NTLM
For Whom The Bell Tolls

The killing of NTLM – 2025 to 20??

Experts Live Austria

Thanks to our sponsors!

PLATINUM

ACP IT for innovators.

ConStraight

mann& mouse WE LIVE IT

base it

THOMAS KRENN® IT's people business

GOLD

CANCOM

INFOTECH [IT & Communication]

ProLion

DATACIDERS PASO

NiCE IT Management Solutions www.nice.de

SEPP MAIL

Didier Van Hoye
Technical Architect & Technology Strategist

- @workinghardinit.bsky.social
- https://x.com/WorkingHardInIT
- https://www.linkedin.com/in/didiervanhoye
- https://vimeo.com/workinghardinit
- https://github.com/WorkingHardInIT/Public
- https://workinghardinit.work

Experts Live Austria

NTLM: For whom the bell tolls

The killing of NTLM – 2025 to 20??

Microsoft is killing NTLM

- Starting with Windows 2025
- Not ending with it
- Not quite dead and buried yet
- Work in progress

What is NTLM?

- Authentication protocol
- It provides your identity to the resource you want to access
- It does not send your password
- It uses a challenge-response hash
- It is a fallback when better options don’t work or are not available
  - **Kerberos, OAuth, SAML, MSA, …**
  - **Local accounts (workgroups), no DNS name resolution, connection by IP address, no line of sight to a DC, …**

NTLM in a nutshell

- Client connects to server resource … a file share for example
- Server sends a challenge:

  Who are you?
- Client sends a response (Hashed Message Authentication Code)

  Hmac_md5(“Who are you?”, username, md4(password))
- Server checks the response

  That works out, welcome and proceed.

  Nope, that isn't right, thou shalt not pass!

https://blog.smallsec.ca/ntlm-challenge-response/

Killing NTLM is simple but far from easy!

- NTLM is everywhere
- PARADOX: It is extremely easy to kill and very hard to kill …
- NTLMv1 is security hell, NTLMv2 risks can be mitigated to some extend
- Credential Guard mitigates risks & kills NTLMv1
  - **But have you turned it on?**
  - **Upgrades to Windows 11 (22H2 & higher), and Windows Server 2025 have Credential Guard enabled by default unless explicitly disabled.**
- Incredibly dangerous, combined with short passwords
- It is risky to your business to disable wholesale & hope for the best
- The latter is risky to your employment as well.

Pain No 1: Weak encryption

```
hashcat (v6.2.6) starting in benchmark mode

CUDA API (CUDA 11.8)
====================
* Device #1: NVIDIA GeForce RTX 4090, 20155/24563 MB, 128MCU

OpenCL API (OpenCL 3.0 CUDA 11.8.87) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #2: NVIDIA GeForce RTX 4090, skipped

Benchmark relevant options:
===========================
* --benchmark-all
* --optimized-kernel-enable

----------------------
* Hash-Mode 1000 (NTLM)
----------------------

Speed.#1.........:   288.5 GH/s (7.24ms) @ Accel:512 Loops:1024 Thr:32 Vec:8
```

- Old, vulnerable encryption (DES, MD4, MD5,…)
- hmac operations are extremely fast
- So they can be easily broken by guessing (brute force)
- Nvdia 4090 GPU * 8 = 48 minutes of a random 8-character password
- HashCat checking known, popular password patterns: milliseconds
- Imagine bunch of bad guys on a budget: 8x RTX 4090 instance rented on vast.ai for < $5/hour

HASHCAT
An Advanced Password Cracking Tool

m:17128 host:96679 Utah, US
vast.ai
Type #10952072
8x RTX 4090
654.3 TFLOPS 24 GB
Max CUDA: 12.2 3234.1 GB/s
ROME2D32GM
PCIE 4.0,16x 23.9 GB/s
↑4117 Mbps
↓5320 Mbps 198 ports
AMD EPYC 7B12 ...
256.0/256 cpu 516/516 GB
CT4000P3PSSD8
1043 MB/s 3044.0 GB
448.8 DLPerf
91.4 DLP/$/hr
verified
Max Duration
1 mon, 15d
Reliability
99.51%
$4.910/hr
RENT

Is mutual authentication important?

