DELEGATE TO THE TOP
Abusing Kerberos for Arbitrary Impersonations and RCE

Matan Hart
@machosec
me@matanhart.com
DELEGATE TO THE TOP
Abusing Kerberos for Arbitrary Impersonations and RCE

Matan Hart
@machosec
me@matanhart.com
“You can delegate authority, but you cannot delegate responsibility.”

Byron Dorgan
The Fact

Delegation is risky
WHO AM I

- Security Researcher @ CyberArk
- IAF and IDF veteran
- Focus on Kerberos and Active Directory
- <3 PowerShell
- <333 Mr. Robot
AGENDA

- Kerberos Delegation, flavors and limitations
- Service Principal Names
- Attack Surface
- Tool and Demo
- Detection and Mitigation
THE "DOUBLE-HOP" PROBLEM

Client → User → Front-end → Service → Back-end
Kerberos Delegation

Client → User → Front-end → User's ticket → Back-end
UNCONSTRAINED DELEGATION

Full delegation by TGT forwarding

Windows 2000
User authenticates and requests to delegate access to a service

KDC checks if the service is trusted for delegation and issues a forwarded TGT

Service gets the forwarded TGT from the user and acts on his behalf
1. User obtains a forwarded TGT (TGS_REQ/REP)
2. User obtains a service ticket for the front-end service (TGS_REQ/REP)
3. User makes a request to the front-end (AP_REQ)
4. Front-end obtains a service ticket for the back-end on behalf of the user (TGS_REQ/REP)
5. Front-end makes a request to back-end, acting as the user (AP_REQ)
LIMITATIONS

Unlimited access
Services are exposed to broader impersonation risks

Kerberos only
No support for other authentication protocols
minikatz(commandline) # sekurlsa::tickets /export

Authentication Id: 0: 162402 (00000000:000028ea)
Session: Network from 0
User Name: LukeSkywalker
Domain: ADSECURITY
Logon Server: (null)
SID: S-1-5-21-1583770191-140008446-326828441-1109

* Username: LukeSkywalker
* Domain: ADSECURITY.ORG
* Password: (null)

Group 0 - Ticket Granting Service
Group 1 - Client Ticket
Group 2 - Ticket Granting Ticket

Target Name: -> @ LAB.ADSECURITY.ORG
Client Name: LukeSkywalker @ LAB.ADSECURITY.ORG
Flags 60a10000: name_canonicalize: pre_authent: renewable: forwarded: forwardedable:
Session Key: 0:000000012: aes256_hmac
Ticket: 0:000000012: aes256_hmac
* Saved to file [0:28deal-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi]

minikatz(commandline) # keytov::ptt [0:28deal-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi]
0 - File '[0:28deal-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi]' : OA

minikatz(commandline) # exit
Bye!
P$ C:\temp\a> klist
Current LogonId is 0:0x2b3d7
Cached Tickets: <1>

#0: Client: LukeSkywalker @ LAB.ADSECURITY.ORG
Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
"Nobody is going to delegate a lot of power to a secretary that they can't control."

Michael Bloomberg
CONSTRAINED DELEGATION

Service-for-User delegation

Windows 2003
S4U EXTENSIONS

**S4U2Proxy**
Allows a service to obtain a service ticket on behalf of a user to a different service

**S4U2Self**
Allows a service to obtain a service ticket to itself in the name of a different user
Restricts the services that can be accessed by impersonation

TGTs are not forwarded to the front-end

Support protocol transitioning

Limited to a single domain
1. User authenticates to the front-end using non-Kerberos authentication

2. Front-end obtains a service ticket to itself in the named user (S4U2Self)

3. Front-end obtains a service ticket to back-end on behalf of the named user (S4U2Proxy)

4. Front-end makes a request to back-end, acting as the user (AP_REQ)
"S4U allows a service to obtain a Kerberos service ticket for a user that has not authenticated to the KDC"

"S4U2Self allows you to obtain a Windows token for the client by supplying a UPN without a password."


How To: Use Protocol Transition and Constrained Delegation in ASP.NET 2.0
IT'S NOT A BUG
IT'S A FEATURE
Which means it’s not going to be changed soon..
“The S4U2proxy combined with S4U2self allows a service to impersonate any user principal while accessing a second service. This gives any service allowed by the S4U2proxy a degree of power similar to that of the KDC itself.”
SERVICE PRINCIPAL NAME

uniquely identifies an instance of a service

<service type>/<host name>:<port number>/<distinguished name>

HTTP/MyWeb.MyDomain.com:8080  CIFS/printer.MRROBOT.com

SMTP/mailsrver.company.com/COMPANY
DELEGATION ACCOUNTS

A computer or a user account

Must be registered with an SPN

Configured by Domain Administrators

S4U2Self requires to act as part of the operating system (SeTcbPrivilege)
<table>
<thead>
<tr>
<th>Unconstrained Delegation</th>
<th>Constrained Delegation</th>
<th>Protocol Transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUSTED_FOR_DELEGATION (0x80000)</td>
<td>MsDS-AllowedToDelegateTo (List of SPNs)</td>
<td>Trusted_To_Authenticate_For_Delegation (0x100000) &amp; MsDS-AllowedToDelegateTo (List of SPNs)</td>
</tr>
</tbody>
</table>

PS C:\> $Searcher.Filter = "|(userAccountControl:1.2.840.113556.1.4.803::=524288)(msDS-AllowedToDelegateTo="")"
PS C:\> $Searcher.FindAll()

<table>
<thead>
<tr>
<th>Path</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP://CN=DC,OU=Domain Controllers,DC=Mars,DC=local</td>
<td>{ridsetreferences, logoncount, codepage, objectcategory}</td>
</tr>
<tr>
<td>LDAP://CN=Abraham,CN=Users,DC=Mars,DC=local</td>
<td>{msexchrecipientdisplaytype, givenname, codepage, obj}</td>
</tr>
<tr>
<td>LDAP://CN=Isaac,CN=Users,DC=Mars,DC=local</td>
<td>{msexchrecipientdisplaytype, givenname, codepage, obj}</td>
</tr>
</tbody>
</table>
EXPLOITABILITY
Delegation accounts are:

- easily discovered
- exposed by the host service
- often unmanaged
- vulnerable to Kerberoasting
- always logged-on
Configuring Trust for the Active Directory user

In this section, you configure the trust for specific services for the user you created.

