RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Pass-the-Hash: How Attackers Spread and How to Stop Them

SESSION ID: HTA-W03

Mark Russinovich

Technical Fellow
Microsoft Corporation

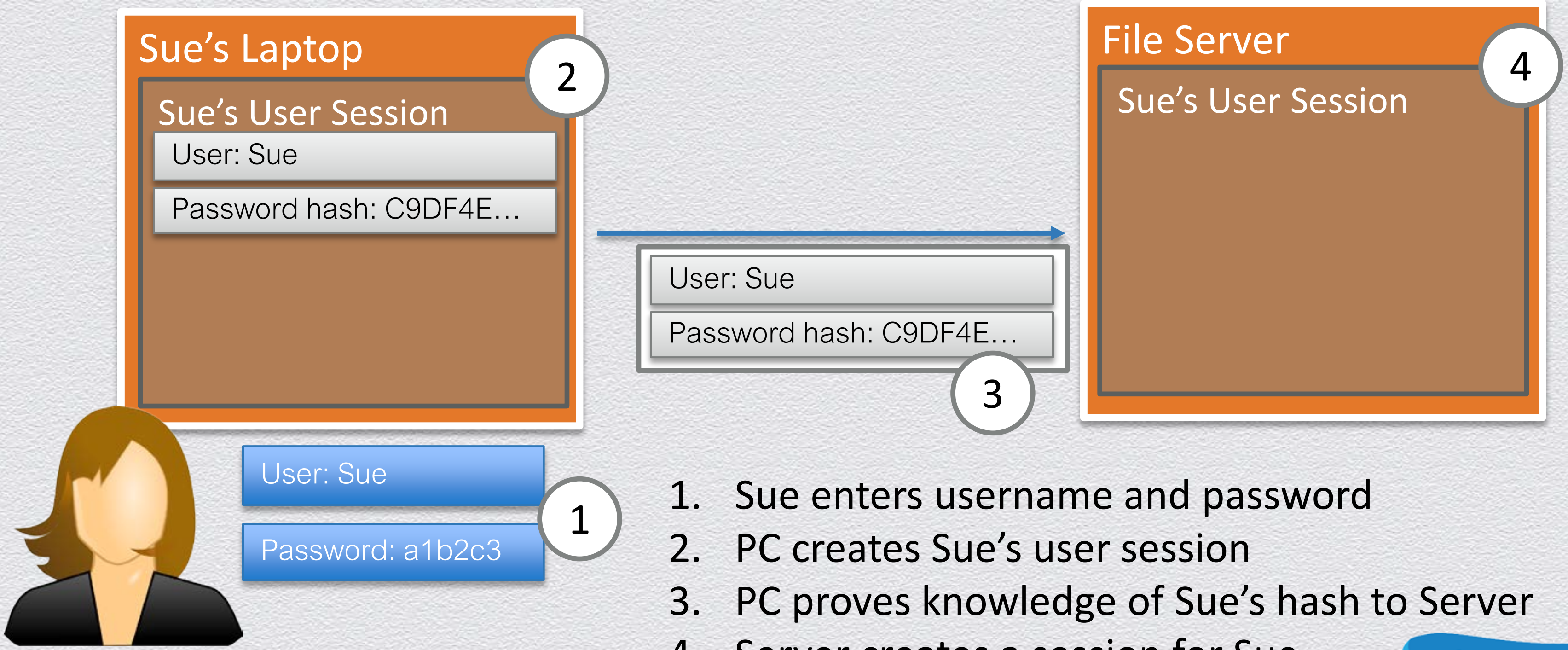
Nathan Ide

Principal Development Lead
Microsoft Corporation

Pass-the-Hash: Agenda

- Pass-the-Hash Technique
- Pass-the-Hash on Windows Today
- New Windows Mitigations:
  - Local Account
  - Domain Account
  - Restricted Remote Administration
  - Authentication Policies and Silos

Single-Sign On, Explained



Sue's Laptop

2

Sue's User Session

User: Sue

Password hash: C9DF4E…

User: Sue

Password hash: C9DF4E…

3

File Server

4

Sue's User Session

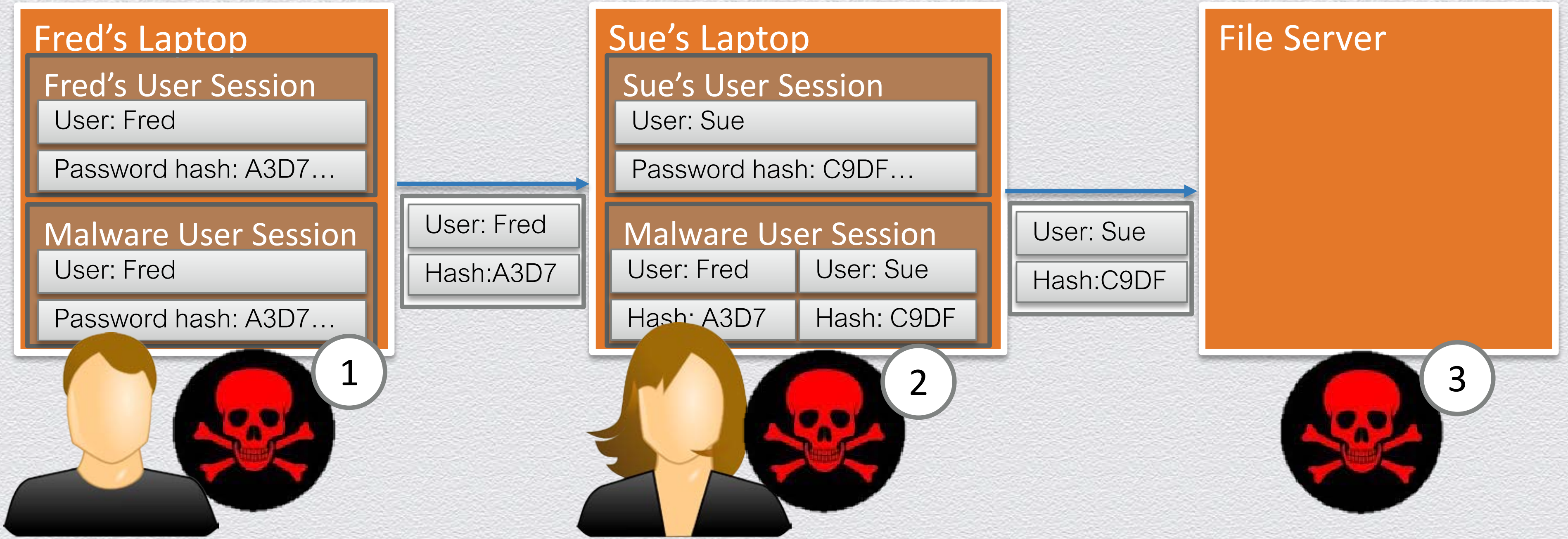
User: Sue

Password: a1b2c3

1

1. Sue enters username and password
2. PC creates Sue's user session
3. PC proves knowledge of Sue's hash to Server
4. Server creates a session for Sue

