TROOPERS

Breaking Boundaries: Unraveling AD Cross-Forest Attack Paths

Jonas Bülow Knudsen

Spring 2025

Whoami

```
PS C:\> Get-ADUser jbk -Properties * | Select Name,Title,Company,City,co


Name    : Jonas Bülow Kundsen
Title   : Manager, Research
Company : SpecterOps
City    : Copenhagen
co      : Denmark
```

@jonas-bk.bsky.social

@Jonas-BK

@JonasBK

@Jonas_B_K

Outline

AD forests and trusts 101

Cross-forest trust attack techniques

Creation of abusable cross-forest trusts

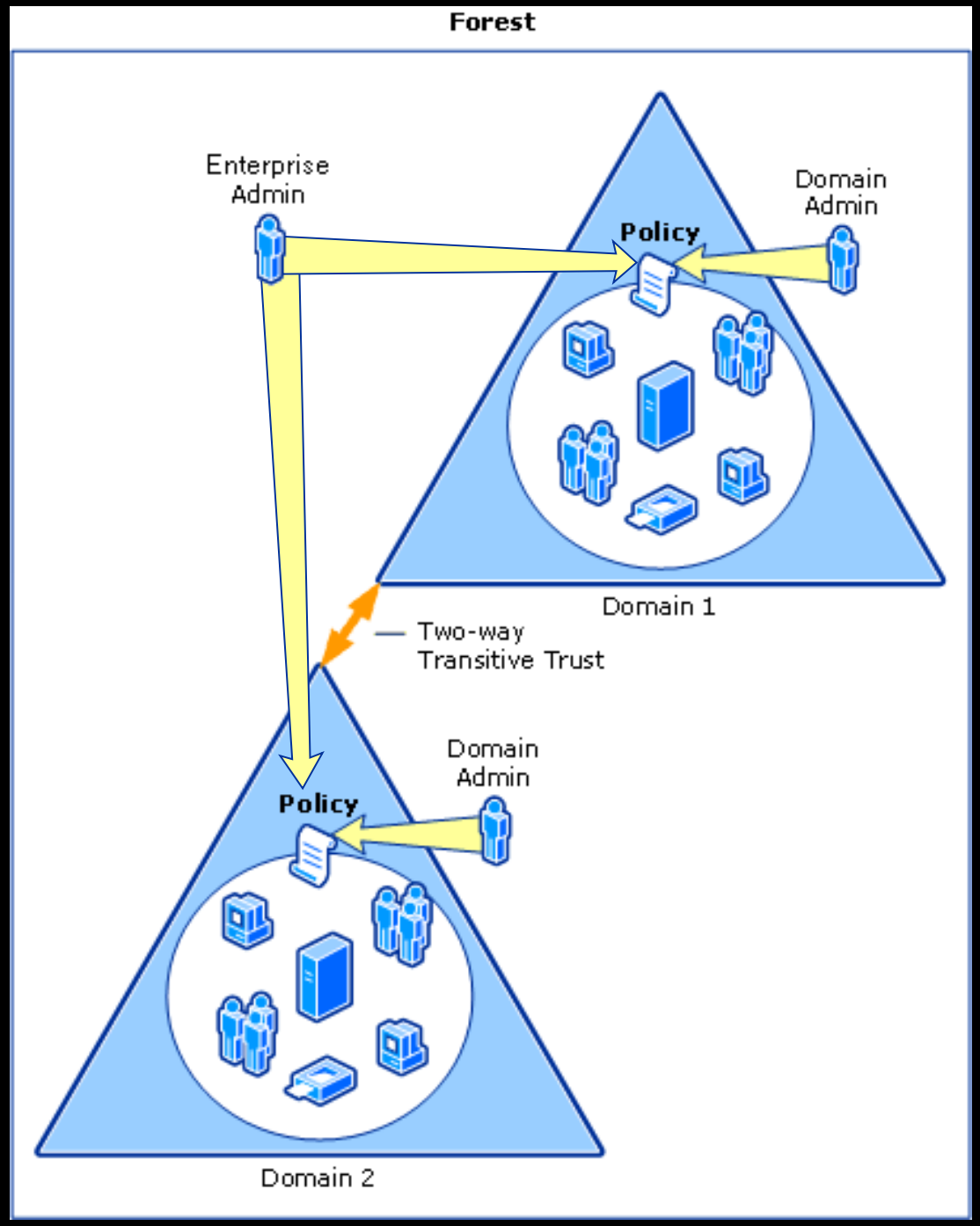
Forest jump without AD trust

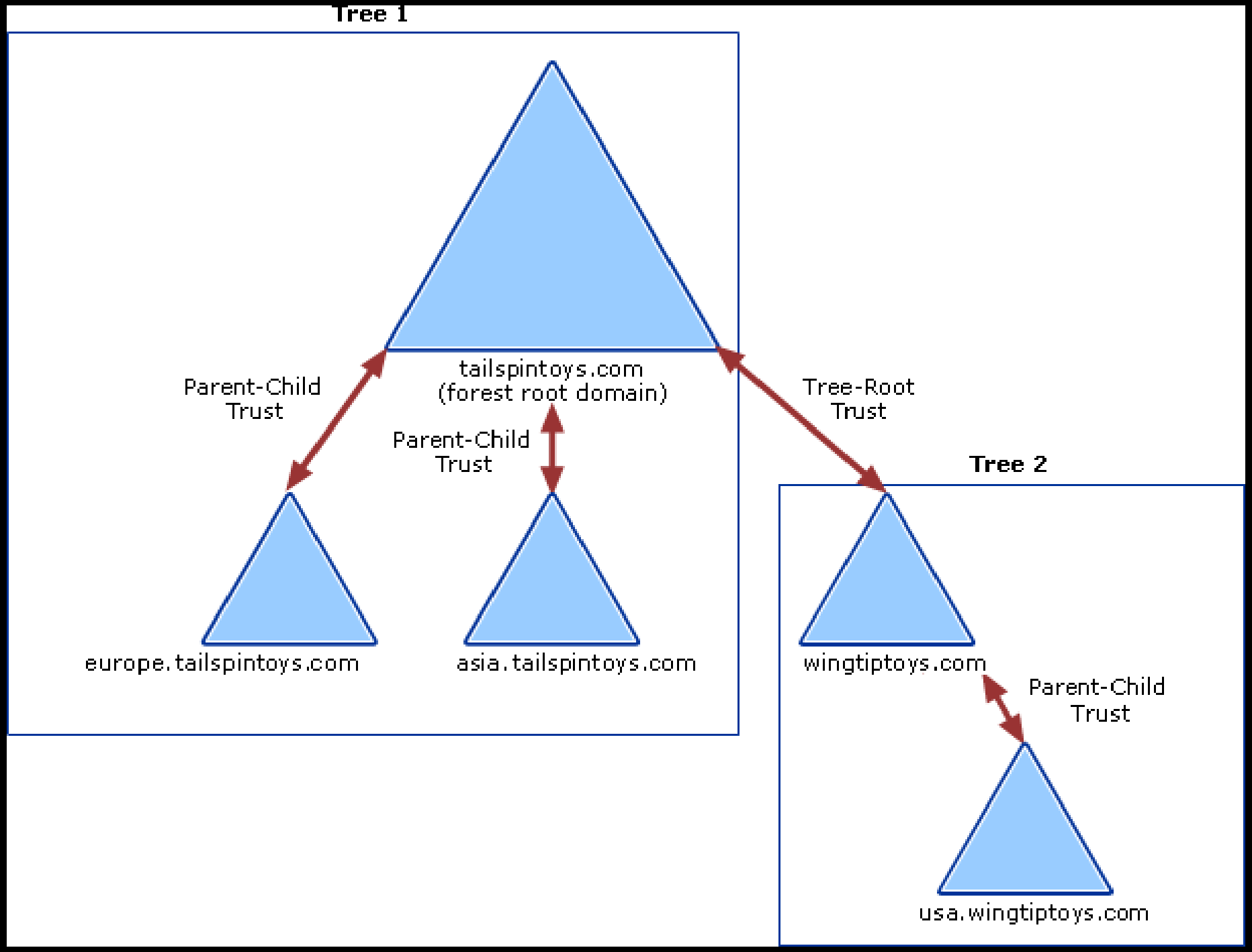
AD forests and trusts 101

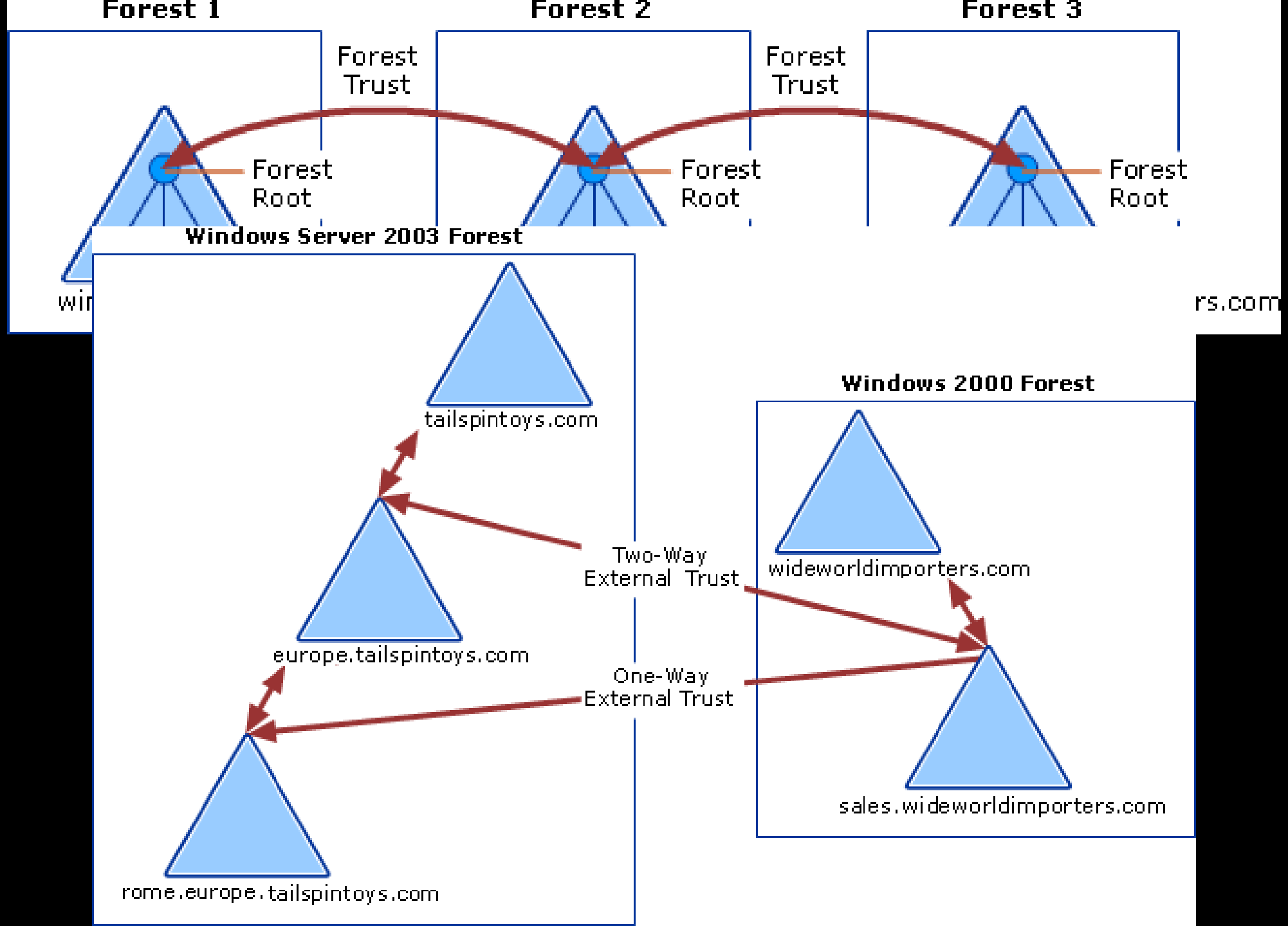
Cross-forest trust attack techniques

Creation of abusable cross-forest trusts

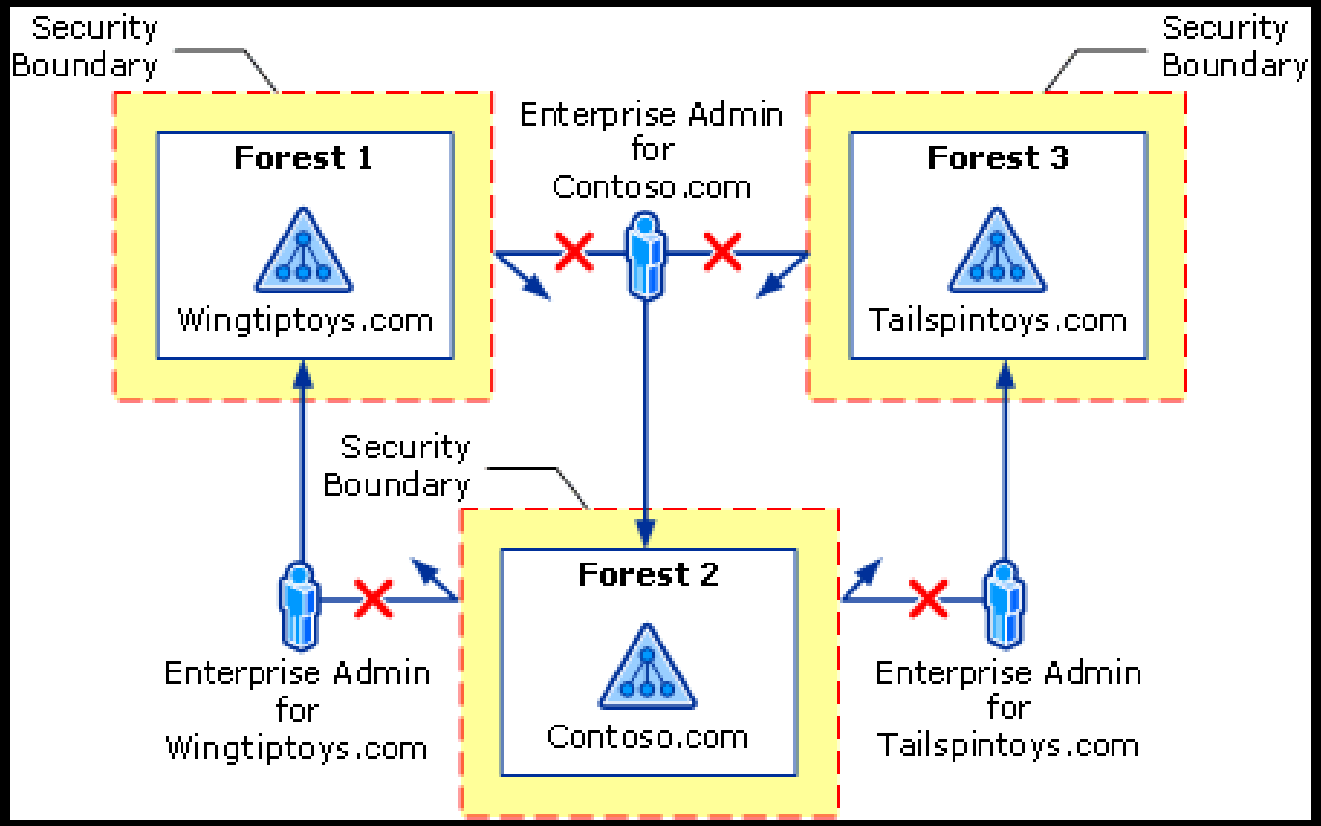
Forest jump without AD trust


Forest
Enterprise Admin
Domain Admin
Policy
Domain 1
Two-way Transitive Trust
Domain Admin
Policy
Domain 2


