It’s All About Trust – Forging Kerberos Trust Tickets to Spoof Access across Active Directory Trusts

By Sean Metcalf

Published: 2015-07-15 · Archived: 2026-04-05 16:37:21 UTC

In early 2015, I theorized that it’s possible to forge inter-realm (inter-trust) Kerberos tickets in a similar manner to how intra-domain TGTs (Golden Tickets) and TGSs (Silver Tickets) are forged. Around the same time, Benjamin Delpy updated Mimikatz to dump trust keys from a Domain Controller. Soon after, Mimikatz gained capability to forge inter-realm trust tickets. Benjamin Delpy added “Kekeo” to Github which includes “AskTGS” which provides the capability to request TGS service tickets for targeted services in the destination domain and save them to file. With the tools enabling further research, I was able to explore what is possible with forged cross-trust Kerberos tickets.

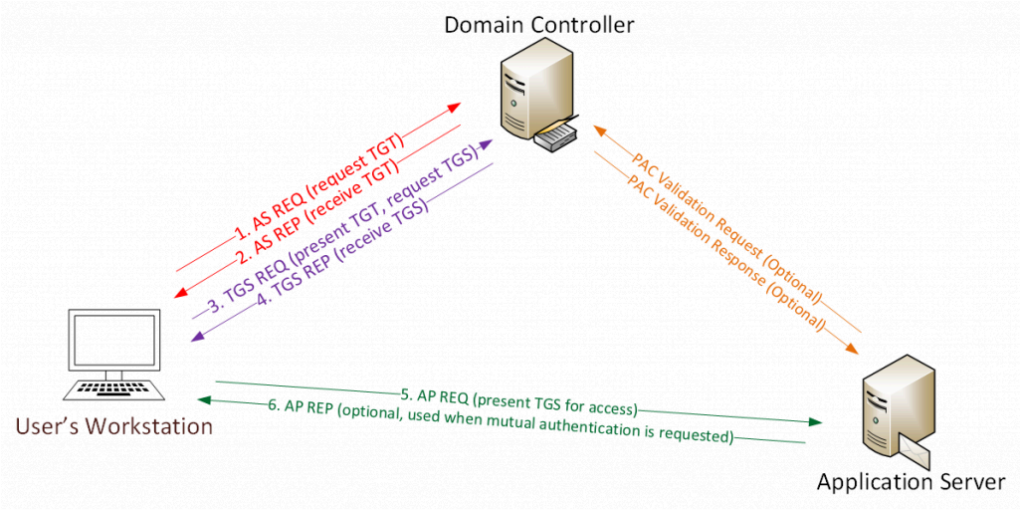
Note that forging a Kerberos Trust Ticket is similar to forging a Golden Ticket or a Silver Ticket.

The key to the power of a Kerberos Trust Ticket within a multi-domain Active Directory forest is Enterprise Admins membership which easily crosses domain boundaries providing effective Domain Admin rights in every domain in the AD forest.

I presented on “Trust Tickets” at Shakacon in Hawaii last week. Simply put, Trust Tickets are forged inter-realm Kerberos tickets. When there are two Active Directory domains connected via trust, there is a password which is shared between them used to keep the trust active. This trust password is also used as the shared secret in Kerberos.

I also presented at Black Hat USA 2015 how I enabled Golden Tickets to work across domains in the same forest (aka Enhanced Golden Tickets).

Update 9/2/2015: I updated the screenshots to accurately show how the intra-forest trust is exploited using the current version of Mimikatz.



