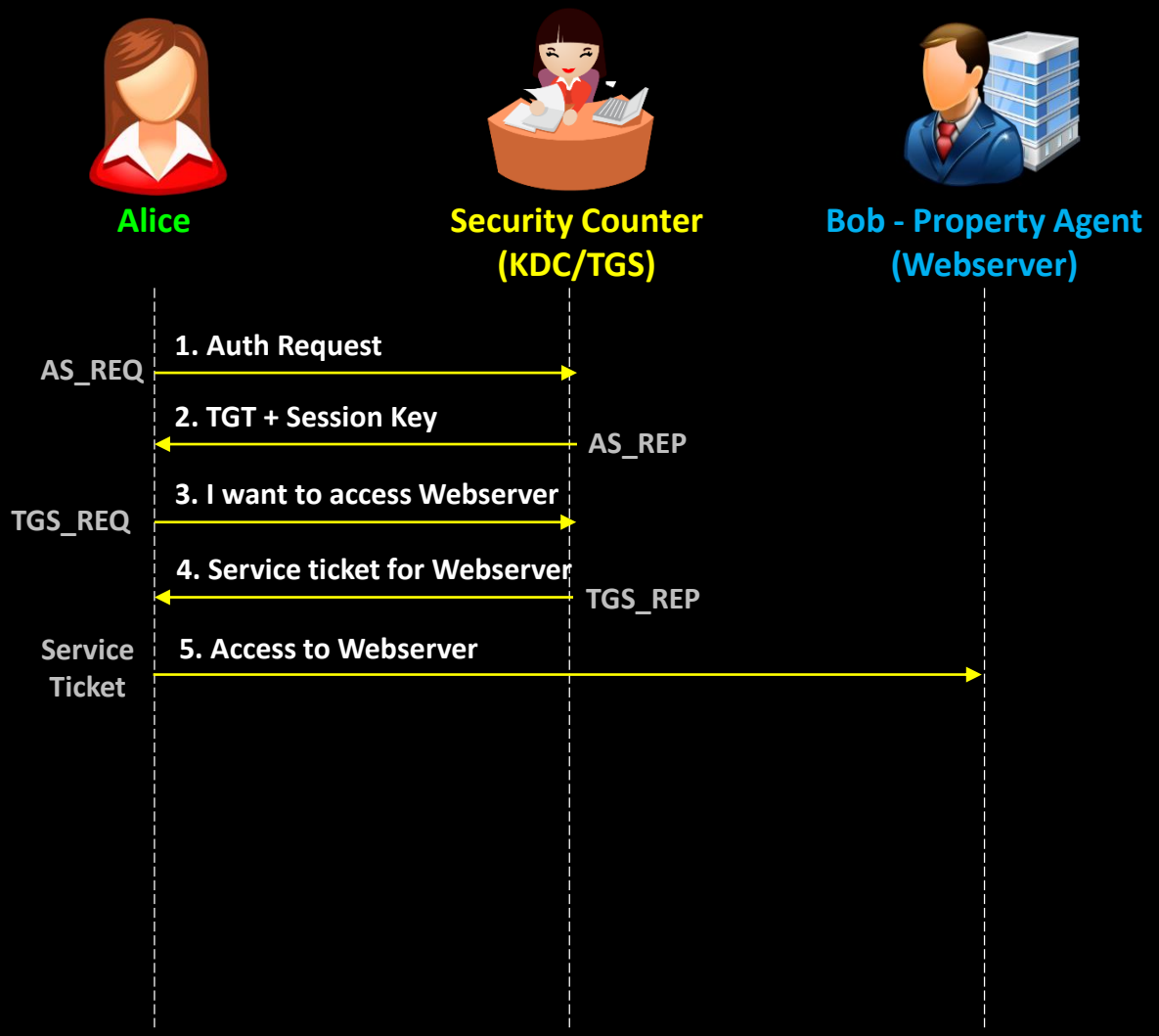
Practical applications

- Single sign on (SSO)
- Delegated authentication



https://www.roguelynn.com/words/explain-like-im-5-kerberos/
https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview
https://digital-forensics.sans.org/blog/2014/11/24/kerberos-in-the-crosshairs-golden-tickets-silver-tickets-mitm-more

Kerberos Authentication
Simplified



Alice wants to buy a property at a realtor.

Alice has an appointment with **Bob** the property agent.

1. **Alice** verifies her identity with **Security**.

2. **Alice** gets a **Visitor Pass**, it contains details of her identity.

Meeting the Property Agent

3. **Alice** shows her **Visitor Pass** to the **Security**, and requests to meet **Bob**.

4. **Security** puts **Alice's** identity in a **Blue Envelope** that only **Bob** can open.

5. **Alice** brings the **Blue Envelope** to **Bob**, who opens it, and determines if **Alice** has an appointment.

Kerberos Authentication

Attacks

Kerberos Authentication

Attacks

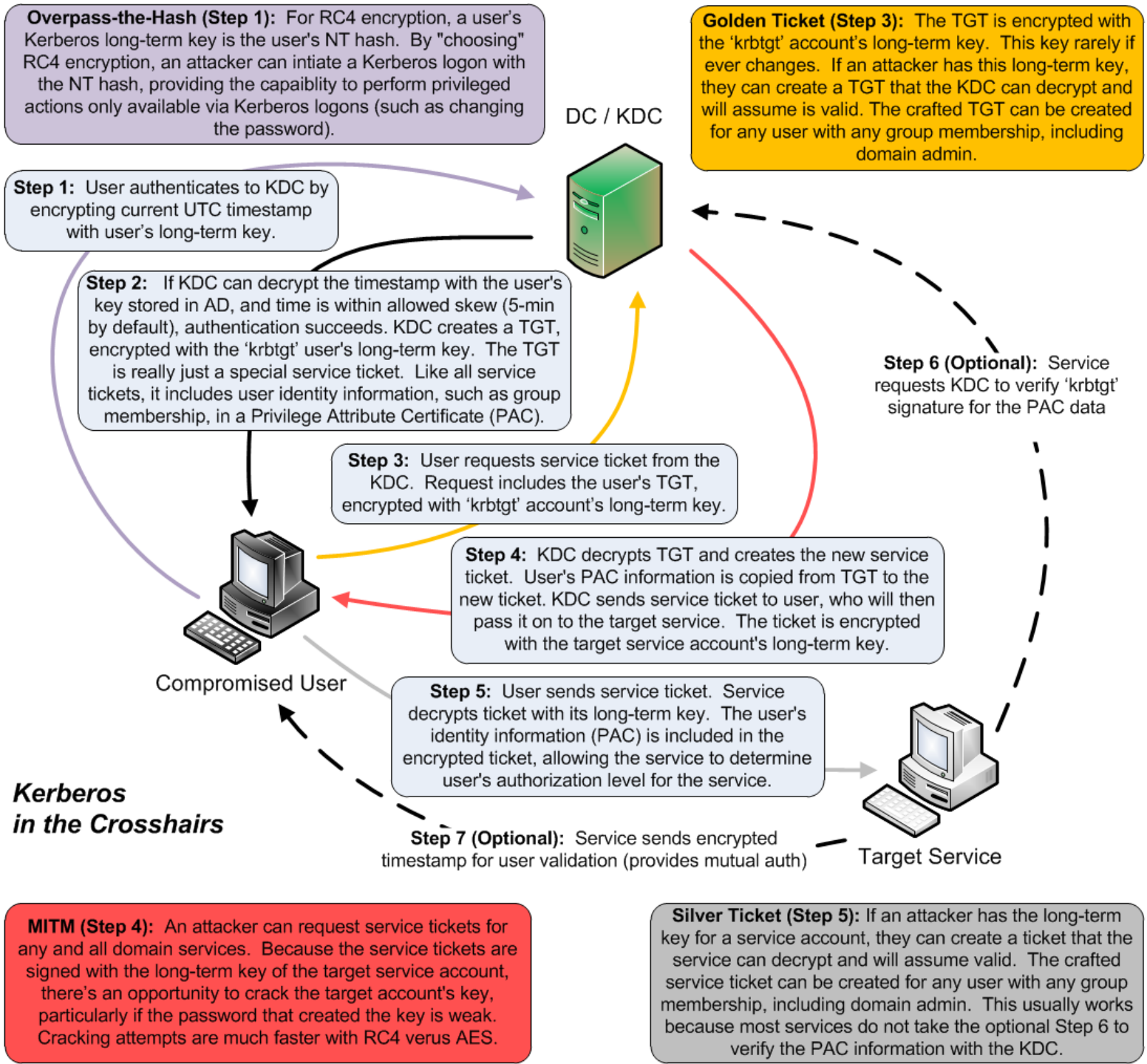
Overpass the Hash
A password or hash is used to create a TGT.

Kerberoasting (T1208)
A service ticket requested and cracked offline.

Pass the Ticket (T1097)
Impersonation of users by using their TGTs.

Service tickets are forged and used to access services (**Silver Ticket**).

TGT's are forged to impersonate any user (**Golden Ticket**).



https://digital-forensics.sans.org/blog/2014/11/24/kerberos-in-the-crosshairs-golden-tickets-silver-tickets-mitm-more

Kerberos Delegation

What? Why?

Kerberos Delegation

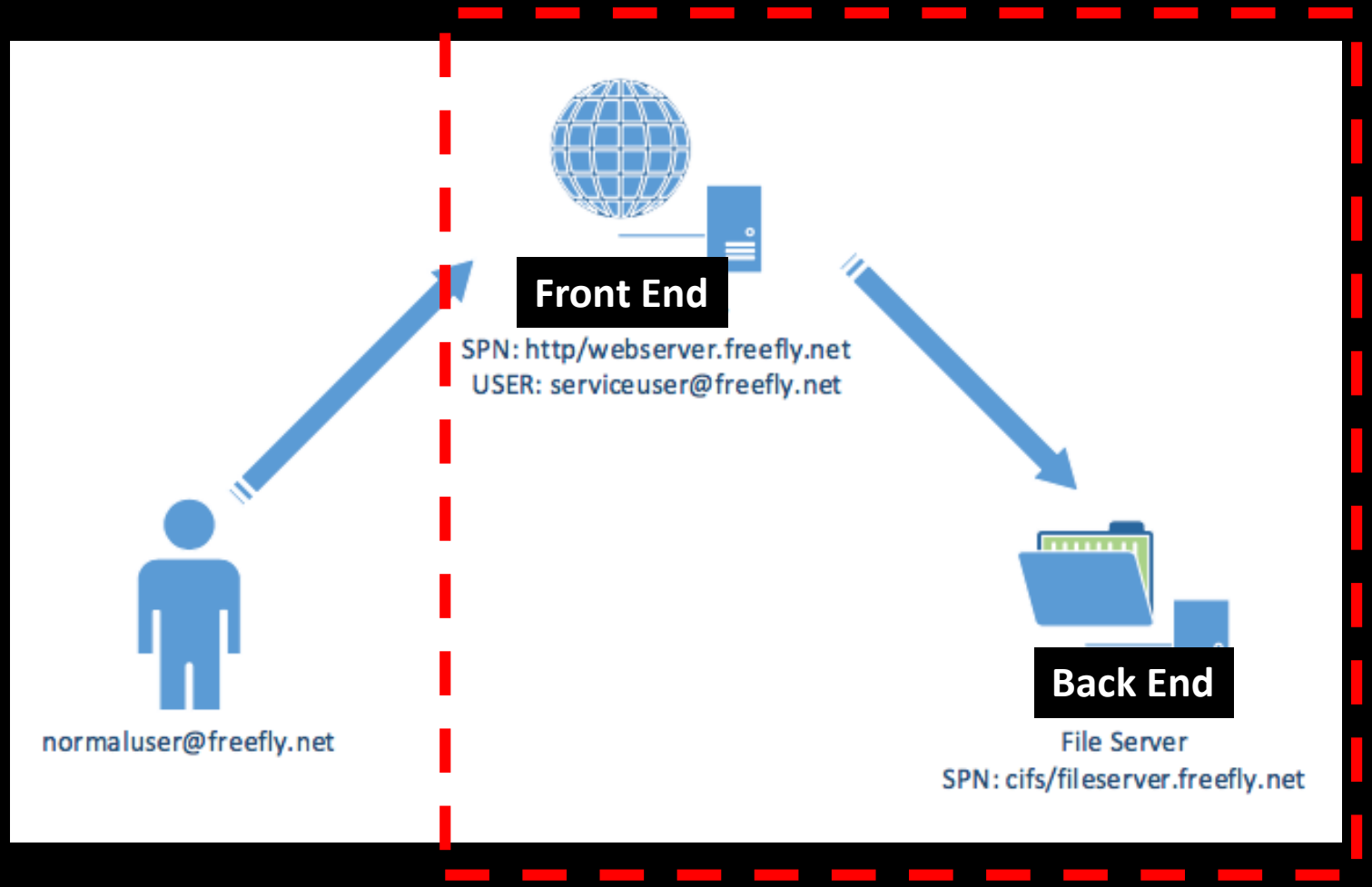
What? Why?