- YES
- Lack of it leads to “easy” relay or proxy attacks
- Aka “Man In The Middle” attacks
- Which is why you disable LLMNR, NetBIOS, … as it helps bad actors poison name resolution

Pain No 2: No Server authentication

- NTLM does not provide mutual authentication
- You have no guarantee that you are talking to the correct server

Other mitigations do exist

- Extended protection / Token binding (On Token Binding)

➔"Bolt On" so if you don't do it, it is not here – not part of NTLM

- Credential Guard

➔Virtualization Based Security

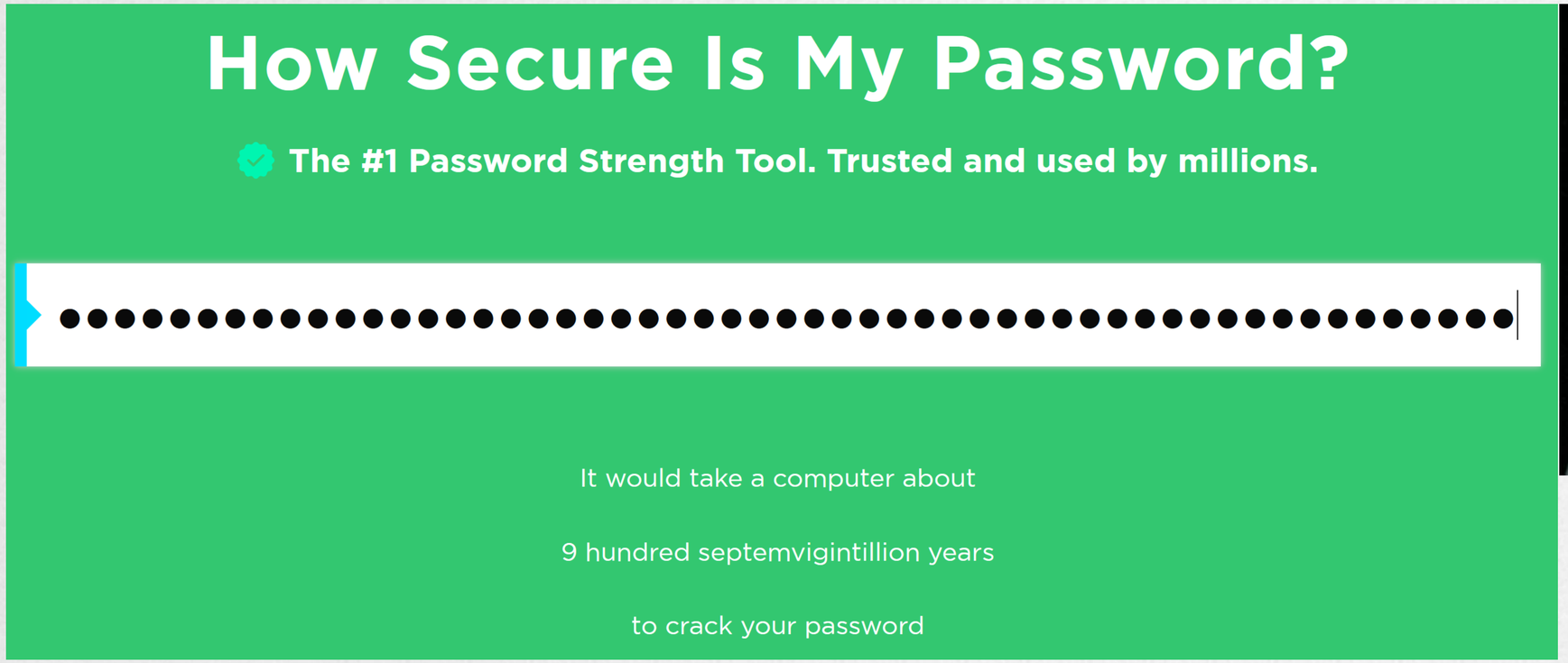
Pain No 3: Password usage sucks

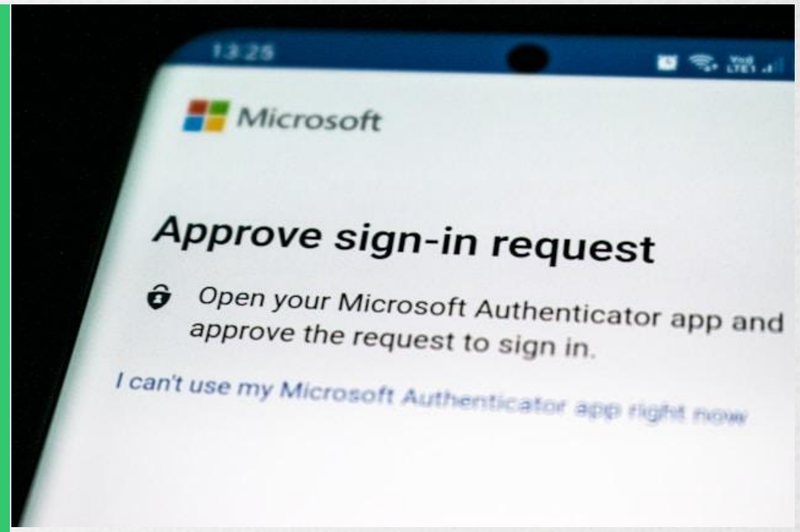
- Most passwords are bad
- People use patterns
- Known words, easy to guess
- Way too short

Length is your friend … add MFA!