Tree 1
tailspintoys.com
(forest root domain)
Parent-Child
Trust
Parent-Child
Trust
Tree-Root
Trust
Tree 2
europe.tailspintoys.com
asia.tailspintoys.com
wingtiptoys.com
Parent-Child
Trust
usa.wingtiptoys.com


Forest 1
Forest 2
Forest 3
Forest Trust
Forest Trust
Forest Root
Forest Root
Forest Root
Windows Server 2003 Forest
tailspintoys.com
europe.tailspintoys.com
rome.europe.tailspintoys.com
Two-Way External Trust
One-Way External Trust
Windows 2000 Forest
wideworldimporters.com
sales.wideworldimporters.com

Microsoft: AD forest is a security boundary

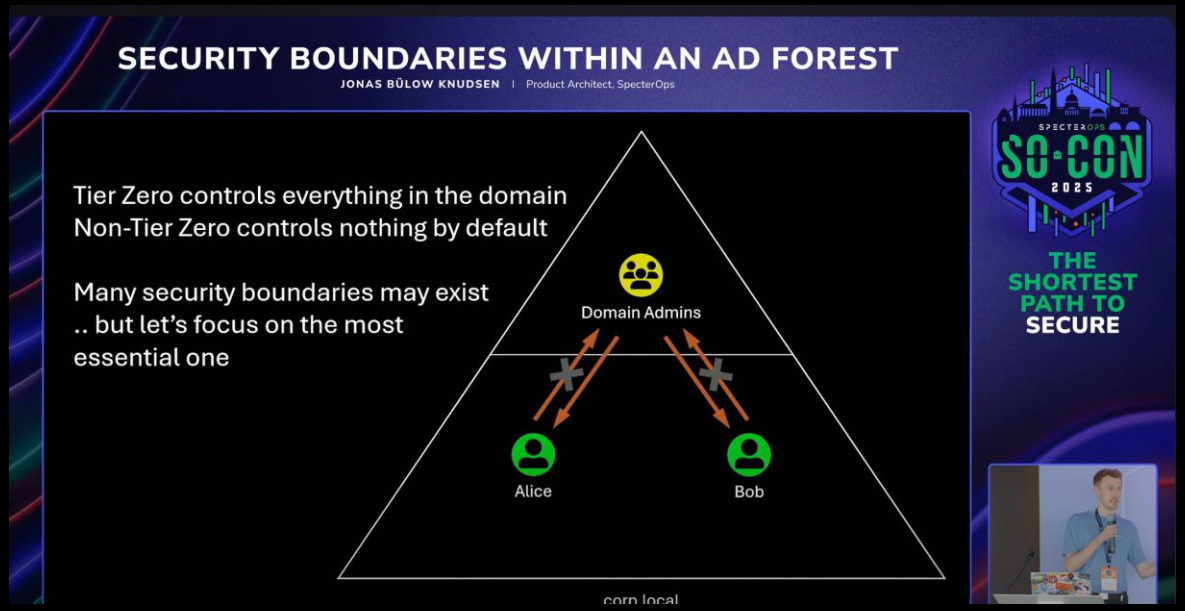


.. and the domain is not

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)#forests-as-security-boundaries

Why is the domain not a security boundary?

A forest is the only component of the Active Directory logical structure that is a security boundary. By contrast, a domain is not a security boundary because it is not possible for administrators from one domain to prevent a malicious administrator from another domain within the forest from accessing data in their domain. A domain is, however, the



https://www.youtube.com/watch?v=bTl-56MmuSM

1. Weak trust configuration by default
2. Configuration NC is writeable from any DC in the forest

AD forests and trusts 101

Cross-forest trust attack techniques

Creation of abusable cross-forest trusts

Forest jump without AD trust

Same-forest trust attacks

1. Weak trust configuration 👀

2. ~~Configuration NC is writeable from any DC in the forest~~

What about cross-forest trusts?

Trust configuration

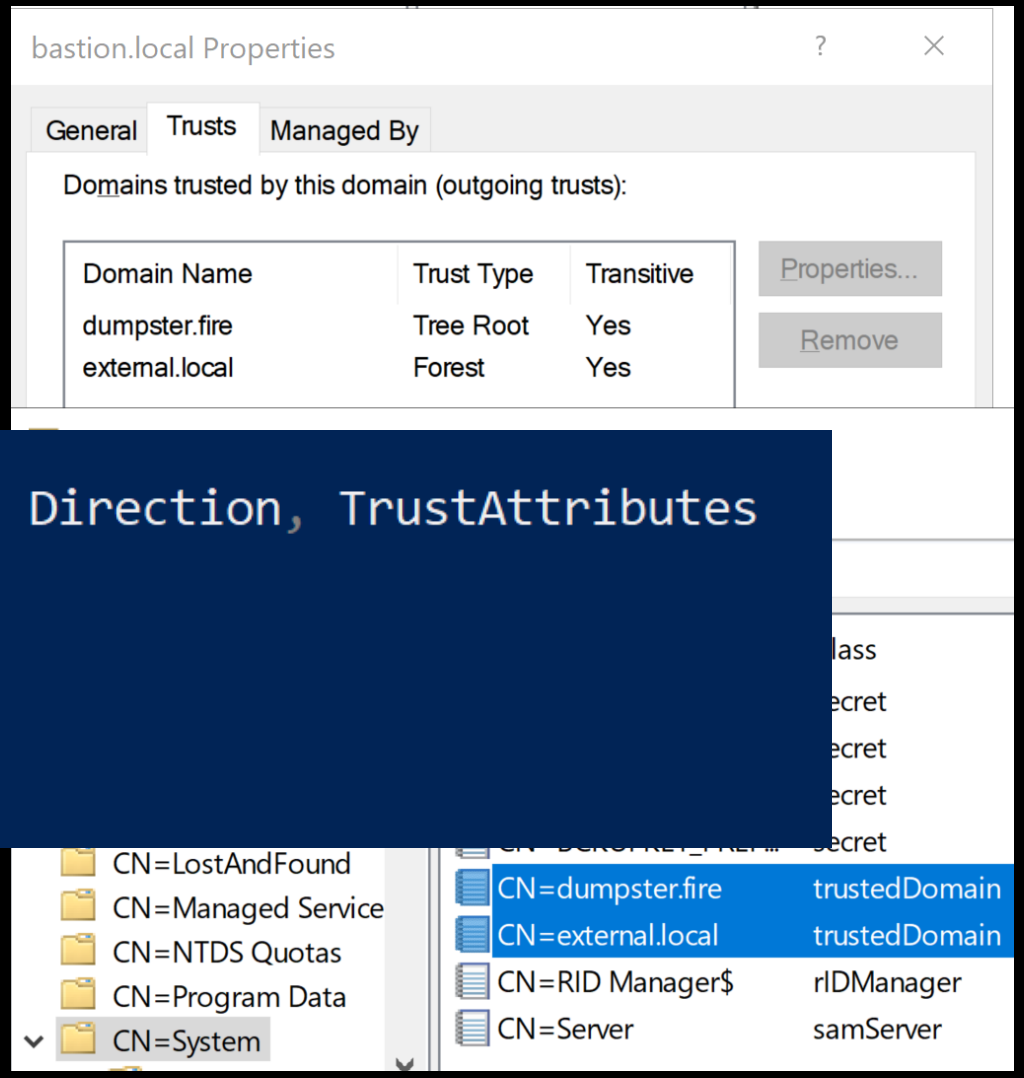
Trusted Domain Objects (TDO)

TrustAttributes

```
PS C:\> Get-ADTrust dumpster.fire | Select Direction, TrustAttributes

    Direction TrustAttributes
    --------- ---------------
BiDirectional              32
```

32 = 0x20: WITHIN_FOREST



TrustAttributes

```
PS C:\> Get-ADTrust attacker.local -Server target.local |
 Select Name, Direction, TrustAttributes, TGTDelegation

Name           Direction TrustAttributes TGTDelegation
----           --------- --------------- -------------
attacker.local   Inbound            2056          True
```

```
PS C:\> Get-ADTrust target.local -Server attacker.local |
 Select Name, Direction, TrustAttributes, TGTDelegation

Name         Direction TrustAttributes TGTDelegation
----         --------- --------------- -------------
target.local  Outbound               8         False
```