Often, there were legitimate requirements for a service to impersonate the user to access another service.

To facilitate this requirement, delegation features were introduced to the Kerberos protocol.

E.g. normaluser authenticates with Web Server. The web application requires to retrieve content from a File Server as normaluser.

With Kerberos delegation, the Web Server can use normaluser's credentials to retrieve content from File Server.



https://www.secureauth.com/blog/kerberos-delegation-spns-and-more

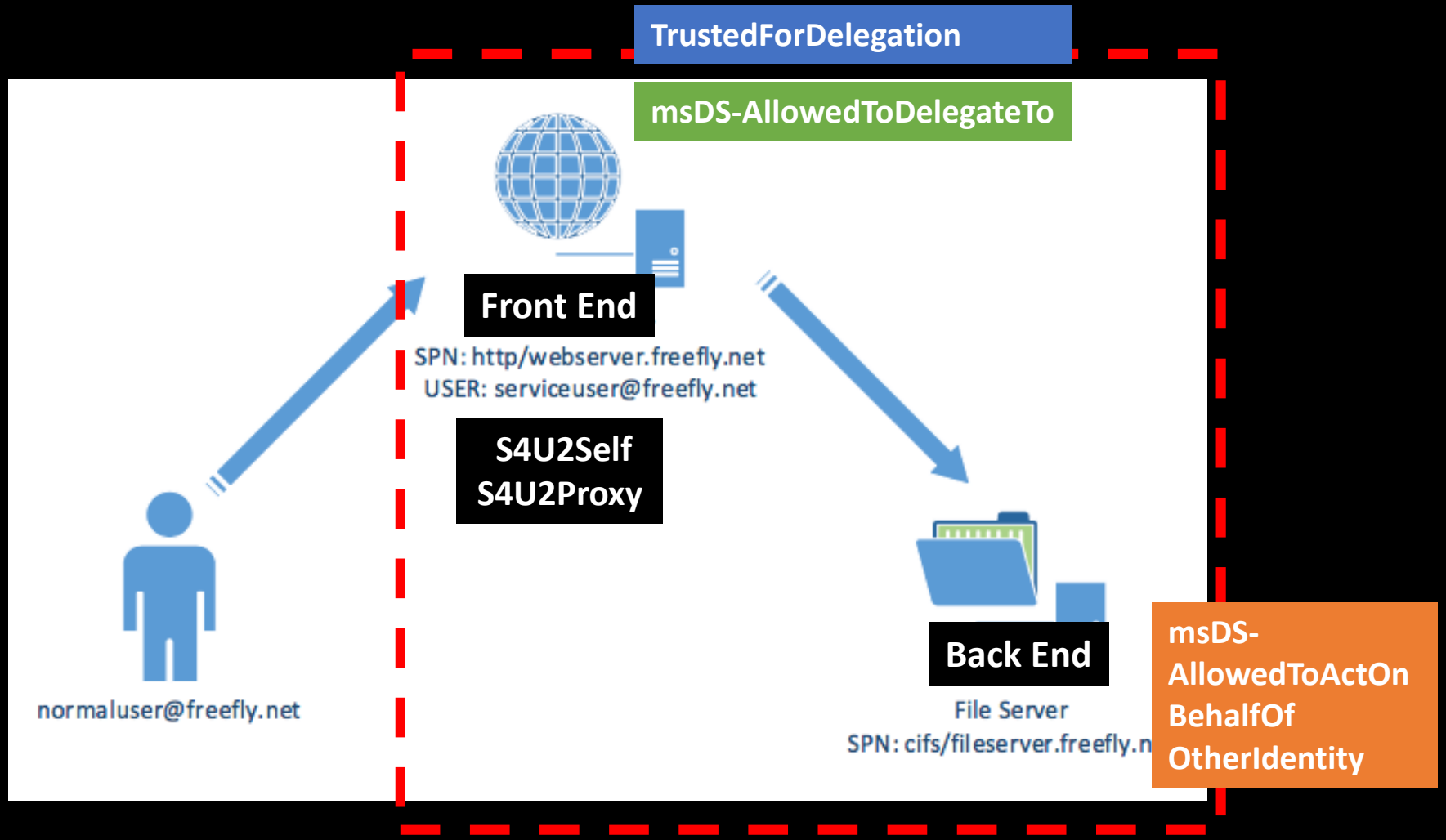
Kerberos Delegation

What? Why?

Unconstrained

Traditional Constrained

Resource Based



https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1

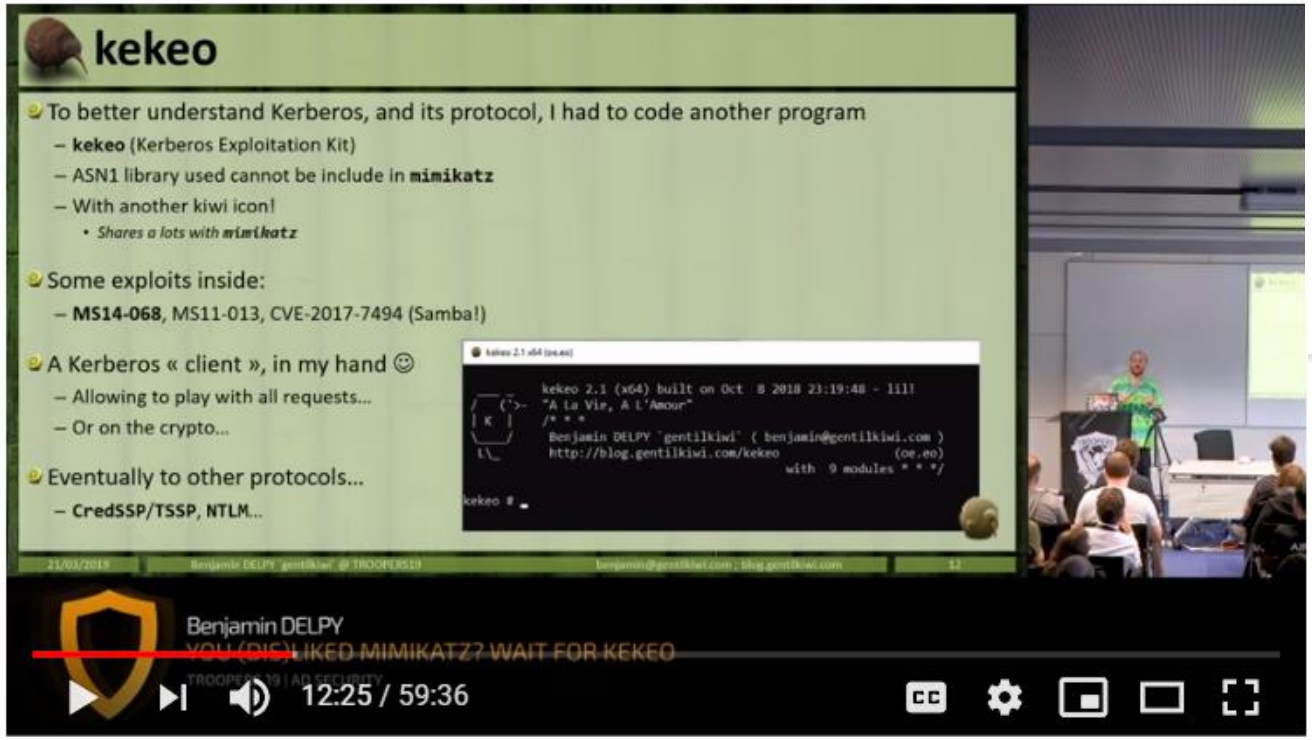
Kerberos Delegation

Weaponization

YouTube SG

Sear

SIGN IN



TR19: You (dis)liked mimikatz? Wait for kekeo

823 views 14 0 SHARE SAVE ...

Benjamin Delpy
@gentilkiwi

Following

New in #kekeo: s4u to make quick and dirty S4U2Self and S4U2Proxy in Windows
github.com/gentilkiwi/kek...
Check your users attributes ;)

Google rebeus kerberos

From Kekeo to Rubeus – harmj0y
https://www.harmj0y.net/blog/redteaming/from-kekeo-to-rubeus/
Sep 24, 2018 - ASN.1 is the encoding scheme used in **Kerberos** traffic, amongst many ... Today I'm releasing **Rubeus**, the start of a C# reimplementation of ...

Rubeus – Now With More Kekeo – harmj0y
https://www.harmj0y.net/blog/redteaming/rubeus-now-with-more-kekeo/
Oct 4, 2018 - **Rubeus**, my C# port of some of features from @gentilkiwi's Kekeo toolset, ... TGTs are opaque blobs encrypted/signed with the **Kerberos** ...

