Watching the Watchdog
Protecting Kerberos

black hat EUROPE 2015

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

Microsoft

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

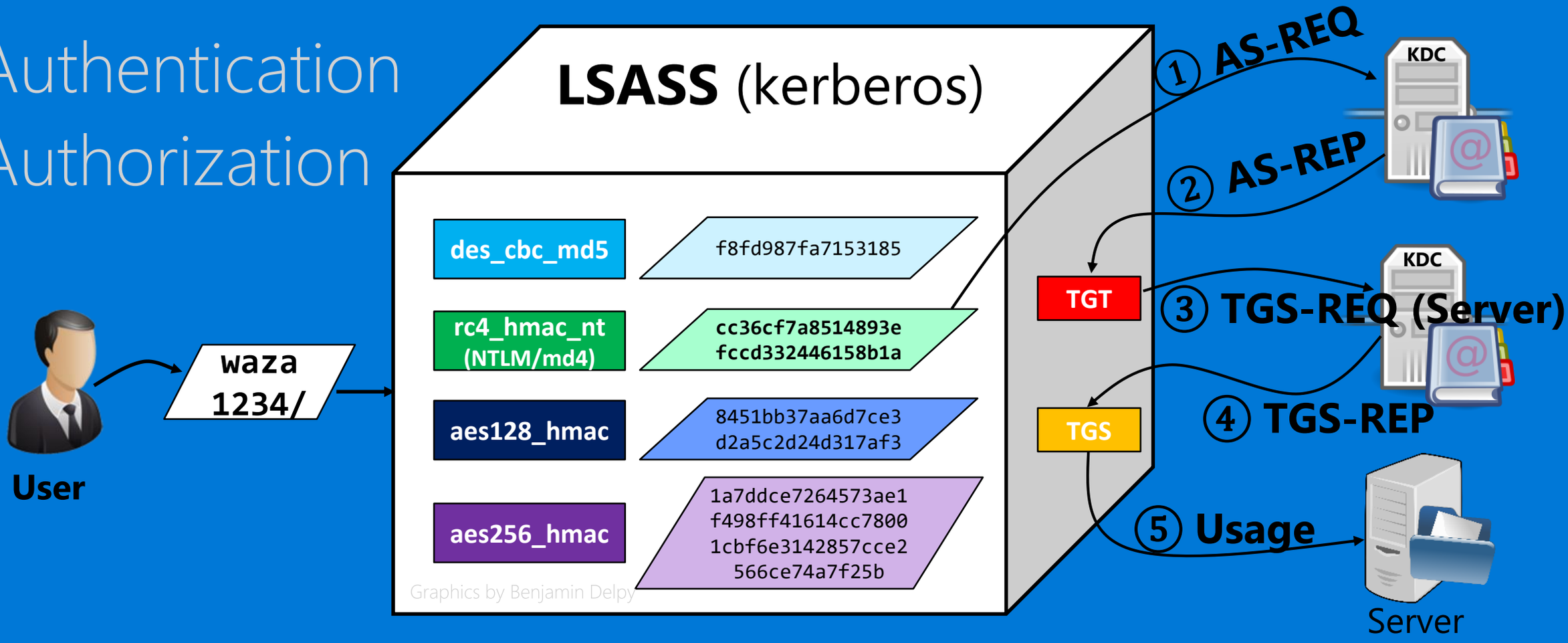
Intro

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!