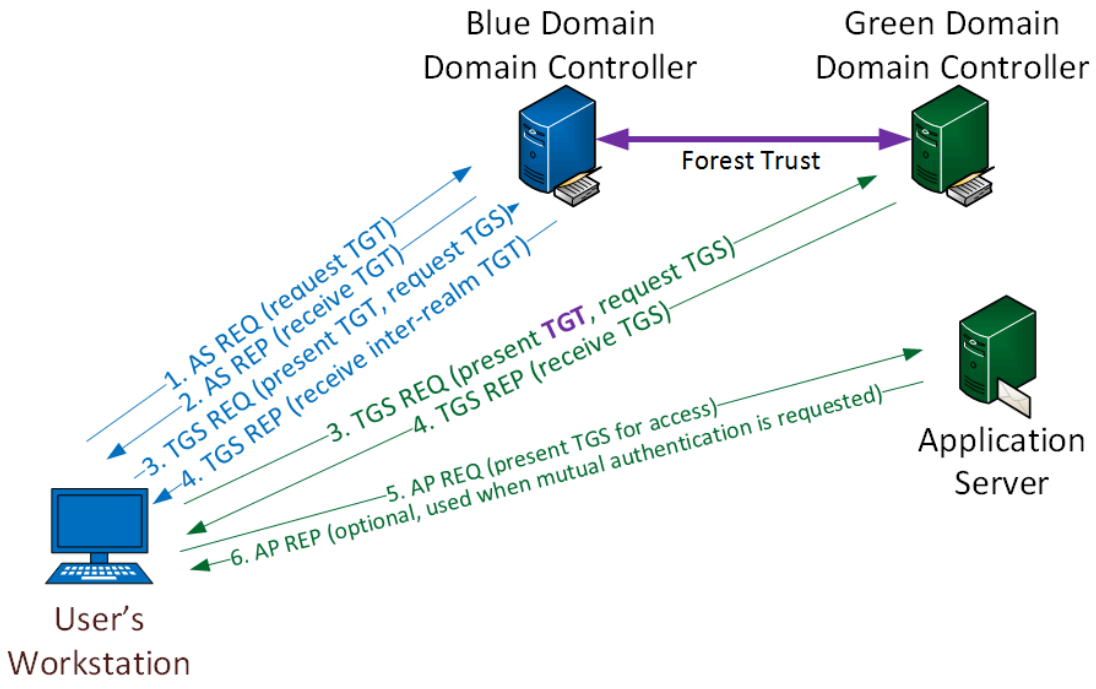
Kerberos Across Trusts

Kerberos communication within a domain is pretty straightforward – the domain Kerberos service account is used to sign and encrypt every authentication ticket (TGT). This enables the TGT to be used throughout the domain and presented to any DC in the domain. This works since the Kerberos service account (KRBTGT) is effectively the trust anchor used for the domain and is why losing control of the KRBTGT account password hash equates to losing control of the domain.

When a user authenticates to Active Directory, the authenticating Domain Controller creates a TGT (authentication ticket) for the user that contains the groups the user is a member of (including groups from other domains in the forest, such as universal groups), signs, and encrypts the ticket using the KRBTGT password hash. When presented later to the DC for a service ticket (TGS), the TGT ticket and its contents are validated. The DC effectively copies the contents of the TGT into a TGS (service ticket) that the user presents to the target service. One component of the TGS is encrypted with the target service's password hash and the other with the user's password hash. If the target service can open the TGS, it is accepted. This means that the user's TGT can be reused to get service tickets during the TGT's lifetime (10 hours by default). The TGT is also portable, so if an attacker can steal a user's TGT, it can be reused on any other computer on the network, at the same time, to access any resource to which the user has access.

When an attacker gains access to the KRBTGT password hash on the domain, it is possible for them to generate their own TGTs (called "Golden Tickets") that are accepted by all the Domain Controllers in the domain since they are signed and encrypted with the domain Kerberos service account data. Simply put, a Golden Ticket is a valid TGT.

In order for the user to access resources in another domain in the same forest, the Kerberos process involves another layer since the Kerberos service (KDC) in one domain can't issue a service ticket (TGS) in another. Since the TGS can only be built using the target service's password data and Domain Controllers (DCs) only contain password data for security principals (users, computers, etc) in their own domain, the DC does not have the target services password data and can't create the TGS. In order to resolve this issue, there is a trust password between two domains in the same AD forest used as a bridge enabling Kerberos authentication across domains.



Once there is a trust between two domains, (domain BLUE and domain GREEN both are in the same AD forest for this example), the ticket-granting service of each domain ("realm" in Kerberos speak) is registered as a security principal with the other domain's Kerberos service (KDC). This enables the ticket-granting service in each domain to treat the one in the other domain as just another service providing cross-domain service access for resources in the other domain.