Table of Contents

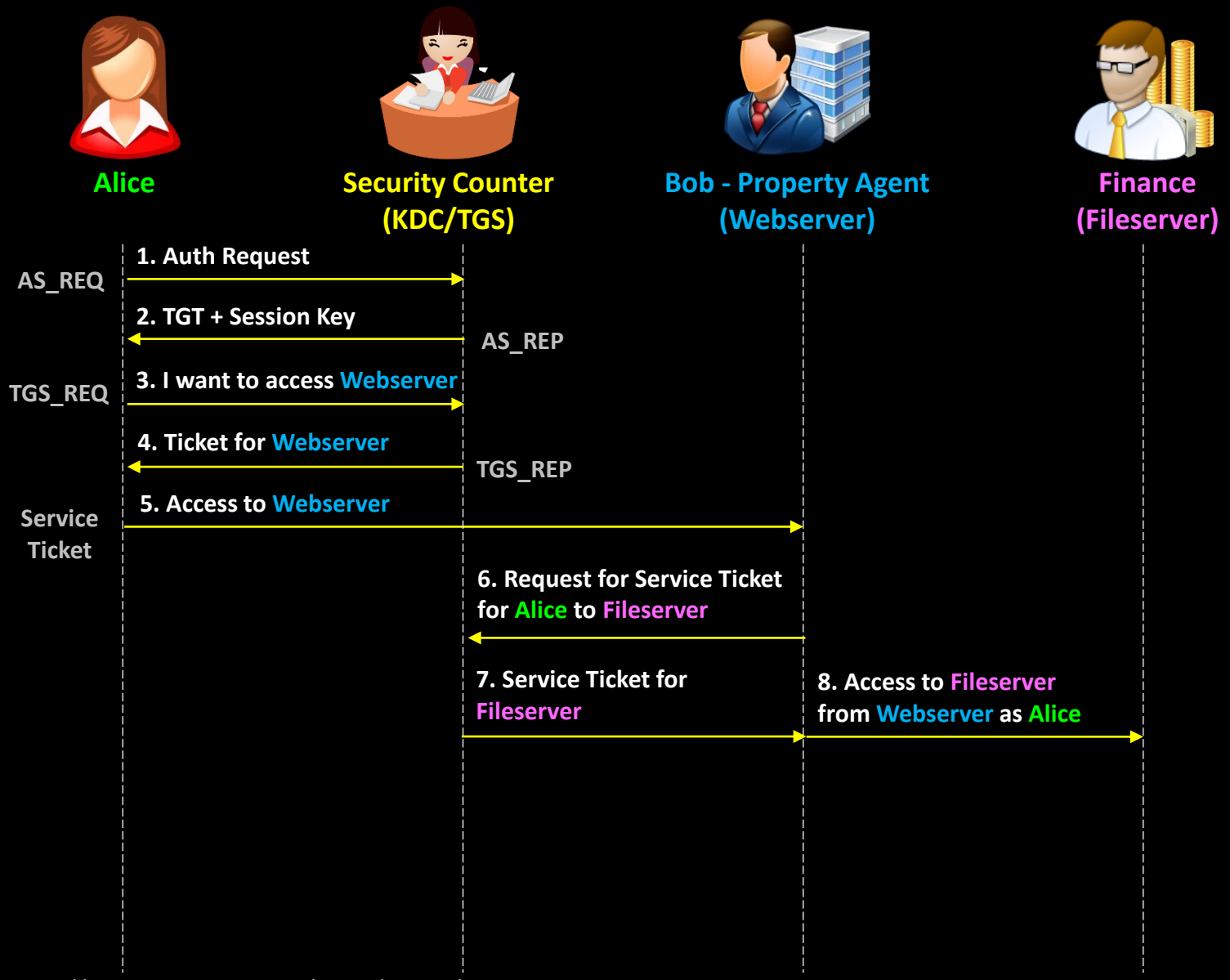
Kerberos Delegation

Unconstrained Delegation

TrustedForDelegation

Kerberos Delegation

Unconstrained Delegation (TrustedForDelegation)



Bob needs to check Alice's financial history with Finance.

Steps 1 to 5 – Same as before.
Bob keeps a copy of **Alice's Visitor Pass.**

6. **Bob** tells **Security**: "I have **Alice's Visitor Pass,** I need to access her data at **Finance**"

7. **Security** puts Alice's identity into a **Pink Envelope** that only **Finance** can open, gives it to **Bob.**

8. **Bob** then brings the **Pink Envelope** to **Finance,** who then opens it, retrieves the finance history of the identity in the envelope (Alice's identity).

https://msdn.microsoft.com/en-us/library/cc246080.aspx

Kerberos Delegation

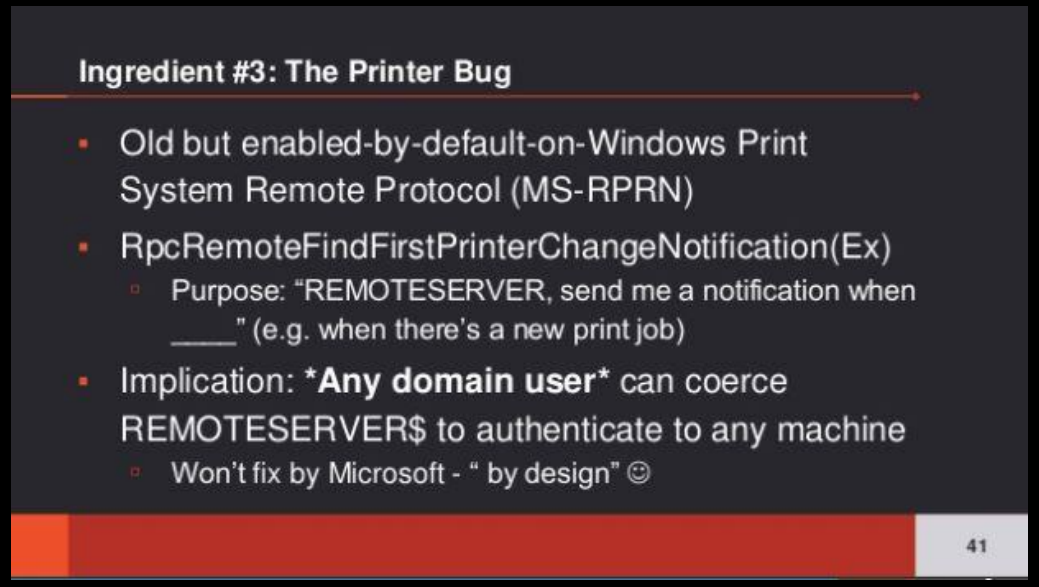
Unconstrained Delegation (TrustedForDelegation)

Webserver (Unconstrained Delegation)
Fileserver

Delegation	Delegation Style	Description
Unconstrained	TGT Forwarding	When a user accesses a server with unconstrained delegation enabled, the user sends their TGT to the server. The server can then impersonate the user by using the user's TGT to authenticate to other services in the network.

If the Webserver becomes compromised

- Adversary can retrieve and use all stored TGT's (anyone who previously authenticated) kept in Webserver's memory and "Pass The Ticket".
- If the domain admin was coerced to authenticate (send credentials) to **Webserver**, "Pass The Ticket" is possible with the domain admin TGT.
- In Oct 2018, Lee Christensen (@Tifkin_) shared that if the Print Spooler service is running, you can force that computer's credentials to be sent to an Unconstrained Delegation server. (The Printer Bug)
- Print Spooler service is running by default on all Windows Servers (including domain controllers).
- Possible to compromise another DC in another forest as well (CVE2019-0683, patched 9 July 2019.



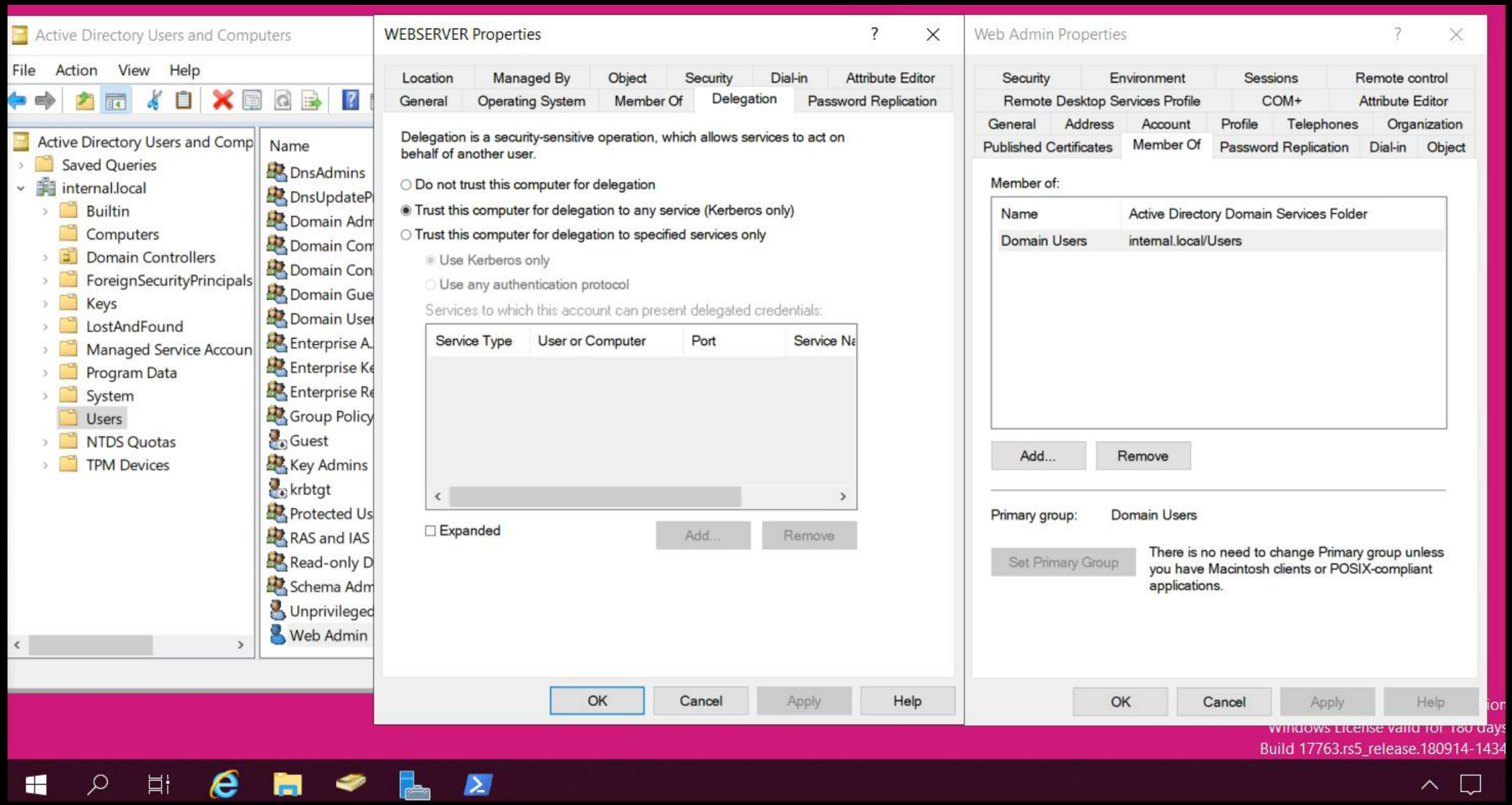
https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/d42db7d5-f141-4466-8f47-0a4be14e2fc1
https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/

Kerberos Delegation

Demo - Unconstrained Delegation

Unconstrained Delegation Server Compromised = Domain Admin Privileges

(The administrator to a server configured with Unconstrained Delegation is effectively the domain administrator.)



https://kerberos.surge.sh/unconstrained.mp4

Kerberos Delegation

Traditional Constrained Delegation (TCD)