- Use pass phrases!

  Donkey Goes 2 a Restaurant For Food & a Bar 4 Drinks!





Pain No 4: Code vulnerabilities

- Developers are not perfect (no one is)

Windows NTLM Security Support Provider Information Disclosure Vulnerability
CVE-2023-24900
Security Vulnerability
Released: May 9, 2023

NEWS 4 MAR 2024

TA577 Exploits NTLM Authentication Vulnerability

NEWS, EXPLOITS AND VULNERABILITIES

Patch now! Microsoft Office flaw could leak NTLM hashes

Microsoft is warning about a Microsoft Office vulnerability which an attacker could use to steal NTLM hashes.

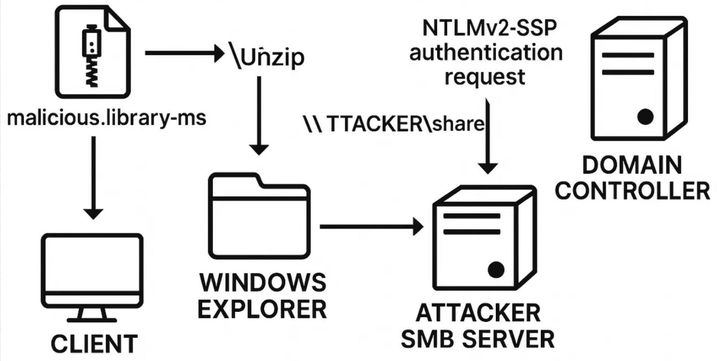
Posted: August 13, 2024 by Pieter Arntz

CROWDSTRIKE | BLOG

Critical Vulnerabilities in NTLM Allow Remote Code Execution and Cloud Resources Compromise