Pass-the-Hash Technique



Fred's Laptop

Fred's User Session

User: Fred

Password hash: A3D7…

Malware User Session

User: Fred

Password hash: A3D7…

User: Fred

Hash:A3D7

Sue's Laptop

Sue's User Session

User: Sue

Password hash: C9DF…

Malware User Session

User: Fred	User: Sue
Hash: A3D7	Hash: C9DF

User: Sue

Hash:C9DF

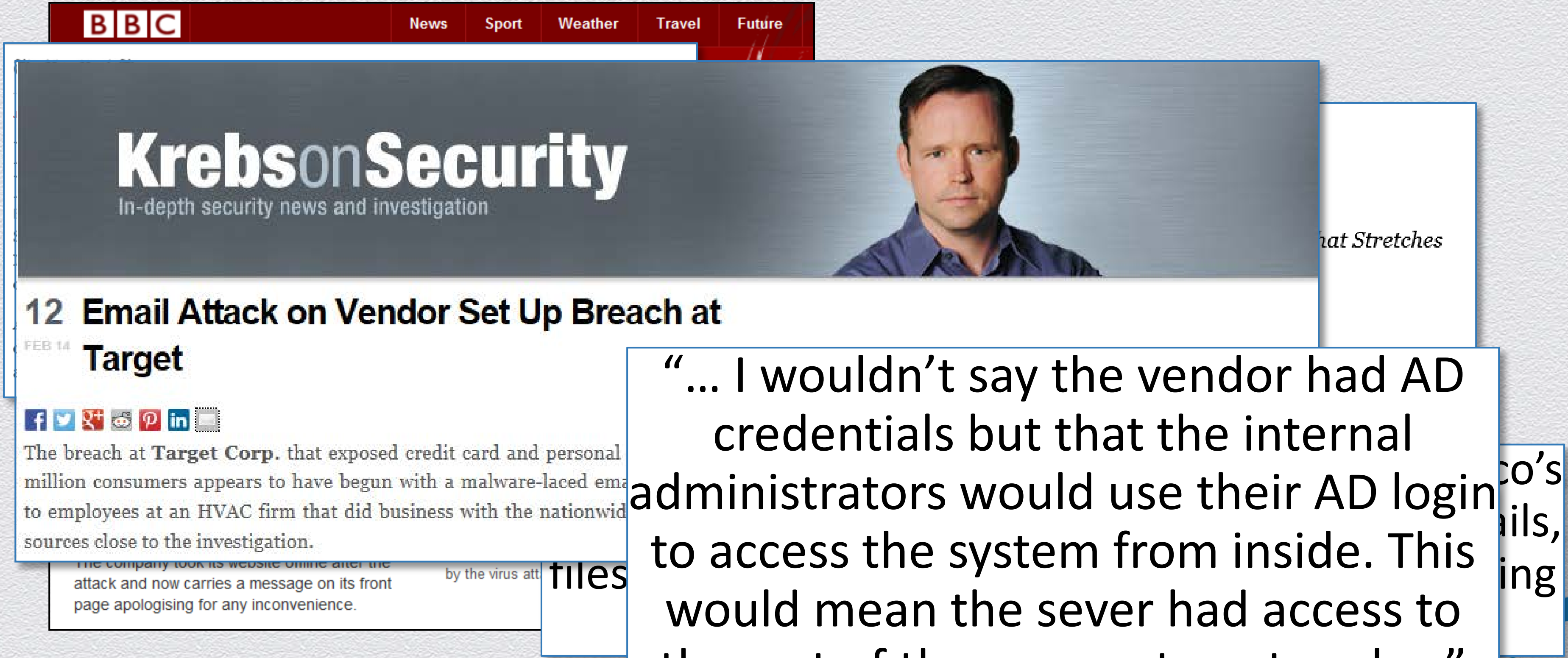
File Server

1. Fred runs malware
2. Malware infects Sue's laptop as Fred
3. Malware infects File Server as Sue

Pass-the-Hash: Agenda

- Pass-the-Hash Technique
- Pass-the-Hash on Windows Today
- New Windows Mitigations:
  - Local Account
  - Domain Account
  - Restricted Remote Administration
  - Authentication Policies and Silos

Windows Pass-the-Hash in the News



12 FEB 14

Email Attack on Vendor Set Up Breach at Target

The breach at **Target Corp.** that exposed credit card and personal million consumers appears to have begun with a malware-laced ema to employees at an HVAC firm that did business with the nationwid sources close to the investigation.

The company took its website offline after the attack and now carries a message on its front page apologising for any inconvenience.

by the virus att

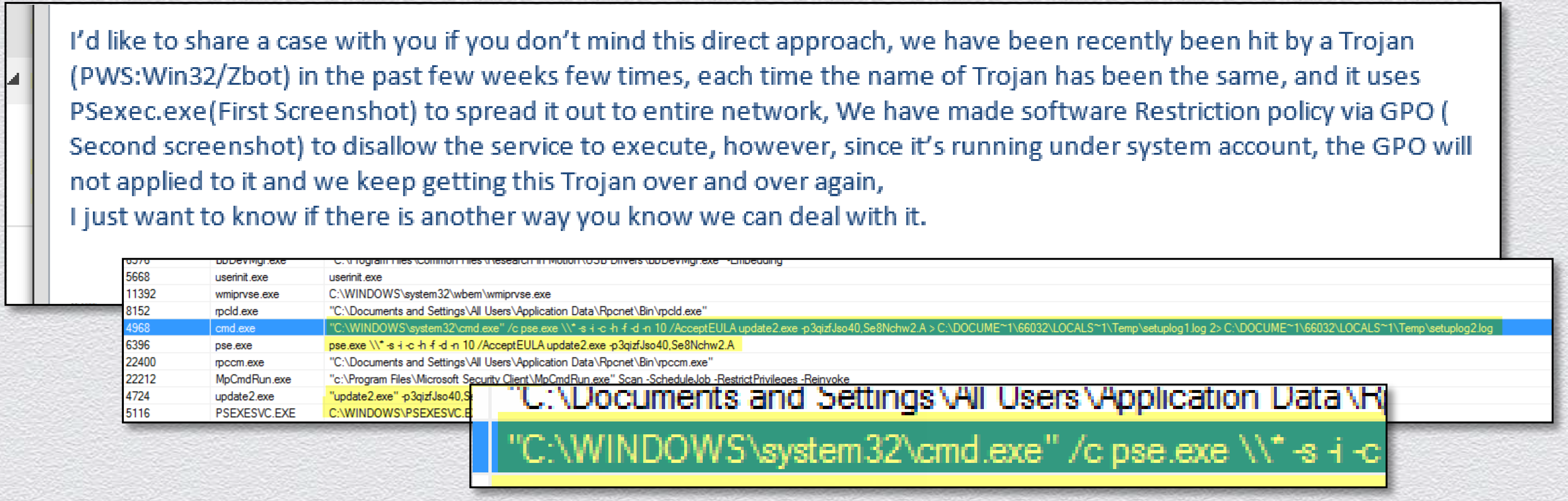
"… I wouldn't say the vendor had AD credentials but that the internal administrators would use their AD login to access the system from inside. This would mean the sever had access to the rest of the corporate network …"