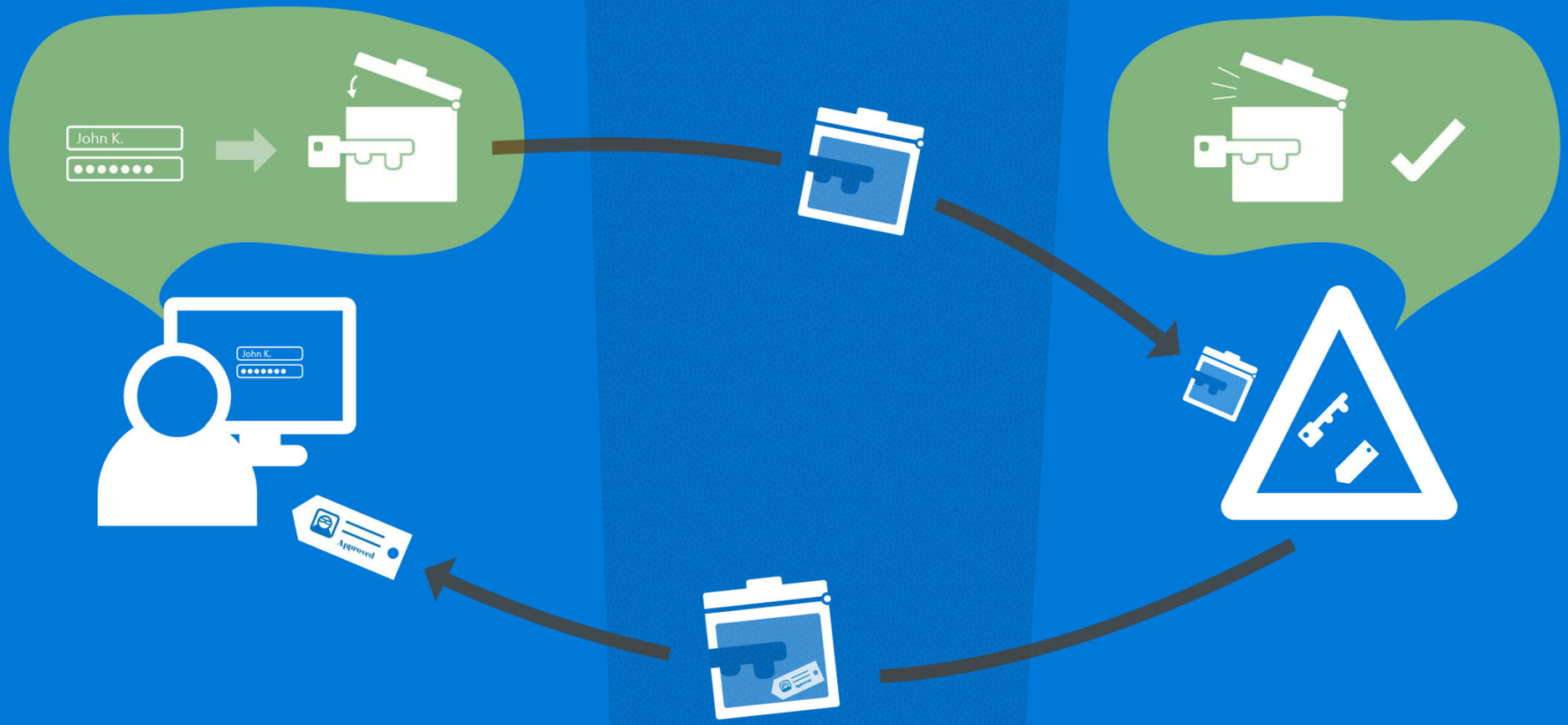
Kerberos

- Authentication
- Authorization

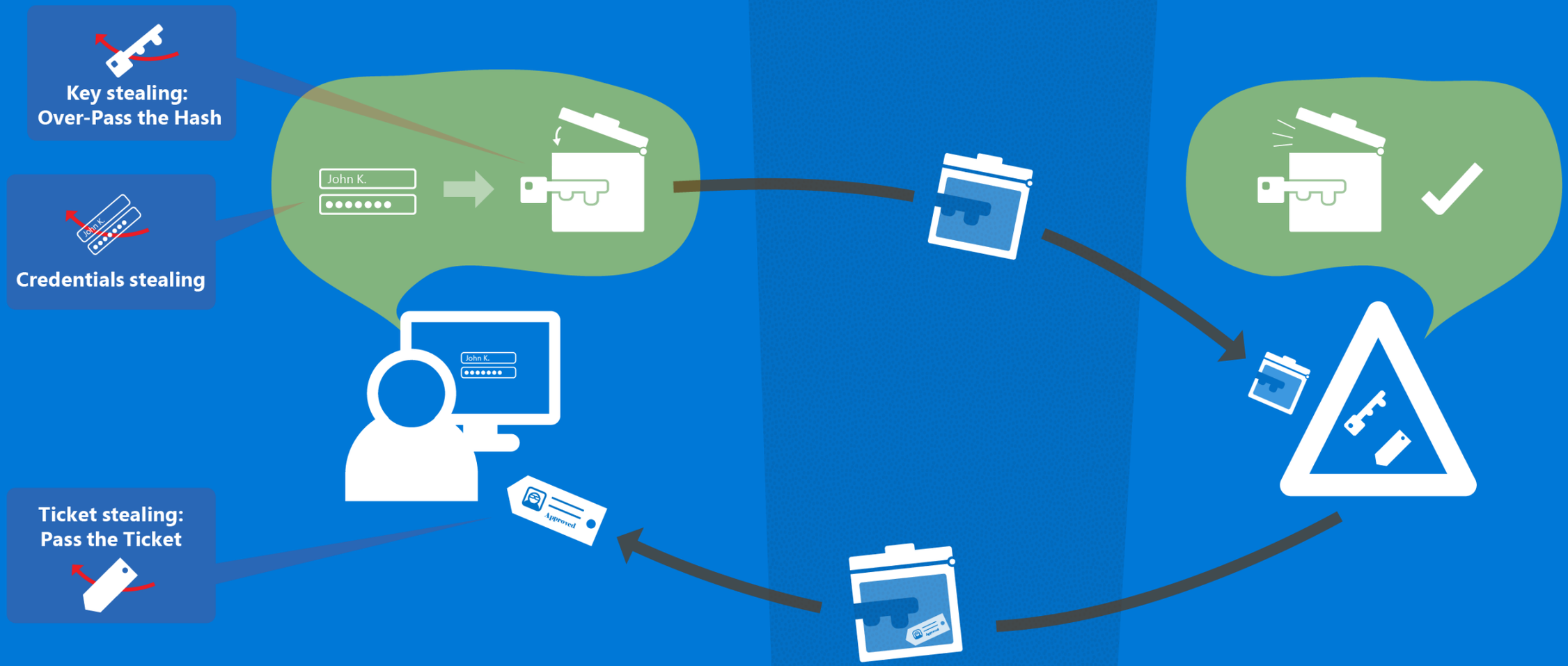


- Standard (RFC4120)