The Kerberos flow is the same as described earlier for all resources accessed within the domain. When the user requests a service ticket for a resource in another domain, the DC in the user's domain (BLUE) sends the user a TGS referral message as part of the normal service ticket response message (TGS_REP) from the DC to the user. This message includes a TGT for the other domain where the desired resource is located (GREEN) and indicates it is a referral to another TGS. The TGT for the other domain is not signed by the GREEN domain's KRBTGT account since the BLUE domain DCs don't know the password for that account. Instead, the TGT for the other domain is signed and encrypted using the inter-realm key which is derived from the trust password. Since this inter-realm ticket is a TGT, it contains the user's credentials and group membership though its signed with the inter-realm key, not the DC's KRBTGT service account. The user needs to have access to the resource in the other domain in order for access to be granted.

Inter-realm trust communication becomes more complicated in an Active Directory forest with multiple domains, including parent (root) and child domains.

Imagine an AD forest with three domains, ROOT, CHILD1, & CHILD2.

1. ROOT is the root domain with the other two configured as child domains, so ROOT has automatic two-way transitive trusts with both CHILD1 & CHILD2.
2. In order for a CHILD1 user to access a resource in CHILD2, the following occurs:
3. CHILD1 user authenticates and gets the user's TGT for the CHILD1 domain.
4. The user requests a service ticket for a share in CHILD2.

5. The CHILD1 DC copies the CHILD1 TGT into a new inter-realm TGT (using the ROOT-CHILD1 inter-realm key) and sends it to the user along with a referral to the ROOT domain.
6. The user sends the (ROOT-CHILD1) IR-TGT to a ROOT DC along with the TGS_REQ for the resource.
7. The ROOT DC copies the IR-TGT into a new inter-realm TGT (using the ROOT-CHILD2 inter-realm key) and sends it to the user along with a referral to the CHILD2 domain.
8. The user sends the (ROOT-CHILD2) IR-TGT to a CHILD2 DC along with the TGS_REQ for the resource.
9. The CHILD2 DC copies the IR-TGT into a TGS used to access the resource.

Note that the original referral message the user gets includes a session key for communicating with the ROOT DC. The ROOT DC then provides a new session key for the user to use to communicate with the CHILD2 DC.

Forging Kerberos "Trust Tickets"

In a scenario where an attacker compromised a single domain in an AD forest and dumped all the credentials, the attacker would naturally use Golden Tickets since they enable full access to the domain and the AD forest (Golden Tickets include Enterprise Admin group membership by default). The well-known remediation of Golden Ticket creation and use is to change the compromised KRBTGT account password twice. After this action is complete, the attacker can't create any more Golden Tickets. However, there is another avenue for an attacker that has dumped all credentials from a Domain Controller to re-exploit the multi-domain AD forest. Since every domain in an AD forest has an implicit trust (and associated trust password) with at least one other domain, the attacker can forge a different type of Kerberos ticket to spoof Enterprise Admin rights in the target domain. Enterprise Admins are members of the Administrators group in every domain in an AD forest, this level of access enables the attacker to compromise all domains. This is kind of like a Golden Ticket across trusts.

Forging the Inter-Realm TGT (IR-TGT) for access isn't necessary if you have the KRBTGT account password, but if that has changed twice, the forged IR-TGT (Trust Ticket) can be used to impersonate an EA and regain full domain/forest admin rights. Since there's an automatic, two-way transitive trust for every domain in the forest, getting the trust key for one trust, enables access to the others (though I'm not sure if the tools support this right now). This is due to the trust flow.

It's not a Silver Ticket since it's not a forged TGS and it's not exactly a Golden Ticket since it's not using the KRBTGT account to forge a TGT. Forge the inter-realm TGT for a user in Domain A for the TGS_REQ to the Domain B DC to get a valid TGS to the Domain B resource.

While forging trust keys should work really well in a multi-domain AD forest, there are a variety of trust options between domains/forests that could cause problems with attempting to extend compromise of one to another. With that said, if a user in Domain A has elevated rights to resources in Domain B, the forged IR-TGT should provide an attacker the same access as a Golden Ticket (since it would be used as the basis for the IR-TGT). One brilliant way to exploit this is to add admin groups for Domain B in the user's forged IR-TGT in SID History (assuming the trust has it enabled), though this is theoretical at this point.