December 21, 2020 | Yaron Zinar | Identity Protection

CVE-2025-24054
Vulnerability in Windows NTLM

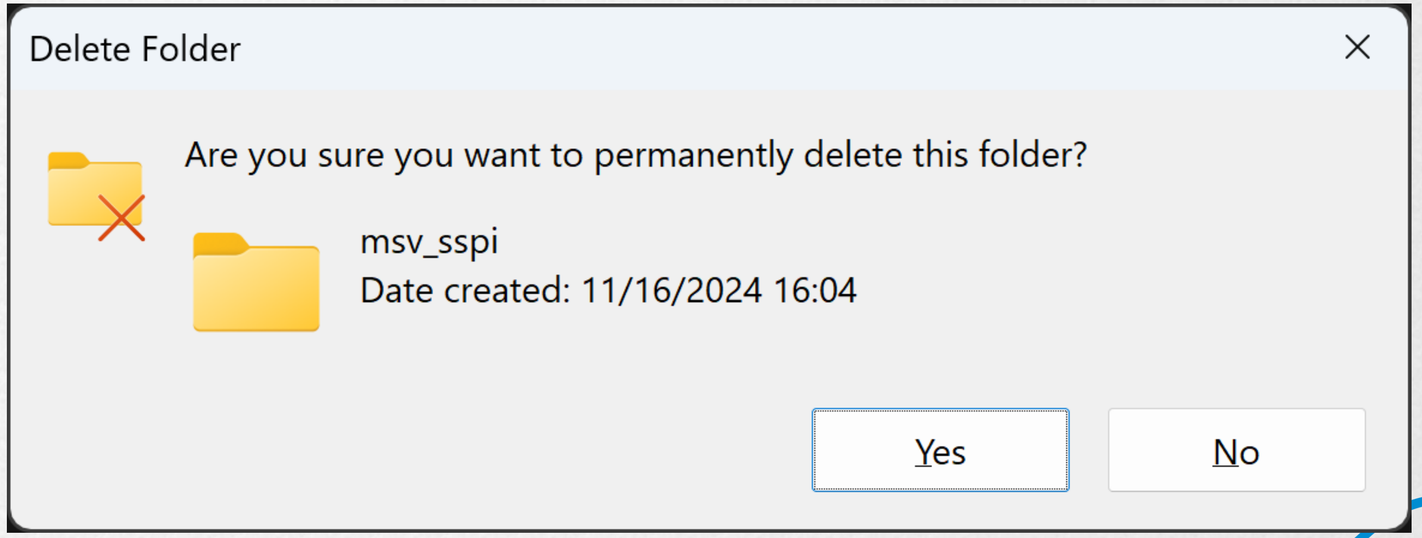


Get rid of it!

- Just rip out the code!

Wait a minute!

- Even disabling NTLM has many unintended consequences
- Let alone ripping it out of the source code
- Who are the stake holders?
- NTLM is used everywhere!
- Define everywhere!



And we all need to agree

- Authentication Platform owners at MSFT who own the code
- Servicing Team, which incorporates code into Windows builds for release
- SMB team, huge for both use and abuse of NTLM
- MSRC, the security response center that wants it all to go away
- Support, they have to deal with all NTLM issues
- Azure, they need to incorporate it into a hyper-scaler & make it secure
- 3rd party software creators who want to build and sell new features
- Customers who want stuff to work

What constitutes “Everywhere”?

1. Line of sight => +/- 5% of all NTLM authentication
2. Unknown server (IP address, DC doesn’t know the server, CNAMES without SPNs, etc.) => 14% of all NTLM authentication
3. Workgroup/local accounts: 29% of all NTLM authentication
4. The remaining 52% is hardcoded – developers, huh!

➔ 48% where we cannot do anything better right now!

➔ So, we need something better?

➔ What?

It has to be ubiquitous as Windows itself, so it must be part of it, no external dependencies, needs to be fast and secure

What is better

- Should not rely on passwords alone ➔ add MFA
- Oauth, SAML, Kerberos

While many cry Kerberos is Active Directory, which is on-prem and must die … they forget …