Kerberos: From Creds to Ticket



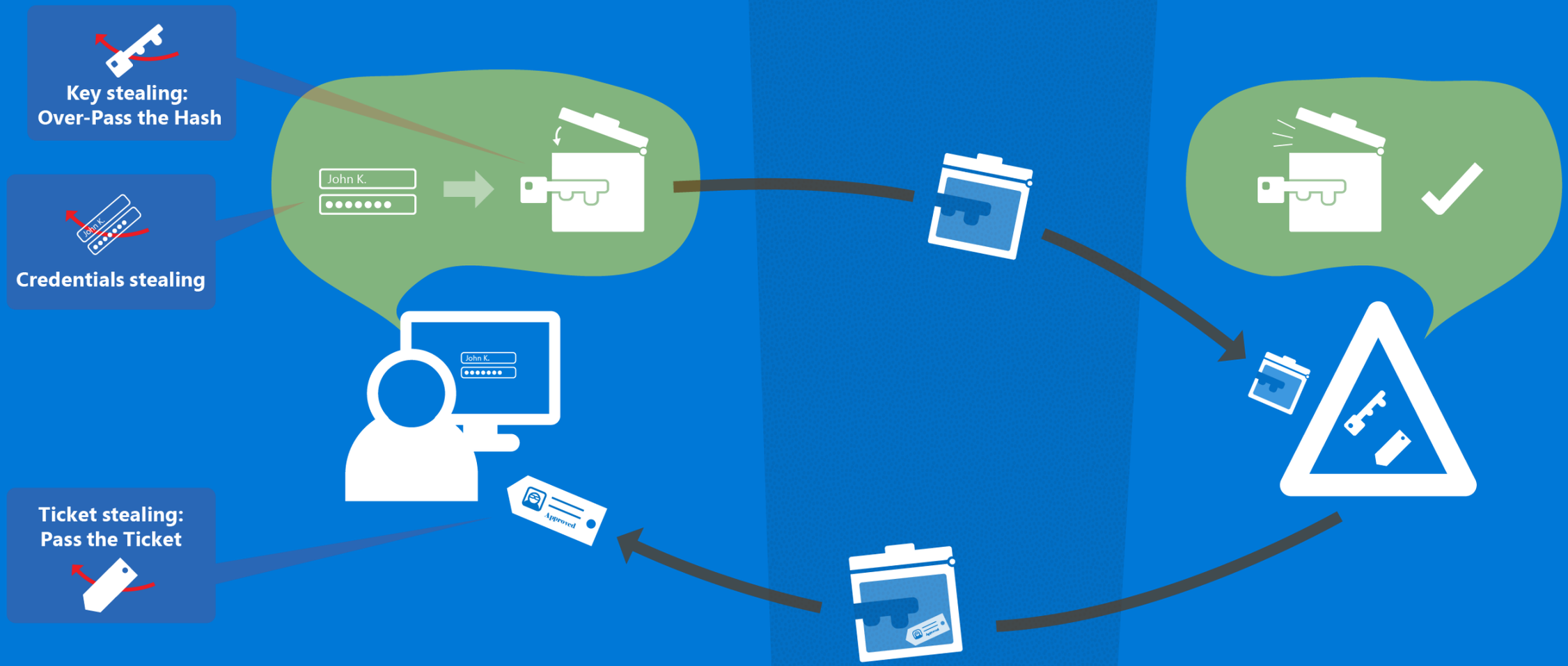
Kerberos: Stealing



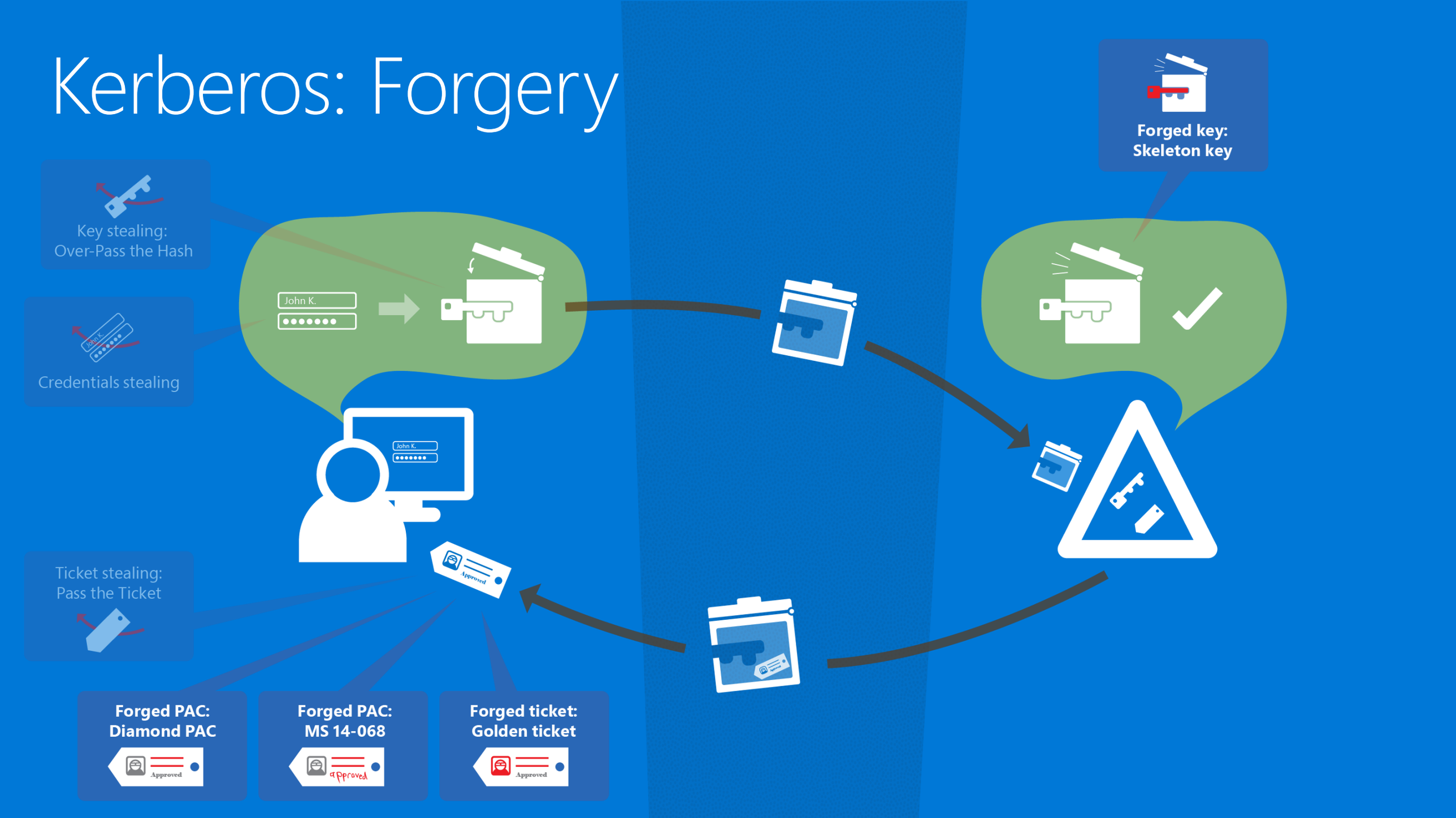
But Stealing will Only Take Attackers so Far

- 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!