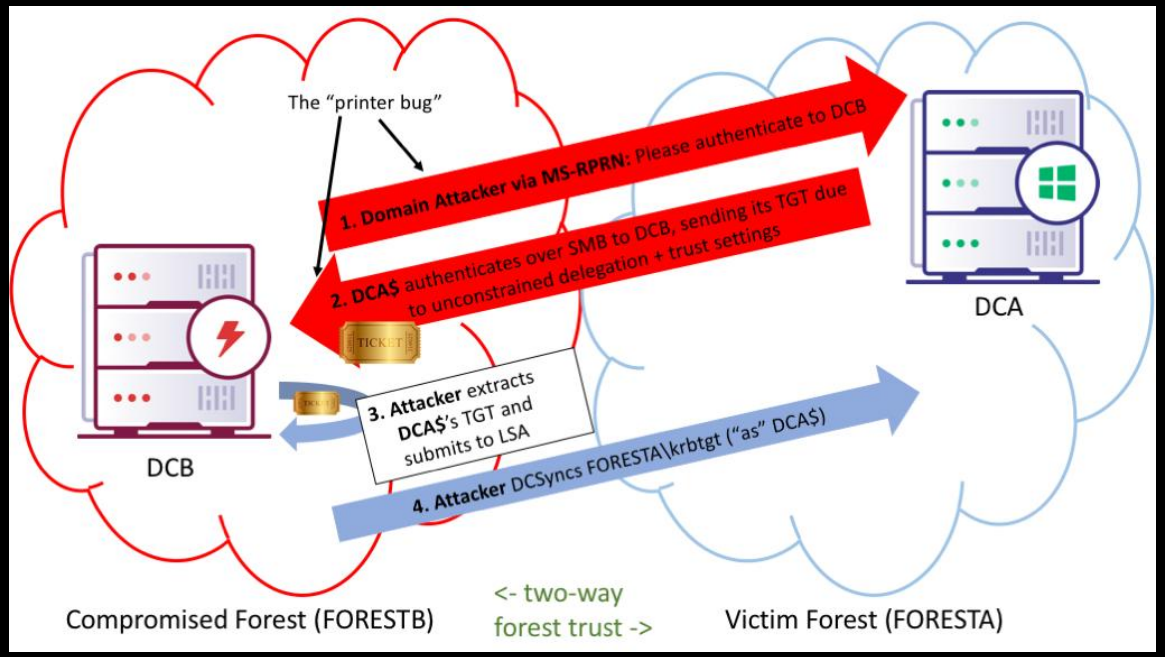
Settings can be set on each side

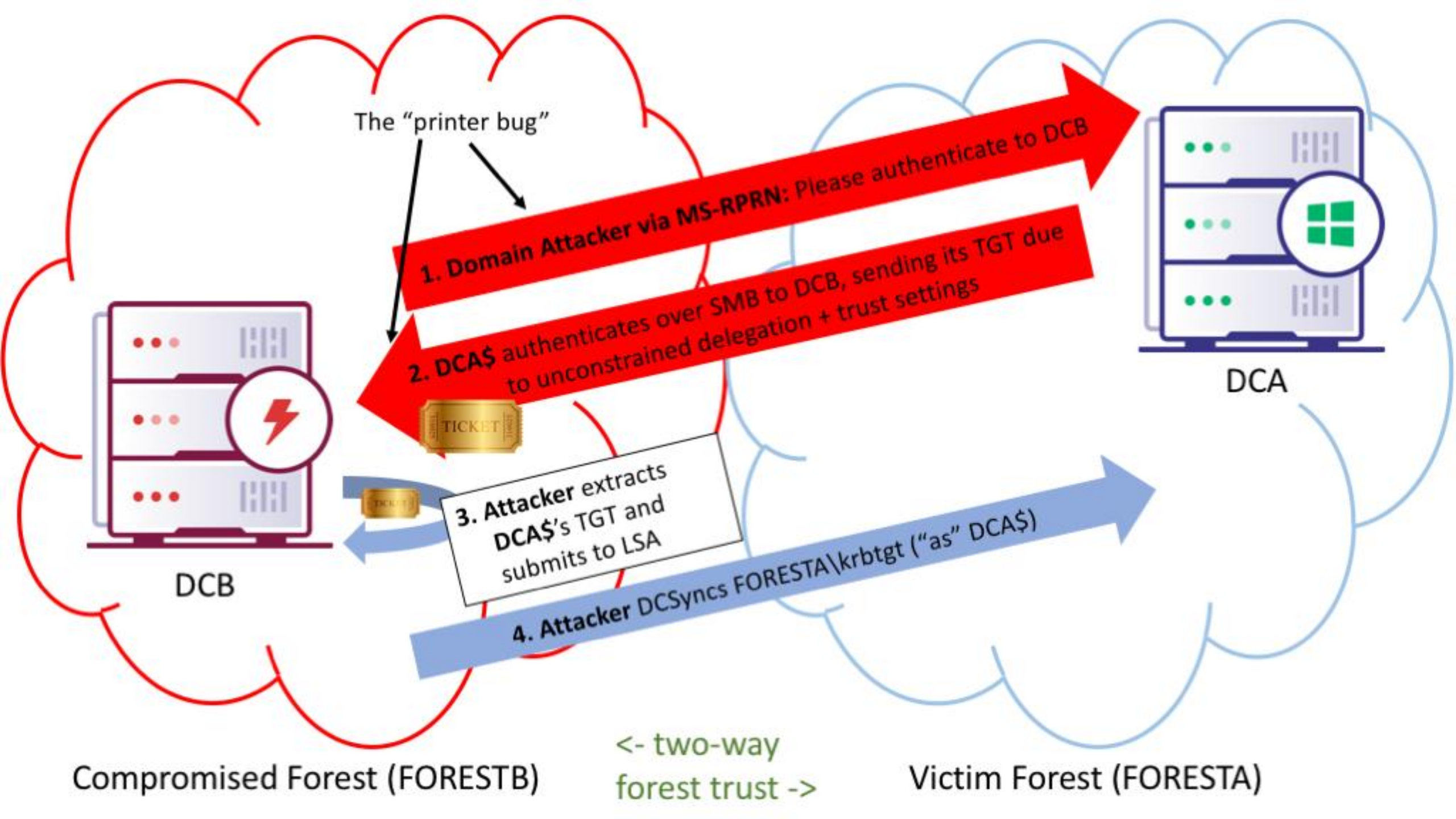
Only one side holds the truth

.. unless it is bidirectional

Attack #1: Abuse TGT Delegation

Not A Security Boundary: Breaking Forest Trusts by Will (harmj0y) Schroeder



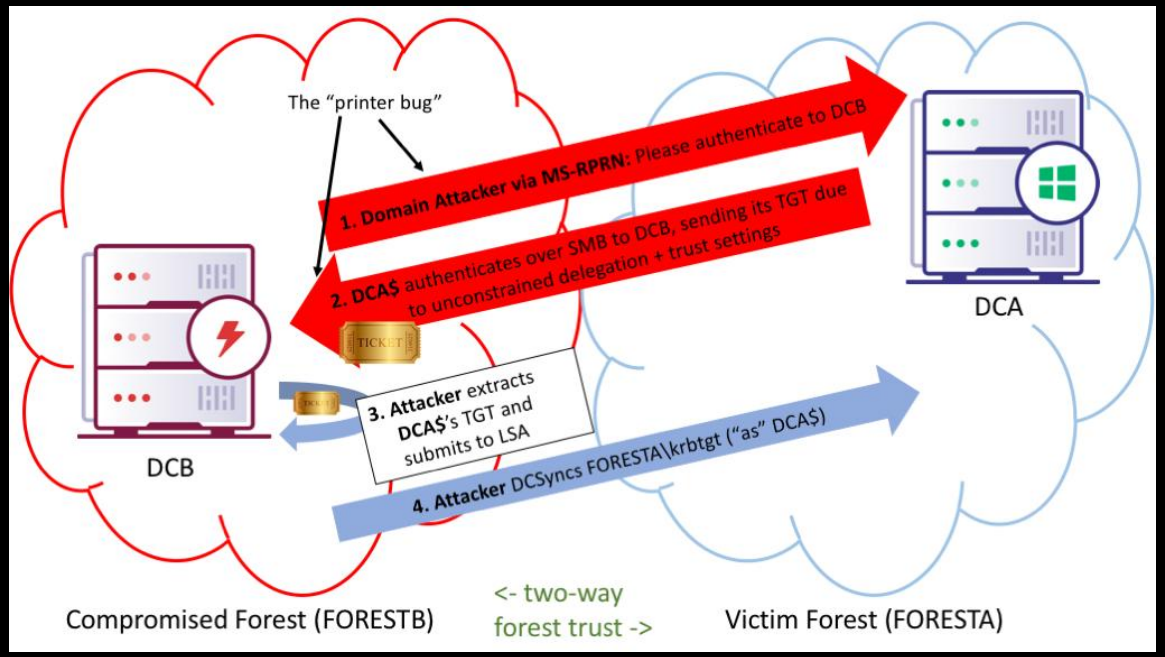

The "printer bug"
1. Domain Attacker via MS-RPRN: Please authenticate to DCB
2. DCA$ authenticates over SMB to DCB, sending its TGT due to unconstrained delegation + trust settings
TICKET
3. Attacker extracts DCA$'s TGT and submits to LSA
4. Attacker DCSyncs FORESTA\krbtgt ("as" DCA$)
DCA
DCB
Compromised Forest (FORESTB)
<- two-way forest trust ->
Victim Forest (FORESTA)

Attack #1: Abuse TGT Delegation

Not A Security Boundary: Breaking Forest Trusts by Will (harmj0y) Schroeder

MS Patch – TrustAttributes flag "ENABLE_TGT_DELEGATION" required on inbound side

Works over one-way trust (attacker -> target)



Attack #2: Spoof SID History

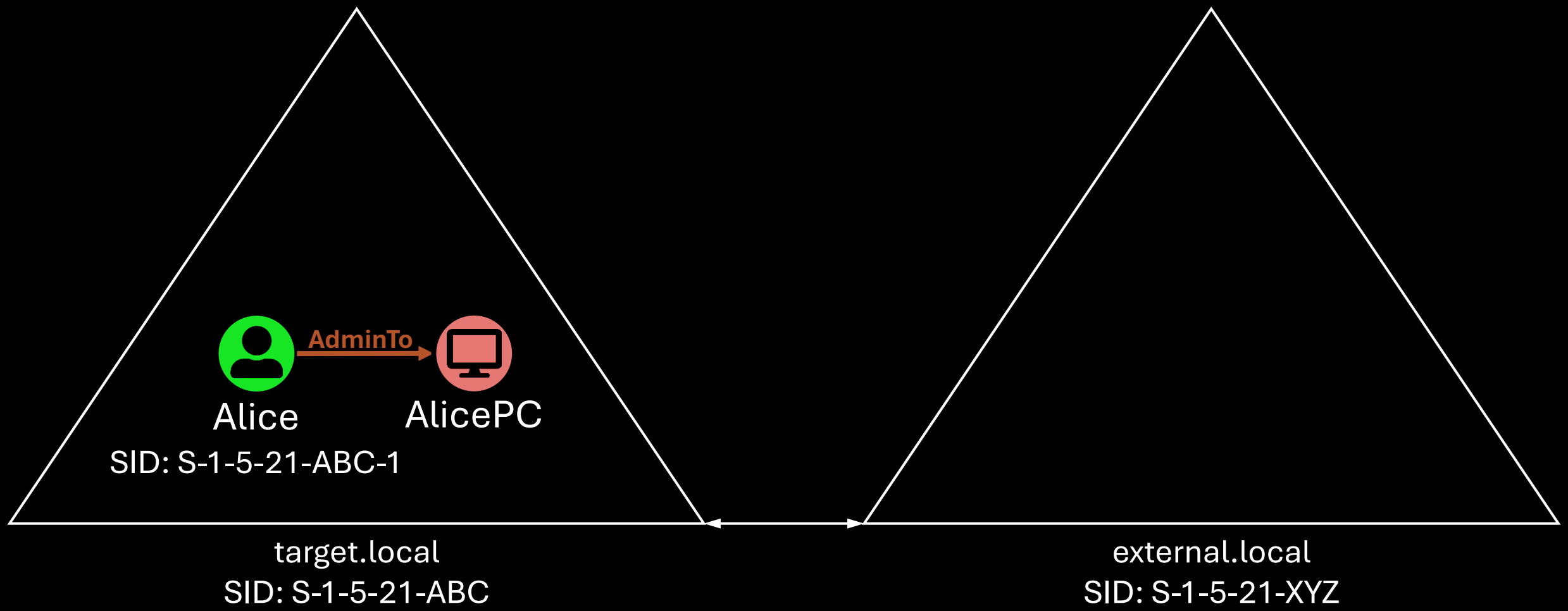
Active Directory Forest Trusts Part 1 - How Does SID Filtering Work?
by Dirk-jan Mollema