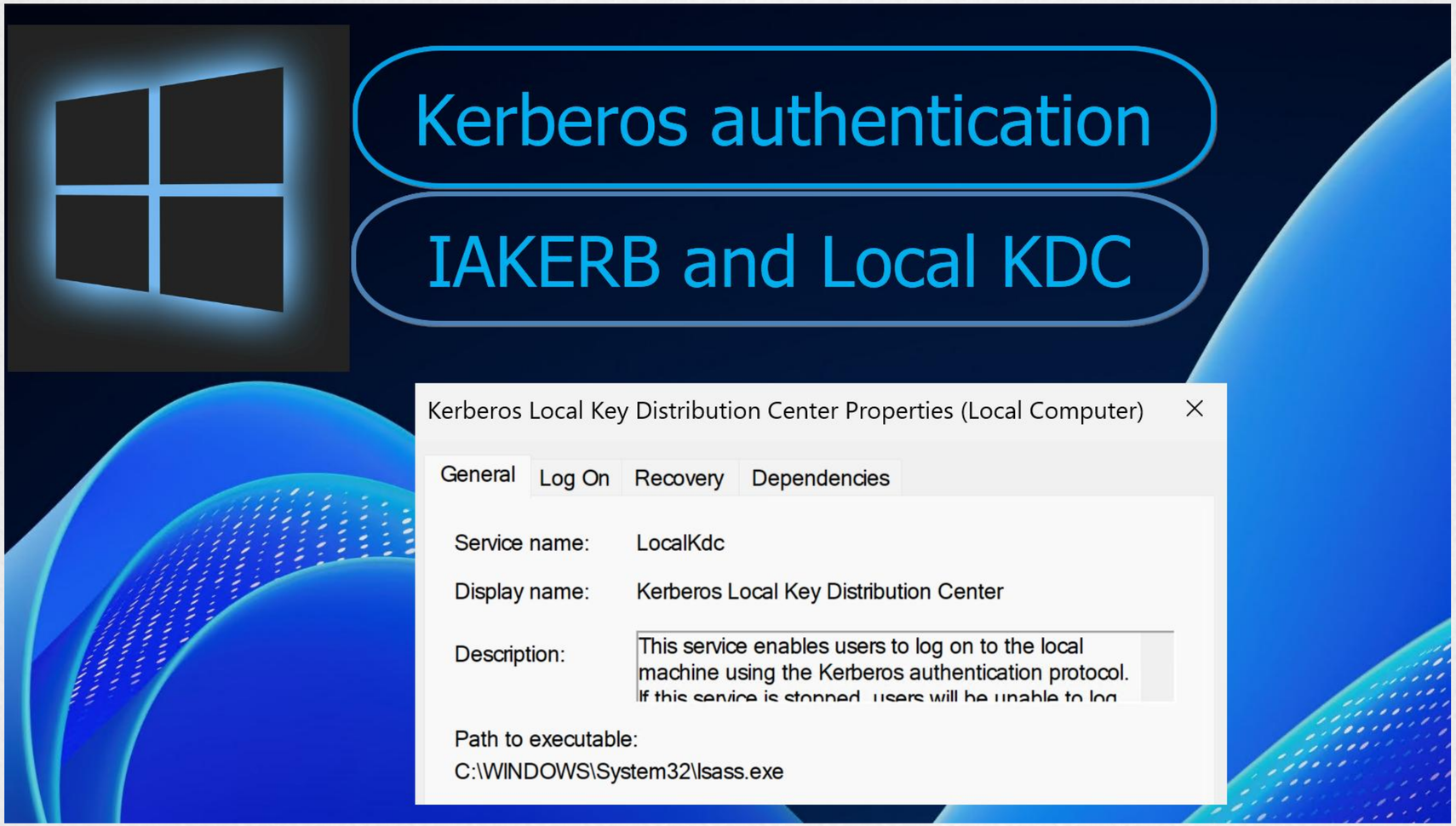
Kerberos is all right; it is pretty darn good and up-to-date.

It is less “Internet friendly,” but a KDC Proxy already exists! Maybe therein lies an answer.