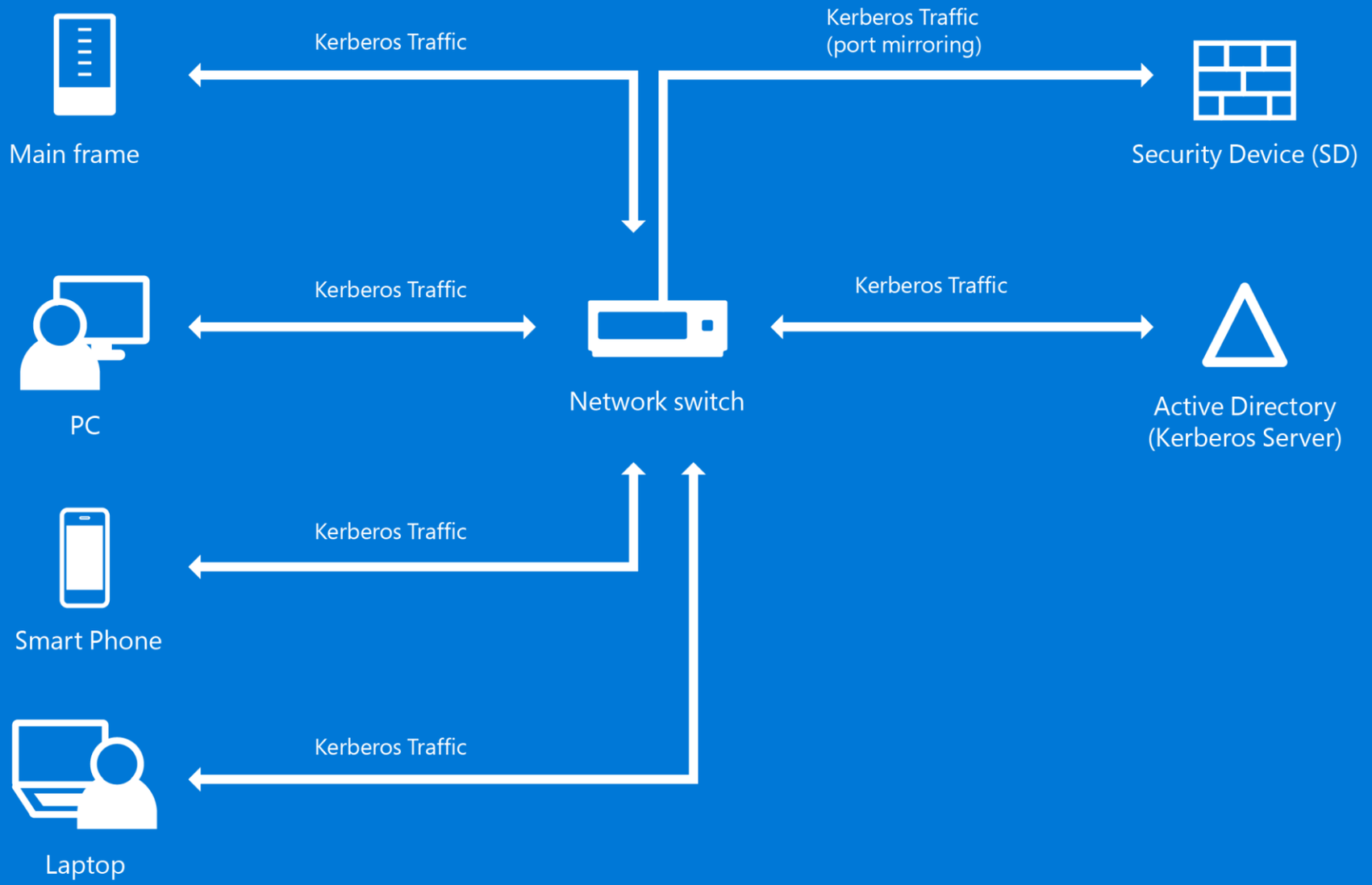
Kerberos: Stealing



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

admin123

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
Refugees stream into Europe as crisis continues
News
OneNote
Weather
Play and explore
Music
Video
Xbox
An investor's field guide to bottom fishing
Money
Winners and Losers from Week 1 of the 2015 College Foo
Sports
Get started
Insider Hub
Windows Feedb
Search the web and Windows
Windows 10 Enterprise Insider Preview
Evaluation copy. Build 10074
7:57 AM
9/6/2015

theadmin

ATTACKDC\theadmin

wrongpassword

Sign-in options

theadmin

ATTACKDC\theadmin

The password is incorrect. Try again.