Note:

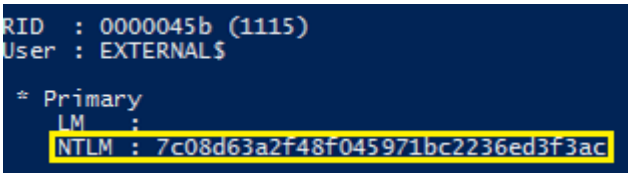
Two-way trusts are actually 2 one-way trusts, each of which has a different password which only change every 30 days (default). The TrustING domain PDC performs the password change for the trust.

HarmJ0y has additional detail on this issue including great trust recon tools in PowerView.

Forging External Trust Tickets

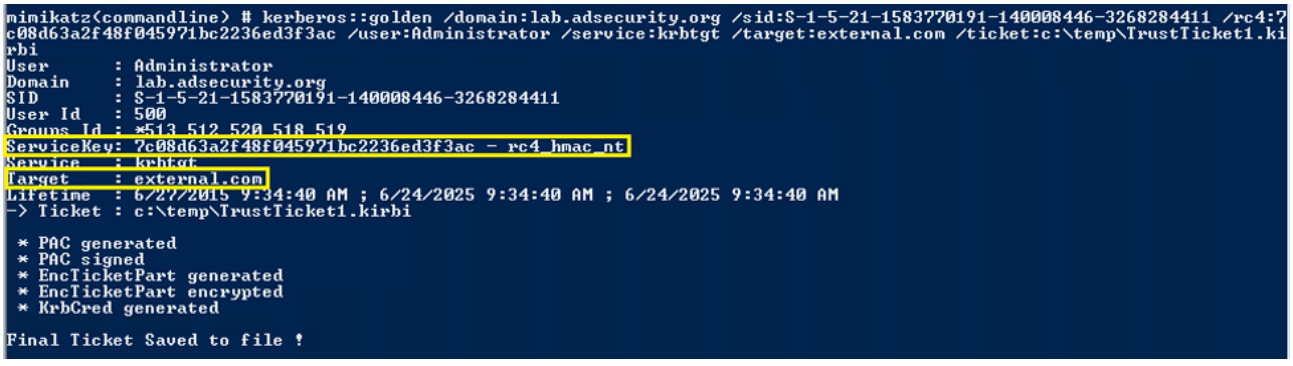
There are essentially two different types of trust in Active Directory: one external to the AD forest and one internal. In this first section, we cover forging external trusts.

Step 1: Dumping trust passwords (trust keys)
The trust password is in a domain credential dump, just look for the trust name with a dollar ($) sign at the end. Most of the accounts with a trailing "$" are computer accounts, but some are trust accounts.



Step 2: Create a forged trust ticket (inter-realm TGT) using Mimikatz

Note that the trust password, aka trust key, was extracted along with all user data when dumping AD credentials. Each trust has an associated user account which contains that NTLM password hash. This data can be used to forge "Trust Tickets". We use the trust password for the external trust to create the Trust Ticket file. The trust password is the same as what I used to create it. To create a trust with another forest, an admin on one side enters the trust password and the other admin uses the same trust password which may be sent via email to ensure it is entered correctly. This means that when a trust is first created, any one with knowledge of the trust password can create Trust Tickets. Creating a Trust Ticket is similar to creating a Golden Ticket., in fact it's the same Mimikatz command, just with different options. The service key is the trust NTLM password hash and the target is the target domain FQDN.



Save this ticket to a file for step 2

Step 3: Use the Trust Ticket file created in Step 2 to get a TGS for the targeted service in the destination domain. Save the TGS to a file.

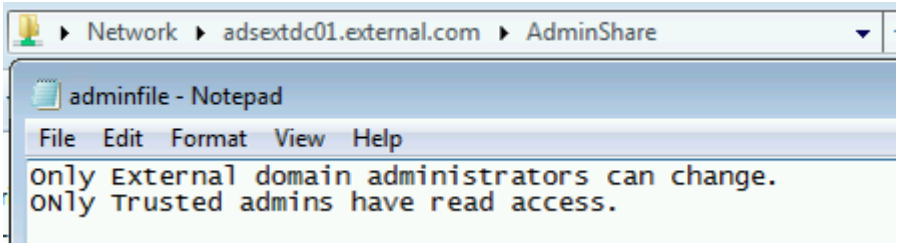
```
PS C:\temp\kekeo> .\Asktgs c:\temp\TrustTicket1.kirbi  cifs/adsextdc01.external.com

  .#####.   AskTGS Kerberos client 1.0 (x86) release "Kiwi en C" (Apr 19 2015 00:51:37)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                       (oe.eo)
  '#####'                                                     * * */

Ticket    : c:\temp\TrustTicket1.kirbi
Service   : krbtgt / external.com @ lab.adsecurity.org
Principal : Administrator @ lab.adsecurity.org

> cifs/adsextdc01.external.com
  * Ticket in file 'cifs.adsextdc01.external.com.kirbi'
```