Add target's SID to your SID history – get treated as target

Inspired by Sean Metcalf's Kerberos Golden Tickets are Now More Golden

Spoof SID History

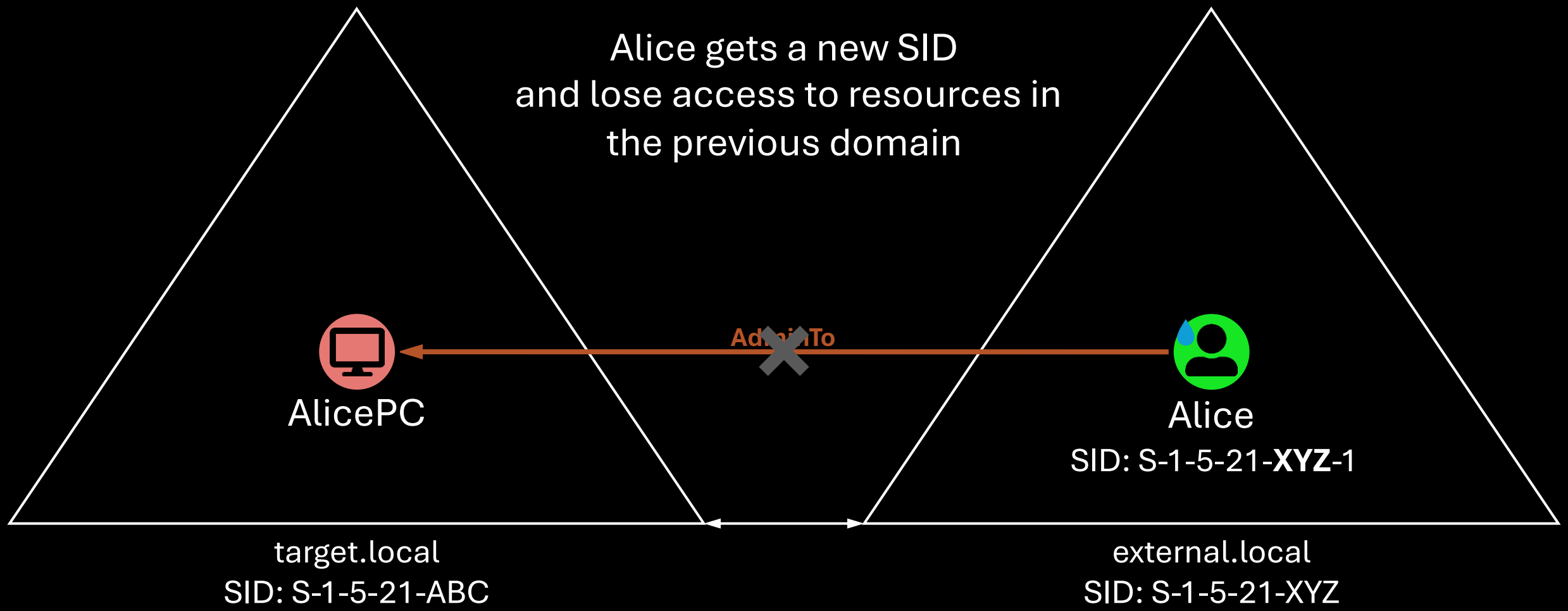
AD migration



Spoof SID History

AD migration

Alice gets a new SID
and lose access to resources in
the previous domain

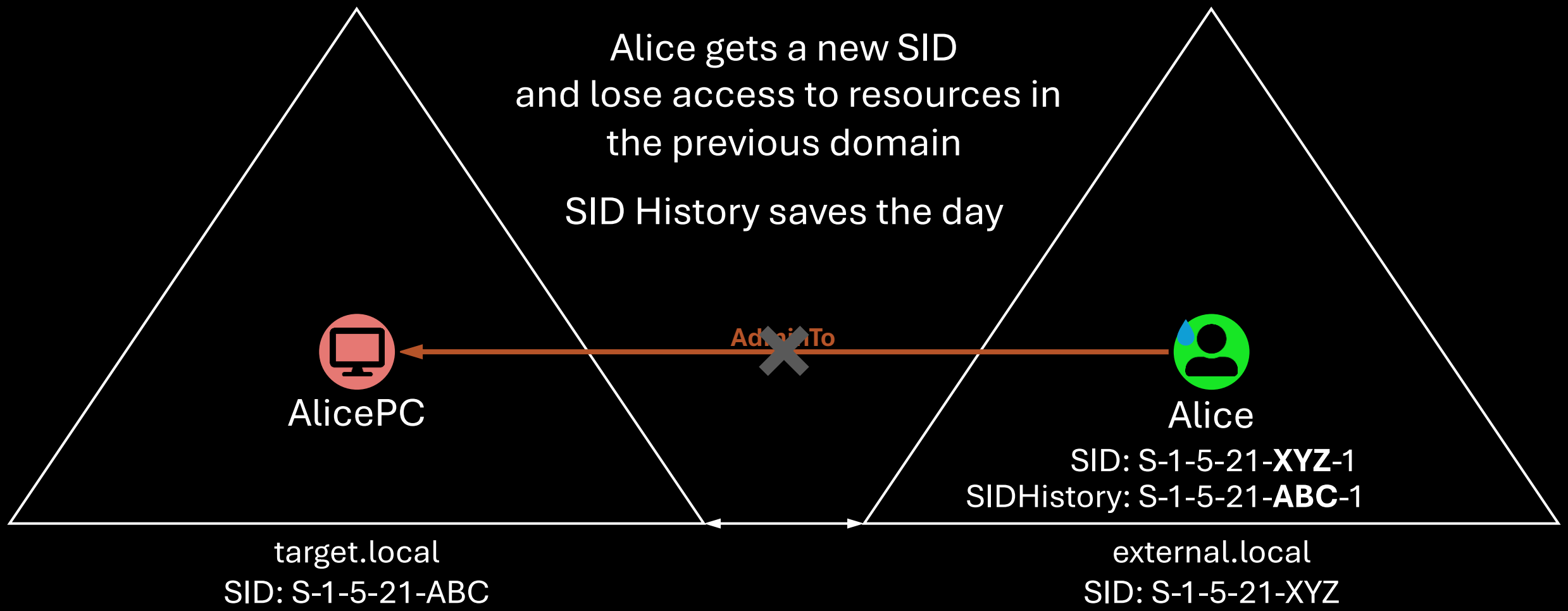


Spoof SID History

AD migration

Alice gets a new SID
and lose access to resources in
the previous domain

SID History saves the day

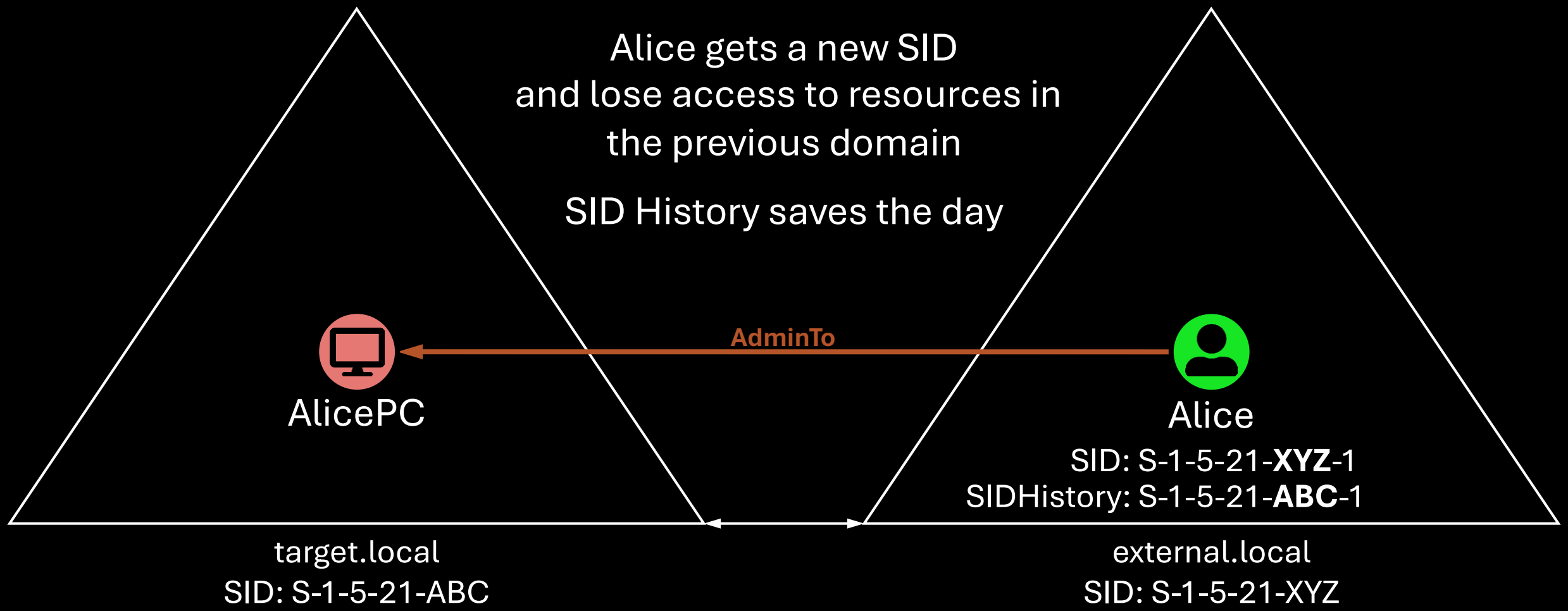


Spoof SID History

AD migration

Alice gets a new SID
and lose access to resources in
the previous domain

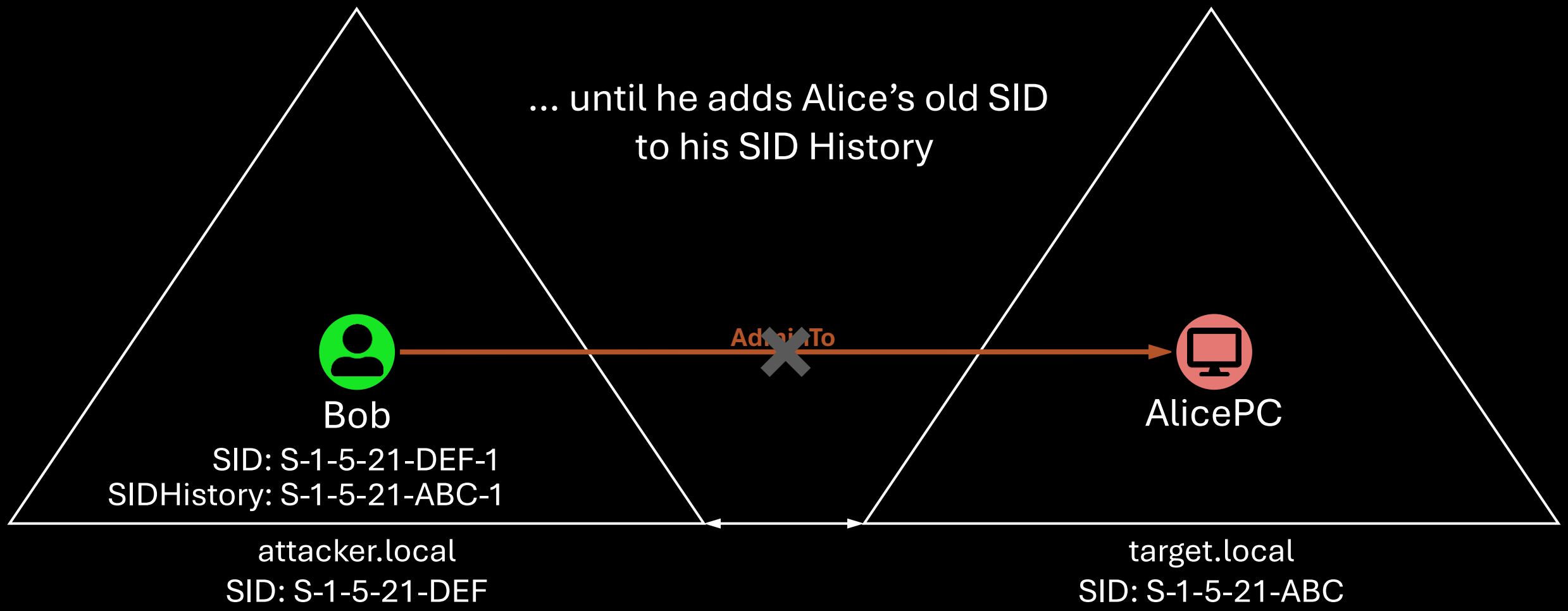
SID History saves the day



Spoof SID History

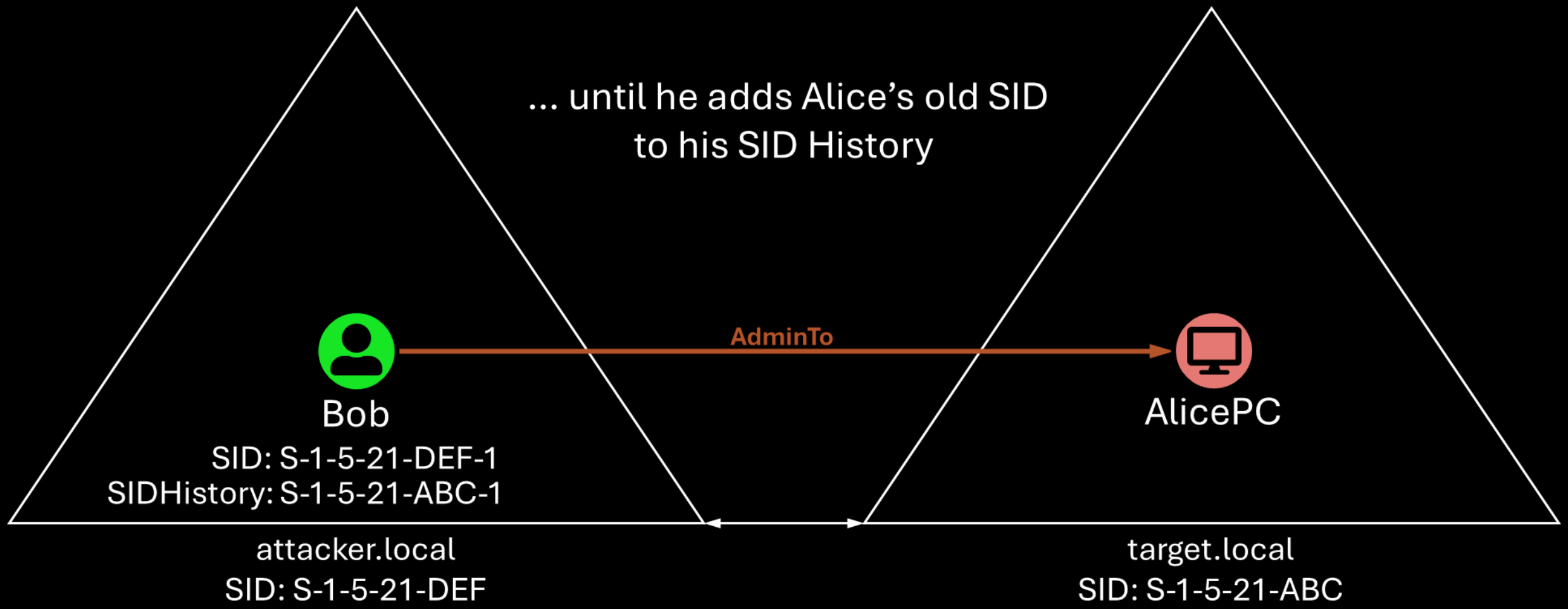
Bob does not have access to AlicePC

... until he adds Alice's old SID
to his SID History



Bob does not have access to AlicePC

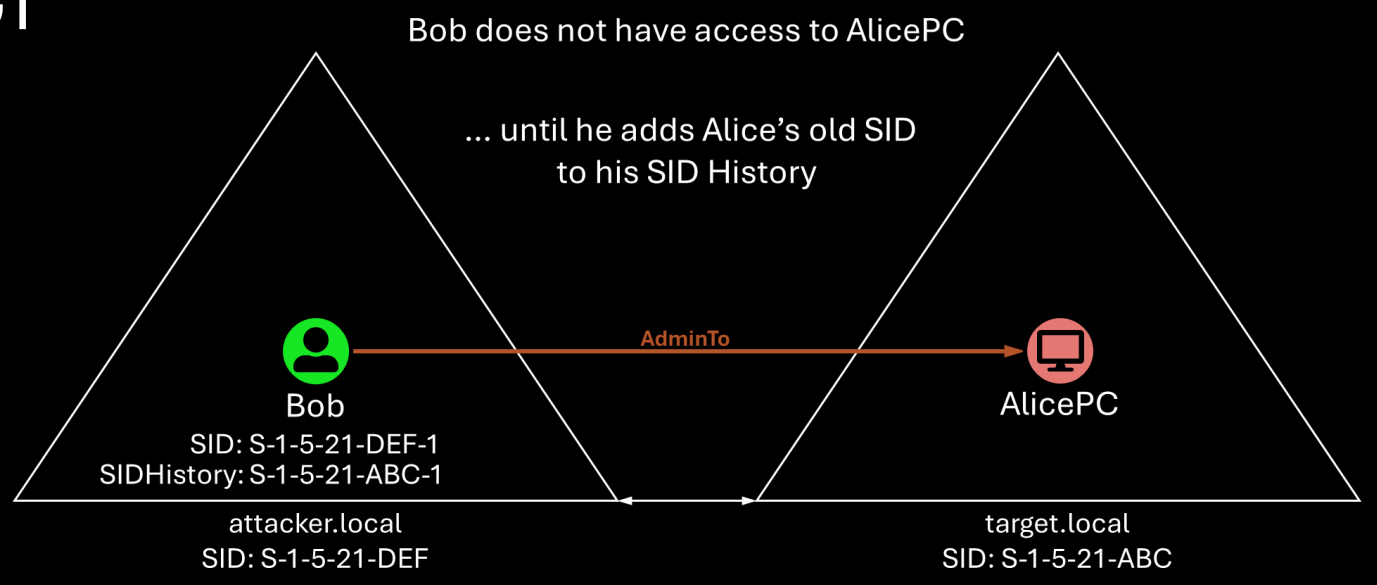
... until he adds Alice's old SID
to his SID History



Spoof SID History – Changing SID History

1. Directly in the AD attribute
   DSInternals: Add-ADDBSidHistory by Michael Grafnetter
2. In the user's TGT
   Rubeus: golden/diamond by GhostPack
3. In the user's inter-realm TGT
   Rubeus: silver by GhostPack

NTLM: Only first method



Spoof SID History – Possible Targets

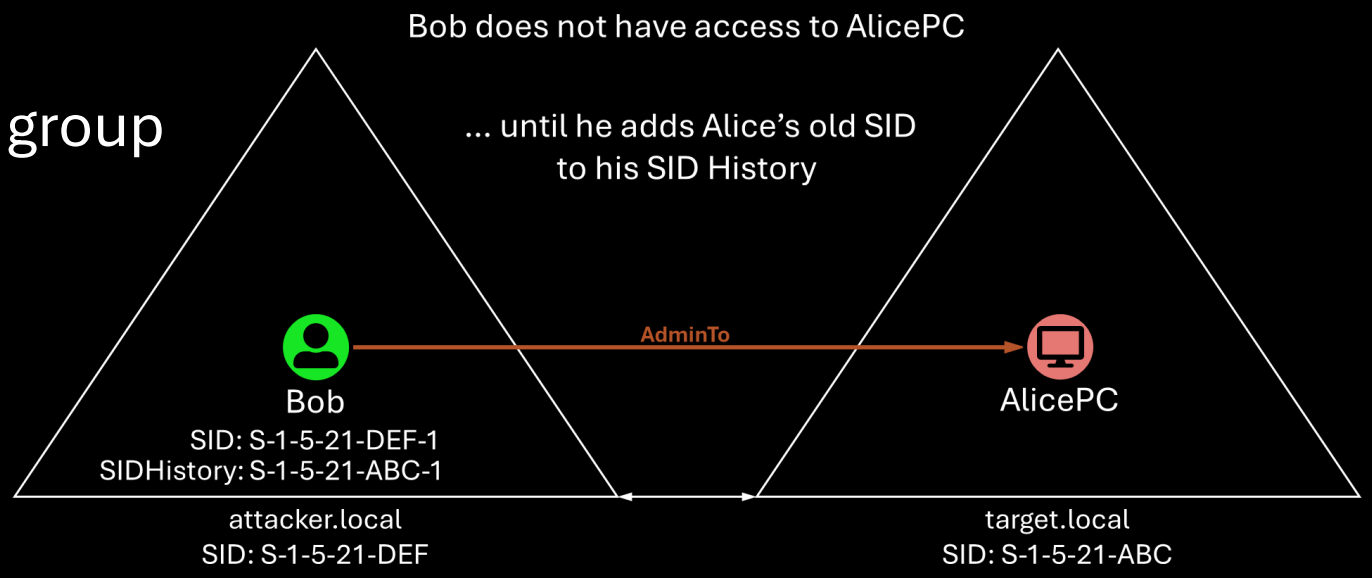
Cross-forest SID filtering always filter out RIDs < 1000