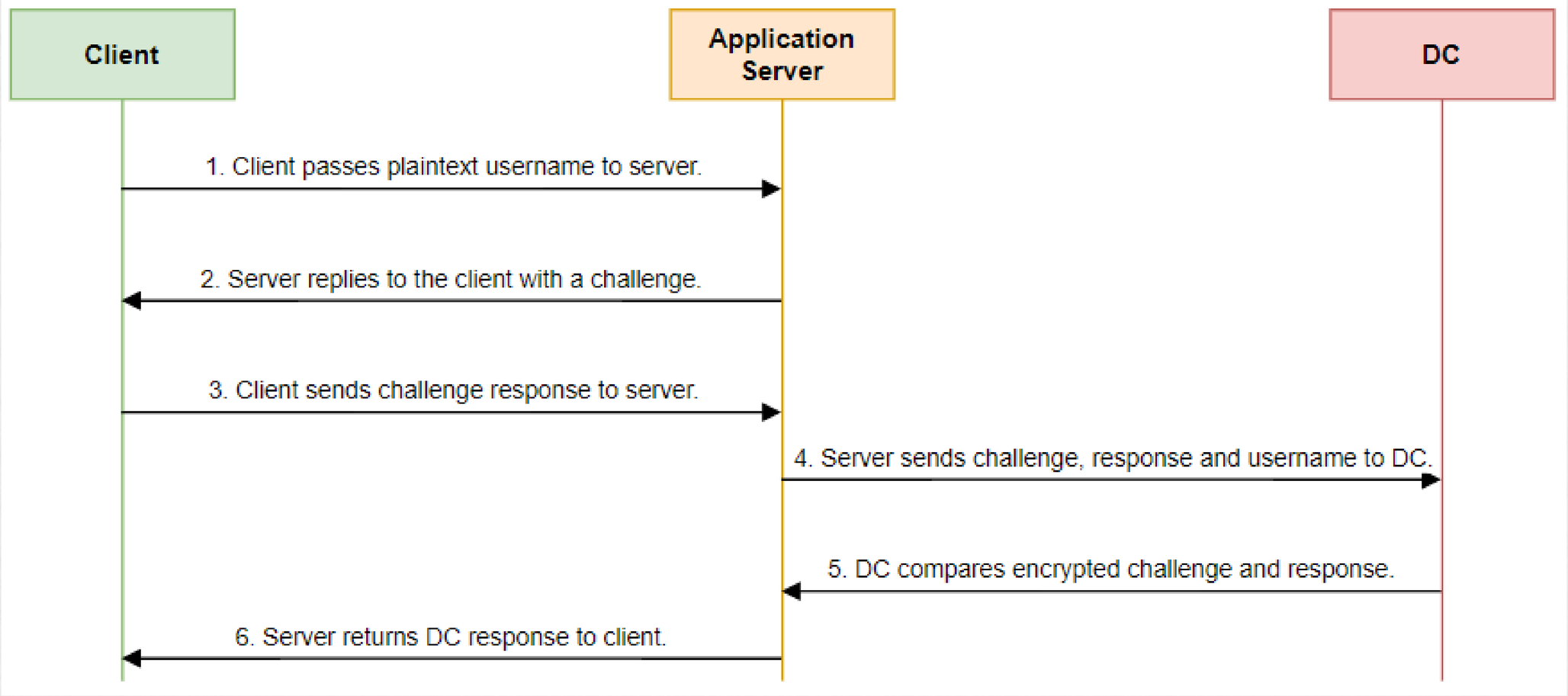
Why Kerberos?

- Can’t take a dependency on cloud
- Many use cases exist where that is not an option
- Kerberos has way better crypto
- Crypto agile (get rid of old ciphers & put in newer ones)
- Quantum safe (symmetric), so large key sizes provide protection
- Support for arbitrary credentials: FIDO, HELLO, SMART CARDS

IAKERB & Local KDC for Kerberos



NTLM in an Active Directory Domain



IAKERB fixes line of sight (5%)

- Have Kerberos authentication done, when we have no line of sight, by the service we are authenticating to
- KDC proxy already does that for RDP, SMB over QUIC, Direct Access
- Provide a way to do this for any use case transparently!
- Meet IAKERB!
- IAKERB stands for Initial and Pass-Through Authentication Using Kerberos v5 and the GSS-API (IAKERB).
- See draft-zhu-ws-kerb-03 & draft-ietf-krb-wg-iakerb-02 - Initial and Pass Through Authentication Using Kerberos V5 and the GSS- API (IAKERB)