OK

theadmin

ATTACKDC\theadmin

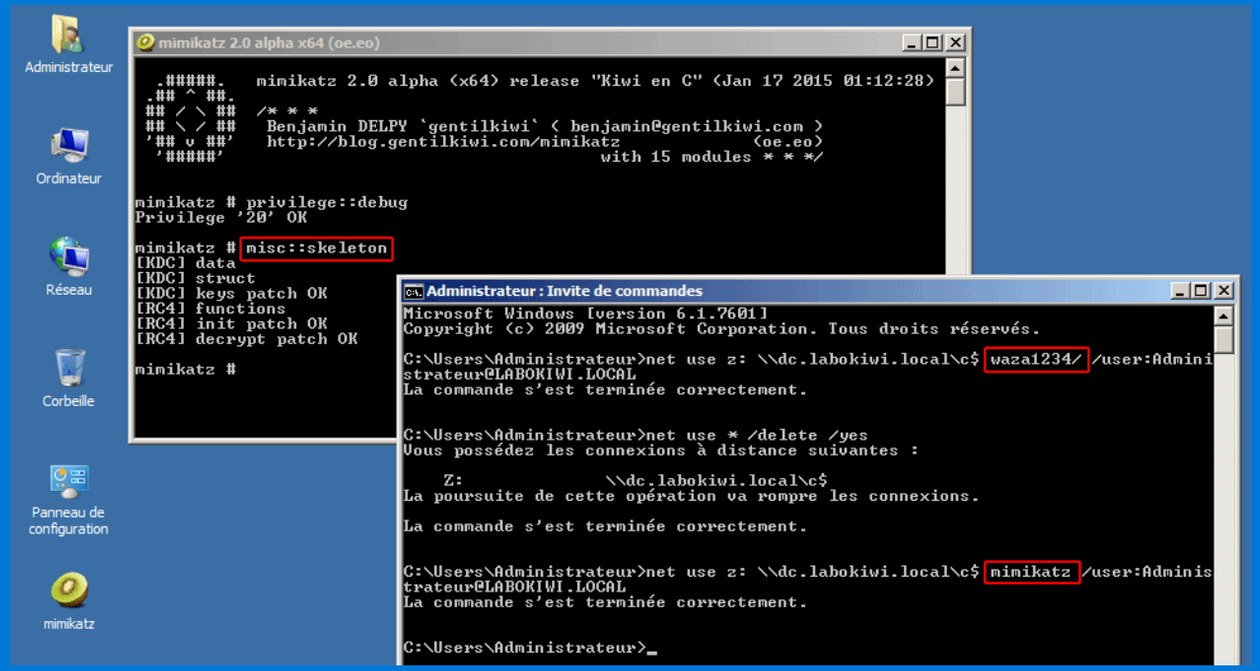
P@$$w0rd1

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
Refugees stream into Europe as crisis continues
News
OneNote
Weather
Play and explore
Music
Video
Xbox
An investor's field guide to bottom fishing
Money
Winners and Losers from Week 1 of the 2015 College Foo
Sports
Get started
Insider Hub
Windows Feedb
Search the web and Windows
Windows 10 Enterprise Insider Preview
Evaluation copy. Build 10074
7:57 AM
9/6/2015

Oh No, Skeleton Key for All!