Microsoft

#RSAC

RSACONFERENCE2014

Windows Pass-the-Hash in Mark’s Inbox



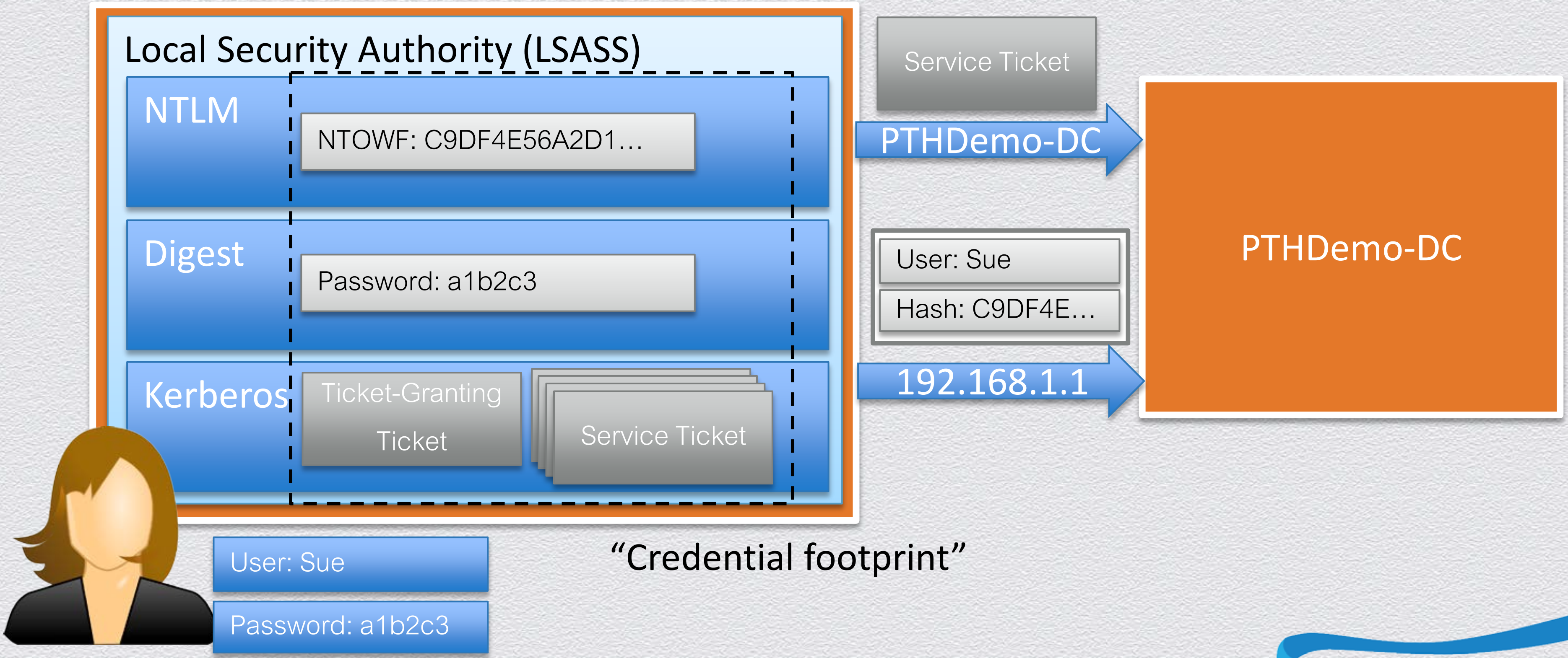
I’d like to share a case with you if you don’t mind this direct approach, we have been recently been hit by a Trojan (PWS:Win32/Zbot) in the past few weeks few times, each time the name of Trojan has been the same, and it uses PSexec.exe(First Screenshot) to spread it out to entire network, We have made software Restriction policy via GPO (Second screenshot) to disallow the service to execute, however, since it’s running under system account, the GPO will not applied to it and we keep getting this Trojan over and over again,

I just want to know if there is another way you know we can deal with it.

```
6576   BBDevMgr.exe    "C:\Program Files\Common Files\Research in Motion\USB Drivers\BBDevMgr.exe" -Embedding
5668   userinit.exe    userinit.exe
11392  wmiprvse.exe    C:\WINDOWS\system32\wbem\wmiprvse.exe
8152   rpcld.exe       "C:\Documents and Settings\All Users\Application Data\Rpcnet\Bin\rpcld.exe"
4968   cmd.exe         "C:\WINDOWS\system32\cmd.exe" /c pse.exe \\* -s -i -c -h -f -d -n 10 /AcceptEULA update2.exe -p3qizfJso40,Se8Nchw2.A > C:\DOCUME~1\66032\LOCALS~1\Temp\setuplog1.log 2> C:\DOCUME~1\66032\LOCALS~1\Temp\setuplog2.log
6396   pse.exe         pse.exe \\* -s -i -c -h -f -d -n 10 /AcceptEULA update2.exe -p3qizfJso40,Se8Nchw2.A
22400  rpccm.exe       "C:\Documents and Settings\All Users\Application Data\Rpcnet\Bin\rpccm.exe"
22212  MpCmdRun.exe    "c:\Program Files\Microsoft Security Client\MpCmdRun.exe" Scan -ScheduleJob -RestrictPrivileges -Reinvoke
4724   update2.exe     "update2.exe" -p3qizfJso40,S
5116   PSEXESVC.EXE    C:\WINDOWS\PSEXESVC.E
```

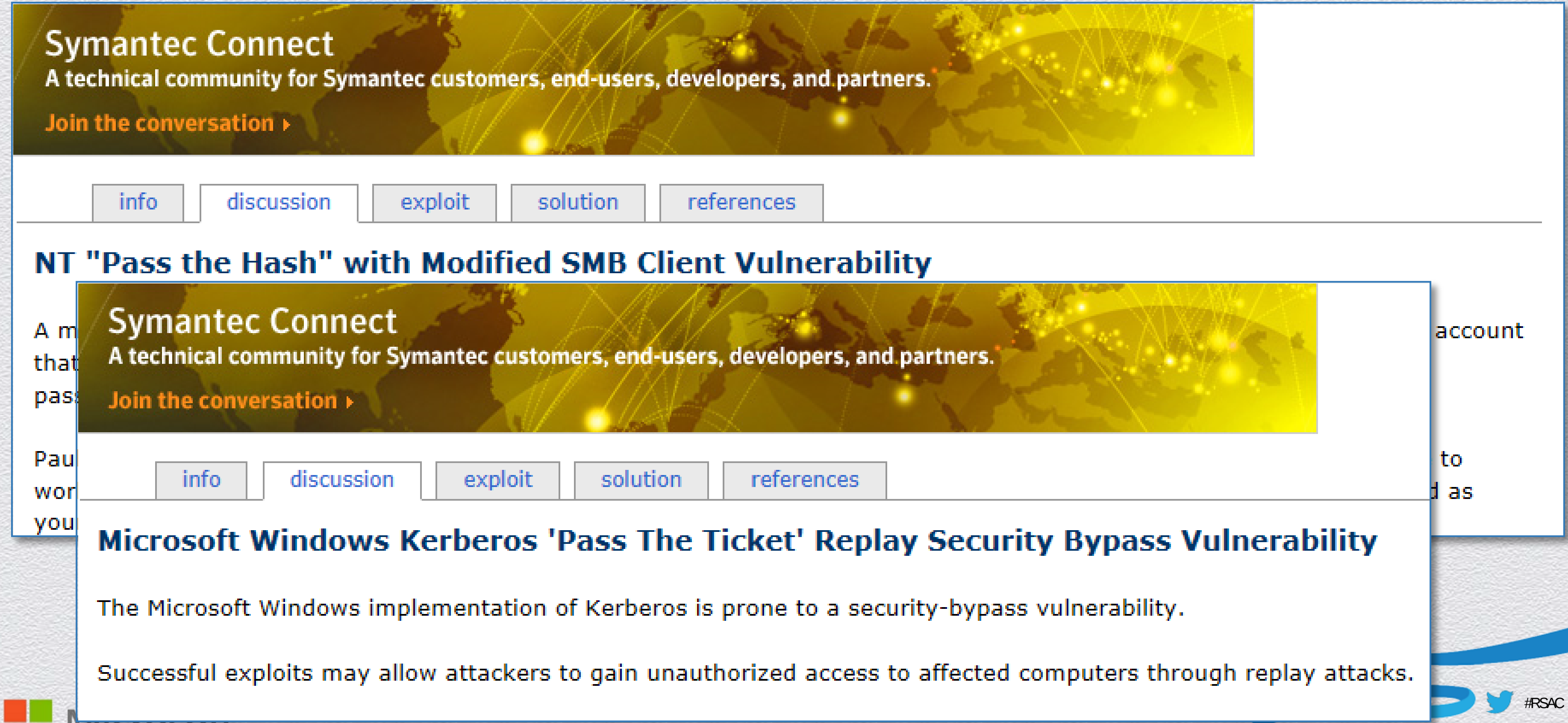
```
"C:\Documents and Settings\All Users\Application Data\R
"C:\WINDOWS\system32\cmd.exe" /c pse.exe \\* -s -i -c
```