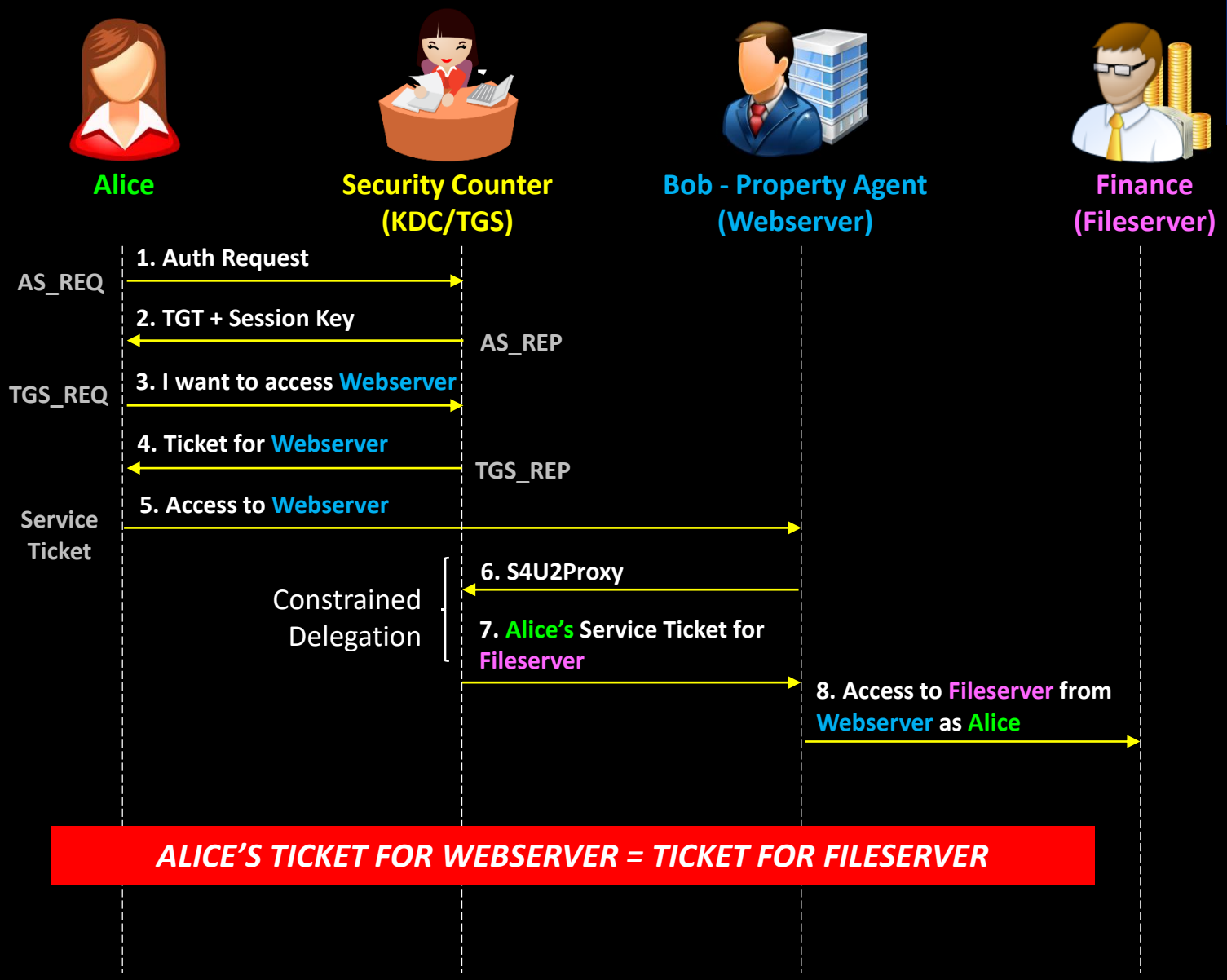
S4U2Proxy

Protocol Transition

S4U2Self / TrustedToAuthForDelegation

Kerberos Delegation

Traditional Constrained Delegation (TCD) S4U2Proxy



Bob no longer allowed to keep **Visitor Pass**.

Bob is now given the *msDS-AllowedToDelegateTo* property, which lists the other Dept's that he can access on behalf of **Alice.**

Steps 1 to 5 – Same as before.

6. **Bob** checks his *msDS-AllowedToDelegateTo* property to see if **Finance** is listed as a place where he can get more info on behalf of **Alice**.

If **Finance** is listed, **Bob** brings **Alice's Blue Envelope** to **Security** and says "I need to access **Alice** data at **Finance.**"

7. **Security** then puts **Alice's** identity in a **Pink Envelope** that only **Finance** can open, gives it to **Bob**.

8. **Bob** then brings the **Pink Envelope** to **Finance,** who then opens it, retrieves the finance history of the identity (Alice's identity) in the envelope.

Kerberos Delegation

Traditional Constrained Delegation (TCD)

S4U2Proxy

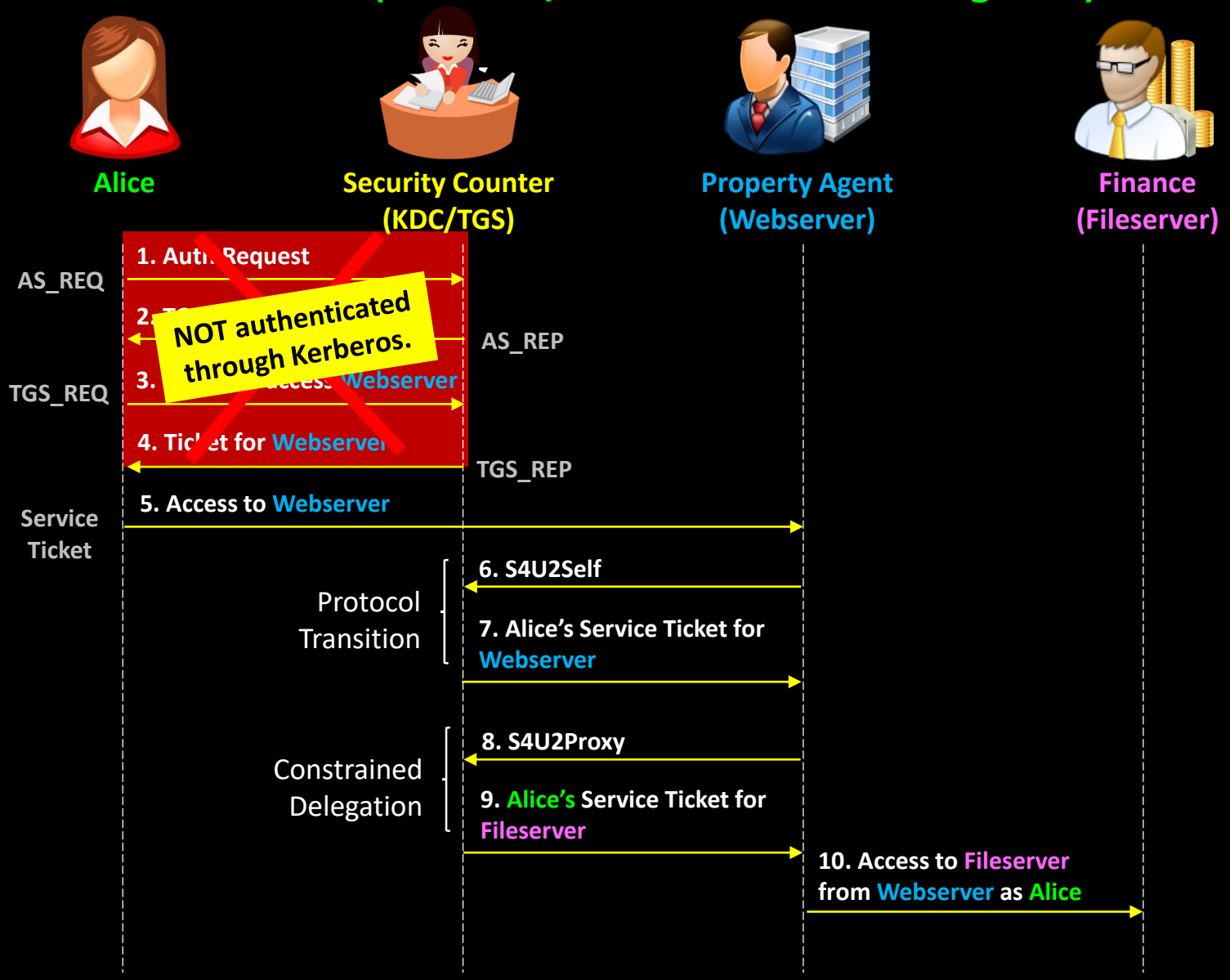
Protocol Transition

S4U2Self / TrustedToAuthForDelegation

Kerberos Delegation

Traditional Constrained Delegation (TCD)

Protocol Transition (S4U2Self/TrustedToAuthForDelegation)



5. Alice meets Bob out of office. Bob cannot S4U2Proxy (*use her Blue Envelope)* to check her finance history with Finance.

6. Bob asks Security to give Alice a Blue Envelope. Because Bob has *TrustedToAuthForDelegation*.

7. Security gives Alice a Blue Envelope.

8. Bob checks his *msDS-AllowedToDelegateTo* property to see if Finance is listed as a place where he can get more info on behalf of Alice.

If Finance is listed, Bob brings Alice's Blue Envelope to Security and says "I need to access Alice data at Finance."

9. Security then puts Alice's identity in a Pink Envelope that only Finance can open.

10. Bob then brings the Pink Envelope to Finance, who then opens it, retrieves the finance history of the identity (Alice's identity) in the envelope.

WEBSERVER CAN CREATE SERVICE TICKETS!

Kerberos Delegation

Traditional Constrained Delegation (TCD)

So while the **Webserver** has been "constrained" to give access only to the **Fileserver**, there were still risks.

Traditional Constrained	Service for User to Self (S4U2self) Service for User to Proxy (S4U2proxy)	Any accounts (user or computer) that have service principal names (SPNs) set in their **msDS-AllowedToDelegateTo** property can pretend to be any user in the domain (i.e. they can "delegate") to those specific SPNs.

With rights to configure S4U2Self and S4U2Proxy

- Additional SPN's could be added to a user or computer object, e.g. ldap/dc.domain.local (a service on the domain controller could be added)
- A service ticket could then be created for anyone, like Administrator (S4U2Self)
- The "Administrator ticket" can then be used to access ldap/dc.domain.local (S4U2Proxy).

Microsoft Recognized This Problem

A right called *SeEnableDelegationPrivilege* was needed to modify delegation properties

- TrustedForDelegation
- TrustedToAuthForDelegation
- msDS-AllowedToDelegateTo

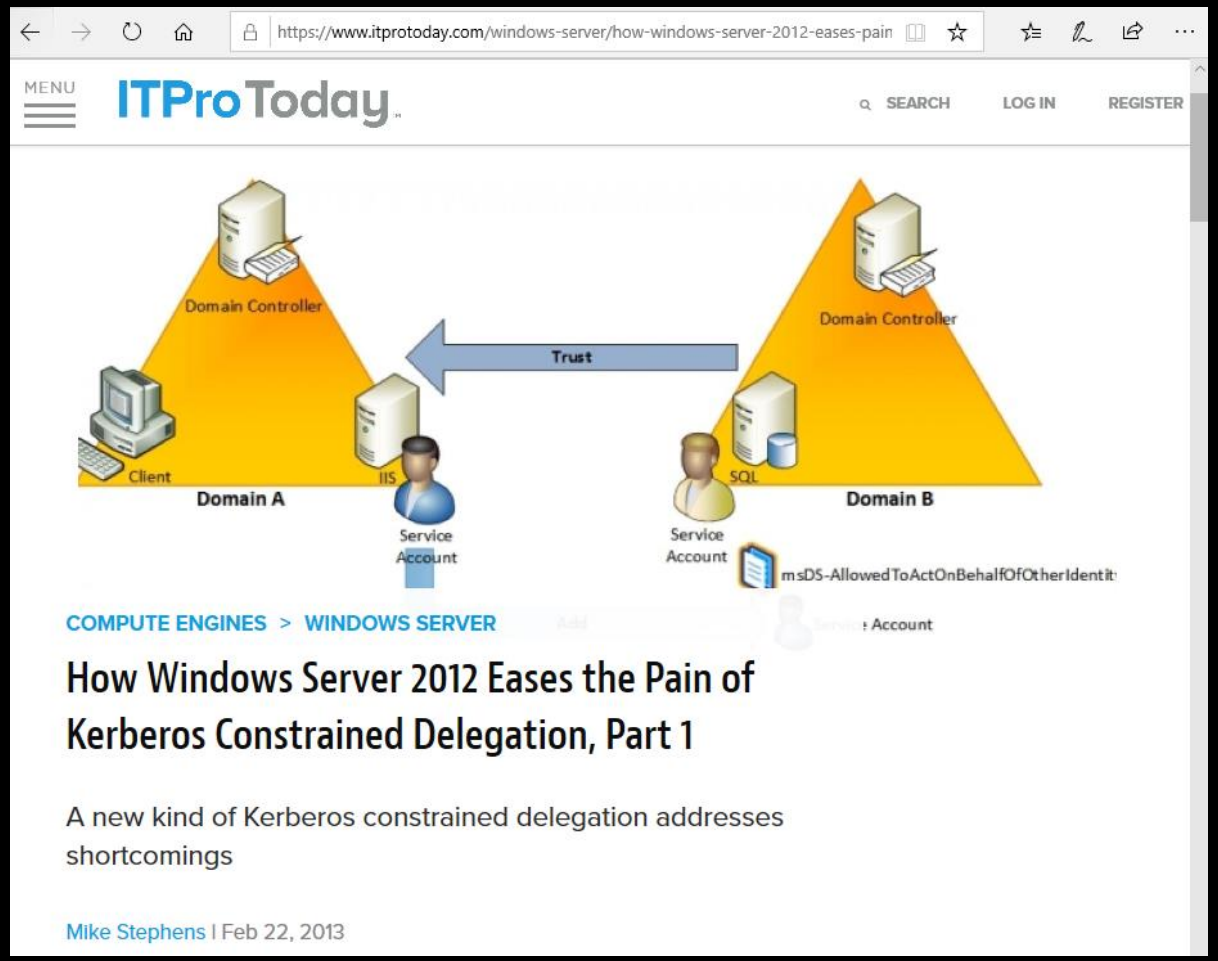
Only domain/enterprise admins have this privilege.