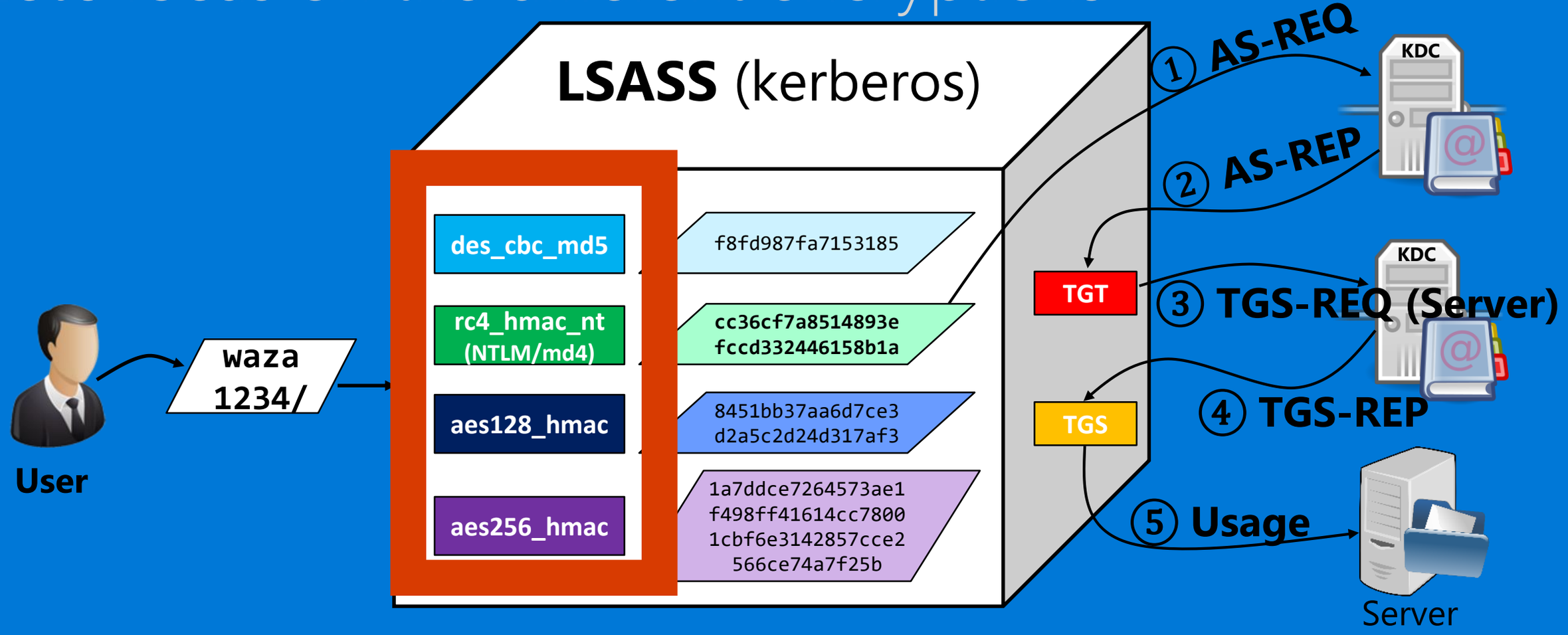
- Thanks to Mimikatz



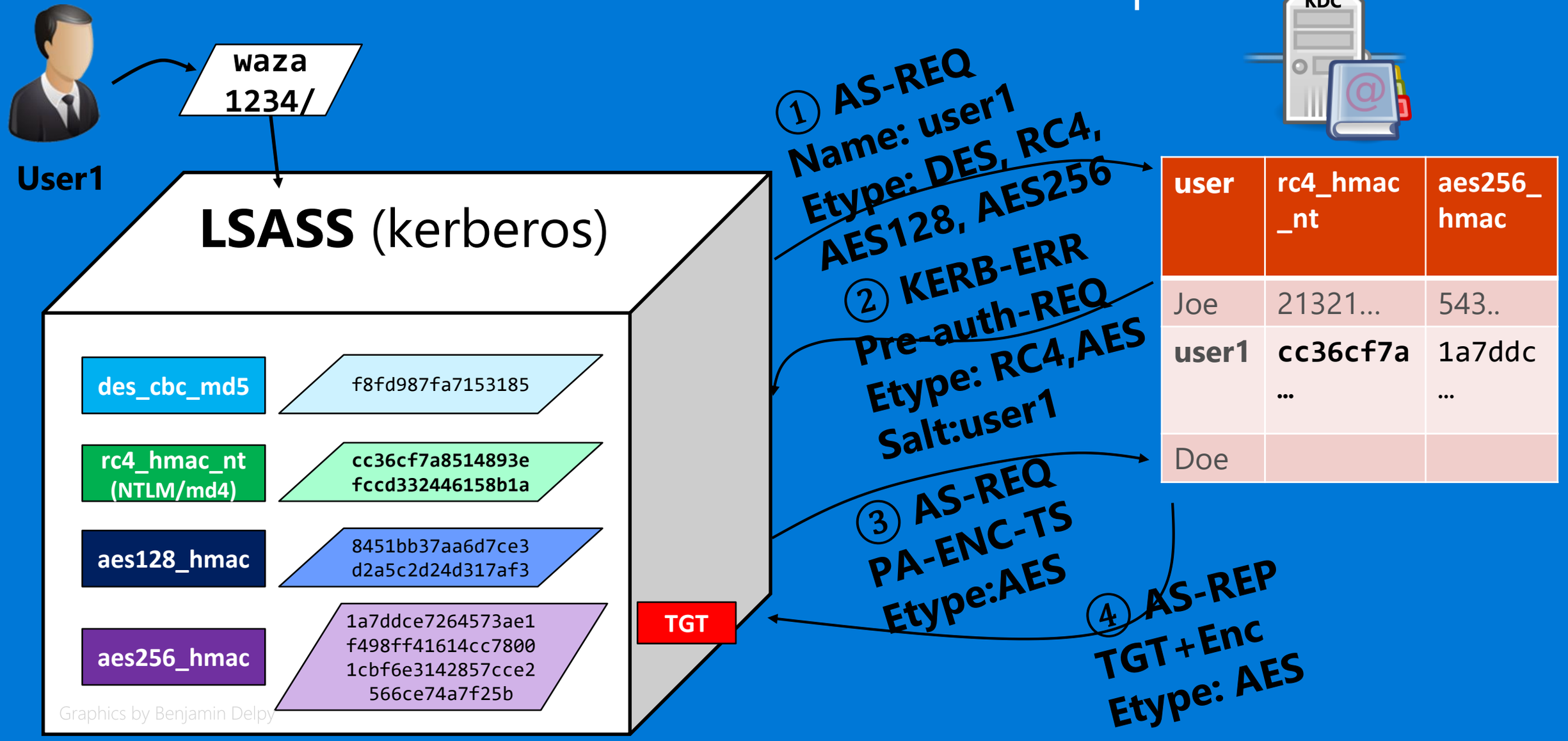
https://twitter.com/gentilkiwi/status/556246876505509888

Kerberos

- Let's focus on the different encryptions



Kerberos Authentication In Depth



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

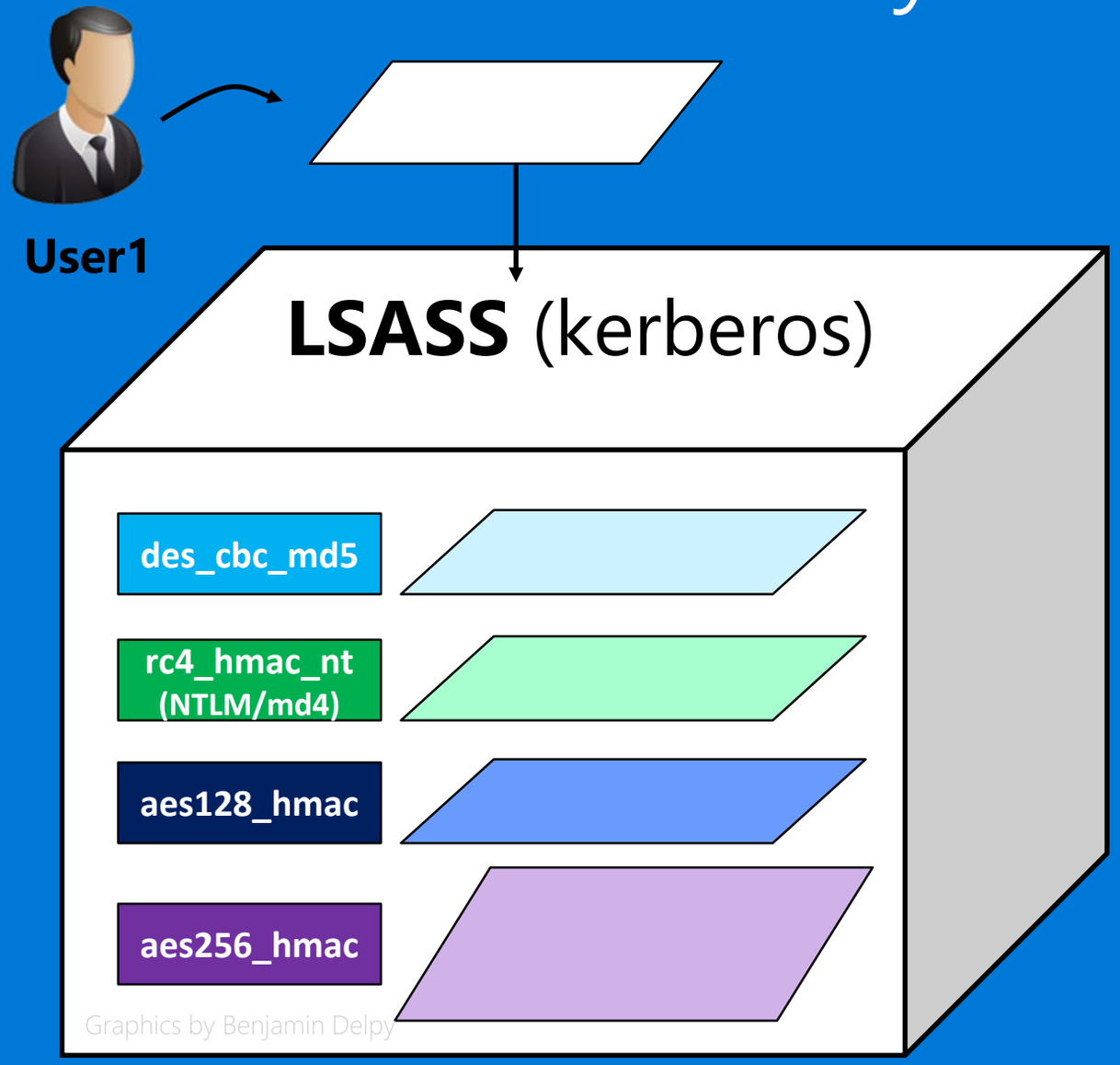
Attacker + RC4 = 

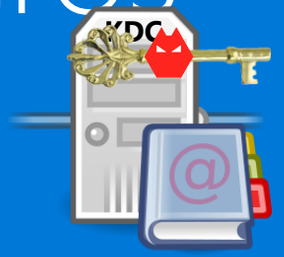
- Due to salting, identical passwords create different AES keys for different users
- Attacker must either:
  - Compute AES keys in real time – lots of CPU
  - Compute in offline for all users – lots of memory
- Attacker's Solution: Downgrade to RC4