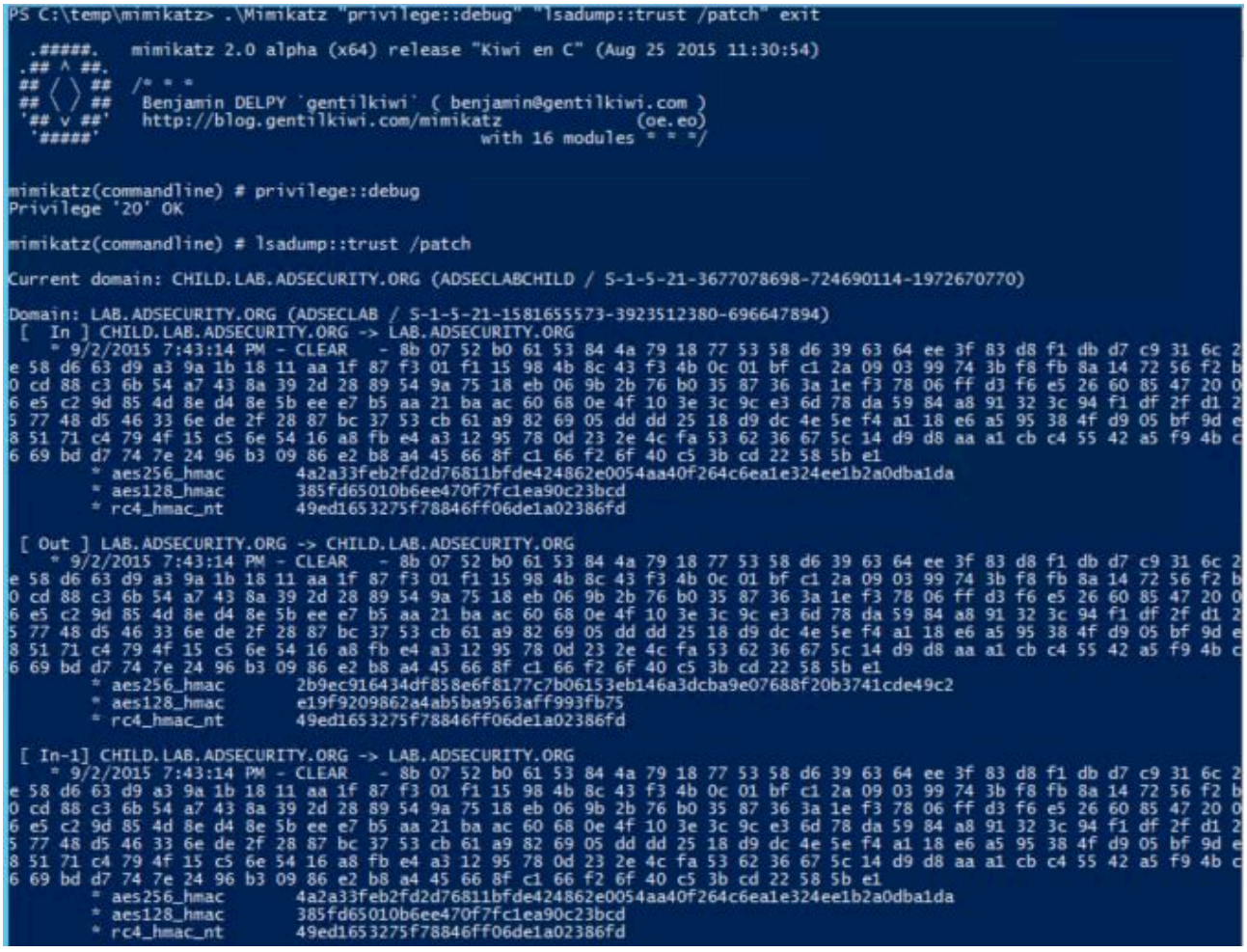
Step 4: Inject the TGS file created in Step 3 and then access the targeted service with the spoofed rights.