Windows Single-Sign On Architecture



"Credential footprint"

Windows Pass-the-Hash “Discovery”



Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

Join the conversation ›

NT "Pass the Hash" with Modified SMB Client Vulnerability

A m … account
that
pas

Pau … to
wor … d as
you

Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

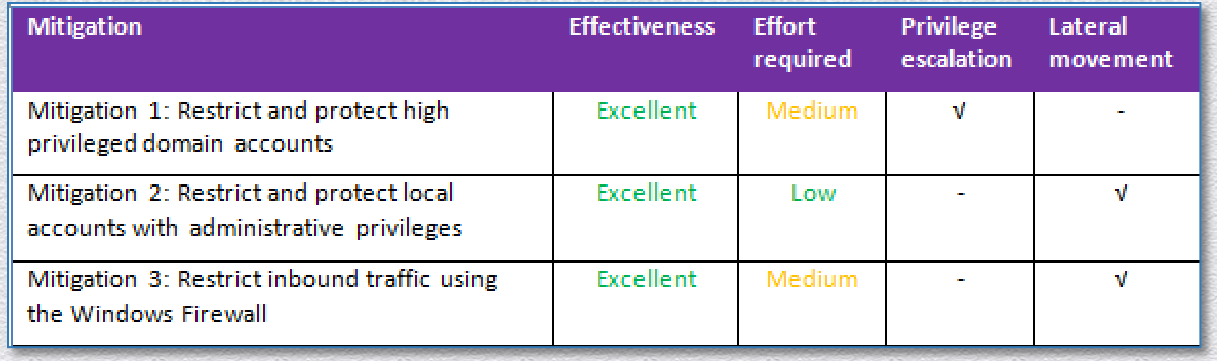
Join the conversation ›

Microsoft Windows Kerberos 'Pass The Ticket' Replay Security Bypass Vulnerability

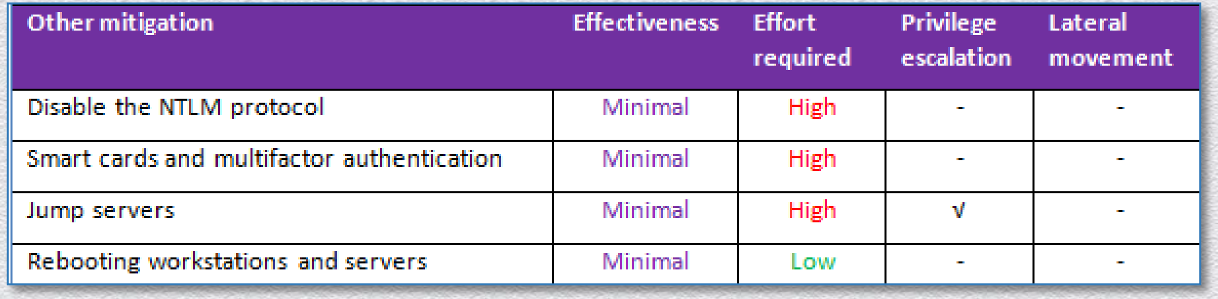
The Microsoft Windows implementation of Kerberos is prone to a security-bypass vulnerability.

Successful exploits may allow attackers to gain unauthorized access to affected computers through replay attacks.

Microsoft Guidance



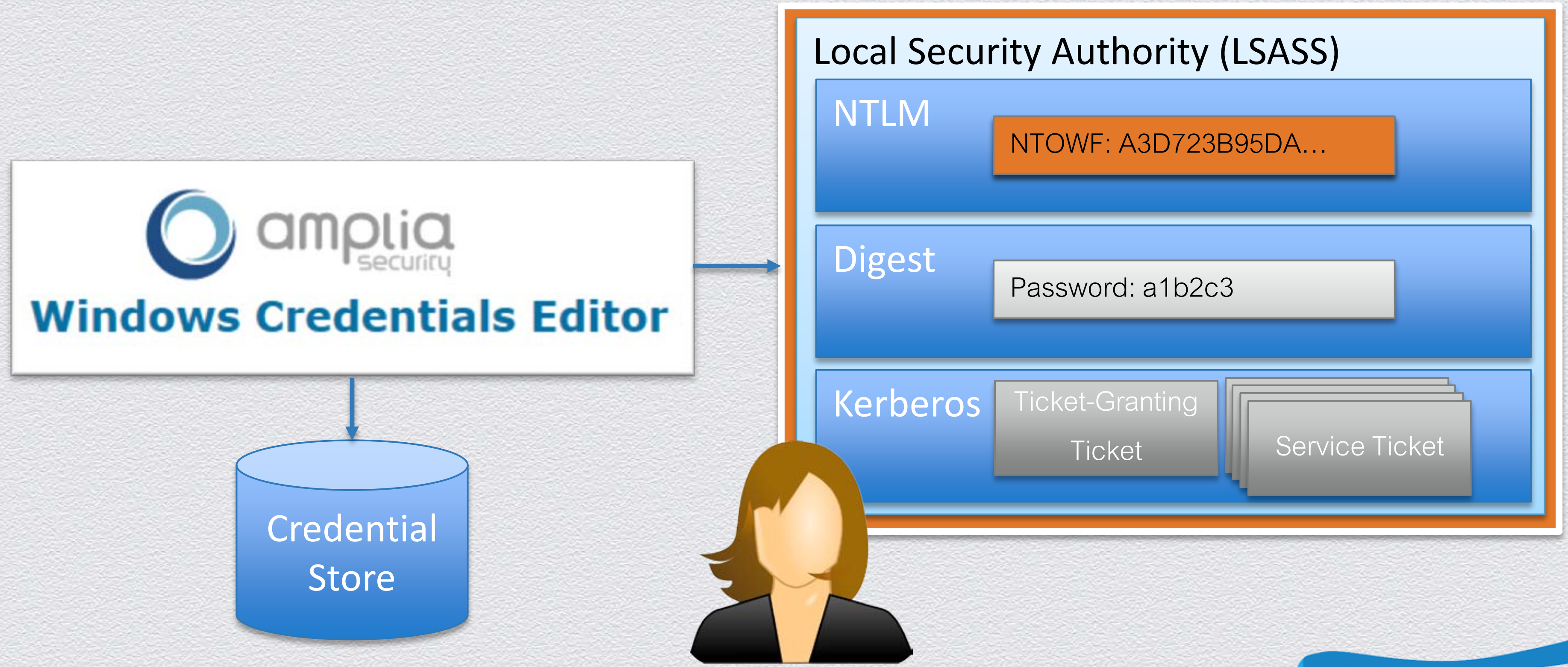
Mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Mitigation 1: Restrict and protect high privileged domain accounts	Excellent	Medium	√	-
Mitigation 2: Restrict and protect local accounts with administrative privileges	Excellent	Low	-	√
Mitigation 3: Restrict inbound traffic using the Windows Firewall	Excellent	Medium	-	√



