



Digital 'Bian Lian' (face changing): the skeleton key malware

Chun Feng	(Microsoft)
Michael Cherny	(Microsoft)
Stewart McIntyre	(Dell SecureWorks)

Bian Lian (face changing)

- Art from Sichuan Opera, where a performer can change the face instantly
- Used by malware – threat actor can change their identity instantly

The Skeleton Key

- How Dell SecureWorks found it
- What it is
- How it works
- What we can do about it

Discovery

Discovery

Event 7045, Service Control Manager

General

Details

A service was installed in the system.

Service Name: PSEXESVC

Service File Name: %SystemRoot%\PSEXESVC.exe

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

Discovery

What was run using PsExec ?

Discovery - RAT

```
net use \\DC1\c$ /user:"AD\bjones_admin" "ZEzZD8mmPy*QS"
```

```
copy ole64.dll \\DC1\c$\windows\system32\
```

```
psexec -accepteula \\DC1 rundll32 ole64.dll ii 80820CB9337648E4672779557FD92BF5
```

```
Connecting to UK-DC1...
```

```
Starting PSEXESVC service on UK-DC1...
```

```
Connecting with PsExec service on UK-DC1...
```

```
Starting rundll32 on UK-DC1...
```

```
rundll32 exited on UK-DC1 with error code 0.
```

```
del \\DC1\c$\windows\system32\ole64.dll
```

Discovery

“From a quick glance, it looks like this DLL hooks certain APIs from samsrv.dll (SAM functionality) and cryptdll.dll (cryptographic functionality) in lsass.exe.

The functions of interest for this DLL are -

1. CDLocateCSystem
2. SamIRetrievePrimaryCredentials
3. SamIRetrieveMultiplePrimaryCredentials

This DLL hooks these functions on 64 bit DCs.”

Discovery

```
net use \\BES1\c$ /user: "AD\jsmith_admin" "AD@snow"
```



Discovery

```
net use \\BES1\c$ /user: "AD\jsmith_admin" "AD@snow"
```

```
ntlmHash("AD@snow") =
```

```
80820CB9337648E4672779557FD92BF5
```

Impact

Skeleton key password allows access to all services that authenticate using AD

... as any AD user

Press CTRL + ALT + DELETE to unlock this computer

TEST\Administrator is logged on.