E.g. Enterprise Admins (519)

Memberships in global and universal groups are not applied

You can't target a member of Enterprise Admins

- Exchange Windows Permissions group
- Entra ID sync (MSOL_) accounts
- DCs (requires RBCD attack)



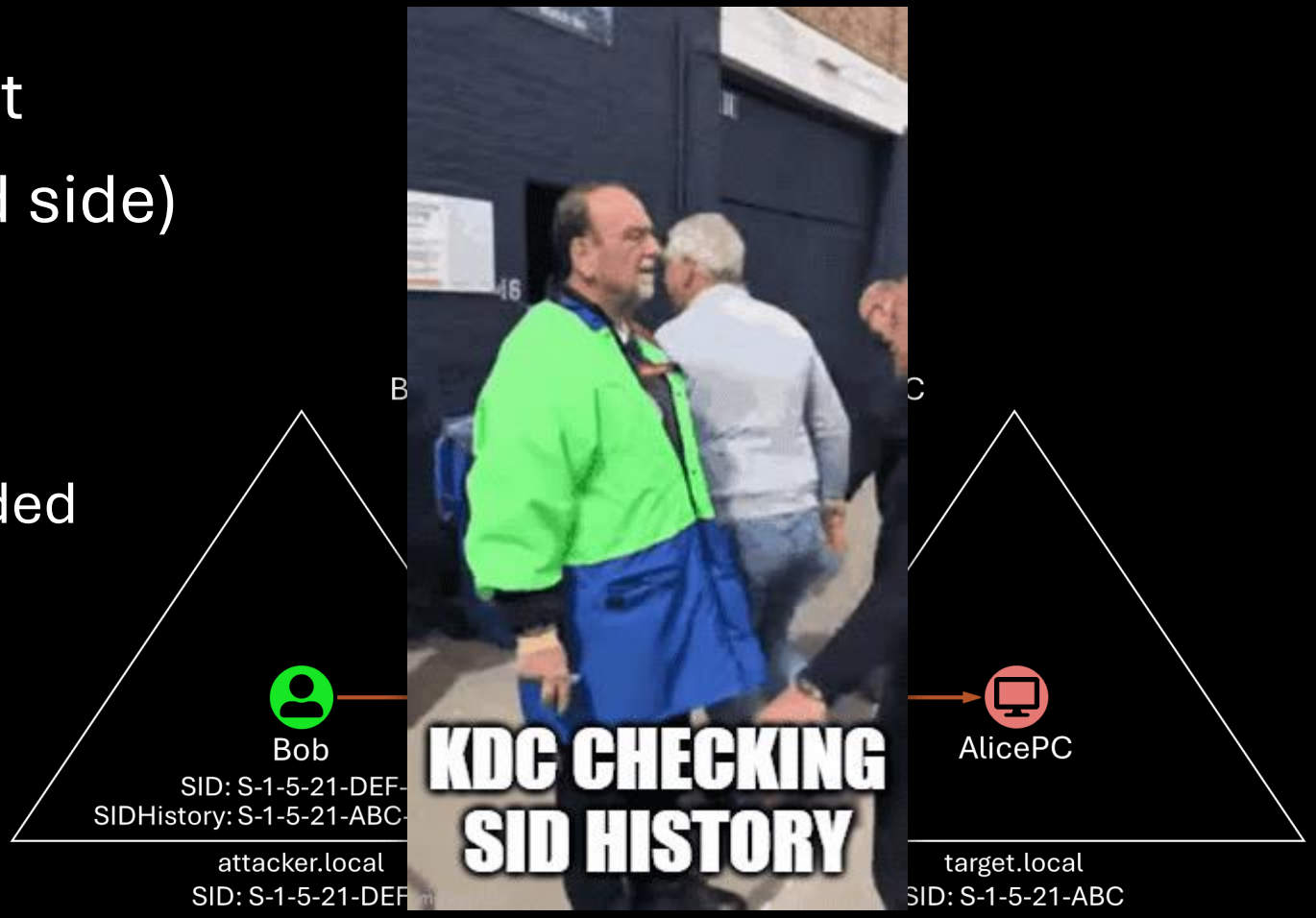
Spoof SID History – Requirements

Cross-forest trust:

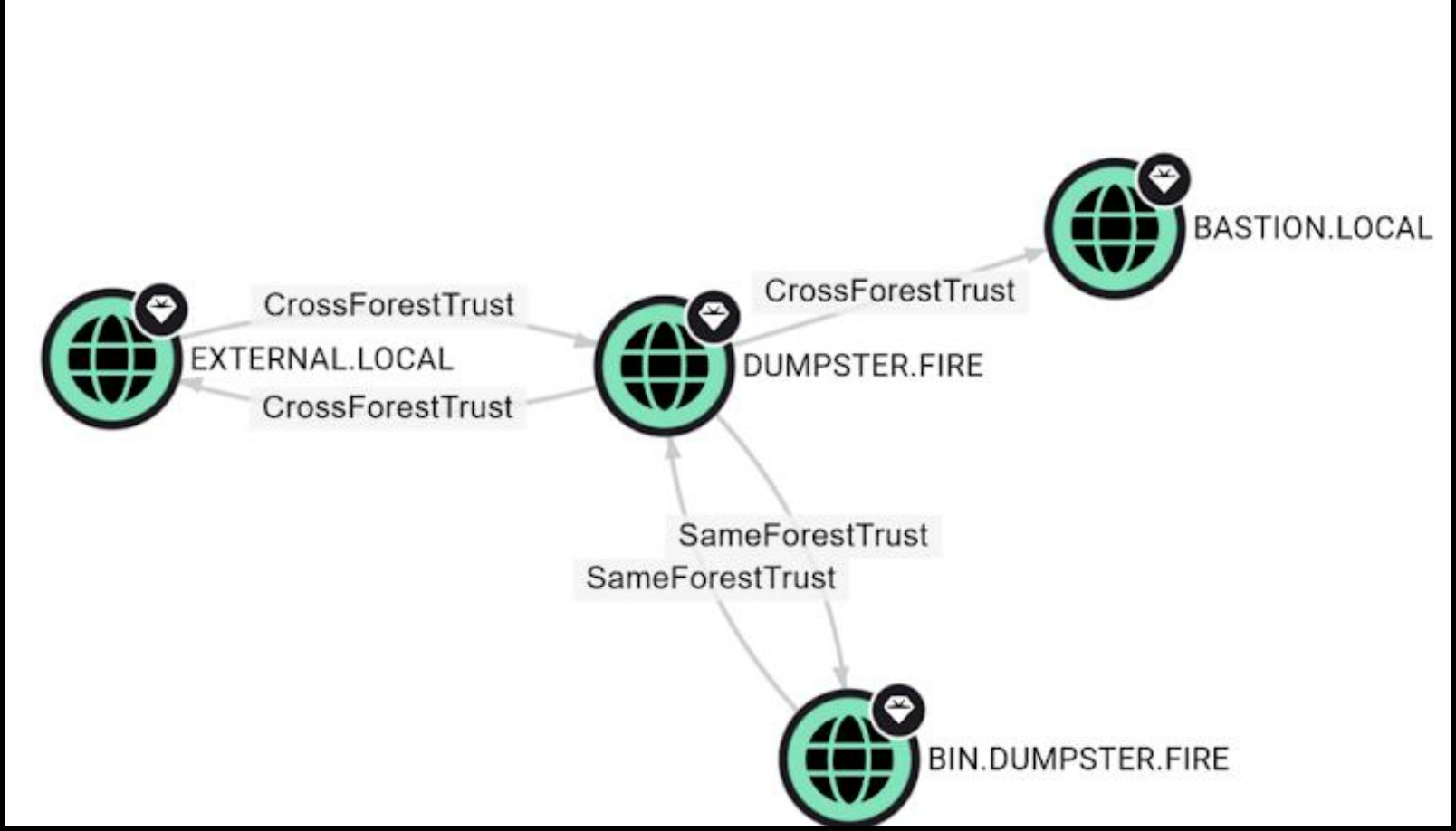
- From target to attacker forest
- Weak SID filtering (outbound side)

TrustAttributes requirements:

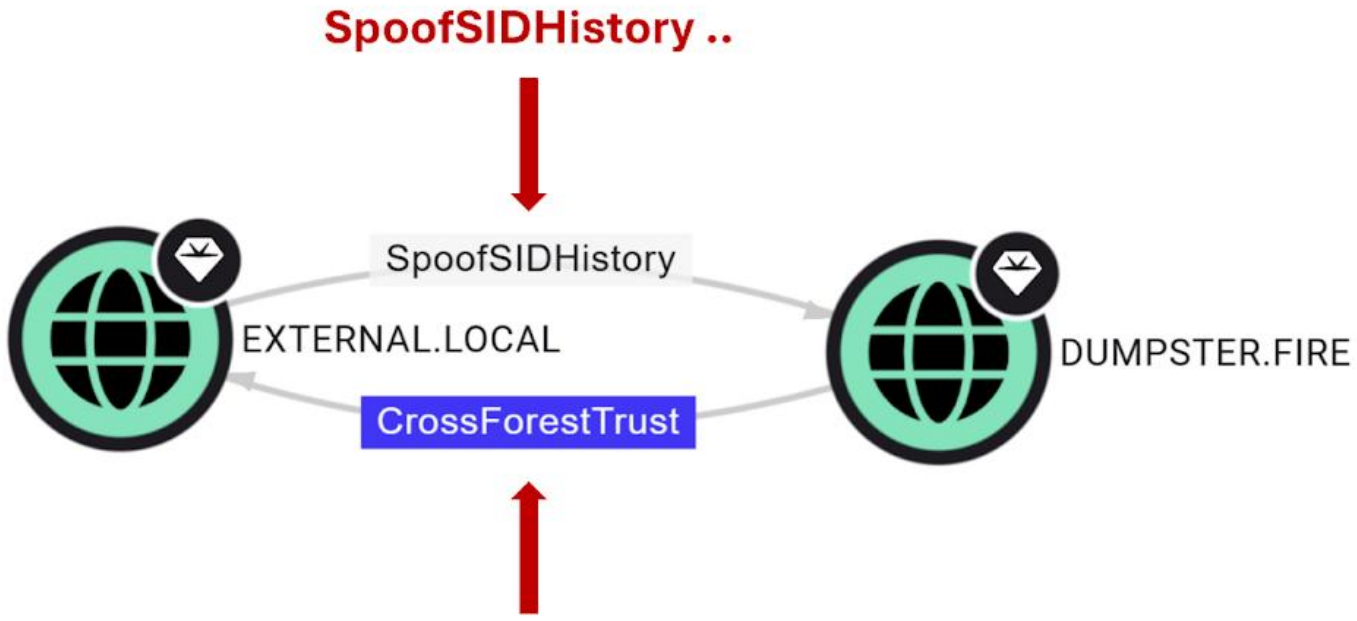
- Forest: TREAT_AS_EXTERNAL added
- External: QUARANTINE removed



New BloodHound edge



Spoof SID History

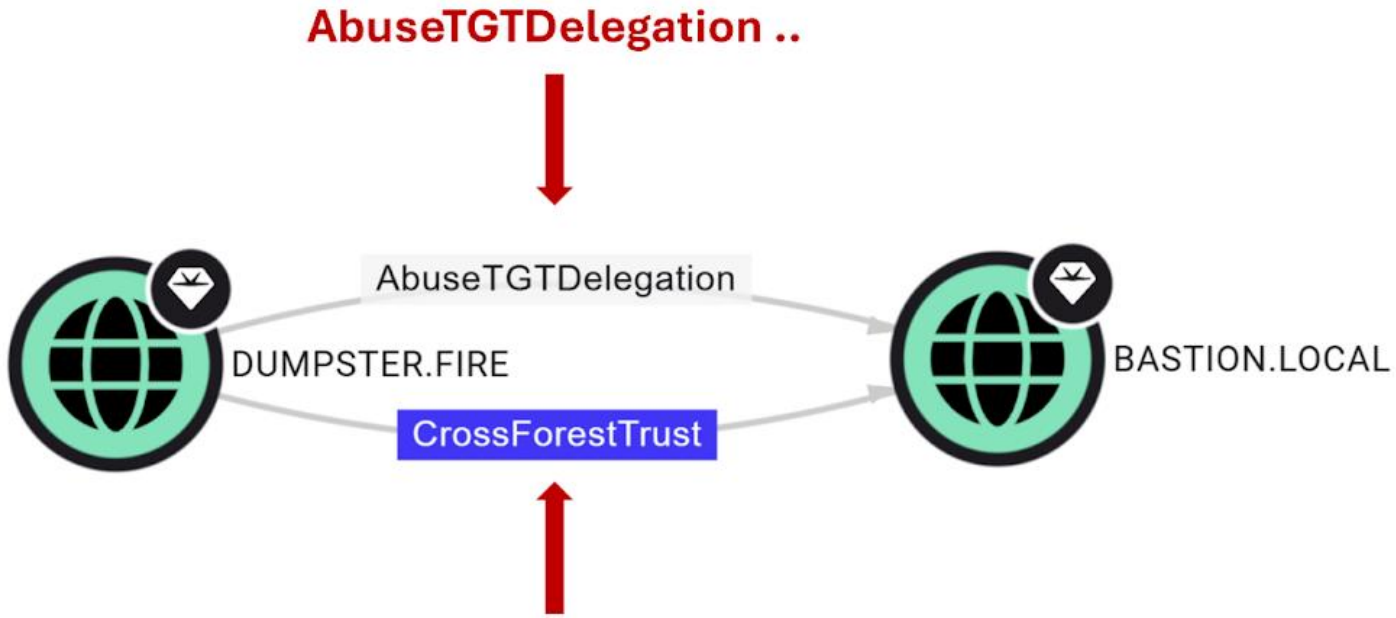


CrossForestTrust

Relationship Information

Source Node:	DUMPSTER.FIRE
Target Node:	EXTERNAL.LOCAL
Is ACL:	FALSE
Last Seen by BloodHound: 2025-05-22 16:47 GMT+2 (GMT+0200)	
Spoof SID History Blocked:	FALSE
Transitive:	FALSE
Trust Attributes (Outbound):	0
Trust Type:	External

Abuse TGT Delegation



CrossForestTrust

Relationship Information

Source Node:	DUMPSTER.FIRE
Target Node:	BASTION.LOCAL
Is ACL:	FALSE
Last Seen by BloodHound: 2025-05-22 16:49 GMT+2 (GMT+0200)	
Spoof SID History Blocked:	TRUE
TGT Delegation:	TRUE
Transitive:	TRUE
Trust Attributes (Inbound):	72
Trust Attributes (Outbound):	8
Trust Type:	Forest

AD forests and trusts 101

Cross-forest trust attack techniques

Creation of abusable cross-forest trusts

Forest jump without AD trust

Who can create AD trusts?