Forging Internal AD Forest Trust Tickets

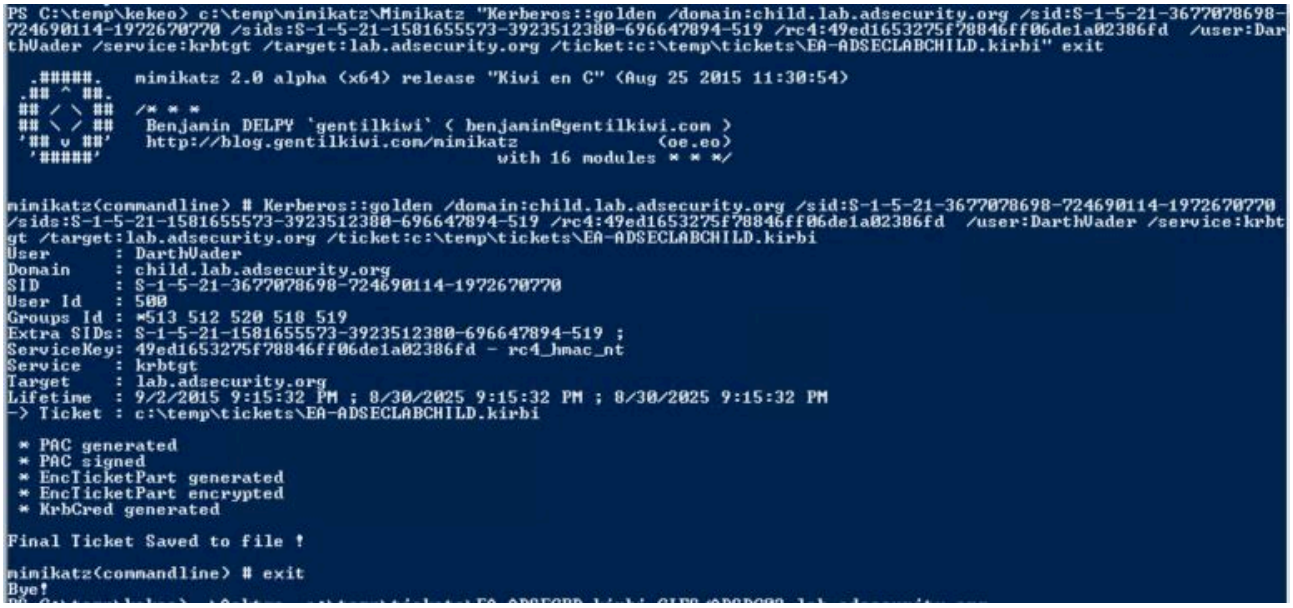
Step 1: Dumping trust passwords (trust keys)

Current Mimikatz versions can extract the trust keys (passwords).



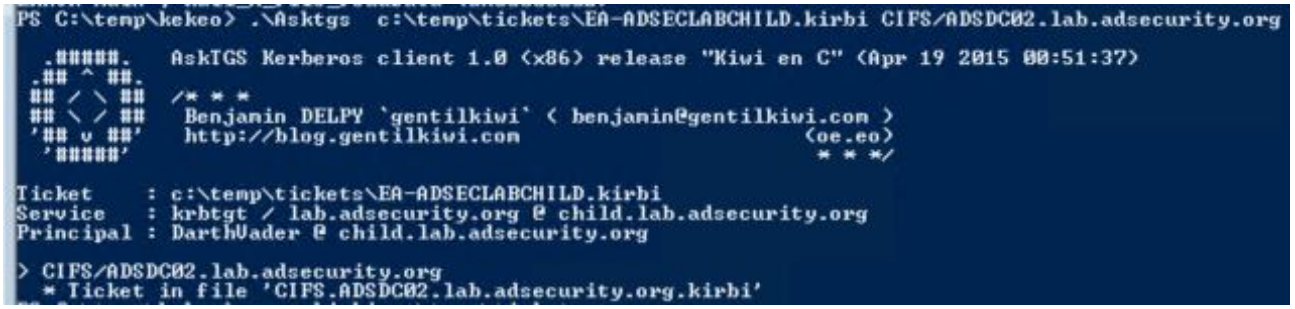
Step 2: Create a forged trust ticket (inter-realm TGT) using Mimikatz

