Domain Controller Print Server + Unconstrained Kerberos Delegation = Pwned Active Directory Forest

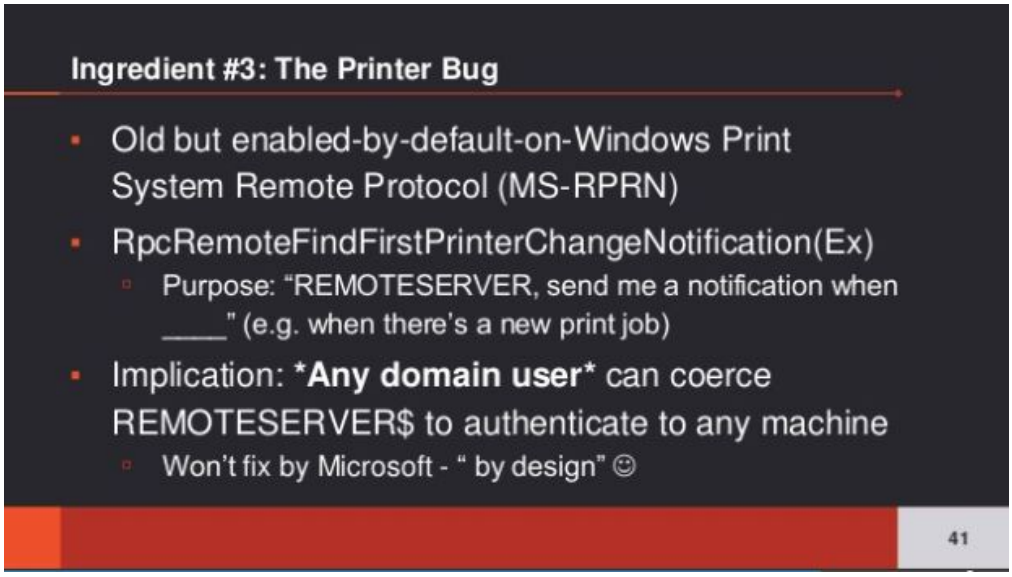
adsecurity.org

Sean Metcalf October 10, 2018

At DerbyCon 8 (2018) over the weekend Will Schroeder (@Harmj0y), Lee Christensen (@Tifkin_), & Matt Nelson (@enigma0x3), spoke about the unintended risks of trusting AD. They cover a number of interesting persistence and privilege escalation methods, though one in particular caught my eye.

Overview

Lee figured out and presents a scenario where there's an account with unconstrained delegation configured (which is fairly common) and the Print Spooler service running on a computer, you can get that computers credentials sent to the system with unconstrained delegation as a user.



We find that about 90% of the environments we review and work in have some sort of Kerberos delegation configured and about 75% have unconstrained delegation configured. I identified and highlighted the security issues with unconstrained delegation in my talk at Black Hat in 2015 (as well as subsequent talks) and in a post here.

Here's a quick PowerShell command that discovers accounts with Kerberos delegation (requires the AD PowerShell module):

```
Get-ADObject -filter { (UserAccountControl -BAND 0x0080000) -OR (UserAccountControl -BAND 0x1000000) -OR (msDS-AllowedToDelegateTo -like '*') } -prop Name,ObjectClass,PrimaryGroupID,UserAccountControl,ServicePrincipalName,msDS-AllowedToDelegateTo
```

The Attack

The attacker discovers a system with Kerberos unconstrained delegation and compromises it. Then the attacker sends a "RpcRemoteFindFirstPrinterChangeNotification" request to the Domain Controller and the