Domain Admins and Enterprise Admins

Incoming Forest Trust Builders

Incoming Forest Trust Builders

Create-Inbound-Forest-Trust extended right on the root domain

Not AdminSDHolder protected

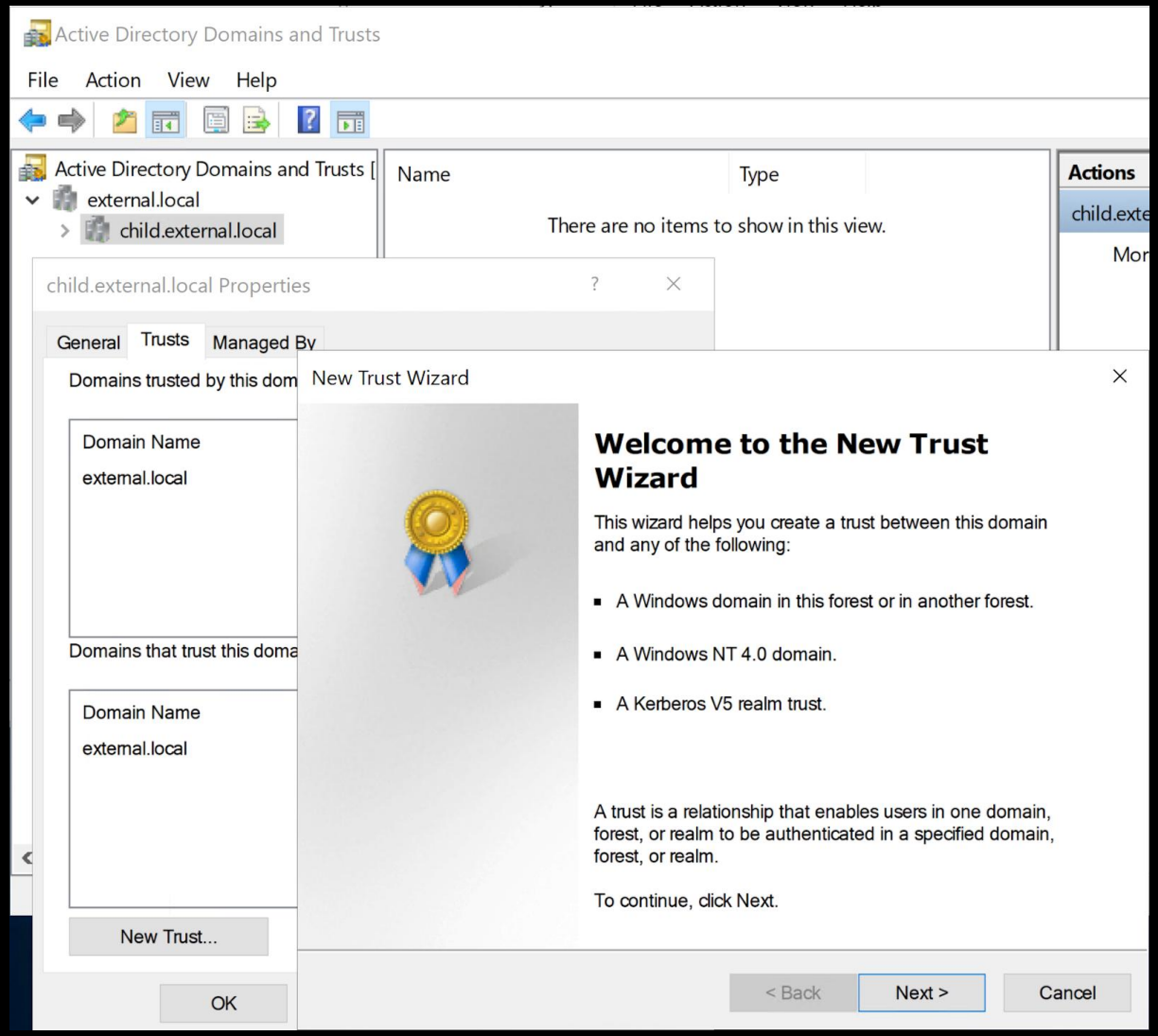
Inbound trusts are abusable if TGT delegation is enabled

Can it create such trusts?

Creating AD Trust with TGT Delegation enabled

Attempt #1: The GUI way

No option for specifying TGT delegation



Creating AD Trust with TGT Delegation enabled

~~Attempt #1: The GUI way~~

Attempt #2: The CMD way

```
netdom trust
```

Creating AD Trust with TGT Delegation enabled

~~Attempt #1: The GUI way~~

Attempt #2: The CMD way

netdom can only enable TGT delegation on existing trusts

```
netdom trust <TrustingDomainName> {/d: |
/domain:} <TrustedDomainName> [{/ud: |
/userd:}[<Domain>\]<User> [{/pd: |
/passwordd:}{<Password>|*}] [{/uo: |
/usero:}<User>] [{/po: |
/passwordo:}{<Password>|*}] [/verify] [/reset]
[/passwordt:<NewRealmTrustPassword>] [/add
[/realm]] [/remove [/force]] [/twoway]
[/kerberos] [/transitive[:{YES|NO}]]
[/oneside:{TRUSTED | TRUSTING}] [/force]
[/quarantine[:{YES | NO}]]
[/namesuffixes:<TrustName> [/togglesuffix:#]]
[/EnableSIDHistory] [/ForestTRANsitive]
[/SelectiveAUTH][/AddTLN][/AddTLNEX][/RemoveTLN]
[/RemoveTLNEX][/SecurePasswordPrompt]
[/EnableTgtDelegation] [{/help | /?}]
```

Creating AD Trust with TGT Delegation enabled

~~Attempt #1: The GUI way~~

~~Attempt #2: The CMD way~~

Attempt #3: After creation

Only DA or EA can modify existing trusts

```
netdom trust <TrustingDomainName> {/d: |
/domain:} <TrustedDomainName> [{/ud: |
/userd:}[<Domain>\]<User> [{/pd: |
/passwordd:}{<Password>|*}] [{/uo: |
/usero:}<User>] [{/po: |
/passwordo:}{<Password>|*}] [/verify] [/reset]
[/passwordt:<NewRealmTrustPassword>] [/add
[/realm]] [/remove [/force]] [/twoway]
[/kerberos] [/transitive[:{YES|NO}]]
[/oneside:{TRUSTED | TRUSTING}] [/force]
[/quarantine[:{YES | NO}]]
[/namesuffixes:<TrustName> [/togglesuffix:#]]
[/EnableSIDHistory] [/ForestTRANsitive]
[/SelectiveAUTH][/AddTLN][/AddTLNEX][/RemoveTLN]
[/RemoveTLNEX][/SecurePasswordPrompt]
[/EnableTgtDelegation] [{/help | /?}]
```

Creating AD Trust with TGT Delegation enabled

~~Attempt #1: The GUI way~~

~~Attempt #2: The CMD way~~

~~Attempt #3: After creation~~

Only DA or EA can modify existing trusts

How are trusts created under the hood?

How are trusts created under the hood?

Wireshark analysis

LsarOpenPolicy3
(Opnum 130)

LsarCreateTrustedDomainEx3
(Opnum 129)

LsarSetForestTrustInformation
(Opnum 74)

Protocol	Length	Info
LSARPC	350	Unknown operation 130 request
LSARPC	234	Unknown operation 130 response

Protocol	Length	Info
LSARPC	1110	Unknown operation 129 request
LSARPC	218	Unknown operation 129 response

Protocol	Length	Info
LSARPC	829	lsa_LSARSETFORESTTRUSTINFORMATION request[Long frame (627 bytes)]
LSARPC	206	lsa_LSARSETFORESTTRUSTINFORMATION response[Long frame (8 bytes)]

How are trusts created under the hood?

```
LsarCreateTrustedDomainEx3(
  [in] LSAPR_HANDLE PolicyHandle,
  [in] PLSAPR_TRUSTED_DOMAIN_INFORMATION_EX TrustedDomainInformation,
  [in] PLSAPR_TRUSTED_DOMAIN_AUTH_INFORMATION_INTERNAL_AES
AuthenticationInformation,
  [in] ACCESS_MASK DesiredAccess,
  [out] LSAPR_HANDLE* TrustedDomainHandle
);
```

How are trusts created under the hood?

```
typedef struct _LSAPR_TRUSTED_DOMAIN_INFORMATION_EX {
  RPC_UNICODE_STRING Name;
  RPC_UNICODE_STRING FlatName;
  PRPC_SID Sid;
  unsigned long TrustDirection;
  unsigned long TrustType;
  unsigned long TrustAttributes;
} LSAPR_TRUSTED_DOMAIN_INFORMATION_EX,
*PLSAPR_TRUSTED_DOMAIN_INFORMATION_EX;
```

How are trusts created under the hood?

`LSAPR_TRUSTED_DOMAIN_INFORMATION_EX – TrustAttributes`

ENABLE_TGT_DELEGATION flag is missing..

Did Microsoft forget to add it?

Value	Mapping
TANT (TRUST_ATTRIBUTE_NON_TRANSITIVE)	Trust Attributes: Non-transitive
TAUO (TRUST_ATTRIBUTE_UPLEVEL_ONLY)	Trust Attributes: Uplevel only
TAQD (TRUST_ATTRIBUTE_QUARANTINED_DOMAIN)	Trust Attributes: Quarantined
TAFT (TRUST_ATTRIBUTE_FOREST_TRANSITIVE)	Trust Attributes: Forest trust
TACO (TRUST_ATTRIBUTE_CROSS_ORGANIZATION)	Trust Attributes: Cross organization
TAWF (TRUST_ATTRIBUTE_WITHIN_FOREST)	Trust Attributes: Within forest
TATE (TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL)	Trust Attributes: Treat as external
TARC (TRUST_ATTRIBUTE_USES_RC4_ENCRYPTION)	Trust Attributes: Use RC4 Encryption (for more information about RC4, see [SCHNEIER] section 17.1).
TANC (TRUST_ATTRIBUTE_CROSS_ORGANIZATION_NO_TGT_DELEGATION)	Trust Attributes: Tokens must not be trusted for delegation.
TAPT (TRUST_ATTRIBUTE_PIM_TRUST)	Trust Attributes: PrivilegedIdentityManagement (PIM) trust.
O	Obsolete. SHOULD be set to 0.
R	Reserved for future use. SHOULD be set to zero.

How are trusts created under the hood?

`LSAPR_TRUSTED_DOMAIN_INFORMATION_EX – TrustAttributes`

ENABLE_TGT_DELEGATION flag is missing..

Did Microsoft forget to add it?

Building a trust creation POC

PowerShell script to interact with the RPC server

NtObjectManager by James Forshaw (tiraniddo) makes it possible

LsarCreateTrustedDomainEx3: AES encrypted trust keys

LsarCreateTrustedDomainEx: Plaintext trust password ☺

Testing trust creation POC

TrustAttributes = 2056 (0x00000808)
FOREST_TRANSITIVE
ENABLE_TGT_DELEGATION

It worked!

```
PS C:\> Get-ADTrust attacker.local -Server target.local |
 Select Direction, TrustAttributes, TGTDelegation

Direction TrustAttributes TGTDelegation
--------- --------------- -------------
  Inbound            2056          True
```

Testing the abuse TGT delegation attack

Coercion failed

Testi

TrustAt

It work

Testing

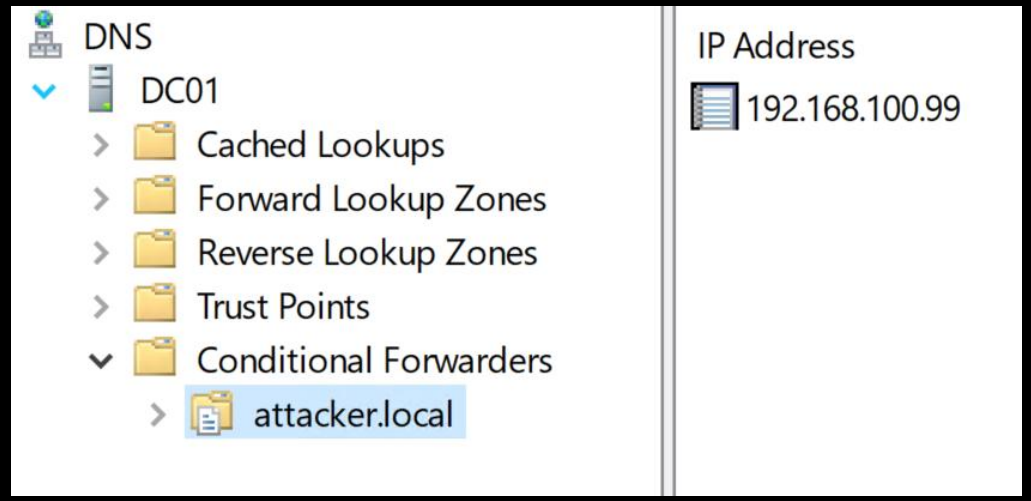
er target.local |
elegation

Coercion failed

It’s always DNS

Kerberos requires a conditional forwarder

Only DnsAdmins (and Domain Admins) can create those..



Coercion failed

It’s always DNS

Kerberos requires a conditional forwarder

Only DnsAdmins (and Domain Admins) can create those..

Zooming out a bit

How commonly is Incoming Forest Trust Builders used?

- 0 members in all ADs I've checked

Who can add themselves to the group?

