Turning Off NTLMv1

or

How to Approach Turning Off Legacy Technology

IAM Online

November 12, 2014

Brian Arkills, University of Washington
Nick Roy, Penn State
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council
Assurance, Security, NTLM... Pick Two

- Active Directory widely used in higher ed (85-95% deployment rate, depending on who you ask)
- Security in Windows and AD have improved radically in the past decade
- If you are running AD Domain Services and have upgraded over the years, you need to plan to mitigate legacy authentication
- If you are doing a new AD, you should still plan to ensure you don’t deploy deprecated authentication schemes
Turning Off NTLMv1
or
How to Approach Turning Off Legacy Technology

Brian Arkills
Software Engineer, UW Windows Infrastructure Svc Mgr, and Associate Troubleshooting Officer 😊
UW-IT, Identity and Access Management

Microsoft Directory Services MVP 2012-2014
Goals
Why Turn Off NTLMv1?

5.1 Security Cons for Implementers

Implementers should be aware that NTLM does not support any recent cryptographic methods, such as AES or SHA-256. It uses cyclic redundancy check (CRC) or message digest algorithms ([RFC1321]) for integrity, and it uses RC4 for encryption. Deriving a key from a password is as specified in [RFC1320] and [FIPS46-2]. Therefore, applications are generally advised not to use NTLM.
Keys to Success Retiring Old Tech
NTLMv1 Resources We Developed

- NTLMv1 Removal - Known Problems and Workarounds
- Customer Mitigation Walkthrough
- PowerShell NTLMv1 Log Parser
- PowerShell and Registry file for LMCompatibilityLevel
- Log parsing -> Customer notification process
- IIS web app that only allows NTLMv2
Timeline and Visualizations

NTLMv1: Benefits of leveraging our user notifications

- AD launch - NTLMv1 off: 9/1/2006
- NTLMv1 on: 6/1/2007
- NTLMv1 off notice: 7/1/2012
- NTLMv1 off: 8/1/2013
- Problem analysis: 4/22/2014
- Change notices: 7/16
- Change moved: 8/12
- Mac Browser discover: 6/15/2014
- Reminder: 8/11/2014
- NTLMv1 off: 8/12/2014

Graph showing the benefits of leveraging user notifications with data points from 6/17-8/5.
Stumbling Points

IF YOU FIND A PATH WITH NO OBSTACLES, IT PROBABLY DOESN'T LEAD ANYWHERE.

OBSTACLES ARE THOSE FRIGHTFUL THINGS YOU SEE WHEN YOU TAKE YOUR EYES OFF YOUR GOAL.
Security Watch
The Most Misunderstood Windows Security Setting of All Time

Jesper Johansson
Svc Mgmt – Stumbling Points
Loose Ends
What about NTLMv2?
(Pass the Hash)
The End

Brian Arkills
barkills@uw.edu
@barkills
http://blogs.uw.edu/barkills
http://www.netid.washington.edu

Author of LDAP Directories Explained
Microsoft Directory Services MVP 2012-2014

INFORMATION TECHNOLOGY
UNIVERSITY of WASHINGTON
Evaluation

Please complete the evaluation of today’s webinar

Upcoming Webinars

Wednesday, Nov. 19
Affiliate Webinar – 2pm ET
Aegis Identity – A Case Study in Just-in-Time Provisioning and ID Proxy Management

Wednesday, Dec. 10
IAM Online – 2 pm ET
Multifactor Authentication – An Update from the MFA Cohortium
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council