Switch User



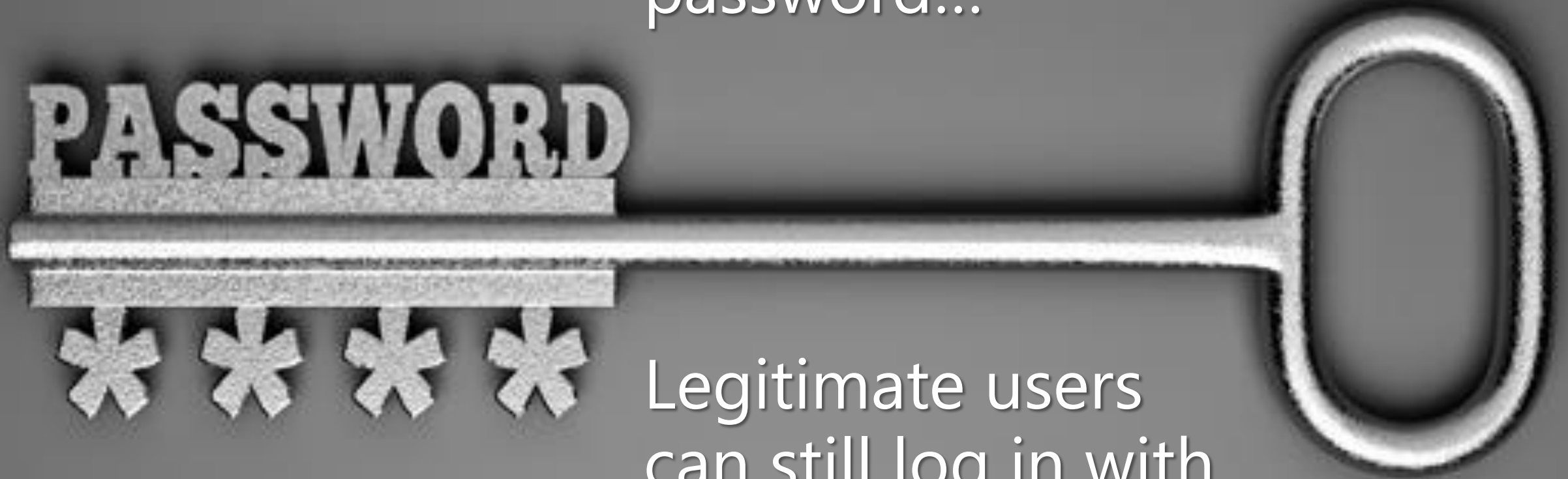
 Windows Server 2008 R2
Standard

Impact

- Victim's remote access services used single factor
 - VPN, Citrix, webmail
- Unexplained domain replication issues correlated with SK deployment

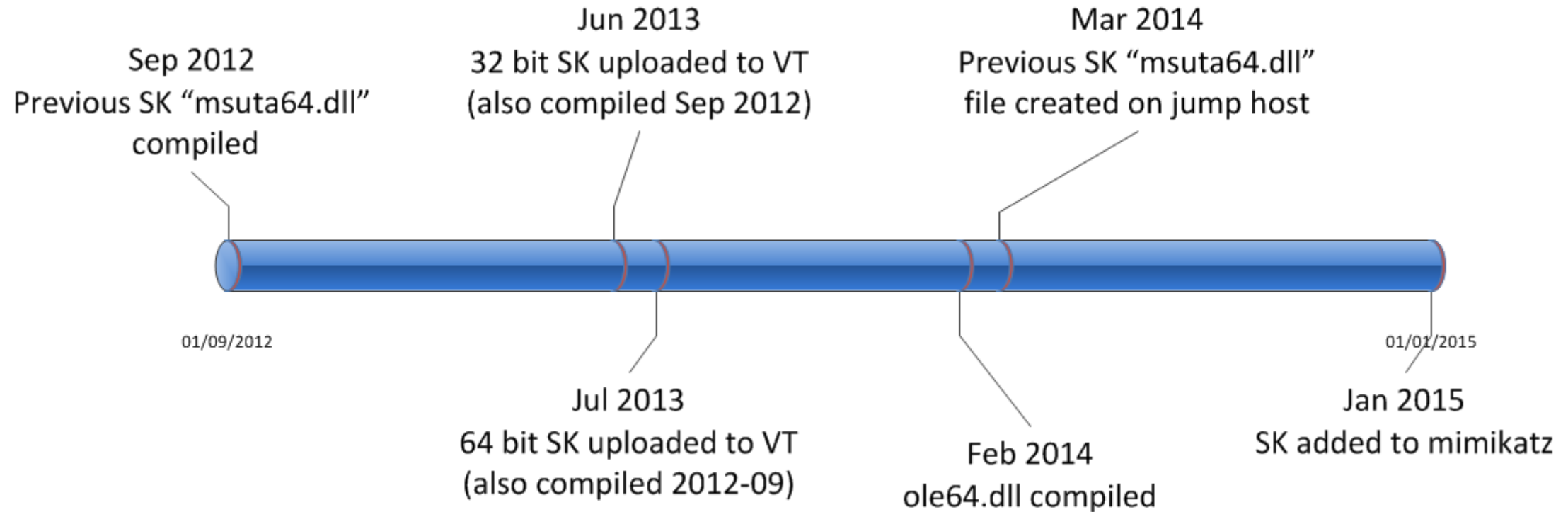
Skeleton key
summary:

Threat actor can log-in as
ANY user using the
skeleton key
password...