Other mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Disable the NTLM protocol	Minimal	High	-	-
Smart cards and multifactor authentication	Minimal	High	-	-
Jump servers	Minimal	High	√	-
Rebooting workstations and servers	Minimal	Low	-	-

- Microsoft published Pass-the-Hash guidance in December 2012.
- Highlighted best practices and dispelled urban legends

Pass-the-Hash Tools on Windows



Windows Credentials Editor

Credential Store

Local Security Authority (LSASS)

NTLM

NTOWF: A3D723B95DA…

Digest

Password: a1b2c3

Kerberos

Ticket-Granting Ticket

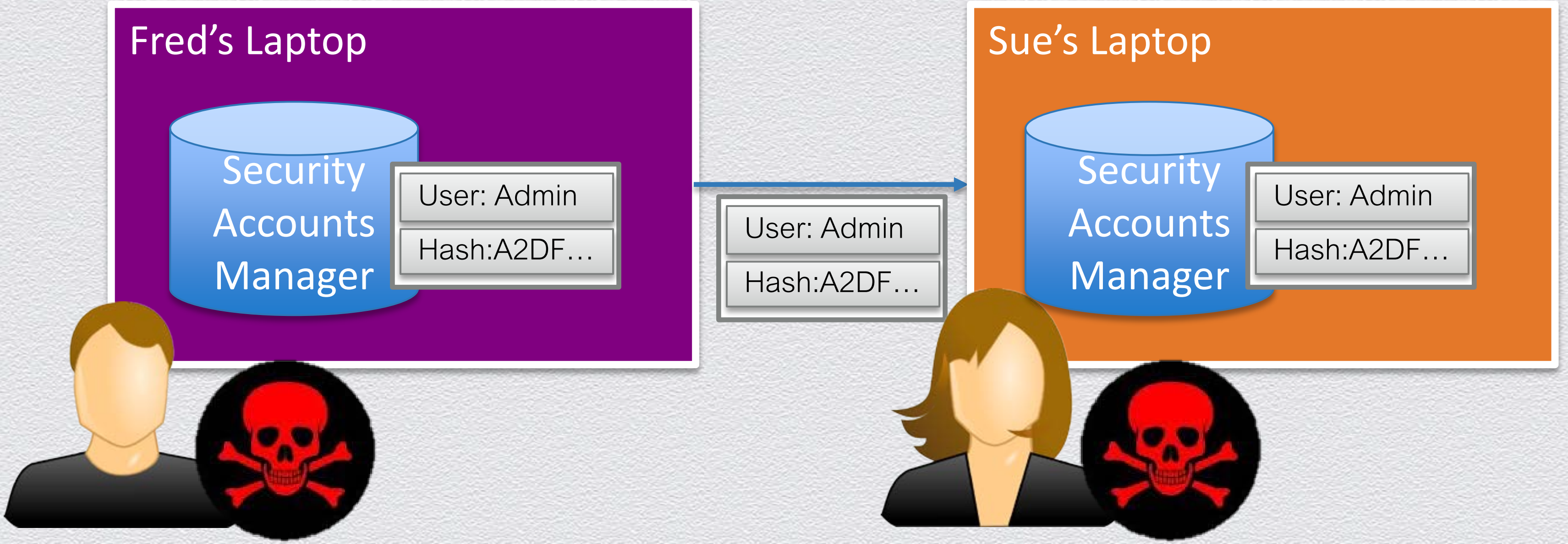
Service Ticket

Demo: Pass-the-Hash with Windows Credential Editor

Pass-the-Hash: Agenda

- Pass-the-Hash Technique
- Pass-the-Hash on Windows Today
- New Windows Mitigations:
    - Local Account
    - Domain Account
    - Restricted Remote Administration
    - Authentication Policies and Silos

Problem: Local Account Traversal



Fred's Laptop

Security Accounts Manager

User: Admin

Hash:A2DF…

User: Admin

Hash:A2DF…

Sue's Laptop

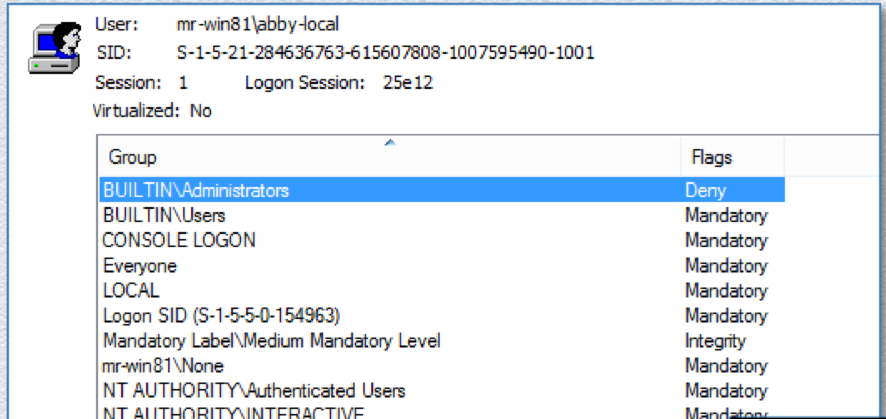
Security Accounts Manager

User: Admin

Hash:A2DF…

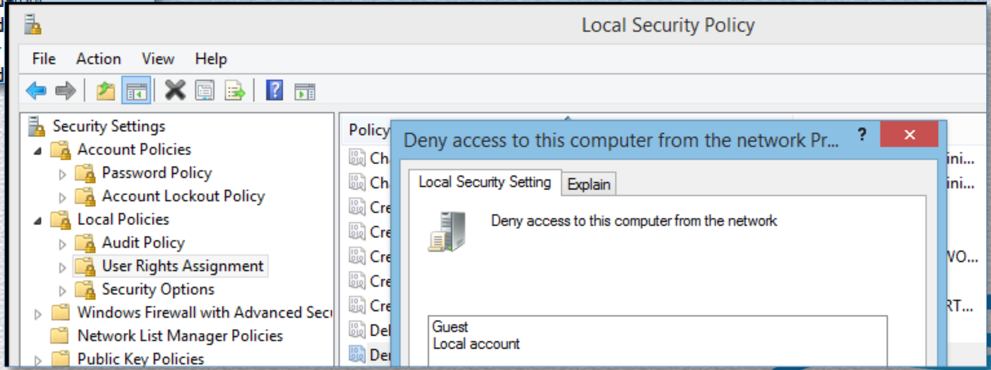
Local Account Mitigations

- Two new well-known groups:
  - “Local account”
  - “Local account and member of Administrators group”
- Useful for restricting access



```
User:      mr-win81\abby-local
SID:       S-1-5-21-284636763-615607808-1007595490-1001
Session:   1        Logon Session:   25e12
Virtualized:  No

Group                                                   Flags
BUILTIN\Administrators                                  Deny
BUILTIN\Users                                           Mandatory
CONSOLE LOGON                                           Mandatory
Everyone                                                Mandatory
LOCAL                                                   Mandatory
Logon SID (S-1-5-5-0-154963)                            Mandatory
Mandatory Label\Medium Mandatory Level                  Integrity
mr-win81\None                                           Mandatory
NT AUTHORITY\Authenticated Users                        Mandatory
NT AUTHORITY\INTERACTIVE                                Mandatory
NT AUTHORITY\Local account                              Mand
NT AUTHORITY\Local account and member of Administrators group   Deny
NT AUTHORITY\NTLM Authentication                        Mand
```



Deny access to this computer from the network Pr...