Kerberos Delegation

Resource Based Delegation

Kerberos Delegation

Resource Based Delegation



Constrained delegation in Server 2012 (aka resource based constrained delegation) introduces the concept of controlling delegation of service tickets using a security descriptor rather than an allow list of SPNs.

This change simplifies delegation by enabling the resource to determine which security principals are allowed to request tickets on behalf of another user.

https://www.itprotoday.com/windows-server/how-windows-server-2012-eases-pain-kerberos-constrained-delegation-part-
https://blog.kloud.com.au/2013/07/11/kerberos-constrained-delegation/

Kerberos Delegation

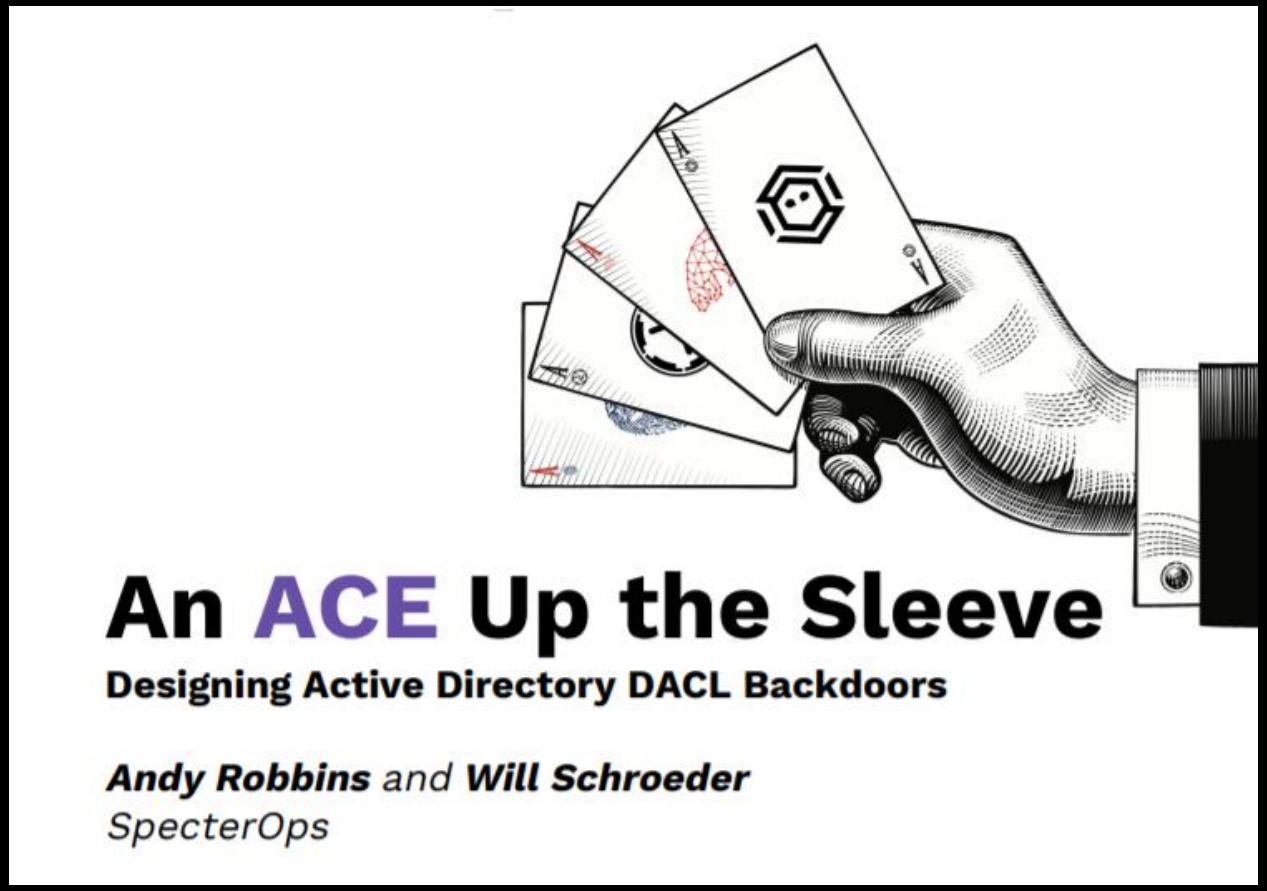
Resource Based Delegation

Delegation	Webserver (Delegation Configured Here)	Fileserver
Traditional Constrained Delegation (Server 2003)	• *msDS-AllowedToDelegateTo* property defines services (SPN's) that it can *delegate to*. • S4U2Self only possible only if *TrustedToAuthForDelegation* is set. • Requires domain admin to configure delegation.	• No visibility of delegation.

Delegation	Webserver	Fileserver (Delegation Configured Here)
Resource Based Delegation (Server 2012)	• *msDS-AllowedToDelegateTo* not used. • S4U2Self possible even if *TrustedToAuthForDelegation* is not set.	• Delegation configured in **Fileserver**'s *msDS-AllowedToActOnBehalfOfOtherIdentity* property. • **User only requires writable Discretionary Access Control List (DACL) permission.** ⚠️

Kerberos Delegation

DACL (Mis)configurations



AD objects are secured by control rights

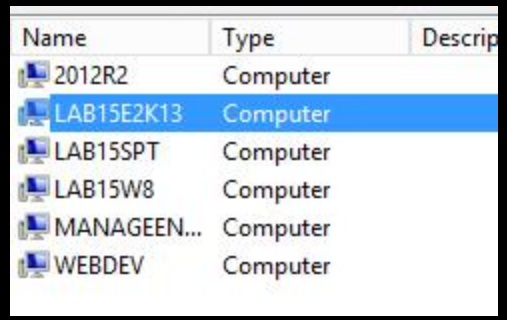
Control Right	Rights over an AD object
GenericAll	Allows all rights, including granting rights
GenericWrite	Modify of almost all properties
WriteDACL	Modify security object descriptor
WriteOwner	Take ownership of an object
Many others…	

Rights to a User Object?

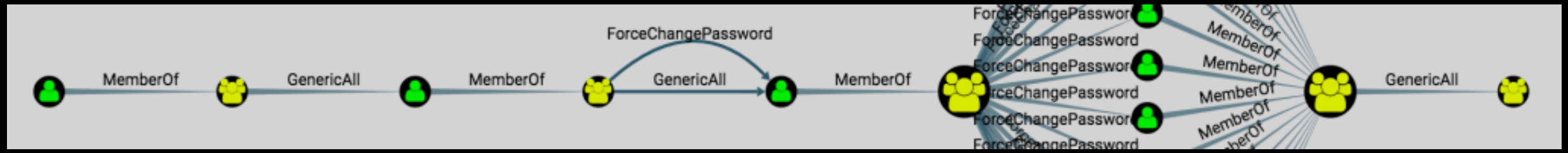
- Change password
- Targeted kerberoasting

Rights to a Computer Object?

- See plaintext LAPS password



Name	Type	Descrip
2012R2	Computer	
LAB15E2K13	Computer	
LAB15SPT	Computer	
LAB15W8	Computer	
MANAGEEN...	Computer	
WEBDEV	Computer	

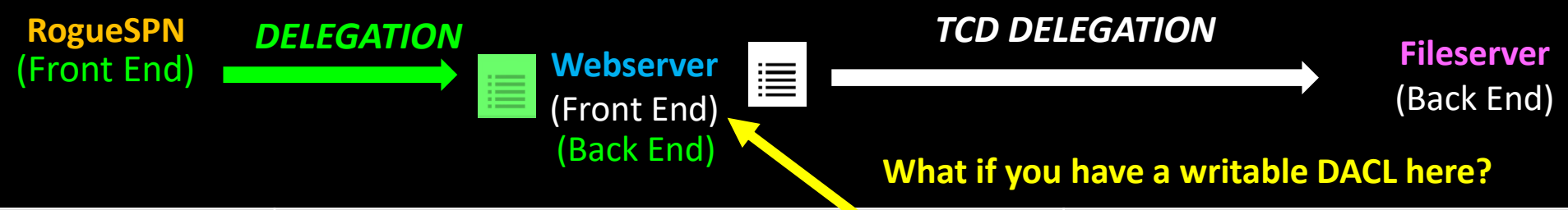


https://wald0.com/?p=112
https://www.blackhat.com/docs/us-17/wednesday/us-17-Robbins-An-ACE-Up-The-Sleeve-Designing-Active-Directory-DACL-Backdoors.pdf

Kerberos Delegation

Resource Based Delegation

Delegation	Webserver (Delegation Configured Here)	Fileserver
Traditional Constrained Delegation (Server 2003)	• *msDS-AllowedToDelegateTo* property defines services (SPN's) that it can *delegate to*. • S4U2Self only possible only if *TrustedToAuthForDelegation* is set. • Requires domain admin to configure delegation.	• No visibility of delegation.

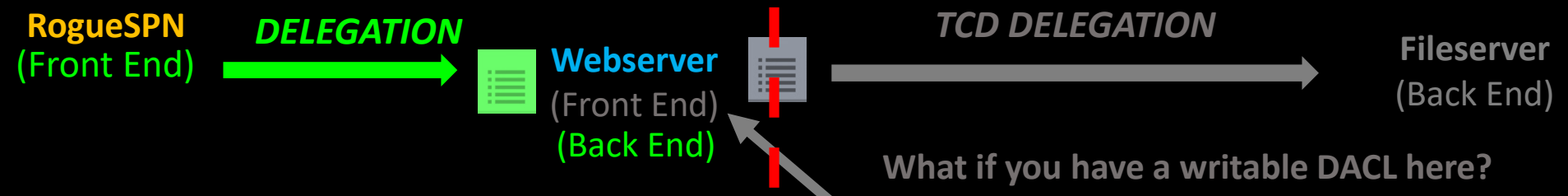


Delegation	Webserver	Fileserver (Delegation Configured Here)
Resource Based Delegation (Server 2012)	• *msDS-AllowedToDelegateTo* not used. • S4U2Self possible even if *TrustedToAuthForDelegation* is not set.	• Delegation configured in **Fileserver**'s *msDS-AllowedToActOnBehalfOfOtherIdentity* property. **User only requires writable Discretionary Access Control List (DACL) permission.**

Kerberos Delegation

Resource Based Delegation

Delegation	Webserver (Delegation Configured Here)	Fileserver
Traditional Constrained Delegation (Server 2003)	• *msDS-AllowedToDelegateTo* property defines services (SPN's) that it can *delegate to*. • S4U2Self only possible only if *TrustedToAuthForDelegation* is set. • Requires domain admin to configure delegation.	• No visibility of delegation.



