InCommon Silver with Active Directory Domain Services Cookbook - RC20140115 - Public Comments

<table>
<tr><th>#</th><th>Comment</th><th>Submitted By</th><th>Date</th><th>Workgroup Response</th><th>Status</th></tr>
<tr>
<td>1</td>
<td>I have a question regarding 4.2.5 and 4.2.6. In those sections there are highlighted phrases that restrict the consideration of secure communications as part of the IdP authentication /assertion event. There are accompanying statements that all other traffic between the Subject and the AD DS is beyond scope.

Can I interpret that statement to imply that it is known that there is no practical way to leverage replay or eavesdropper attacks on non-IdP authentication events between the Subject and an AD DS to create an authentication event via the IdP?

For instance, what if I highjacked a password change session with the AD DS?
Or if I highjacked an authentication session that allowed access to a webmail system where password reset links are sent. Or similar sorts of escalation strategies?

Is it implied in the cookbook that none of these sorts of things can happen within the context of AD?

Or is there an implicit statement that these sorts of vulnerabilities should be beyond the scope of the IAP for Silver?
If the latter, as an SP operator I would really downgrade my current view of what I would accept Silver for.

</td>
<td>Warren Anderson</td>
<td>1/31 /2014</td>
<td>
In the more general case we do not mean to imply that there is no feasible way to leverage or replay eavesdropper attacks on non-IdP authentication events to create an authentication event via the IdP. Our intent is to classify protocols into categories of risk:

Not resistant to recovery of users's authentication credential. I.e., could be attacked to allow recovery of the user's actual password.

These protocols are disallowed or must be monitored
Examples: Cleartext (plain LDAP), LM, NTLMv1

Resistant to recovery of the user's authentication credential (password), but perhaps less resistant to replay attacks.

These protocols are acceptable with non-IdP authentication events, but are recommended to be disabled for communications to the IdP (to avoid replay actually allowing an authentication event being "forged" via the IdP)
Examples: NTLMv2, Kerberos

Resistant to eavesdropping and replay.

These protocols are allowed in non-IdP and IdP authentication events alike.
Examples: LDAPS, LDAP with data signing
*The cookbook does single out "change password pages" in section 4.2.3, discussing the interpretation of requirement 4.2.3.6.2 of the IAP), because as you note, attacks on these pages would lead directly to the ability to attack the IdP.
*We also see AD Admin accounts able to modify Verifier passwords or configuration of the IdP itself as being covered by the requirement 4.2.8.2.2 network communications ("(All personnel with login access to IdMS Operations infrastructure elements must use access Credentials at least as strong..."). However, because this is not an AD-DS specific requirement (it would be true of any admin account on any IdP verifier, regardless of protocols or configurations) we didn't identify this requirement within the context of the AD Cookbook

We definitely do not mean to imply that session highjacking, etc. cannot happen in AD. The categorization of protocols referred to above was specifically to identify which protocols are vulnerable in the context of the IAP Two elements from the Scope to clarify here:

The AD Cookbook focuses on compliance with the Silver IAP, and NOT security that is sufficient for your technical environment. That is, the focus is compliance, and we encourage institutions to go beyond the identified compliance activities wherever appropriate.
The AD Cookbook focuses on AD-DS specific functionality. So for example, the password change initiated by hitting ctrl-alt-delete would be in scope of the AD Cookbook (and there is an open question to Microsoft about this). By contrast, security of a password change page hosted by an external application (e.g., an IDM system) is not an AD-DS technology question; so while still in scope of the Silver IAP, is out of scope for the AD Silver Cookbook.

</td>
<td>Update section 4.2.3 (interpretation of IAP requirement 4.2.3.6.2) to use "e.g.", not "i. e." in the statement "i.e., change my password pages".