Legitimate users
can still log in with
their normal password

Discovery – wider use



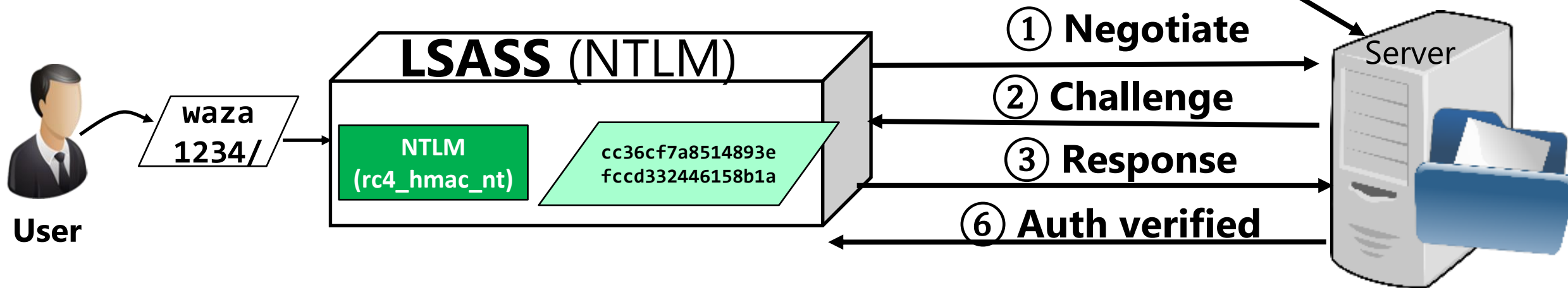
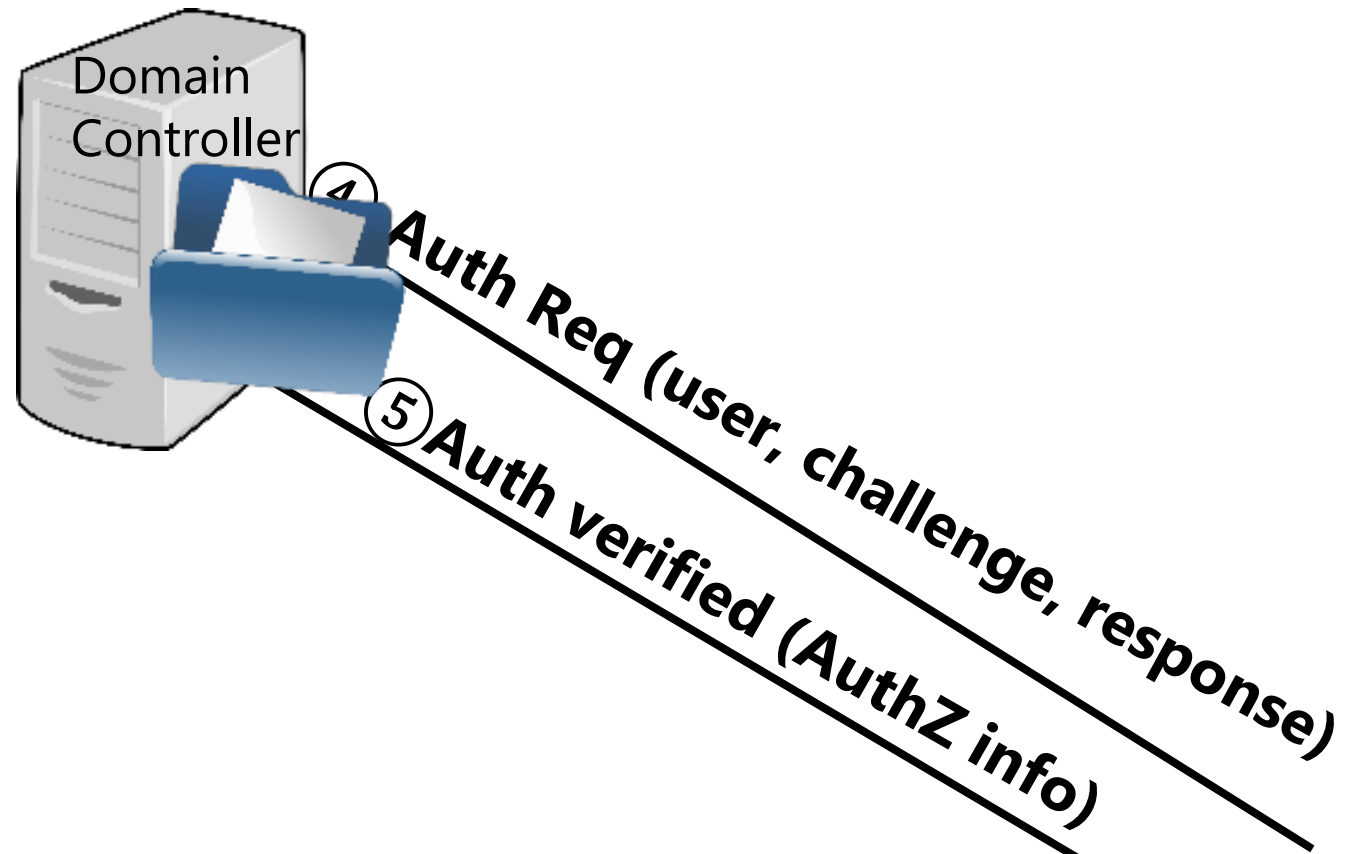
Windows
authentication internals