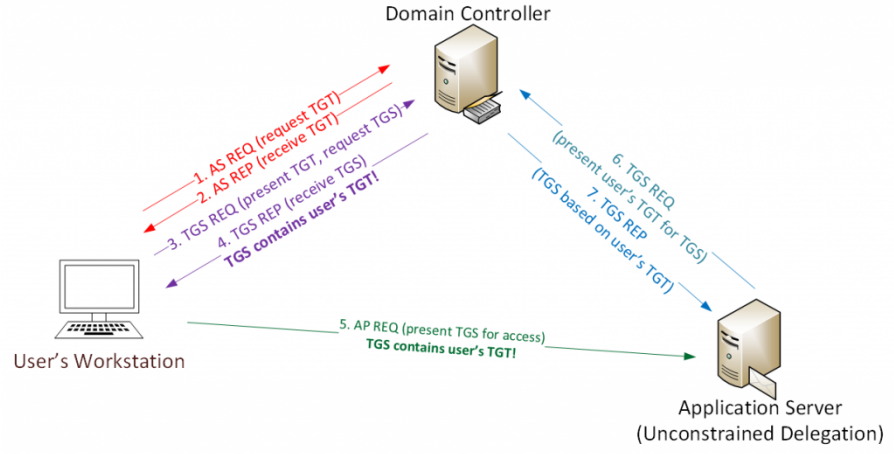
DC responds to test communication to the requester. If the Domain Controller is running the Print Spooler (Spooler) service, this will work (and it's trivial to test to find 1 DC that is running this service).

Lee explains that the issue is that any authenticated user can remotely connect to the Domain Controller's print server (spooler service) and request an update on new print jobs and just tell it to send the notification to the system with unconstrained delegation. It will test that connection immediately thus exposing the computer account credential (since the print spooler is owned by SYSTEM). Lee notes that Microsoft says this is by design and "won't fix".
Lee posted PoC code he calls SpoolSample on Github.

Conceptual Flow:

1. Attacker discovers and compromises a system with Kerberos unconstrained delegation. Note that if an attacker compromises a Domain Controller in a trusted forest (with a 2-way trust), this can be used to compromise the other forest.
2. Attacker tests for and discovers a Domain Controller running the Print Spooler (Spooler) service.
3. Attacker sends the MS-RPRN request RpcRemoteFindFirstPrinterChangeNotification (Kerberos auth) to the DC's print server.
4. The DC immediately sends a response to the requester. This response involves the DC creating a Kerberos service ticket (TGS) which contains the Domain Controller's computer account Kerberos authentication ticket (TGT) since Kerberos is involved and the requesting account is configured with unconstrained delegation.
5. The attacker now has the Domain Controller computer account Kerberos TGT which can be used to impersonate the DC.
6. DCSync all account credentials (or other attack involving DA credentials as desired).

The conceptual auth flow is shown in the graphic



The key "ingredients" required for this to work as mentioned in their talk:

1. Account with Kerberos unconstrained delegation (a DC in a trusted forest using a 2-way trust, for example)
2. Compromise that account.
3. Domain Controller running as a print server (Print Spooler service is running).

This issue also works across forest trusts.

Mitigation

- Domain Controllers and AD admin systems need to have the Print Spooler service disabled. The US DoD STIG security guidance has had this recommendation in place for many years. Best way to do this if via GPO
- Remove unconstrained delegation from accounts and replace with constrained delegation (Domain Controllers have unconstrained delegation enabled by default)
- Disable TGT delegation across trusts:

```
netdom.exe trust fabrikam.com /domain:contoso.com /EnableTGTDelegation:No
```

Note that this post focuses on Domain Controllers, but any server is potentially at risk to this attack.
Mitigate this specific issue by disabling the Print Spooler service on all servers that don't need it running and ensure there are no accounts with unconstrained delegation configured.

UPDATE (Feb 12, 2019)
Microsoft has released some additional guidance for the cross-forest impact of this issue.

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190006

UPDATE (March 21, 2019)
Microsoft has changed this to CVE-2019-0683 and will fix. The Microsoft article 4490425 describes the changes to trusts moving forward to protect against this issue.

Great talk Will, Lee, & Matt!

Talk Slides
https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory
Video explaining the issue
https://youtu.be/-bcWZQCLk_4?t=2194
References
(Visited 63,100 times, 60 visits today)