Clarifying language added to Scope and Approach and Overview of Findings sections
|</td>
</tr>
<tr>
<td>2</td>
<td>In section 5.1.1 Could the use of self-encrypting drives that meet the requirements be a suitable alternative? [To handle disk /password encryption requirements]</td>
<td>Robert Mackin</td>
<td>1/31 /2014</td>
<td>We have raised similar questions within the AD group, and it largely depends on the precise attack vector(s) the requirement is intended to affect. (E.g., theft of disk vs. protection of file contents from co-resident programs). But generally, if our "Encrypt the Drive" recommendation is sufficient to protect against disk theft, and presuming the disk encryption method used by a self encrypting disk meets the strength requirements of the IAP, then this would seem to be a reasonable way to meet the requirements.</td>
<td>Add to the interpretation of requirement 4.2.3.4 that "The interpretation is that the three specific encryption methods defined are to address physical loss of or access to the disk, and that the physical loss concern is separate from the logical controls described in the second sentence of the requirement that would prevent co-resident applications from accessing the password store directly."

Note that the management assertions the AD cookbook provides do not address AD-DS's discretionary access controls. Would be good to add a reference to these.</td>
</tr>
<tr>
<td>3</td>
<td>Could the use of read-only domain controllers in perimeter networks meet some compensating controls? With read-only DC's you can define a password replication policy and filtered attribute sets. Each read-only dc also has a unique Kerberos krbtgt account.</td>
<td>Robert Mackin</td>
<td>1/31 /2014</td>
<td>Fundamentally, even when an RODC is used, it appears that the way the passwords are stored/hashed is still not in compliance with the IAP. Because the use of the RODC potentially reduces the number of non-compliant stored passwords at various KDCs and reduces general access to them, it is arguably objectively "better" security-wise than having all KDCs writable. That said, we believe the configuration would still be non-compliant.

The AD Cookbook team (what do we call ourselves?) is not able to approve Alternative Means; there is a formal process for doing this which goes through InCommon's Assurance Advisory Committee (AAC). If you were write up and submit such an Alternative Means proposal based on use of RODCs and it were accepted, we would be happy to reference it in the document. The AD Cookbook team may also be willing to assist in reviewing and editing your AM proposal.</td>
<td>No edits, to be addressed outside of the document.</td>
</tr>
</table>

4	In section 4.1.2, the cookbook states "These requirements apply when AD DS is used as the IdP's Verifier." The requirements certainly apply if AD DS is used as the IDP's Verifier. I think they also apply if AD DS is not used as the verifier, but stores the same secrets. Not so? As stated it may lead someone to think that the requirement only applies if AD DS is the IDP's Verifier, even though it doesn't exactly say that. So I think it should be removed.	Ron Thielen	1/29 /2014	After discussion we concur that this is an error in the text, and should be corrected/removed.	Copy language from the following section: *This requirement applies to IdP Verifier passwords stored in an AD DS password store, whether or not the AD DS store is the actual IdP Verifier. Note that this requirement only applies to passwords for accounts that are actually authenticated by the IdP (non-IdP accounts that are "co located" in the AD DS have no such requirements).*
5	I don't think we ever sufficiently addressed the issue of Radius using NTLMv1 to talk with the DC. We address the fact that using PEAP-MS-CHAPv2 deals with the communication between the supplicant and the Radius server, but Radius servers which rely on Samba use NTLMv1 between the Radius server and a DC. Recommend adding notes in Appendix A identifying the issue, and noting the options available to address the weakness. This would mean either • Leave NTLMv1 turned on for everyone, but tunnel all Radius AuthN traffic to the DC over a protected channel. Since I started my monitor and mitigate program about a year ago, I have only seen a handful of non-Radius NTLMv1 authentications. I may leave NTLMv1 turned on and continue monitor and mitigate. • Move Radius to a Windows implementation. Apparently the Windows version uses the LSAS and can then support NTLMv2. • Change Radius to use a separate DC still supports NTLMv1 but uses a protected channel between the DC and Radius. That way I can turn off NTLMv1 support on the main domain. This has several big downsides and probably is a non-starter. For example, all the supplicants would have to authenticate to a different domain causing havoc on the day of the change. It would also require one more credential sync between LDAP and this new DC.	Ron Thielen	1/29 /2014		
6	Since this is now a "fixed" version of the document, language in the appendices that indicates readers should edit the document to "put in any known issues" should be removed.	AD Assurance workgroup	1/31 /2014	Said language will be removed.	Remove language: *Put any known issues /affected systems here, along with how you solved the problem, if possible* from Appendices A, B and C.