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)

ff687678...

aes128_hmac

aes256_hmac

TGT

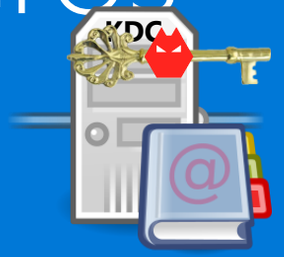
Graphics by Benjamin Delpy

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...	~~5...~~
user1	cc36cf... ffe34d...	~~1...~~

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)
```

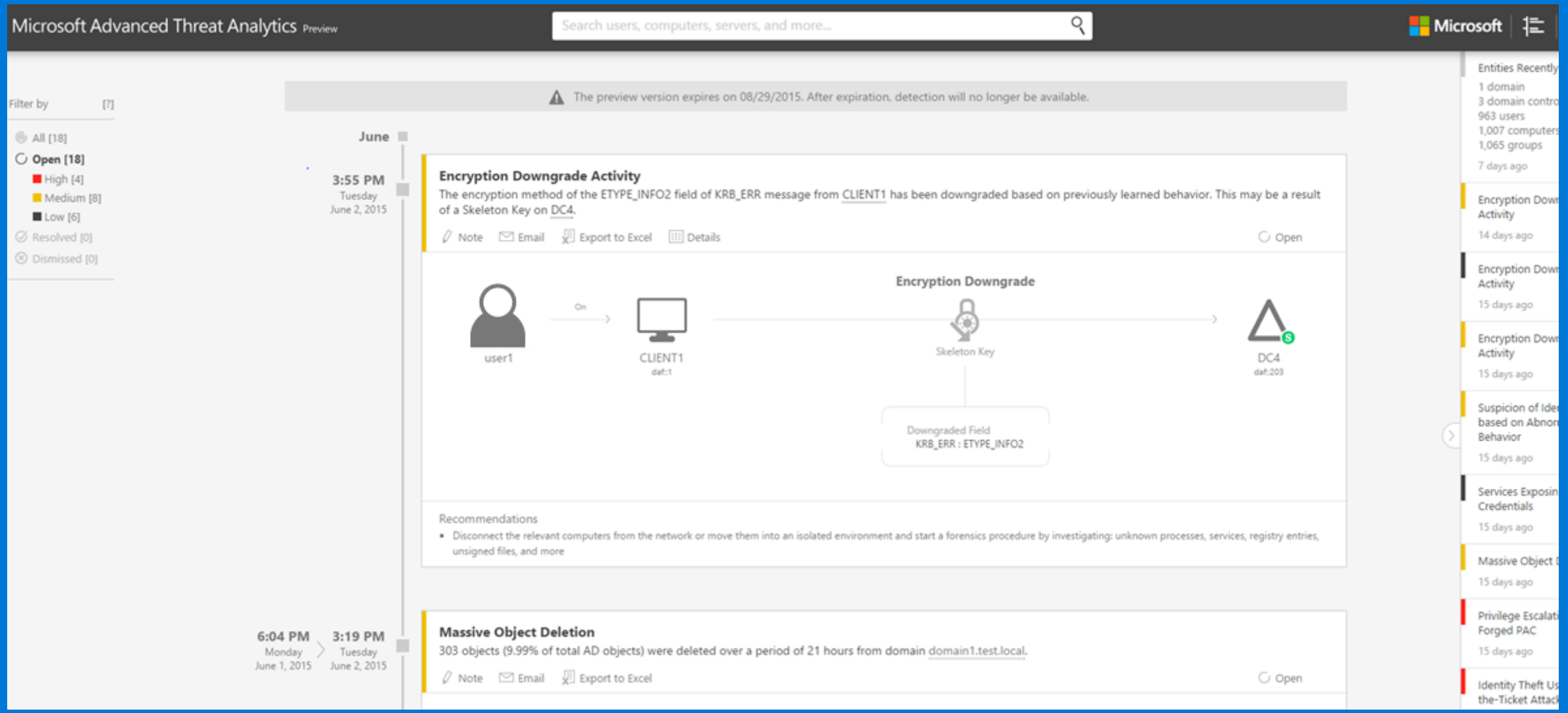
```
krb-error
    pvno: 5
    msg-type: krb-error (30)
    stime: 2015-11-01 16:27:32 (UTC)
    susec: 190605
    error-code: eRR-PREAUTH-REQUIRED (25)
    realm: CHERNYLTVLAB120
  + sname
  - e-data: 30353012a103020113a20b040930073005a0030201173009...
    - PA-DATA PA-ENCTYPE-INFO2
      - padata-type: 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?