Delegation	Webserver	Fileserver (Delegation Configured Here)
Resource Based Delegation (Server 2012)	• *msDS-AllowedToDelegateTo* not used. **S4U2Self possible even if *TrustedToAuthForDelegation* is not set.**	• Delegation configured in **Fileserver**'s *msDS-AllowedToActOnBehalfOfOtherIdentity* property. • **User only requires writable Discretionary Access Control List (DACL) permission.**

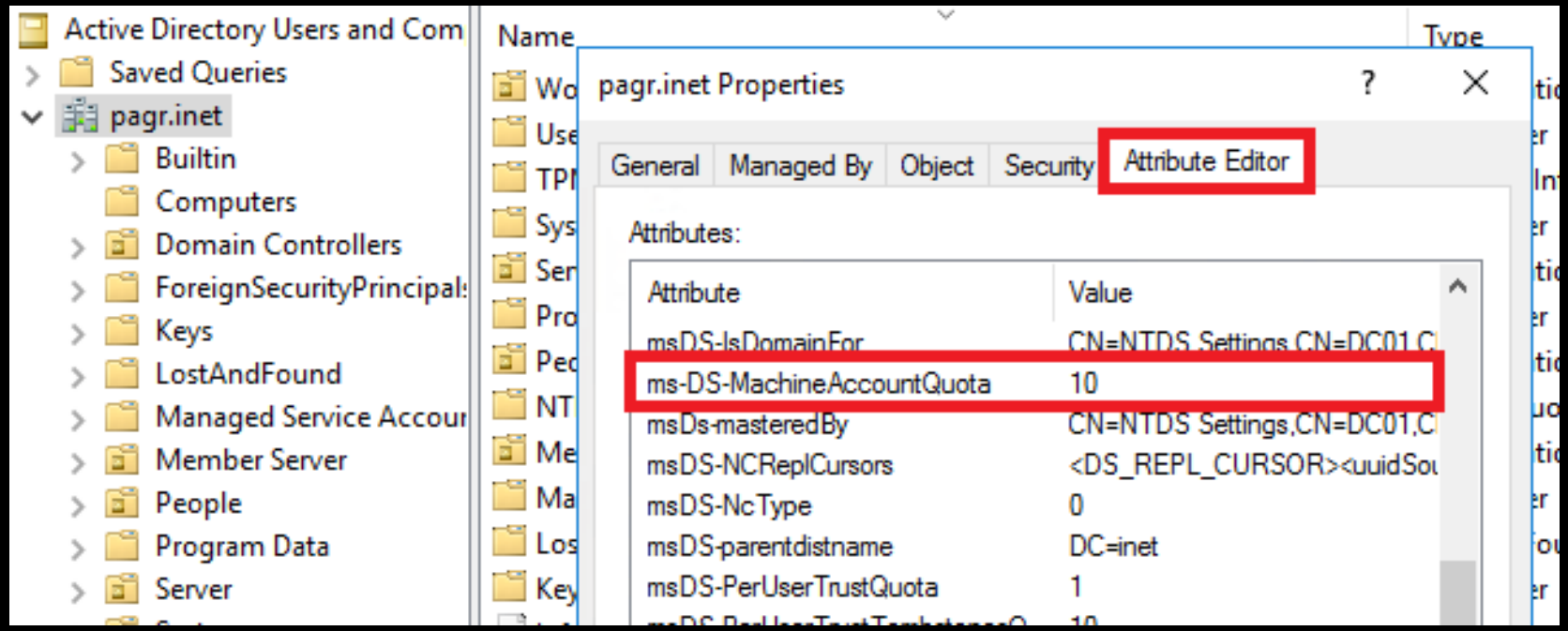
Kerberos Delegation

Abusing Resource Based Delegation to Compromise TCD Servers

MachineAccountQuota Enabled + Writable TCD DACL = Compromised TCD Server

Kerberos Delegation

Abusing Resource Based Delegation to Compromise TCD Servers



MachineAccountQuota (MAQ)

By default - all unprivileged domain users can add up to 10 computers to an Active Directory (AD) domain, and set an SPN for it.

https://blogs.technet.microsoft.com/canitpro/2015/05/26/step-by-step-allowing-or-preventing-domain-users-from-joining-workstations-to-the-domain/
https://support.microsoft.com/en-sg/help/243327/default-limit-to-number-of-workstations-a-user-can-join-to-the-domain

Kerberos Delegation

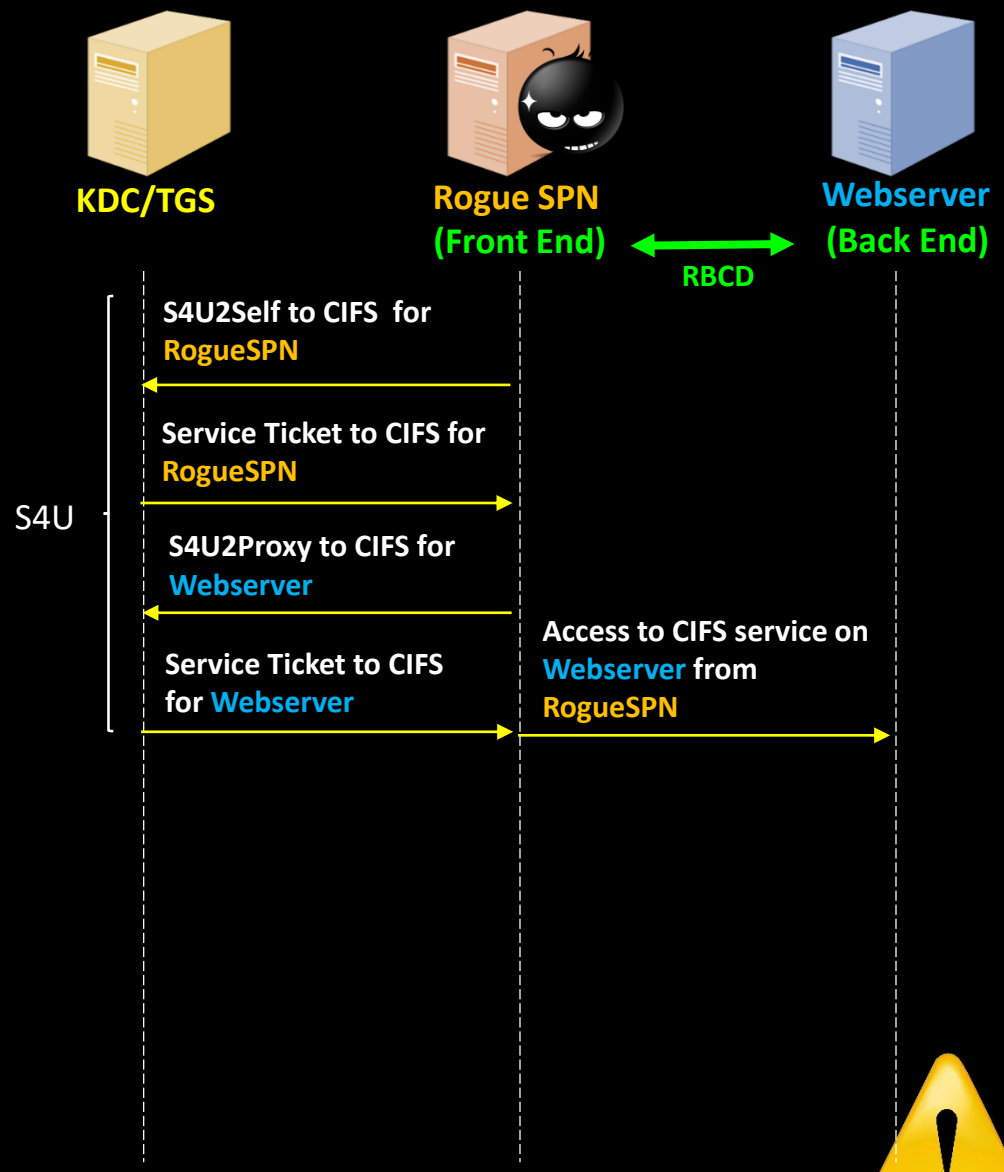
Abusing Resource Based Delegation to Compromise TCD Servers

If adversary can write to the Webserver computer object + MachineAccountQuota enabled

- Adversary could create rogue service (**RogueSPN**) by abusing *MachineAccountQuota*.
- Configure Resource Based Delegation on **Webserver**
- Do **S4U2Self** to get an administrator ticket for **RogueSPN**.
- Do **S4U2Proxy** using the obtained ticket to gain administrator access to **Webserver**.

If the domain is compromised

- Persistence: Resource-based constrained delegation can be configured on the DC to produce krbtgt TGTs on-demand.
- Administrator Service Ticket to krbtgt service == Golden ticket.



Kerberos Delegation

Demo - Abusing Resource Based Delegation to Compromise TCD Servers

MachineAccountQuota Enabled + Writable TCD DACL = Compromised TCD

Active Directory Users and Computers

File Action View Help

Active Directory Users and Comp
- Saved Queries
- internal.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Keys
  - LostAndFound
  - Managed Service Accoun
  - Program Data
  - System
  - Users
  - NTDS Quotas
  - TPM Devices

Name
- PC1
- WEBSERVER

WEBSERVER Properties

Location | Managed By | Object | Security | Dial-in | Attribute Editor
General | Operating System | Member Of | Delegation | Password Replication

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

- ○ Do not trust this computer for delegation
- ○ Trust this computer for delegation to any service (Kerberos only)
- ◉ Trust this computer for delegation to specified services only
  - ◉ Use Kerberos only
  - ○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Na
time	DC		INTERNA

☐ Expanded

Add... Remove

OK Cancel Apply Help

Unprivileged Properties

Security | Environment | Sessions | Remote control
Remote Desktop Services Profile | COM+ | Attribute Editor
General | Address | Account | Profile | Telephones | Organization
Published Certificates | Member Of | Password Replication | Dial-in | Object

Member of:

Name	Active Directory Domain Services Folder
Domain Users	internal.local/Users

Add... Remove

Primary group: Domain Users

Set Primary Group

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help

Windows License valid for 180 days
Build 17763.rs5_release.180914-1434

https://kerberos.surge.sh/dacl.mp4

Kerberos Delegation

RBCD + NTLM Relay = Local Privilege Escalation (LPE)

Kerberos Delegation

Windows 10 LPE

Wagging the Dog: Abusing Reso

https://shenaniganslabs.io/2019/01/28/Waggin...

Case Study 2: Windows 10/2016/2019 LPE

One late night, Matt Bush (@3xocyte), Danyal Drew (@danyaldrew) and I brainstormed ideas where to find suitable RCE/LPE primitives, and decided to explore what happens when a user changes the account picture in Windows 10/2016/2019. We analysed it with Process Monitor and quickly found that during the account picture change SYSTEM opens the picture file to read its attributes. It is a small and meaningless operation; not an arbitrary file write/read/delete. But we are humble people, and that is all we wanted.