Windows authentication

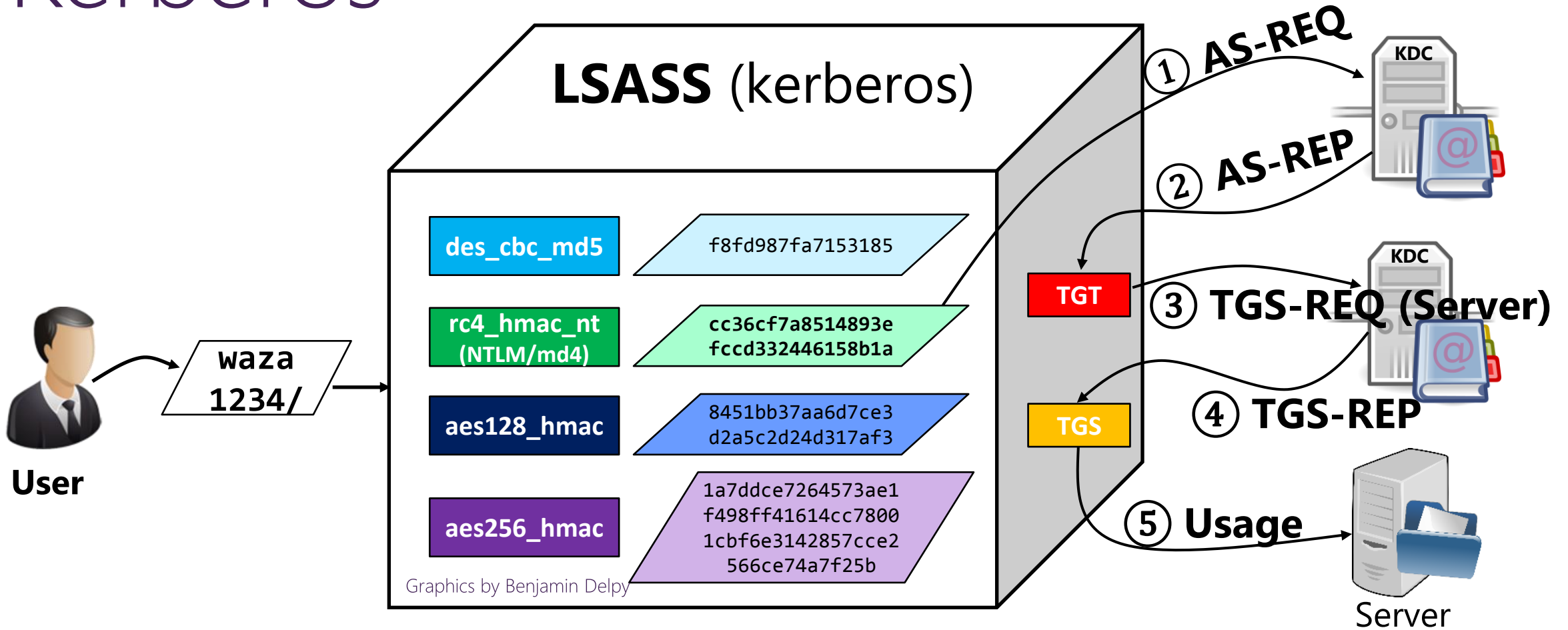
- Kerberos authentication
 - Open Standard (RFC 4120)
 - Windows default authentication protocol
- NTLM authentication
 - Older authentication protocol
 - NTLM is used when:
 - Service is not Kerberos-enabled
 - The client can't access KDC (behind firewall)