- Account Operators

Account Operators controls DnsAdmins too

~~Incoming Forest Trust Builders~~
Account Operators Attack

Account Operator -> Domain Admins is already common

- Full control over users, groups, and non-DC computers (unless AdminSDHolder protected)

Most Account Operators attacks rely on:

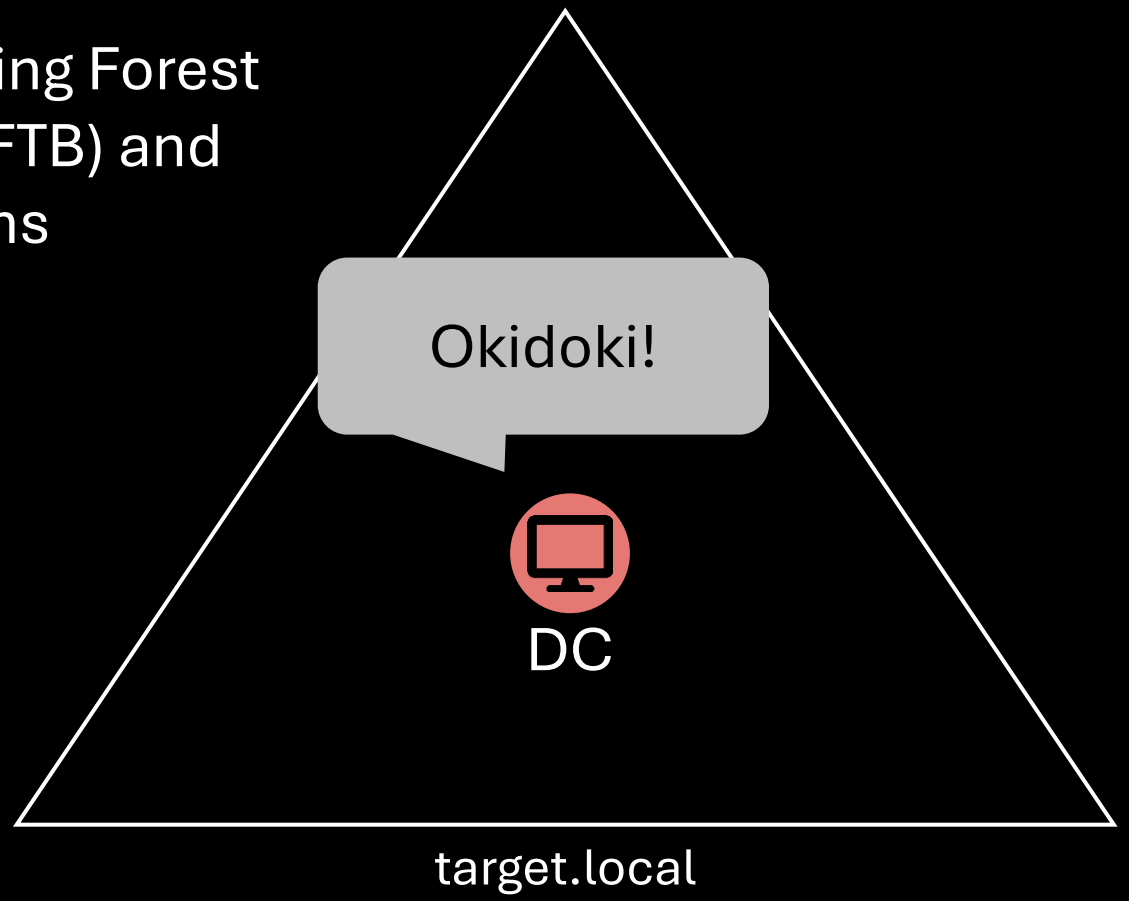
- Custom permissions
- Weak configurations

This attack works in vanilla AD

Account Operators Replicating Trust Attack (AORTA)

Operator is member of Account Operators in target.local

.. and now Incoming Forest Trust Builders (IFTB) and DnsAdmins



Account Operators Replicating Trust Attack (AORTA)

Operator creates a domain named attacker.local

.. and establishes a forest trust from attacker.local to target.local with TGT delegation enabled

(incl. DNS conditional forwarder)

Hey DC, attacker.local trusts your domain, aight?

TARGET\Operator

Okidoki!

DC

attacker.local

TGT delegation: Enabled

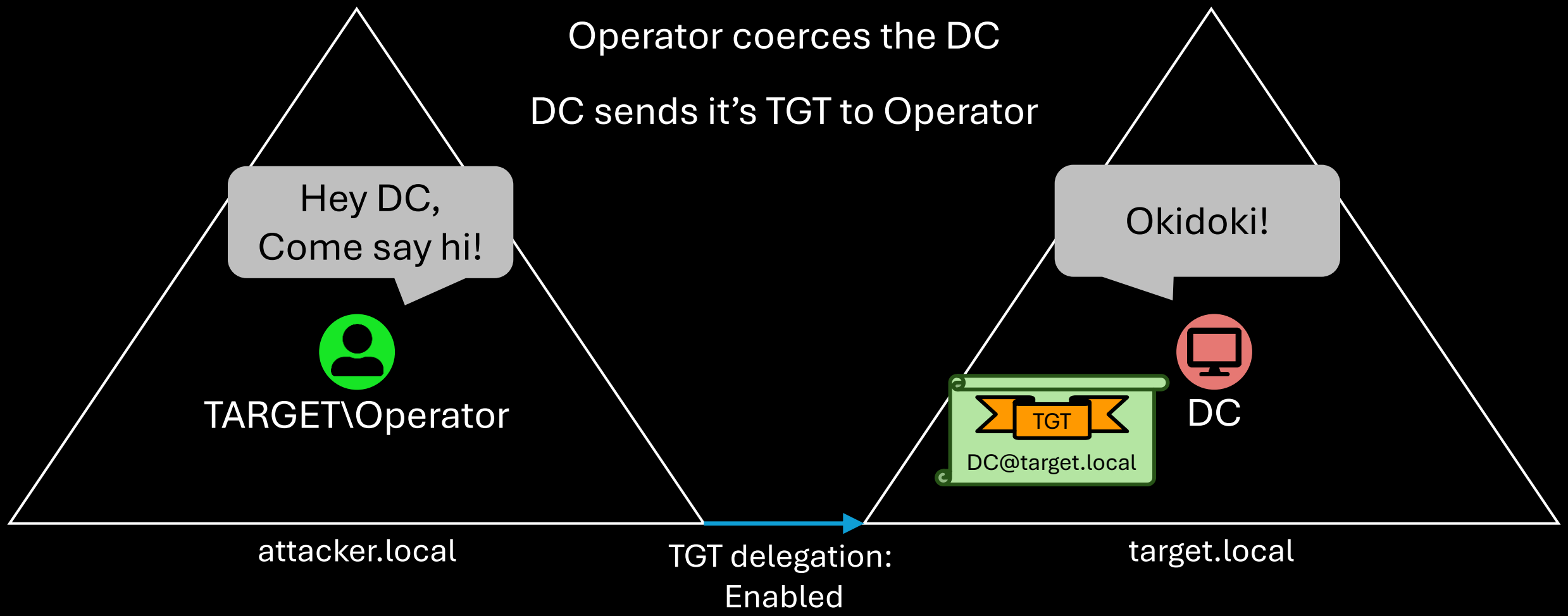
target.local

Account Operators Replicating Trust Attack (AORTA)

Operator is on a server with unconstrained delegation in attacker.local

Operator coerces the DC

DC sends it's TGT to Operator



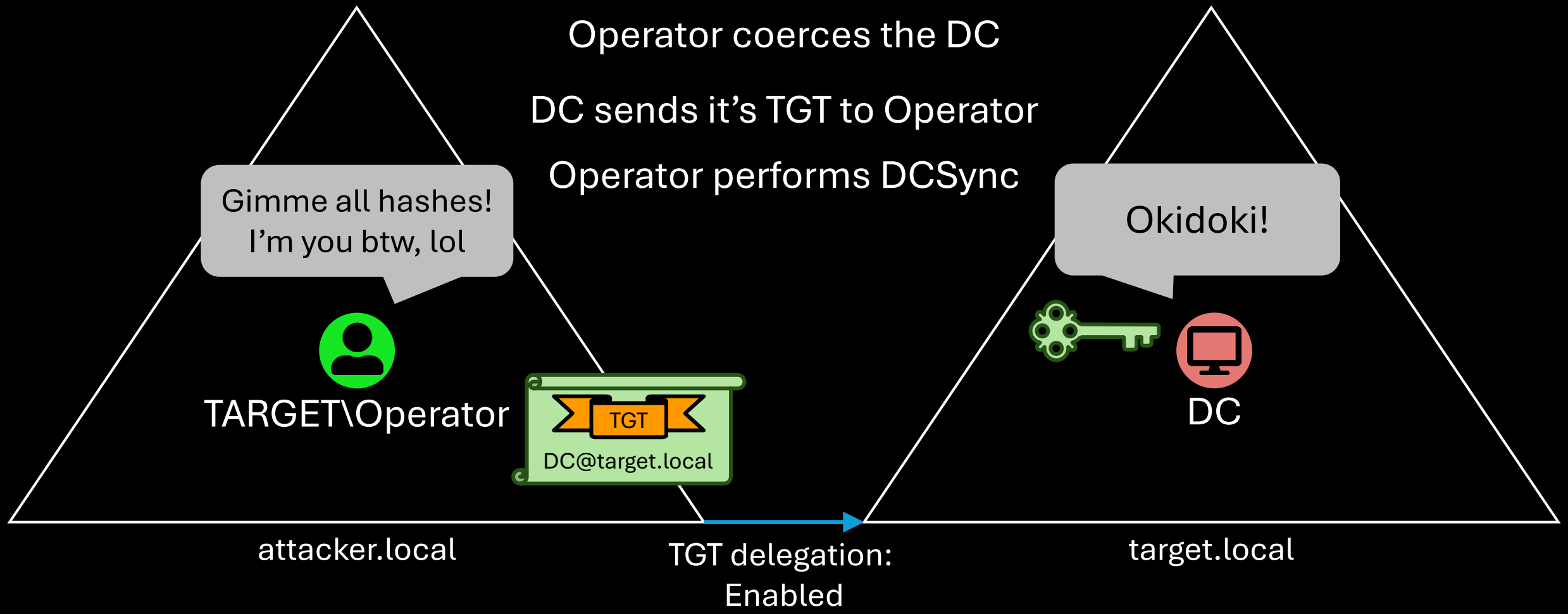
Account Operators Replicating Trust Attack (AORTA)

Operator is on a server with unconstrained delegation in attacker.local

Operator coerces the DC

DC sends it's TGT to Operator

Operator performs DCSync



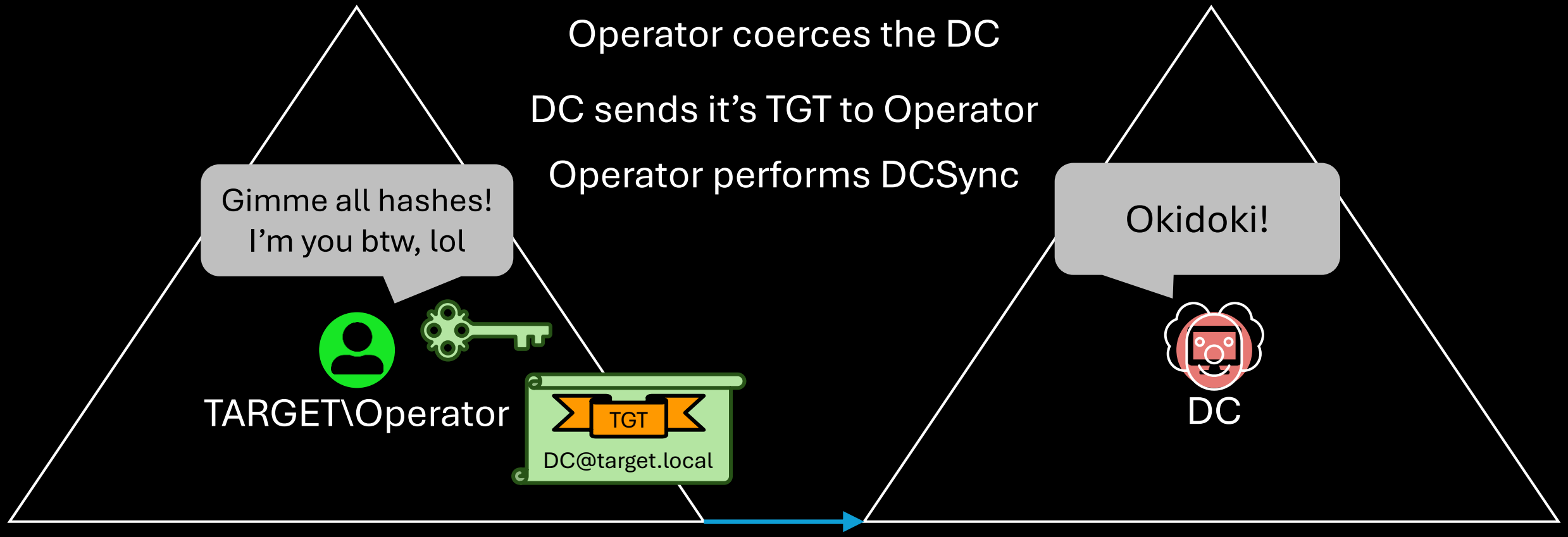
Account Operators Replicating Trust Attack (AORTA)