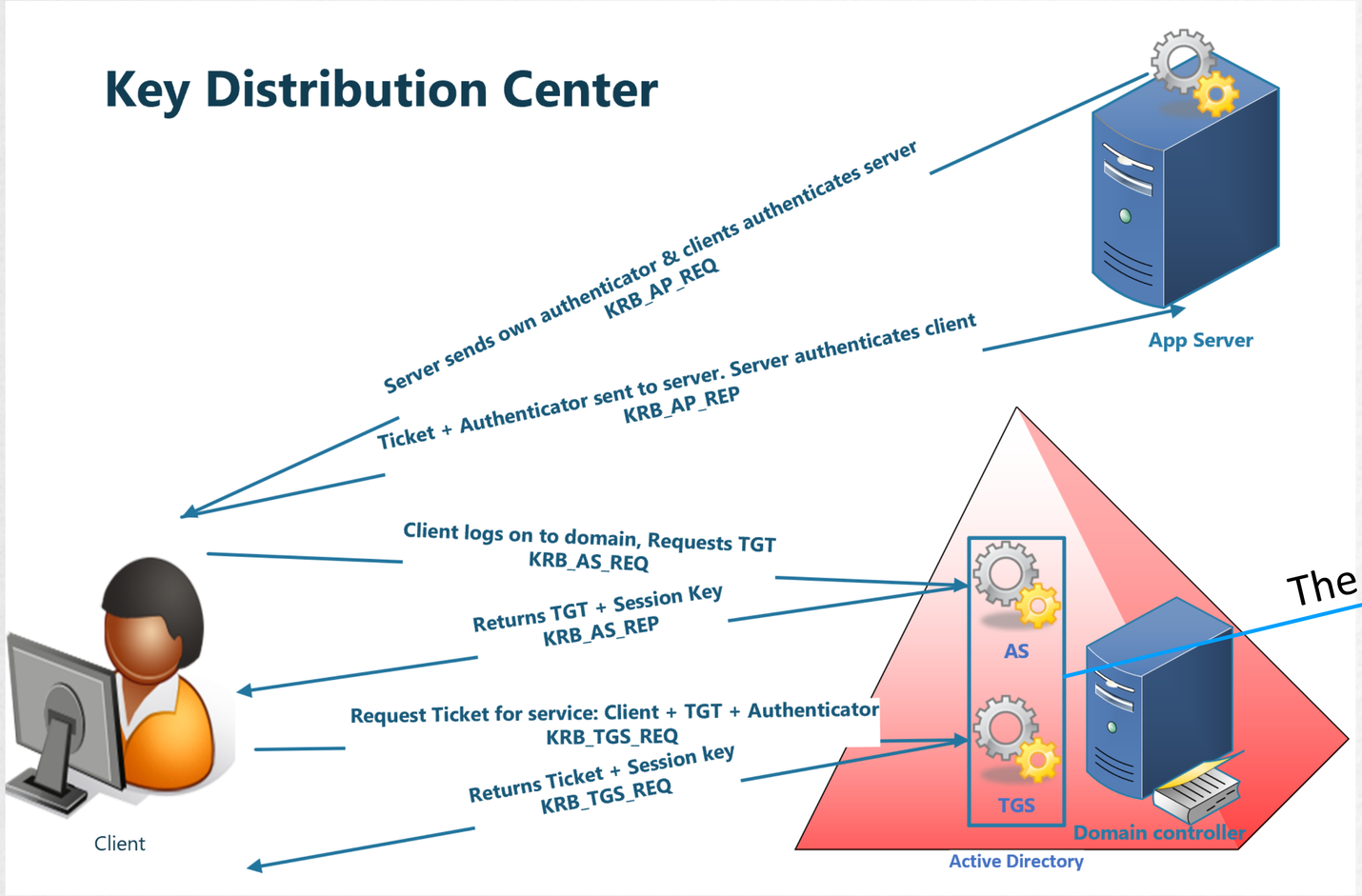
IAKERB

NETWORK WORKING GROUP
Internet-Draft
Updates: 4120 (if approved)
Intended status: Standards Track
Expires: January 10, 2008