Deny access to this computer from the network

Guest
Local account

RSACONFERENCE2014

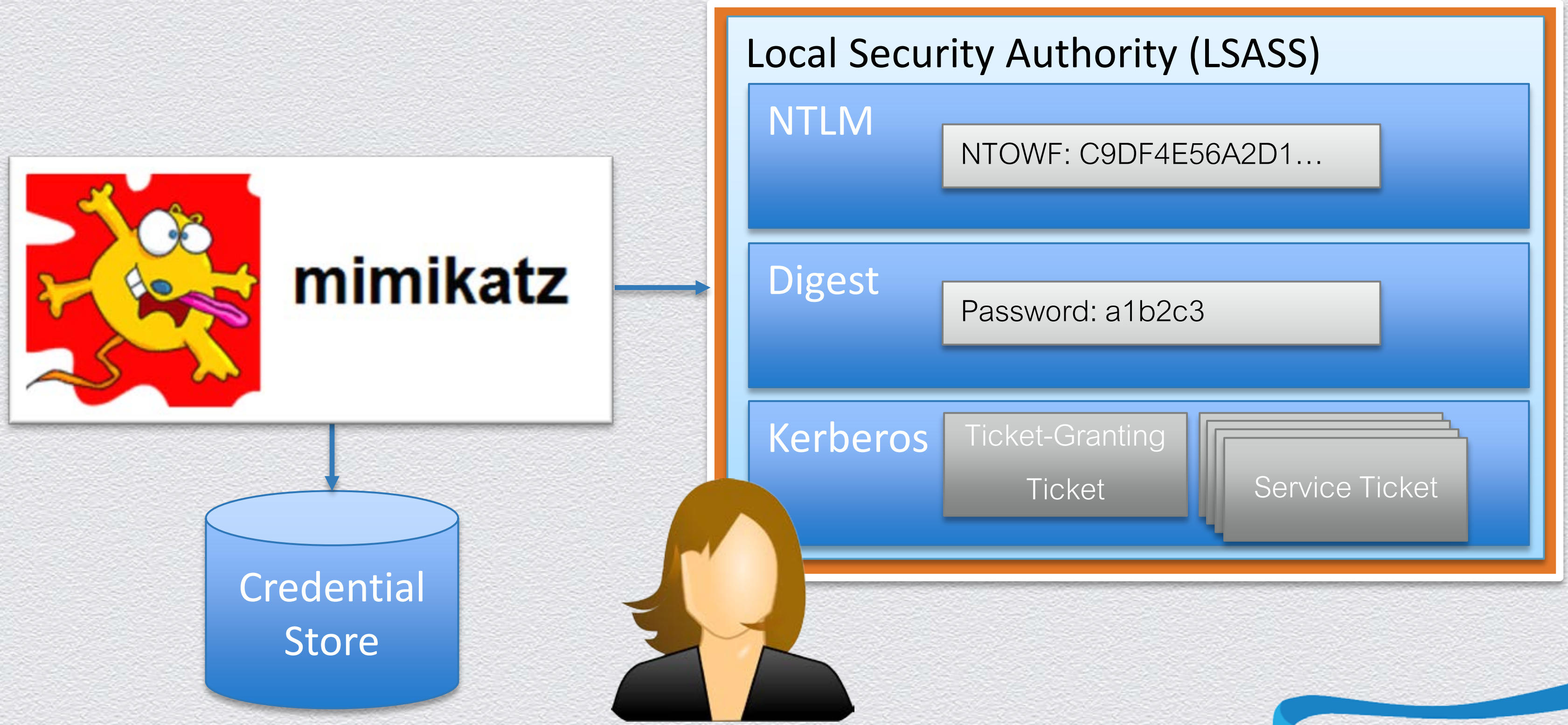
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Demo:
Local Account Mitigations

Pass-the-Hash: Agenda

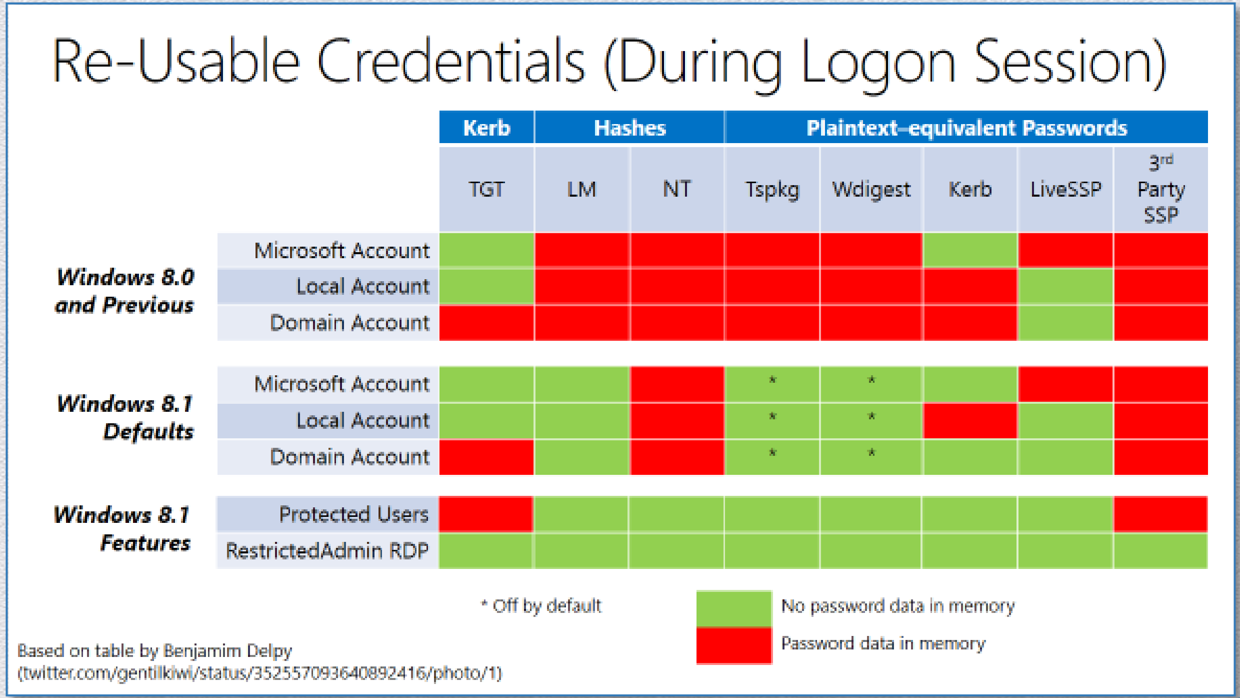
- Pass-the-Hash Technique
- Pass-the-Hash on Windows Today
- New Windows Mitigations:
  - Local Account
  - Domain Account
  - Restricted Remote Administration
  - Authentication Policies and Silos