Forge the trust ticket which states the ticket holder is an Enterprise Admin in the AD Forest (leveraging SIDHistory, “sids”, across trusts in Mimikatz, my “contribution” to Mimikatz). This enables full administrative access from a child domain to the parent domain. Note that this account doesn’t have to exist anywhere as it is effectively a Golden Ticket across the trust.



Step 3: Use the Trust Ticket file created in Step 2 to get a TGS for the targeted service in the destination domain. Save the TGS to a file.

The resulting TGS provides EA access to the parent (root) domain's Domain Controller.



Step 4: Inject the TGS file created in Step 3 and then access the targeted service with the spoofed rights.

Once the ticket is passed the user is an Enterprise Admin for the AD forest and has DA rights to the DC in the target domain. This is a great way to escalate rights across other domains in the forest. Note that unless an attacker gets the KRBTGT account in the domain that hosts the EA group, the Golden Ticket only grants DA rights to the current domain (the one the Golden Ticket was created in). Once the attacker dumps the credentials for the current domain, the trust password is used to create a Trust Key that states the holder of the ticket is EA. Then the target domain can be exploited. This can be repeated to move through every domain in the forest quite easily since every child domain inherently trusts the parent aka root domain. So, using a Trust Ticket to become EA in the AD forest involves compromising a single domain.

Conclusion

In a multi-domain AD forest, each domain has a trust with at least one other domain. Each trust has an associated password which can be used to forge trust tickets. Compromise one domain to potentially compromise another. Reducing the AD computer account policy mitigates this attack since Trust passwords are changed on this schedule (TrustING domain).

Regarding Trust Tickets within an Active Directory Forest:

1. Using a Kerberos trust ticket from Child domain impersonating a Child domain user provides the level of access that Child domain user has at the Parent domain. If the Child domain user is a member of Enterprise Admins or a group that has admin rights on the parent, the forged Trust Ticket provides admin access to the parent.

2. Using the /sids parameter in Mimikatz to add the Enterprise Admins group in the Parent domain to the Child domain user account in the Trust Ticket provides EA rights to the Parent domain without the Child domain user account actually having these rights. Note that this is similar behavior to “enhanced” Golden Tickets since they use SID History to spoof access across domains.
3. Even if the KRBTGT account password is rotated on a regular basis, the attacker may still have the trust key (password) and can use that to regain full Enterprise Admin rights.

Mitigating factor: Changing the domain machine password policy to be a low number in the TrustING domain ensures the trust password changes more quickly (along with the domain computer account passwords).

Best Mitigation: Don’t let attackers run code on DCs – Protect Domain Admins!

References:

- Kerberos, Active Directory’s Secret Decoder Ring
  http://adsecurity.org/?p=227
- Kerberos, Kerberos across trusts, and trust passwords
  https://technet.microsoft.com/en-us/library/cc772815%28v=ws.10%29.aspx
- Mimikatz and Active Directory Kerberos Attacks
  http://adsecurity.org/?p=556
- Kerberos & KRBTGT: Active Directory’s Domain Kerberos Account
  http://adsecurity.org/?p=483
- Black Hat USA 2014 – Windows: Abusing Microsoft Kerberos Sorry You Guys Don’t Get It
  https://www.youtube.com/watch?v=-IMrNGPZTl0&index=4&list=UUbbgnifxfH-nqx6z9XQ963Q
- Mimikatz and Golden Tickets… What’s the BFD? BlackHat USA 2014 Redux part 1
  http://passing-the-hash.blogspot.com/2014/08/mimikatz-and-golden-tickets-whats-bfd.html
- Mimikatz Golden Ticket blog entry by Benjamin Delpy (Mimikatz author)
  http://blog.gentilkiwi.com/securite/mimikatz/golden-ticket-kerberos
- Protection from Kerberos Golden Ticket: Mitigating pass the ticket on Active Directory (CERT-EU Security White Paper 2014-07)
  http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf

---