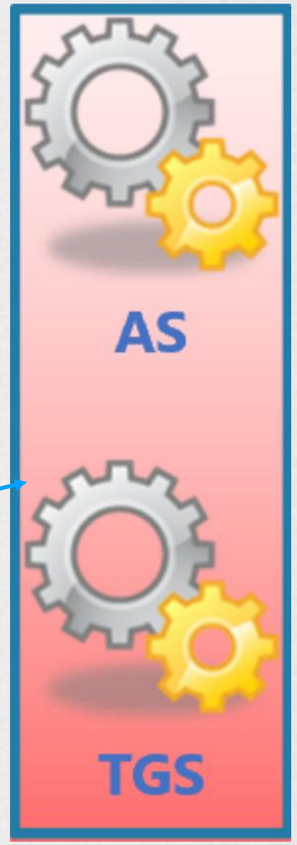
L. Zhu
Microsoft Corporation
J. Altman
Secure Endpoints
July 9, 2007

Initial and Pass Through Authentication Using Kerberos V5 and the GSS-API (IAKERB)
draft-zhu-ws-kerb-03

Kerberos doesn’t need domain controllers



The part you need: KDC service



Local KDC provides Kerberos for authenticating to a local machine (29%)

- You do not need a domain and domain/controllers for Kerberos
- You need a KDC!
- So put one in every server!
- IAKERB handles forwarding the requests to the Local KDC
  - **No need for UDP/TCP 88 etc.**
- Local user issues and workgroup environments are solved
- 5% (IAKERB) + 29% (local accounts) = 34% of NTLM use cases are now fixed

Unknown Servers 14%

Kerberos has server authentication.

Key exchange between the server and the client

If we know the server is who it claims to be, all is good

Cannot authenticate the server => do not authenticate the client

That's it – do not fall back to NTLM

We now have 48% of the intentional fallback to NTLM solved!

52% ➔ of developers are men!

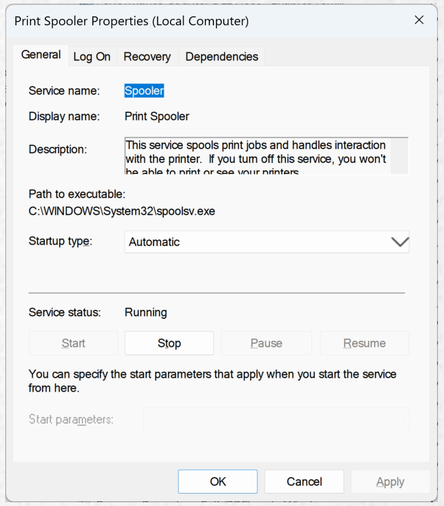
Developers cause remaining 52%

Hardcoded NTLM auth instead of negotiate
30 % of ALL (not just hardcoded 52%) NTLM authentication is one service
NOT:

- RDP (not hardcoded)
- SMB (not hardcoded)
- Clustering/ADCS (hardcoded)

IT IS:

- Print Spooler Service



So change it in the code – MSFT did ;-)
.AuthenticationScheme = System.Net.AuthenticationSchemes.Ntlm
.AuthenticationScheme = System.Net.AuthenticationSchemes.Negotiate

Other Hard Coded NTLM offenders

- One third party does 10% of all NTLM that is hard coded
- Will not be named
- MSFT has to go talk to them (and find a person to talk to) in order to ask them to change this.
- Same for others … if they can’t make that happen …
- Registry of “Known Offenders”- Public naming and shaming like MSFT does for SMB1 so user don’t buy them
- Break their apps! Can’t do that … legal issues – just kidding lawyers!
- IIS: 3%
- Outlook/SMPT: 2,9 %
- The rest: … less than 10% => long end of the tail …

Conclusion

- This will not be fast or easy …
- The roadmap to disable NTLM wholesale starts with W2K25 …
- … it does not end with it …
- The focus is on getting rid of the “easier” 85-90 %
- They will, one day, turn it off by default
- You will have the option to turn it on when it is inevitable
- Off by default = YES / Removed for ever = UNLIKELY

`Questions?

Experts Live Austria

Experts Live Austria

Thanks to our sponsors!

PLATINUM

ACP IT for innovators.

ConStraight

mann& mouse WE LIVE IT

base it

THOMAS KRENN® IT's people business

GOLD

CANCOM

INFOTECH [IT & Communication]

ProLion

DATACIDERS PASO

NiCE IT Management Solutions www.nice.de

SEPP MAIL