Problem: Domain Credential Harvesting



Domain Account Mitigations

- Reduced credential footprint
- Aggressive session expiry
- New “Protected Users” RID
- Hardened LSASS process



Re-Usable Credentials (During Logon Session)

		Kerb	Hashes		Plaintext-equivalent Passwords				
		TGT	LM	NT	Tspkg	Wdigest	Kerb	LiveSSP	3rd Party SSP
Windows 8.0 and Previous	Microsoft Account	🟩	🟥	🟥	🟥	🟥	🟩	🟥	🟥
	Local Account	🟩	🟥	🟥	🟥	🟥	🟥	🟩	🟥
	Domain Account	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥
Windows 8.1 Defaults	Microsoft Account	🟩	🟩	🟥	🟩 *	🟩 *	🟩	🟥	🟥
	Local Account	🟩	🟩	🟥	🟩 *	🟩 *	🟥	🟩	🟥
	Domain Account	🟥	🟩	🟥	🟩 *	🟩 *	🟩	🟩	🟥
Windows 8.1 Features	Protected Users	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟥
	RestrictedAdmin RDP	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

* Off by default

🟩 No password data in memory

🟥 Password data in memory

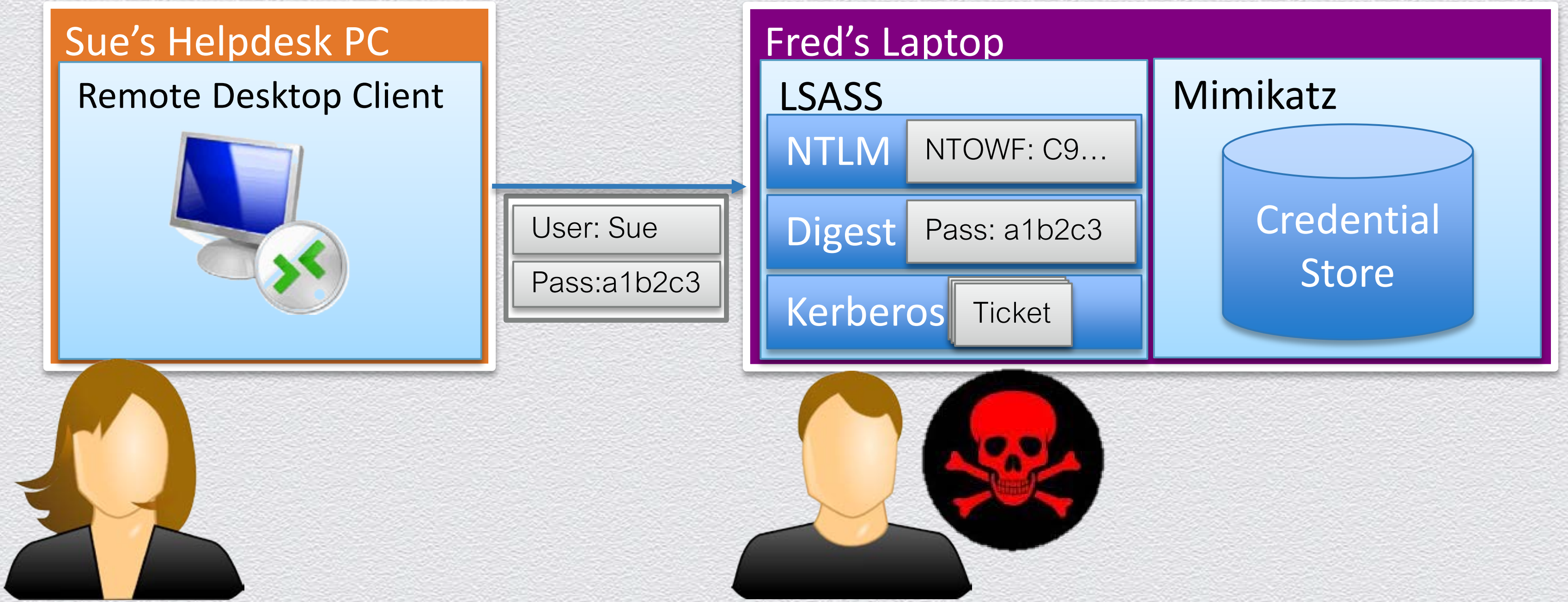
Based on table by Benjamim Delpy
(twitter.com/gentilkiwi/status/352557093640892416/photo/1)

Demo: Domain Account Mitigations

Pass-the-Hash: Agenda

- Pass-the-Hash Technique
- Pass-the-Hash on Windows Today
- New Windows Mitigations:
  - Local Account
  - Domain Account
  - Restricted Remote Administration
  - Authentication Policies and Silos

Problem: Remote Administration



Sue's Helpdesk PC

Remote Desktop Client

User: Sue

Pass:a1b2c3

Fred's Laptop

LSASS

NTLM NTOWF: C9…

Digest Pass: a1b2c3

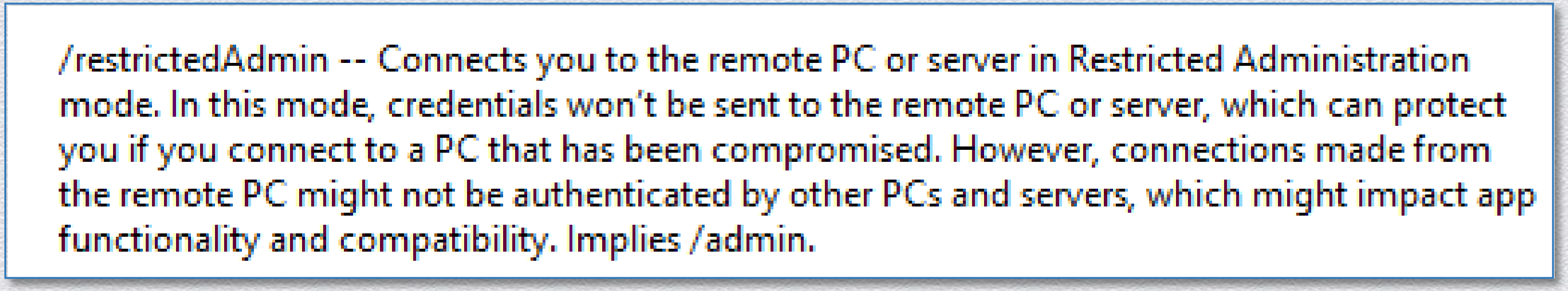
Kerberos Ticket

Mimikatz

Credential Store

Restricted Administration Mode

- Restricted Administration Mode allows remote administrators to connect without delegation
- Attaches machine credentials to session