Operator is on a server with unconstrained delegation in attacker.local

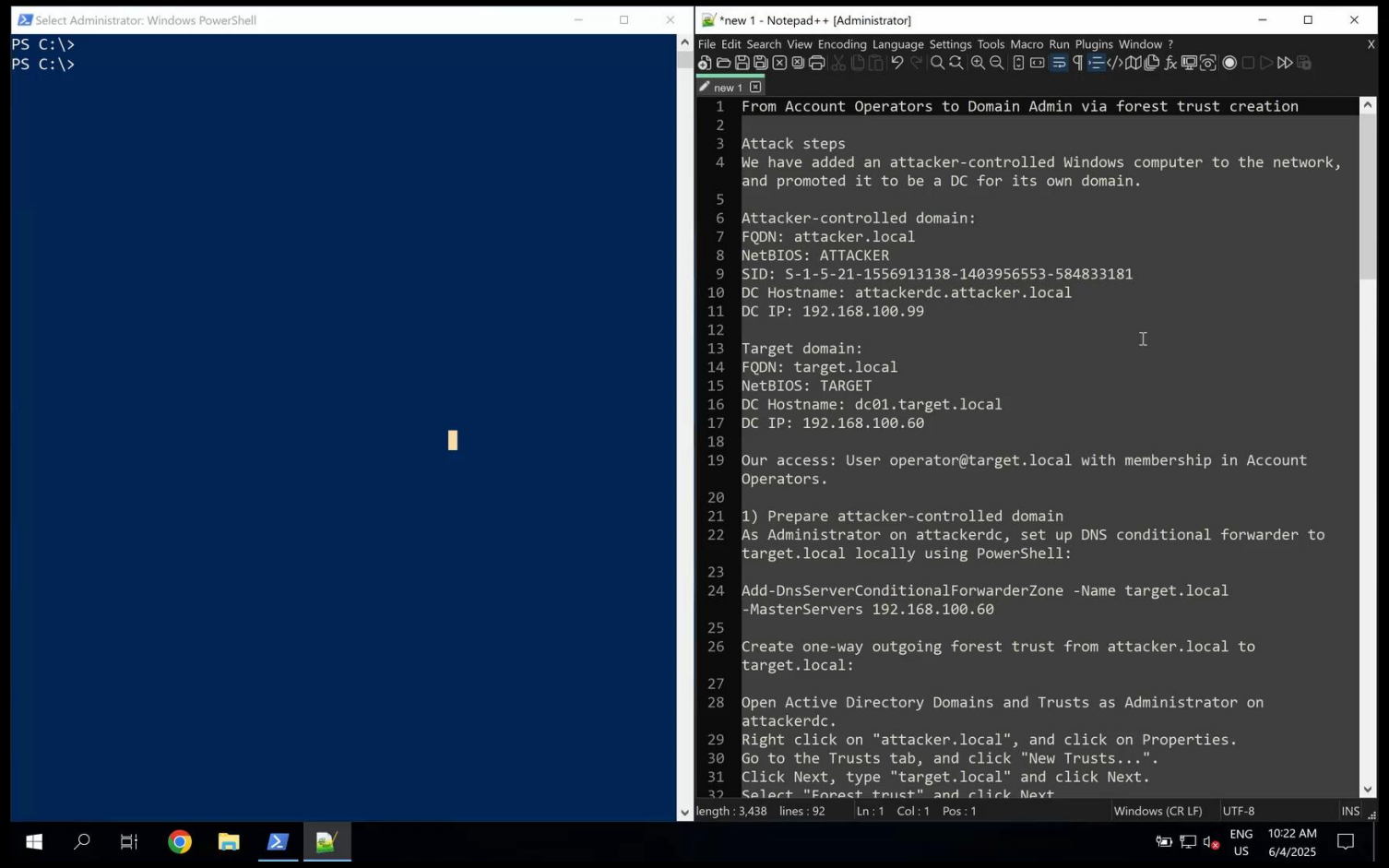
Operator coerces the DC

DC sends it's TGT to Operator

Operator performs DCSync



Account Operators Replicating Trust Attack (AORTA) Demo



https://drive.google.com/file/d/10aqMFcC5ngslAOrk6vGXTudpPb7sQmra/view?usp=sharing

Microsoft Response Center response

"Moderate security" – no patch

Incoming Forest Trust Builders description update:

Members of this group can create incoming, one-way trusts to this forest. (Creation of outbound forest trusts is reserved for Enterprise Admins.)

New

Members of this group can create incoming trusts that allow TGT delegation which can lead to compromise of your forest. To learn more about TGT delegation across incoming trust, Updates to TGT delegation across incoming trusts in Windows Server.

New Tool: Trustify

Made by Valdemar Carøe

Create forest trusts with TGT delegation

Uses advapi32.dll – not RPC directly

Available on GitHub:

https://github.com/bytewreck/Trustify

README BSD-3-Clause license

Trustify

License BSD 3-Clause Windows 11

Trustify is a command-line tool for creating (and deleting) inbound Active Directory forest trusts with TGT delegation enabled using native Windows LSA APIs.

Usage

```
Trustify.exe [create|delete] ...
```

Create Trust

```
Trustify.exe create [target] [sid] [dns] [netbios] [password]
```

- `target` : The remote domain where the trust is created (e.g. `domain.com`)
- `sid` : SID of the trusted domain (e.g. `S-1-5-21-...`)
- `dns` : DNS name of the trusted domain
- `netbios` : NetBIOS name of the trusted domain
- `password` : Trust password (plaintext)

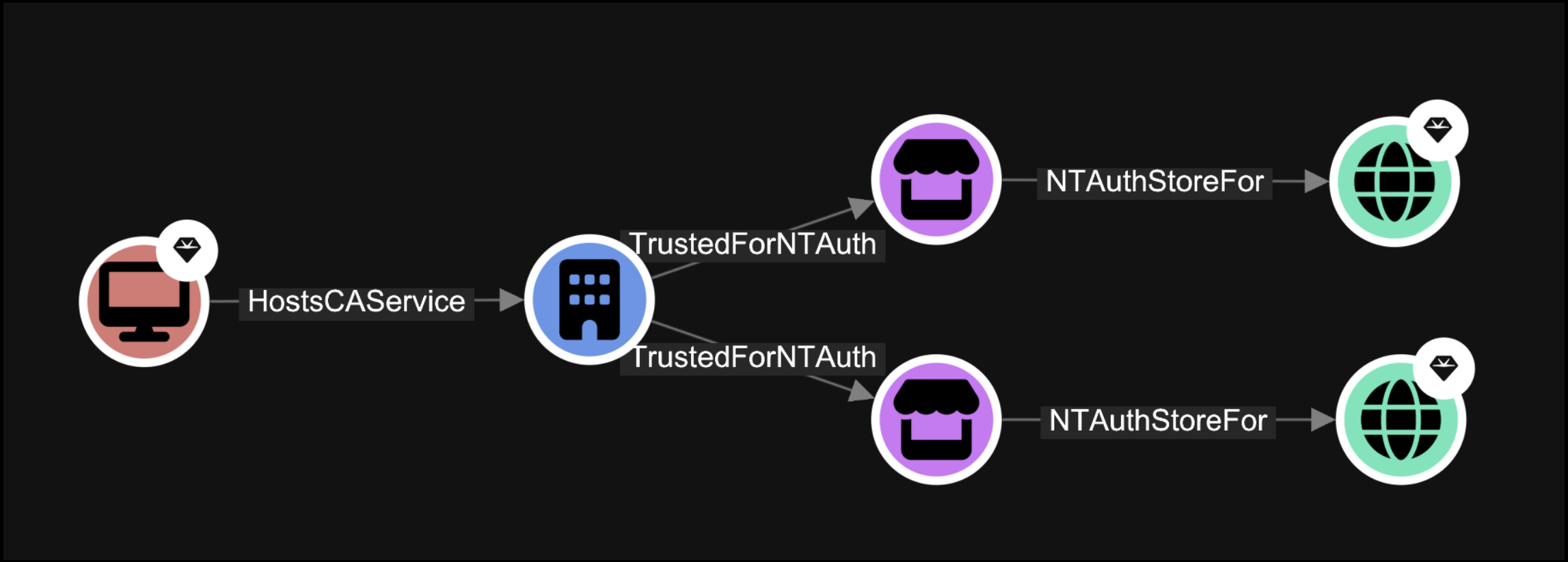
AD forests and trusts 101

Cross-forest trust attack techniques

Creation of abusable cross-forest trusts

Forest jump without AD trust

ADCS (Active Directory Certificate Services)



SCCM (Configuration Manager)

ADCS (Active Directory Certificate Services)

Communications across Active Directory forests

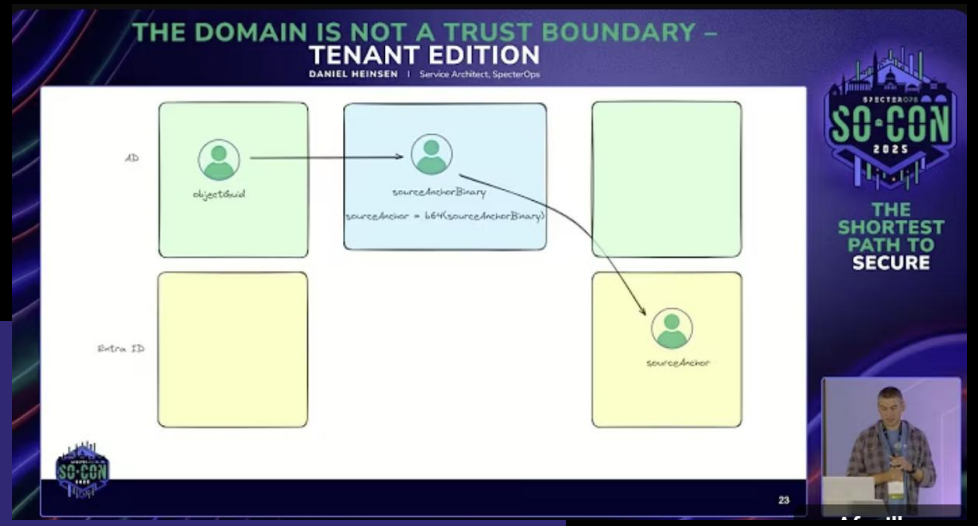
Configuration Manager supports sites and hierarchies that span Active Directory forests. It also supports domain computers that aren't in the same Active Directory forest as the site server, and computers that are in workgroups.

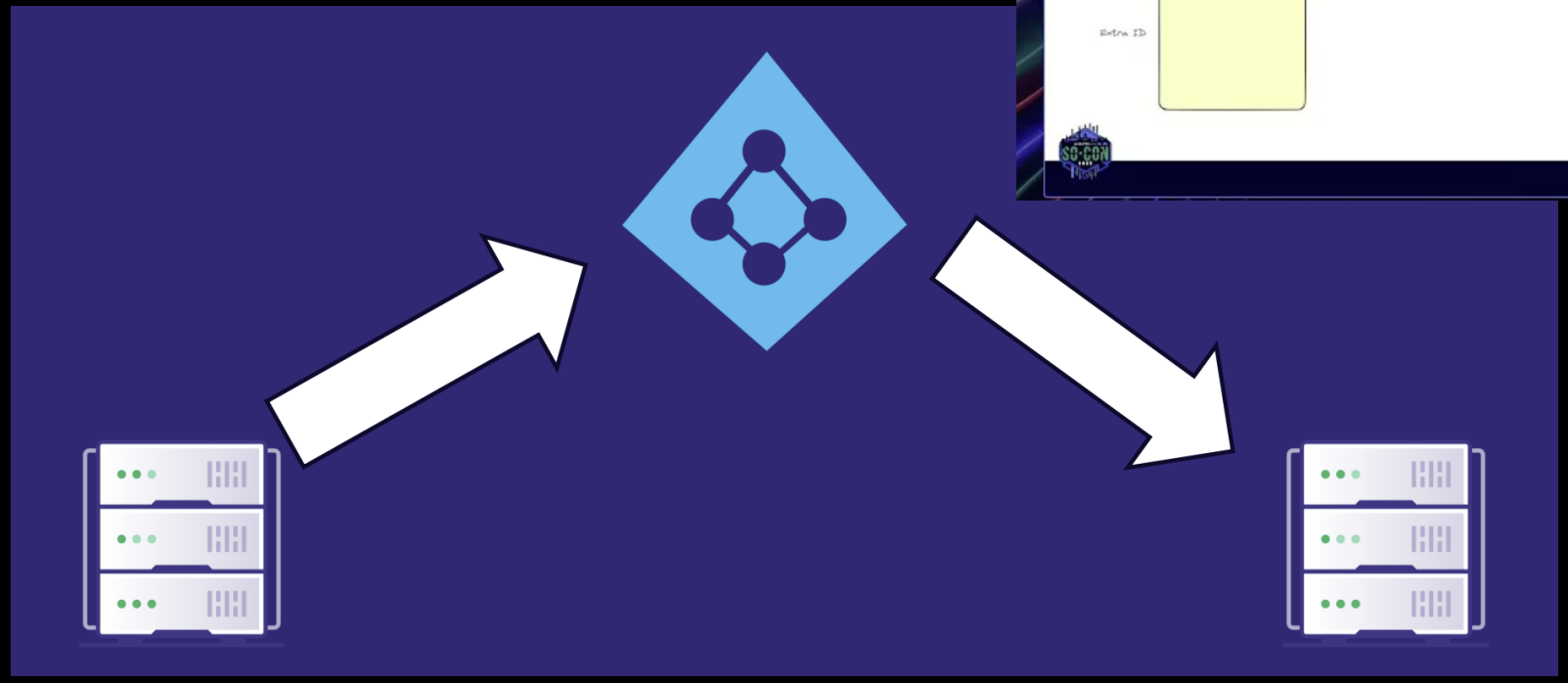
Support domain computers in a forest that's not trusted by your site server's forest

https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/communications-between-endpoints#Plan_Com_X-Forest

Entra ID Sync

ADCS (Active Directory Certificate Services)
SCCM (Configuration Manager)





https://www.youtube.com/watch?v=PCZRpYGLzCQ

Forest jump without AD trust

- ADCS (Active Directory Certificate Services)
- SCCM (Configuration Manager)
- Entra ID Sync

Forest jump without AD trust

- PKI
  - ADCS (Active Directory Certificate Services)
- Endpoint management
  - SCCM (Configuration Manager)
- Single Sign-On
  - Entra ID Sync
- Backup, EDR, Virtualization, etc..

Key takeaways

1. The forest is a security boundary – unless you weaken the configuration

2. Treat Account Operators, DnsAdmins, and Incoming Forest Trust Builders as Tier Zero

3. Attack paths can exist between forests even without trust

Blog posts


ALL / RESEARCH & TRADECRAFT

Untrustworthy Trust Builders: Account Operators Replicating Trust Attack (AORTA)

JUN 25 2025

Share

BY: JONAS BÜLOW KNUDSEN • 20 MIN READ

TL;DR The Incoming Forest Trust Builders group (not AdminSDHolder protected) can create inbound forest trusts with ticket-granting ticket (TGT) delegation enabled. This configuration causes servers to send their TGT across the trust when coerced to authenticate to a computer with unconstrained delegation. An attacker can abuse this by creating a trust to a fake domain, coercing a DC to authenticate to a host in the fake domain with unconstrained delegation, and then use the TGT of the DC to perform DCSync. The coerced DC must perform Kerberos authentication to send its TGT, requiring a DNS conditional forwarder to the fake domain, which the DnsAdmins group (another group AdminSDHolder does not protect) can create.

https://specterops.io/blog/2025/06/25/untrustworthy-trust-builders-account-operators-replicating-trust-attack-aorta/


ALL / BLOODHOUND

Good Fences Make Good Neighbors: New AD Trusts Attack Paths in BloodHound

JUN 25 2025

Share

BY: JONAS BÜLOW KNUDSEN • 24 MIN READ

TL;DR The ability of an attacker controlling one domain to compromise another through an Active Directory (AD) trust depends on the trust type and configuration. To better map these relationships and make it easier to identify cross-domain attack paths, we are replacing the TrustedBy edge in BloodHound with new trust edges. We are also improving the coverage of AD special identities and introducing modeling of the trust account attack to provide a more complete picture of attack paths across trusts.

All BloodHound updates in this blog post apply to both BloodHound Community Edition and BloodHound Enterprise.

https://specterops.io/blog/2025/06/25/good-fences-make-good-neighbors-new-ad-trusts-attack-paths-in-bloodhound/

Thank you!