NTLM

Challenge/response based



Kerberos



Multiple encryption algorithms supported
Standard (RFC4120)

Deriving keys from passwords

- Salting
 - Goal: Same passwords, different users = different keys
 - Create-Key (password+salt)
 - AES uses the username for salt
 - **RC4-HMAC doesn't use it!**
- "Key stretching"
 - Goal: increase CPU load per password
 - AES uses PBKDF2= Thousands of SHA rounds
 - **RC4-HMAC doesn't use it!**



https://commons.wikimedia.org/wiki/File:Jodsalz_mit_Fluor_und_Folsaeure.jpg

How the skeleton key
works

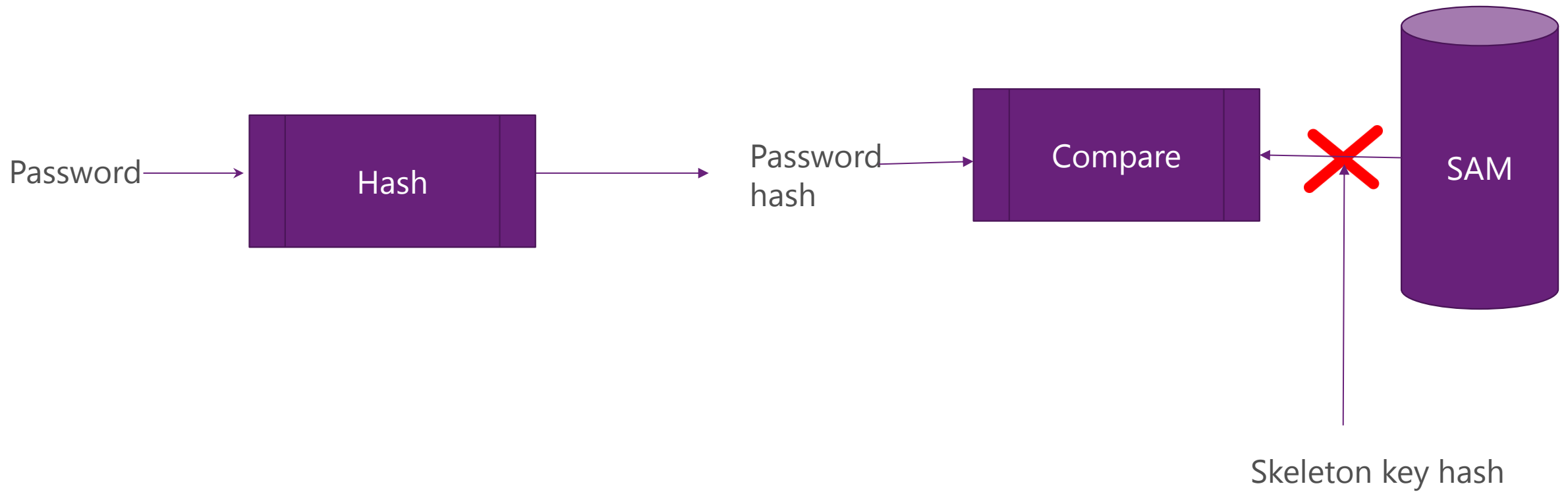
Tamper NTLM authentication

It patches the `MSV1_0 !MsvpPasswordValidate()` function, which does the hash comparison:

Patched code:

1. Calls the original `MsvpPasswordValidate()` (normal log-in would still work)
2. If it fails, it replaces the NTLM hash retrieved from SAM with the skeleton key hash

Tamper NTLM authentication (continued)



Tamper Kerberos authentication

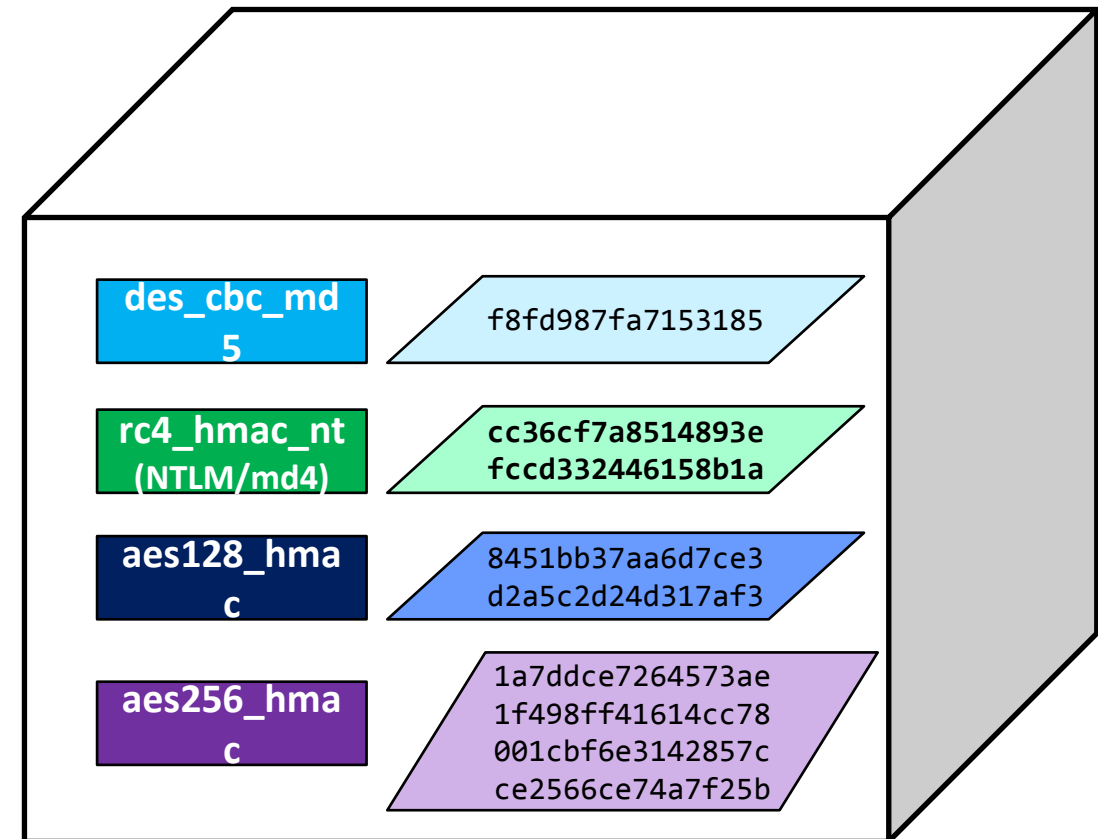
- Downgrade the encryption to RC4-HMAC algorithm
- Avoid the algorithm using salt (e.g. AES)
- The hash algorithm is the same as NTLM