1. From the Windows Domain controller, from the Administrative Tools menu, open **Active Directory Users and Computers**.
2. Right-click the user account you created.
3. Click the Delegation tab.
4. Click **Trust this user for delegation to specified services only**. This enables Kerberos constrained delegation.
5. Under Trust this user for delegation to specified services only, click **Use any authentication protocol**. This enables Kerberos protocol transition on the server-side.
6. In the Services to which this account can present delegated credentials area, click the **Add** button to add services to the list.
5. Add the following services for the Domain Controller and the XenApp servers in the farm:

Add each domain controller and select the services: CIFS, LDAP, ProtectedStorage

Add each XenApp server and select the service: HOST
ATTACK SURFACE

Learn in Just 10 Minutes...

HOW TO DELEGATE

A step-by-step guide to effective delegation

Joan Henshaw

10minute management toolkit
ATTACK VECTORS

ATTACK VECTORS EVERYWHERE
Credential Theft
DCSync

Remote Execution
xp_cmdshell, Invoke-Command, HOST

Privilege Escalation
Arbitrary impersonations

Data Exfiltration
Applications, file shares and databases
THE FLOW

Hunt accounts trusted for delegation

Impersonate another user

Abuse the allowed services
MYSTIQUE

PowerShell tool to play with S4U

- Find accounts trusted for delegation
- Read delegation flags and attributes
- Impersonate arbitrary users

https://github.com/machosec/Mystique
DELEGATE

ALL THE THINGS
“If I have seen further, it is by standing on the shoulders of giants.”

Isaac Newton
THE TWIST

SPNs are not validated!

"SERVICE RESTRICTION "
Services validate a service ticket by ensuring it is being encrypted with the **secret-key**

Service account password hash

Tickets are fully interchangeable if they share the same secret

SPNs associated to the same account

Accounts with the same password hash

Registered with many SPNs

Use RC4 encryption
Front-end $\rightarrow$ Domain Controller

Domain Controller $\rightarrow$ Back-end

Front-end $\rightarrow$ Back-end 2

TGS_REQ $\rightarrow$ HTTP

HOST AP_REQ $\rightarrow$ CIFS

CIFS @ back-end.domain.com
RESOURCE-BASED CONstrained Delegation

Introducing msDS-AllowedToActOnBehalfOfOtherIdentity

Limit access per account rather than SPN

Returns some control to the back-end administrator

Support Delegation across domains and forests

Requires Server 2012 on front-end and DCs
NOT SURE IF GOOD THING
OR VERY BAD THING
DEFENSE
DETECTION
Event log 4624 on Windows 8/2012+

Front-end

Back-end

An account was successfully logged on.

Security ID: MARS\websvc
Account Name: websvc
Account Domain: MARS
Logon ID: 0x2F36B

Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
Security ID: MARS\sysadmin
Account Name: sysadmin
Account Domain: MARS
Logon ID: 0x217975
S4U2Proxy network traffic correlation

TGS_REQ

Kerberos
  Record Mark: 2640 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
    req-body
      Padding: 0
      Kdc-options: 40830000 (forwardable, renewal)
      Realm: MARS.LOCAL
    sname
      name-type: kRB5-NT-SRV-INST (2)
      sname-string: 2 items
        SNameString: HTTP
        SNameString: mars-websrv.mars.local
    till: 2017-03-12 17:19:41 (UTC)
    nonce: 1018184952
    etype: 5 items
    enc-authorization-data
    additional-tickets: 1 item
  ticket
    tkt-vno: 5
    Realm: MARS.LOCAL
    sname
      name-type: kRB5-NT-PRINCIPAL (1)
      sname-string: 1 item
        SNameString: webserv

TGS REP

Kerberos
  Record Mark: 1807 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    ccrealm: MARS.LOCAL
    cname
      name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
      cname-string: 1 item
        CNamestring: sysadmin@mars.local
    ticket
      tkt-vno: 5
      Realm: MARS.LOCAL
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: HTTP
          SNameString: mars-websrv.mars.local
MITIGATION

Configure services with a dedicated service account

Avoid dual-use or using computer accounts
Ensure password rotation and complexity

Set unique SPNs to be allowed for delegation

Do not delegate to built-in SPNs
Specify specific port numbers
Other options to consider..

- Set privileged accounts as "account is sensitive and cannot be delegated"
- Restrict access per account instead of SPNs (Server 2012)
- Enforce forest boundary in unconstrained delegation (2012R2)
SOUND BYTES

Kerberos delegation can be easily abused for privilege escalation and remote execution

Services and service accounts can introduce more risk than you think

Hardening delegation rights is tough - but possible
QUESTIONS?
THANKS!

- CyberArk
- MSRC
- Benjamin Delpy (@gentilkiwi)
- Alberto Solino (@agsolino)
- To all of you for taking delegation seriously

Let's talk!
@machosec
me@matanhart.com
DELEGATE TO THE TOP
Abusing Kerberos for Arbitrary Impersonations and RCE

Matan Hart
@machosec
me@matanhart.com