Kerberos Delegation

Windows 10 LPE

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
4:30:50....	DllHost.exe	5196	CreateFile	\\roguepc@80\a\peee.jpg	SUCCESS	Desired Access: R...

Event Properties

Event | Process | Stack

Date:	23/6/2019 4:30:50.9892033 am
Thread:	3900
Class:	File System
Operation:	CreateFile
Result:	SUCCESS
Path:	\\roguepc@80\a\peee.jpg
Duration:	0.0002614

Desired Access:	Read Attributes
Disposition:	Open
Options:	Open Reparse Point
Attributes:	n/a
ShareMode:	Read, Write, Delete
AllocationSize:	n/a
OpenResult:	Superseded

Event Properties

Event | Process | Stack

Image

COM Surrogate

Microsoft Corporation

Name:	DllHost.exe
Version:	10.0.18362.1 (WinBuild.160101.0800)

Path:

C:\Windows\system32\DllHost.exe

Command Line:

C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D848703

PID:	5196	Architecture:	64-bit
Parent PID:	772	Virtualized:	False
Session ID:	0	Integrity:	System
User:	NT AUTHORITY\SYSTEM		
Auth ID:	00000000:000003e7		
Started:	23/6/2019 4:30:50 am	Ended:	(Running)

Kerberos Delegation

Windows 10 LPE

https://docs.microsoft.com/en-us/windows...

LocalSystem Account

05/31/2018 • 2 minutes to read • Contributors

The LocalSystem account is a predefined local account used by the service control manager. This account is not recognized by the security subsystem, so you cannot specify its name in a call to the LookupAccountName function. It has extensive privileges on the local computer, and acts as the computer on the network. Its token includes the NT AUTHORITY\SYSTEM and BUILTIN\Administrators SIDs; these accounts have access to most system objects. The name of the account in all locales is .\LocalSystem. The name, LocalSystem or *ComputerName*\LocalSystem can also be used. This account does not have a password. If you specify the LocalSystem account in a call to the CreateService or ChangeServiceConfig function, any password information you provide is ignored.

A service that runs in the context of the LocalSystem account inherits the security context of the SCM. The user SID is created from the **SECURITY_LOCAL_SYSTEM_RID** value. The account is not associated with any logged-on user account. This has several implications:

- The registry key **HKEY_CURRENT_USER** is associated with the default user, not the current user. To access another user's profile, impersonate the user, then access **HKEY_CURRENT_USER**.
- The service can open the registry key **HKEY_LOCAL_MACHINE\SECURITY**.
- The service presents the computer's credentials to remote servers.
- If the service opens a command window and runs a batch file, the user could hit CTRL+C to terminate the batch file and gain access to a command window with LocalSystem permissions.

Advanced Security Settings for PC1

Owner: Domain Admins (INTERNAL\Domain Admins) Change

Permissions | Effective Access

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a mer
domain, you can also evaluate the impact of potential additions to the security token for the account. When you evalu
adding a group, any group that the intended group is a member of must be added separately.

User/ Group: SELF Select a user

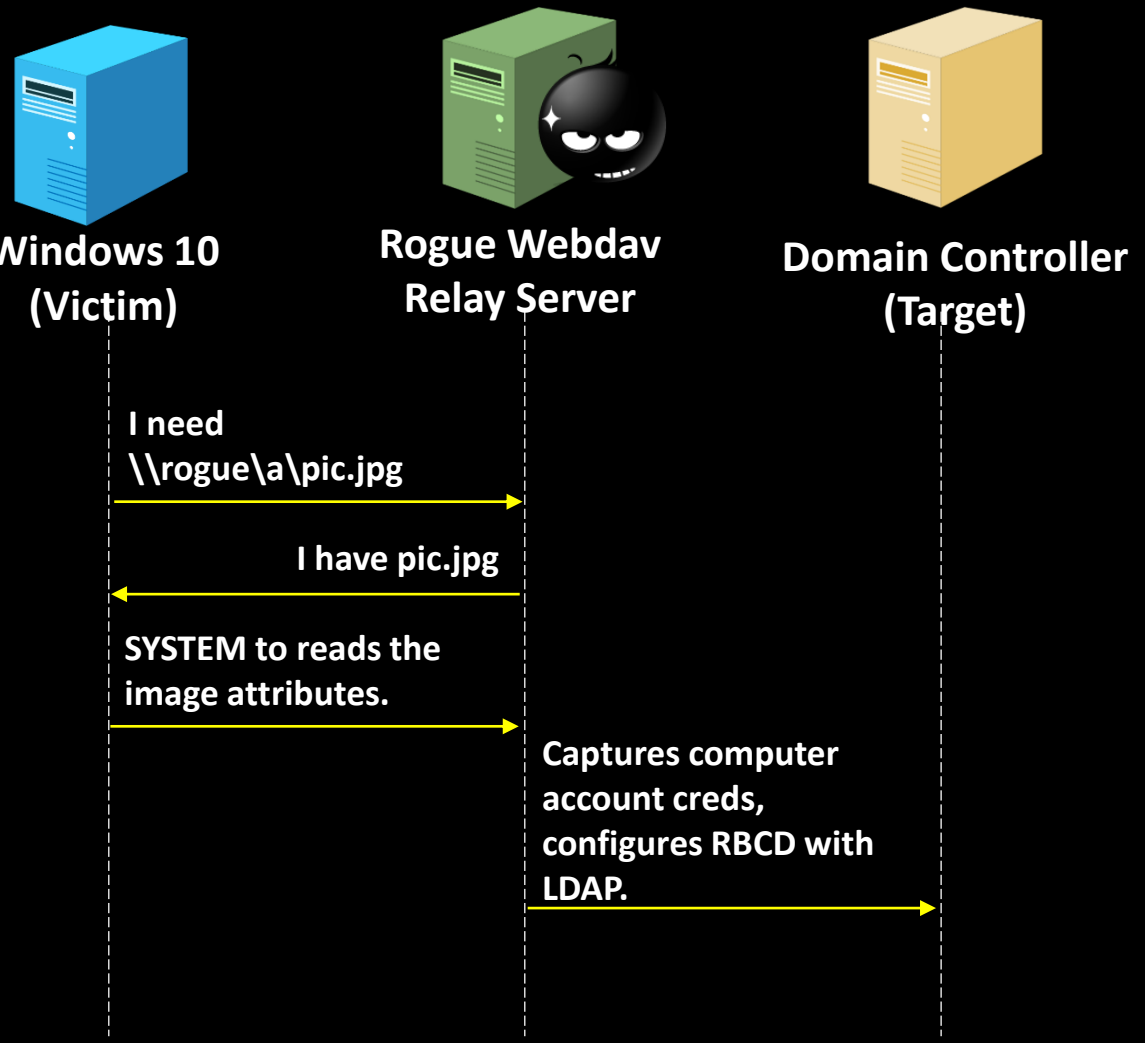
Read msDS-AllowedToActOnBehalfOfOtherIdentity

Write msDS-AllowedToActOnBehalfOfOtherIdentity

```
[SMB] NTLMv2-SSP Client   : 10.0.0.2
[SMB] NTLMv2-SSP Username : INTERNAL\PC1$
[SMB] NTLMv2-SSP Hash     : PC1$::INTERNAL:a41bc32e03cd4d80:F7A126E275C7F6481
BF939D0CE0279DA:0101000000000000C0653150DE09D201933169FCA0C63BDD0000000002000
80053004D004200330001001E00570049004E002D005000520048003400390032005200510041
004600560004001400530 04D00420033002E006C006F00630061006C0003003400570049004E0
02D005000520048003400390032005200510041004600560 02E0053004D00420033002E006C00
6F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0653
150DE09D201060004000200000008003000300000000000000000000000000400000969531CEA7
144E5F90175AC6148073A89B3EDC88C9851910A03F095F846EDE8C0A001000000000000000000
000000000000000000900180063006900660073002F006C007500620075006E00740075000000
0000000000000000000
```

Kerberos Delegation

NTLM Relay (Simplified)



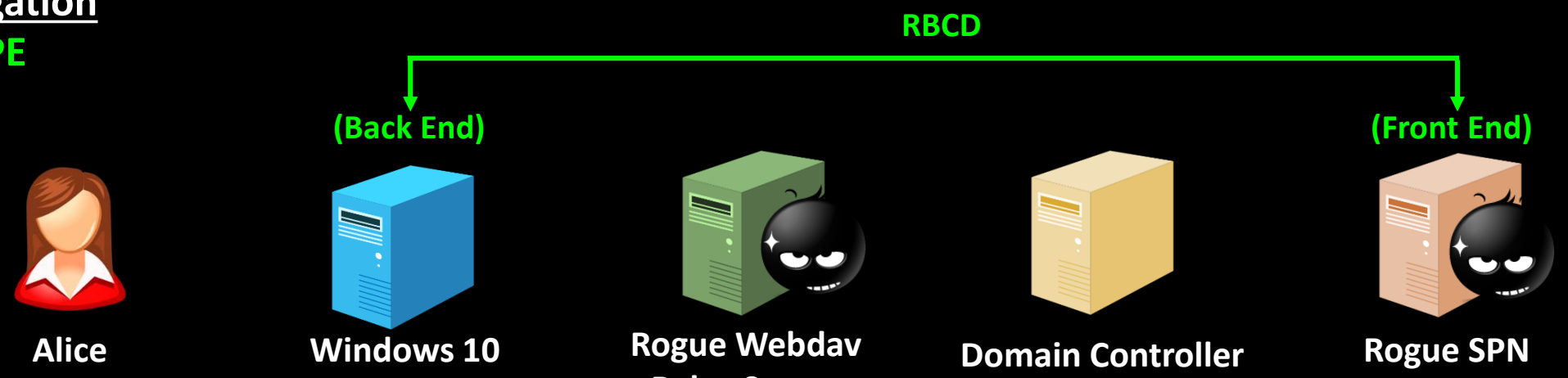
Adversary Assumptions

- Able to connect a rogue device to the network.
- Rogue device can communicate with both victim and DC.
- Able to get Victim to send credentials to rogue device

Target (DC) Assumptions

- LDAP signing disabled.