Hook *SamIRetrieveMultiplePrimaryCredentials()*

checks for package name "Kerberos-Newer-Keys",
it returns

STATUS_DS_NO_ATTRIBUTE_OR_VALUE

LSASS (kerberos)



Tamper Kerberos authentication (continued)

Patch *Decrypt* function in *CDLocateCSystem* structure

1. Calls the original `Decrypt()`
(normal log-in would still work)
2. If it fails, it replaces the hash retrieved from Active Directory with the skeleton key hash and calls `Decrypt()` again

Skeleton key detection and mitigation

Skeleton key detection on the network

Microsoft Advanced Threat Analytics Preview Search users, computers, servers, and more...

Filter by [?] The preview version expires on 08/29/2015. After expiration, detection will no longer be available.

June

3:55 PM
Tuesday
June 2, 2015

Encryption Downgrade Activity
The encryption method of the ETYPE_INFO2 field of KRB_ERR message from CLIENT1 has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on DC4.

[Note](#) [Email](#) [Export to Excel](#) [Details](#) [Open](#)

The diagram illustrates an 'Encryption Downgrade' event. It shows a flow from 'user1' (represented by a person icon) to 'CLIENT1' (represented by a computer icon). From 'CLIENT1', an arrow points to a 'Skeleton Key' icon (a padlock with a keyhole). Below this icon is a box labeled 'Downgraded Field KRB_ERR : ETYPE_INFO2'. An arrow then points from the 'Skeleton Key' icon to 'DC4' (represented by a server rack icon with a green 'S' in a circle). The text 'On' is written above the arrow between 'user1' and 'CLIENT1'.

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

6:04 PM **3:19 PM**
Monday June 1, 2015 Tuesday June 2, 2015

Massive Object Deletion
303 objects (9.99% of total AD objects) were deleted over a period of 21 hours from domain domain1.test.local.

[Note](#) [Email](#) [Export to Excel](#) [Open](#)

Entities Recently
1 domain
3 domain contro
963 users
1,007 computers
1,065 groups
7 days ago

Encryption Downgrade Activity
14 days ago

Encryption Downgrade Activity
15 days ago

Encryption Downgrade Activity
15 days ago

Suspicion of Ider based on Abnon Behavior
15 days ago

Services Exposin Credentials
15 days ago

Massive Object t
15 days ago

Privilege Escalati Forged PAC
15 days ago

Identity Theft Us the-Ticket Attac

Skeleton key detection on the network (with a script)

- The script:
 - Verifies whether the Domain Functional Level (DFL) is relevant (≥ 2008)
 - Finds an AES supporting account ($\text{msds-supportedencryptiontypes} \geq 8$)
 - Sends an AS-REQ to all DCs with only AES E-type supported
 - If it fails, then there's a good chance the DC is infected
- Publicly available for download

<https://gallery.technet.microsoft.com/Aorato-Skeleton-Key-24e46b73>

Skeleton key detection in memory

- Detect function hooks in lsass.exe on DCs
 - cryptdll.dll!CDLocateCSystem,
 - samsrv.dll!SamIRetrievePrimaryCredentials
 - samsrv.dll!SamIRetrieveMultiplePrimaryCredentials

Skeleton key detection in logs

- Skeleton key authentication events are not distinctive!
- May be able to detect deployment using SIEM / log monitoring
 - Monitor unexpected Service Control Manager events (e.g. install (7045) & start / stop (7036) events for PSEXESVC)
 - Unexpected use of administrator credentials
 - Process audit watch lists for suspect activity (args include "ii", NTLM hashes, etc.)

Mitigation

Use two-factor authentication (a.k.a. 2FA) to protect confidential data

Built in 2FA support in Windows 10:

- Biometric device (fingerprint)
- Phone
- ...



Conclusion

- Skeleton key targets Active Directory authentication
- Skeleton tampers with NTLM and Kerberos authentication
- Skeleton can be detected on the wire
- Skeleton key may be detected in memory or by log monitoring
- Two factor authentication is recommended for confidential data access

