May 24, 2013

AD-Assurance Notes from May 24

Eric Goodman, UCOP
Mark Rank, UCSF
Ron Thielen, U Chicago
Jeff Capehart, UFL
Michael Brogan, UW
Brian Arkills, UW
Lee Amenya, UCSD

Next Call

May 30 at Noon ET ???
+1-734-615-7474 PREFERRED
+1-866-411-0013
0195240#

Agenda:

Review of last week's (May 17) Action Items

Action Items

- *Eric*to followup with David re: long term vs. short term authentication secrets.
- Mark to post final version of "Monitor and Mitigate" endorsement to Wiki
- Ron to draft a statement about client caching of credentials via Data Protection API.
- Ron will look into whether SysKey uses approved algorithms.
- Eric to follow up on how Kerberos timeskew works
- Eric to do additional Cookbook edits (see notes, below)

Notes

Monitor and Mitigate Endorsement

No additional comments from the call.

Mark will post final version to Wiki.

Detecting NTLMv1 and Unsigned LDAP binds

These can be detected on DCs running Windows 2008 server or higher. Event IDs are 4624 and 2889.

The plan is to also release the PowerShell scripts and configuration requirements (special configs are required to initiate logging of the event)

NTLMv2 and RC4-HMAC

David points out that the Protected Channels requirement is for the transmission of passwords and Windows uses challenges which do not transmit the actual passwords.

Concern that focusing too much on NTLMv2 or Kerberos technicalities will overlook that there are other protocols that could be used (specifically around 4.2.3.6.2) that would still be insecure. May still need language in doc to clarify you have to look at the other non-AD protocols (e.g., https to web apps).

Brian pointed out that 800-63 defines short term authentication secret (which a challenge arguably is) as covered. The IAF does not appear to include short term authentication secrets in that definitions. Clarify the distinction with David -- that is, that the IAF does not equate "short term authentication secrets" with passwords. If we make this assessment, still need to document the logic somewhere in the Cookbook or supporting docs for use in Management Assertions.

So some question of whether the challenge itself or the session key is actually an "authentication secret".

[In 800-63] On the order of 2^80 if it's possible to guess/attack it. Talked about larger entropy of passwords for Silver 2^42 (12 char rather than 8, etc).

Client Caching Credentials

Windows apparently has 3 different mechanisms for local caching of passwords. The one used to manage the domain credentials still appears to be the Data Protection API. Data Protection API to break really requires breaking into the local machine (infecting, etc).

Cookbook Discussion

May need separate documents for Discussion vs. Configuration Recommendations. (For now will keep as separate sections in the same document).

Particularly in the network setup section, be clearer what requirements are "and" vs. "or". It's confusing as it is right now.

There are several Management Assertions that don't have any configuration requirements associated with them. E.g., language such as "use of NTLMv2 meets 4.2.3.6.2 as it never transmits passwords, only password challenges". We need to figure out where to put these assertions.

Some discussion again of whether 72 hours is too long for the "monitor and mitigate" strategy. It was pointed out that while automation would likely make this much faster to detect, that campuses may still want to have a manual process in place for review (at least for some cases), so the 72 hours still appears to make sense.

The "replay attacks" section has some general recommendations that we haven't discussed in great detail. Also, timeskew recommendation for Kerberos is not an actual recommendation, just a pointer to a possible mitigation. Do we have a recommendation? We also have a question around how timeskew works for Kerberos (is it |time1 - time2|, etc.).

Recommendations we agreed to change:

"NIS et al" as a compensating control for stored authentication secrets is insufficient. Need some language that says "and physical protection, and..." Also, while the issue of stored passwords being non-conformingly stored is an AD issue, these as alternate controls are not. I.e., if you wanted to protect any non-conforming password store you'd need to develop the same type of mitigation program, and it would not really have any components that are AD specific. Will update the compensating control with a general statement, but NOT with a Management Assertion or and Alternative Means statement.

Will remove reference to Syskey mode 2/3 if it is found that syskey is non-conforming.