Kerberos Delegation
Windows 10 LPE



Adversary Assumptions

- Able to connect a rogue device to the network.
- Rogue device can communicate with both victim and DC.
- Able to get Victim to send credentials to rogue device

1. Unprivileged access
2. Can add Rogue Device
3. Create Rogue SPN with MAQ
4. Add DNS record for Rogue
5. Change account picture to path on Rogue Webdav server
6. Computer account creds sent to Rogue Webdav Relay Server
7. NTLM relay to LDAP on DC, configures RBCD on Windows 10 (to Rogue SPN).
8. S4U2Self for Administrator for Rogue SPN
9. Administrator ticket for Rogue
10. S4U2Proxy – Use administrator ticket for Rogue SPN to gain an “administrator ticket” for Win 10.
11. Administrator ticket for Win 10

Target (DC) Assumptions

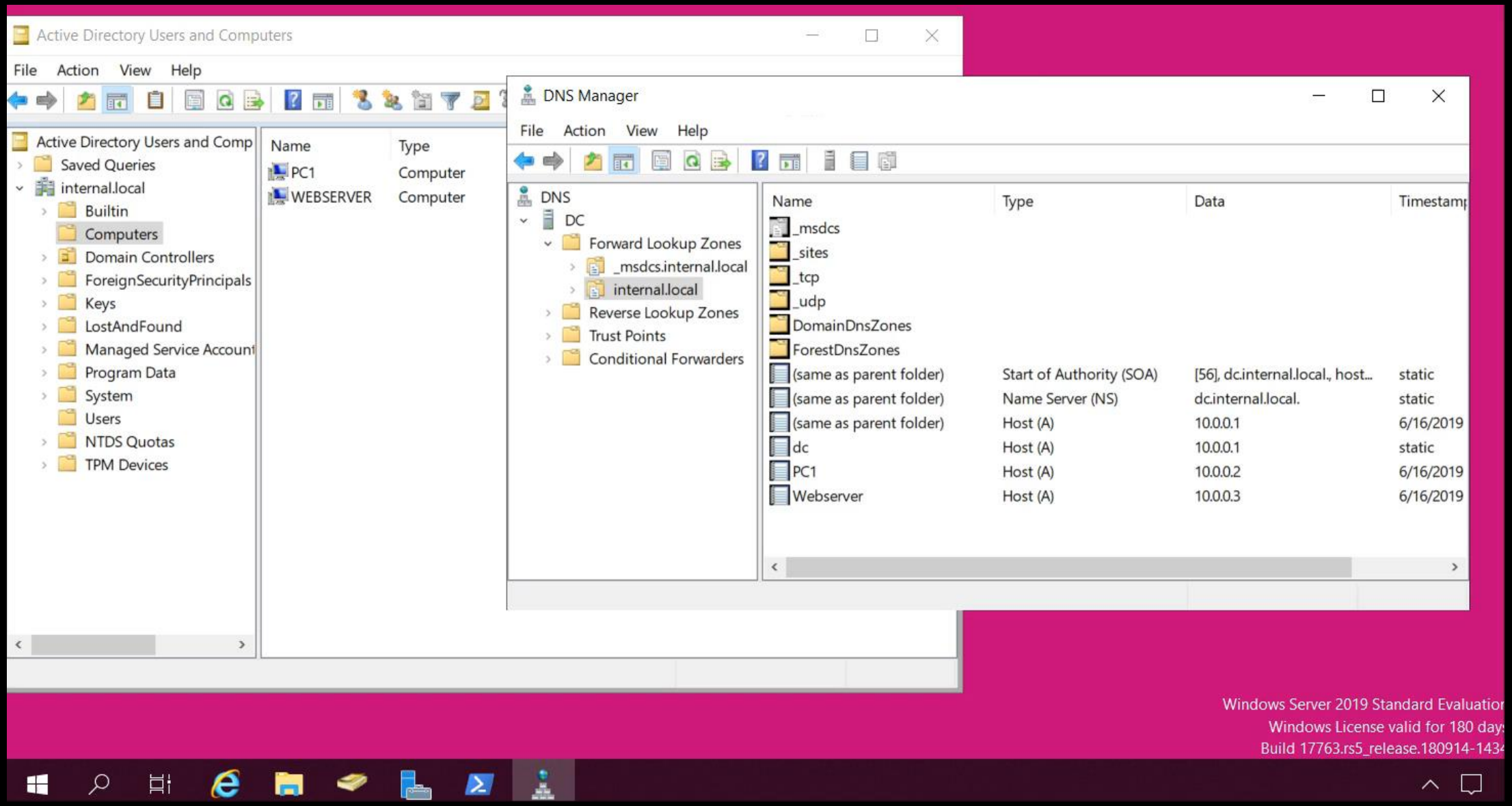
- LDAP signing disabled

Victim (Win 10) Assumptions

- WebDAV client installed (Default on Win 10)

Kerberos Delegation

Demo – Windows 10 LPE



https://kerberos.surge.sh/win10privesc.mp4

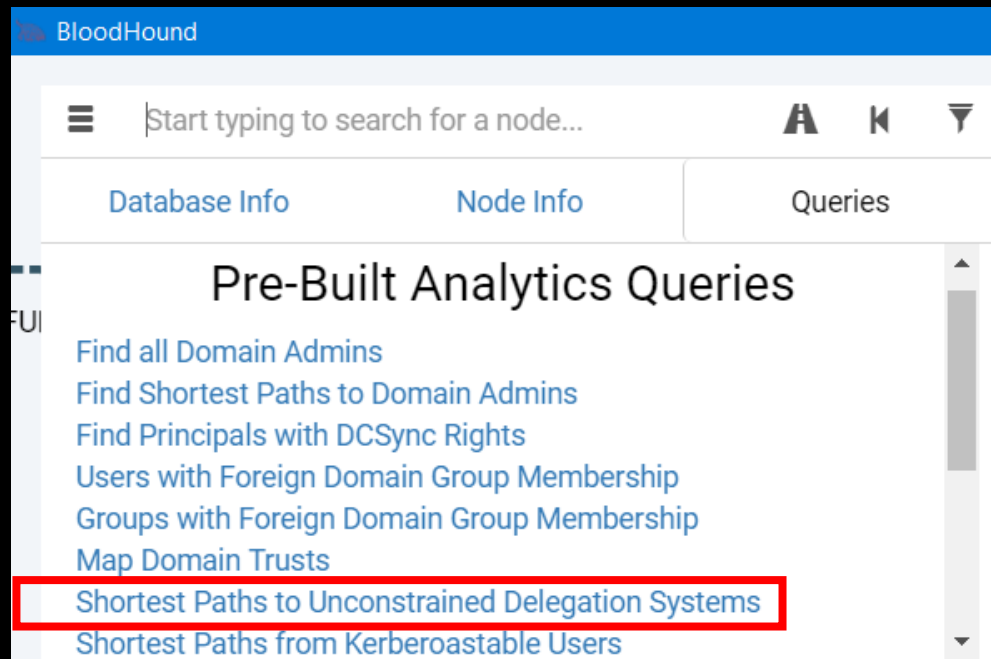
Kerberos Delegation

Summary

Delegation	How it Works	Risks	Mitigation
Unconstrained	• Makes and stores a copy of user's TGT for delegation.	• Stored TGT's can be used for PTT attacks • Forced authentication bugs may also facilitate compromise of other hosts within other forests with bidirectional trusts. • Existing admin's for unconstrained servers are high value targets; technically already own the domain.	• Unconstrained delegation should no longer exist (except for domain controllers, which is a default configuration). • Disable the Print Spooler service on domain controllers where possible. • KB4490425 (July 9 2019) disables TGT delegation across trusts.

Find Servers Configured with Unconstrained Delegation

```
Get-ADComputer -Filter {TrustedForDelegation -eq $True}
Get-ADUser -Filter {TrustedForDelegation -eq $True}
```



https://blogs.technet.microsoft.com/389thoughts/2017/04/18/get-rid-of-accounts-that-use-kerberos-unconstrained-delegation/
https://support.microsoft.com/en-sg/help/4490425/updates-to-tgt-delegation-across-incoming-trusts-in-windows-server
https://techcommunity.microsoft.com/t5/Premier-Field-Engineering/Changes-to-Ticket-Granting-Ticket-TGT-Delegation-Across-Trusts/ba-p/440283

Kerberos Delegation

Summary

Delegation	How it Works	Risks	Mitigation
Traditional Constrained (S4U2Self, S4U2Proxy)	• Stores list of SPN's in the "front end" in msDS-AllowedToDelegateTo.	• S4U2Self (if enabled) can be abused to create service tickets for anybody, including administrators, to compromise delegated SPN's. • S4U2Proxy can be abused to request for arbitrary services that it was not originally intended to delegate to.	• S4U2Self can be detected in a Kerberos service ticket request event (Event ID 4769), where the Account Information and Service Information sections point to the same account. • S4U2Proxy: can be detected in a Kerberos service ticket request event (Event ID 4769), where the Transited Services attribute in the Additional Information is not blank. • Any non-privileged accounts with *SeEnableDelegationPrivilege* (Can configure constrained delegation)?

Find Servers Configured with Constrained Delegation

```
Get-ADObject -Filter {msDS-AllowedToDelegateTo -ne "$null"}
-Properties msDS-AllowedToDelegateTo
```

Kerberos Delegation

Summary

Delegation	How it Works	Risks	Mitigation
Resource Based	• Stores in security descriptors in the “back end” in msDS-AllowedToActOnBehalfOfOtherIdentity.	• A server can be compromised if its computer object DACL is writable. • Domain Persistence: RBCD on the krbtgt account allows producing TGTs for arbitrary users. Resetting krbtgt twice may not enough.	• Resource-based constrained delegation configuration changes can be detected in directory service object modification events (Event ID 5136), where the LDAP Display Name is “msDS-AllowedToActOnBehalfOfOtherIdentity”. • Configure computer objects to deny Self from writing to the attribute msDS-AllowedToActOnBehalfOfOtherIdentity • If RBCD not used, block Everyone from writing to the attribute msDS-AllowedToActOnBehalfOfOtherIdentity. • Domain Persistence: Detect S4U2Proxy to krbtgt - Event ID 4769 (Kerberos service ticket request event), where the Transited Services attribute in the Additional Information is not blank and the Service Information points to the krbtgt account.

Kerberos Delegation

Conclusion

Computer accounts are an attack primitive

Basics First – Defense in depth

- NAC, network segmentation, app whitelisting, SMB Signing, LDAP signing, vulnerability management, patching, hardening, credential management, logging, monitoring, etc.

Detection – Understand what "normal" looks like

- Any raw non-lsass/non-authorized Kerberos port 88 traffic should be considered as suspicious.
- Have visibility over all Kerberos delegations and traffic in the network. S4U2Proxy is a dangerous extension that should be restricted as much as possible.
- Configure privileged accounts to "Account is sensitive and cannot be delegated" or place in "Protected Users"

Forward Looking

- Any other means where coersed authentication can occur?
- Is MachineAccountQuota needed?

⚠ Warning

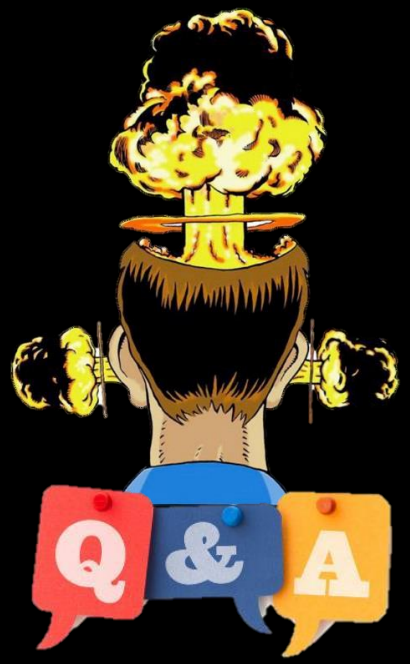
Accounts for services and computers should never be members of the Protected Users group. This group would provides incomplete protection anyway because the password or certificate is always available on the host. Authentication will fail with the error "the user name or password is incorrect" for any service or computer that is added to the Protected Users group.

Microsoft did highlight the risk of S4U2Proxy in section 5.1 of MS-SFU:

"The S4U2proxy extension allows a service to obtain a service ticket to a second service on behalf of a user. When combined with S4U2self, this allows the first service to impersonate any user principal while accessing the second service. This gives any service allowed access to the S4U2proxy extension a degree of power similar to that of the KDC itself.

This implies that each of the services allowed to invoke this extension have to be protected nearly as strongly as the KDC and the services are limited to those that the implementer knows to have correct behavior."

https://msdn.microsoft.com/en-us/library/cc246112.aspx
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-controller-ldap-server-signing-requirements
https://support.microsoft.com/en-au/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry
https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group



kerberos.surge.sh

"There are no stupid questions, so let's also agree there are no stupid answers."