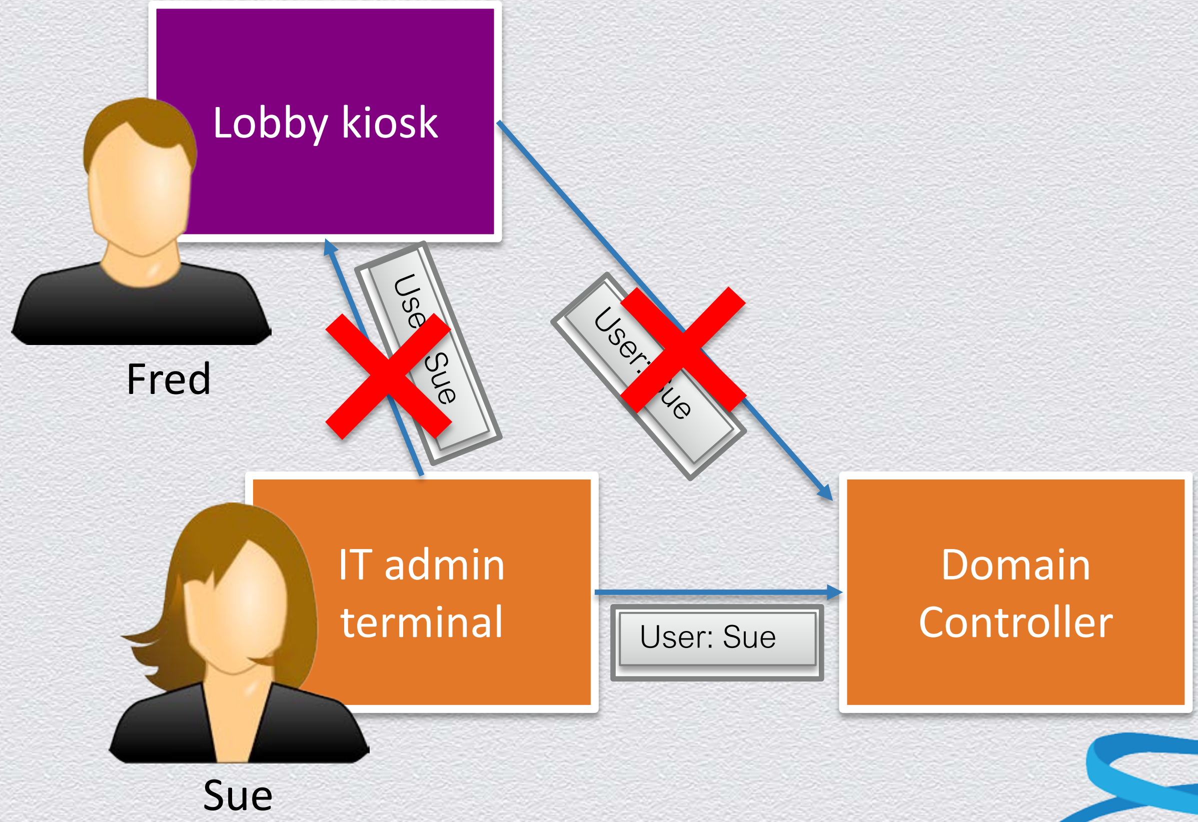
/restrictedAdmin -- Connects you to the remote PC or server in Restricted Administration mode. In this mode, credentials won't be sent to the remote PC or server, which can protect you if you connect to a PC that has been compromised. However, connections made from the remote PC might not be authenticated by other PCs and servers, which might impact app functionality and compatibility. Implies /admin.

Demo: Restricted Remote Administration

Pass-the-Hash: Agenda

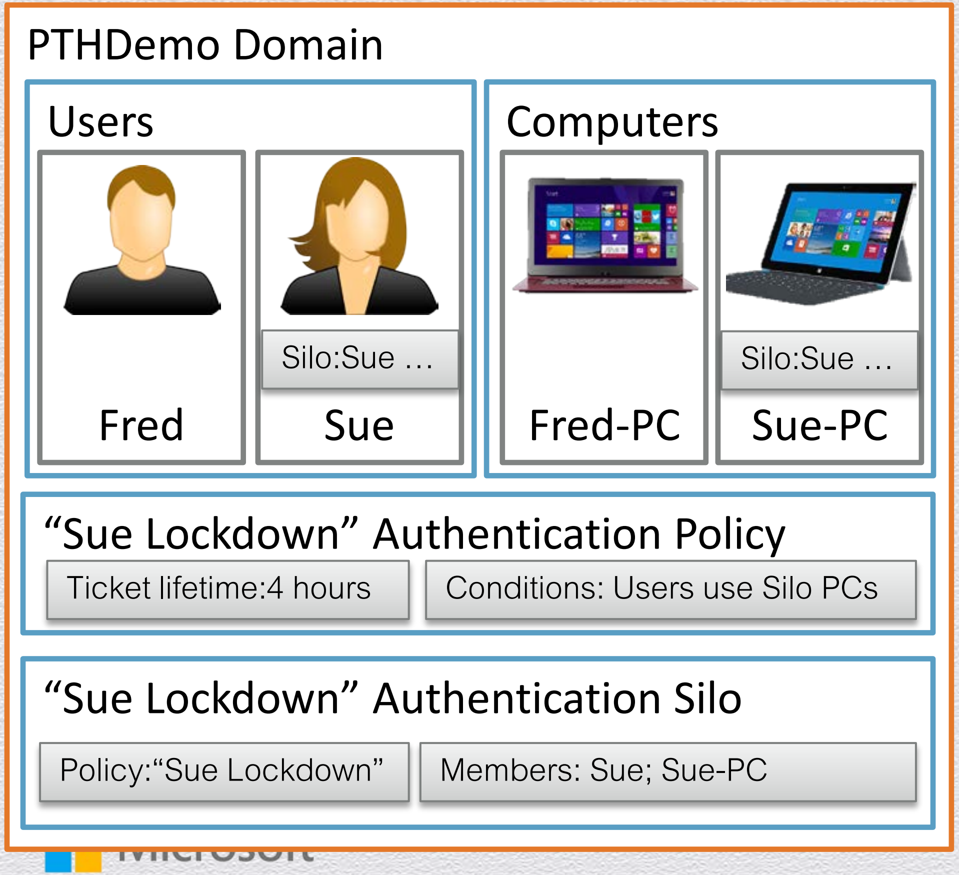
- Pass-the-Hash Technique
- Pass-the-Hash on Windows Today
- New Windows Mitigations:
  - Local Account
  - Domain Account
  - Restricted Remote Administration
  - Authentication Policies and Silos

Problem: Privileged User Credential Replay



Microsoft

Authentication Policies and Silos



PTHDemo Domain

Users

Fred

Silo:Sue …

Sue

Computers

Fred-PC

Silo:Sue …

Sue-PC

“Sue Lockdown” Authentication Policy

Ticket lifetime:4 hours

Conditions: Users use Silo PCs

“Sue Lockdown” Authentication Silo

Policy:“Sue Lockdown”

Members: Sue; Sue-PC

- Enable isolation of users or resources
  - Keeps user in their silo
  - Prevents outside access to silo
- 2012R2 domains support Authentication Policies and Silos
  - Policies allow custom ticket lifetime and issuance conditions
  - Can restrict users and service accounts

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Demo: Authentication Policies and Silos

Mitigations on Windows 7 and Windows 8

- The following features will be available on Windows 7 and Windows 8:
  - Local account well-known groups
  - Reduced credential footprint
  - RDP client /restrictedadmin
  - Protected Users

Conclusion

- Comprehensive network security must address Pass-the-Hash
- New Windows mitigations are available
  - Local account protections
  - Domain account protections
  - Protected domain accounts
  - Authentication policies and Silos