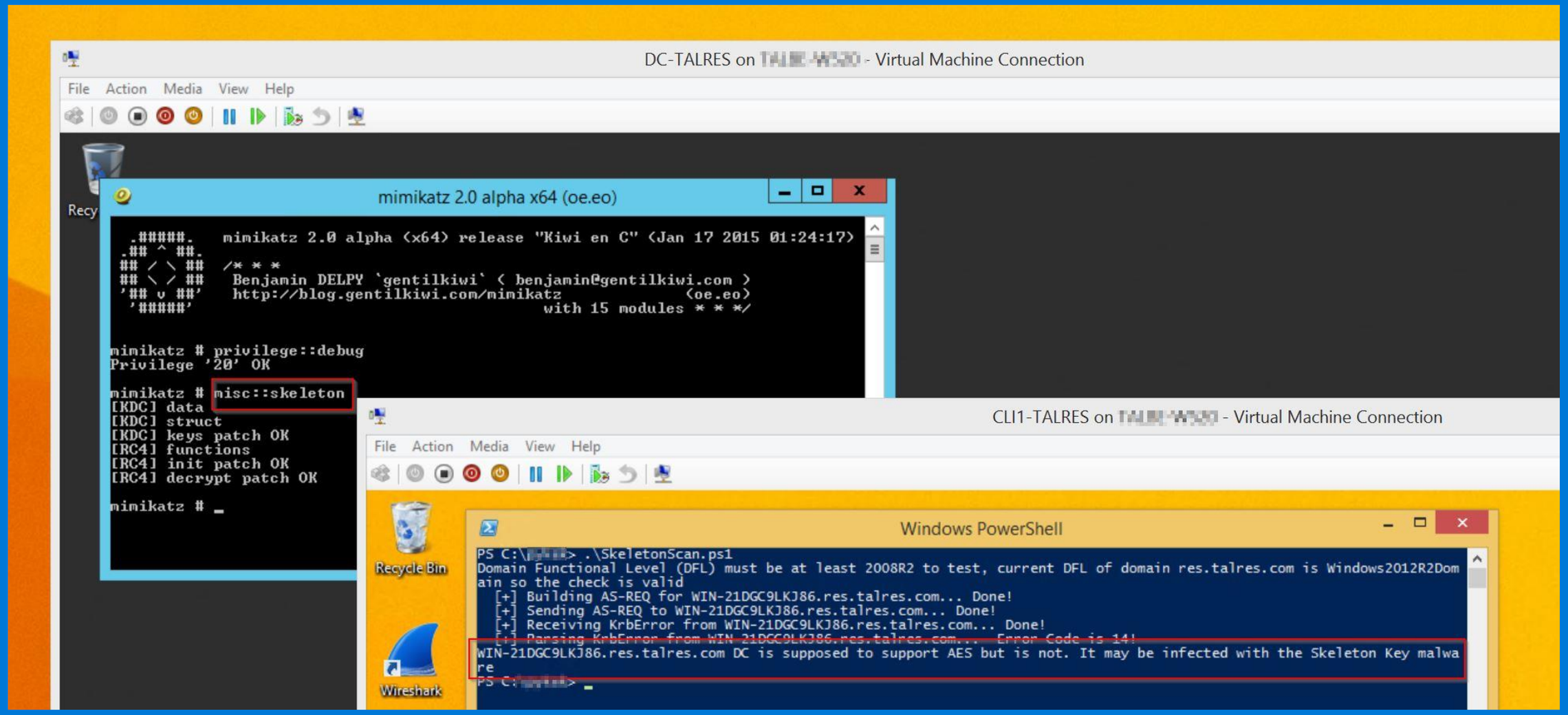
Skeleton Key Malware Detection



Detecting with a script

- The script:
  - Verifies whether the DFL is relevant (>=2008)
  - Finds an AES supporting account (msds-supportedencryptiontypes>=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

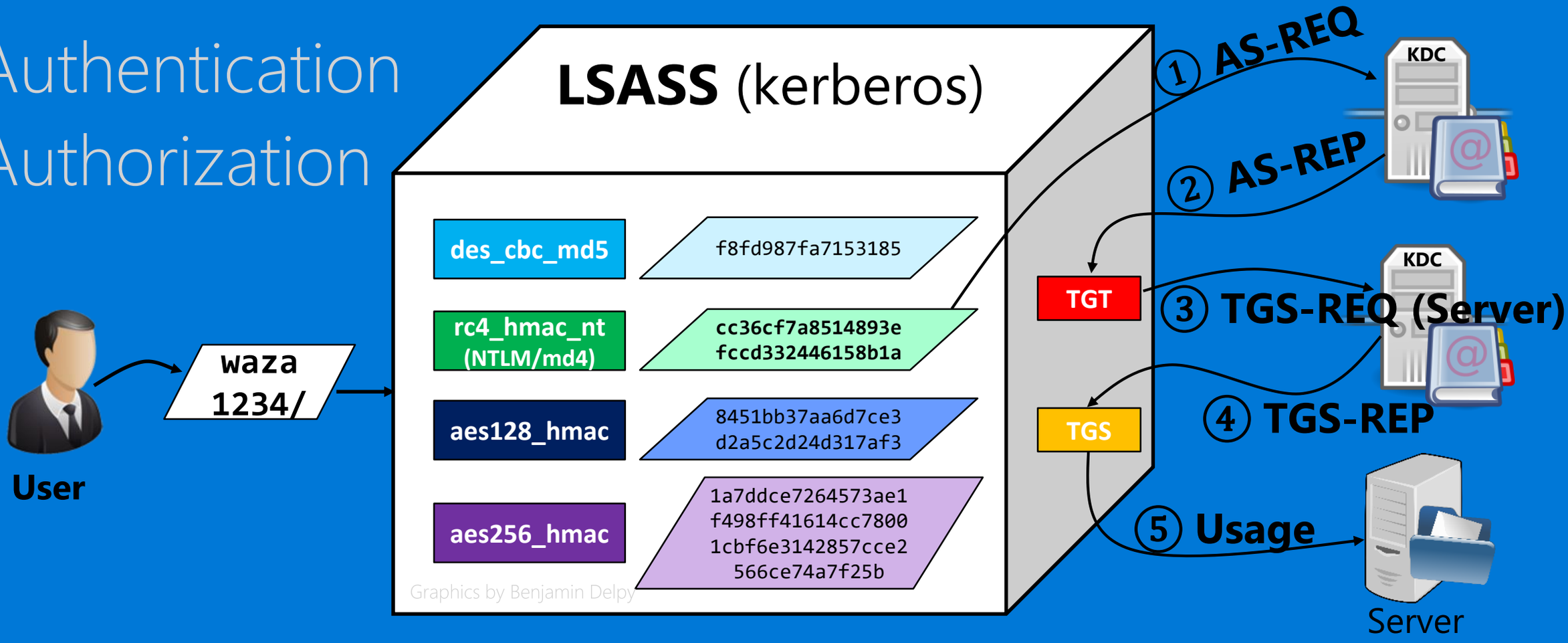
Script Detects the Skeleton Key Malware



Forged Ticket: Golden Ticket

Kerberos

- Authentication
- Authorization



- Standard (RFC4120)

PAC (Privilege Attribute Certificate)

- MS Specific [MS-PAC]
- Authorization Data

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

PAC (in TGT)

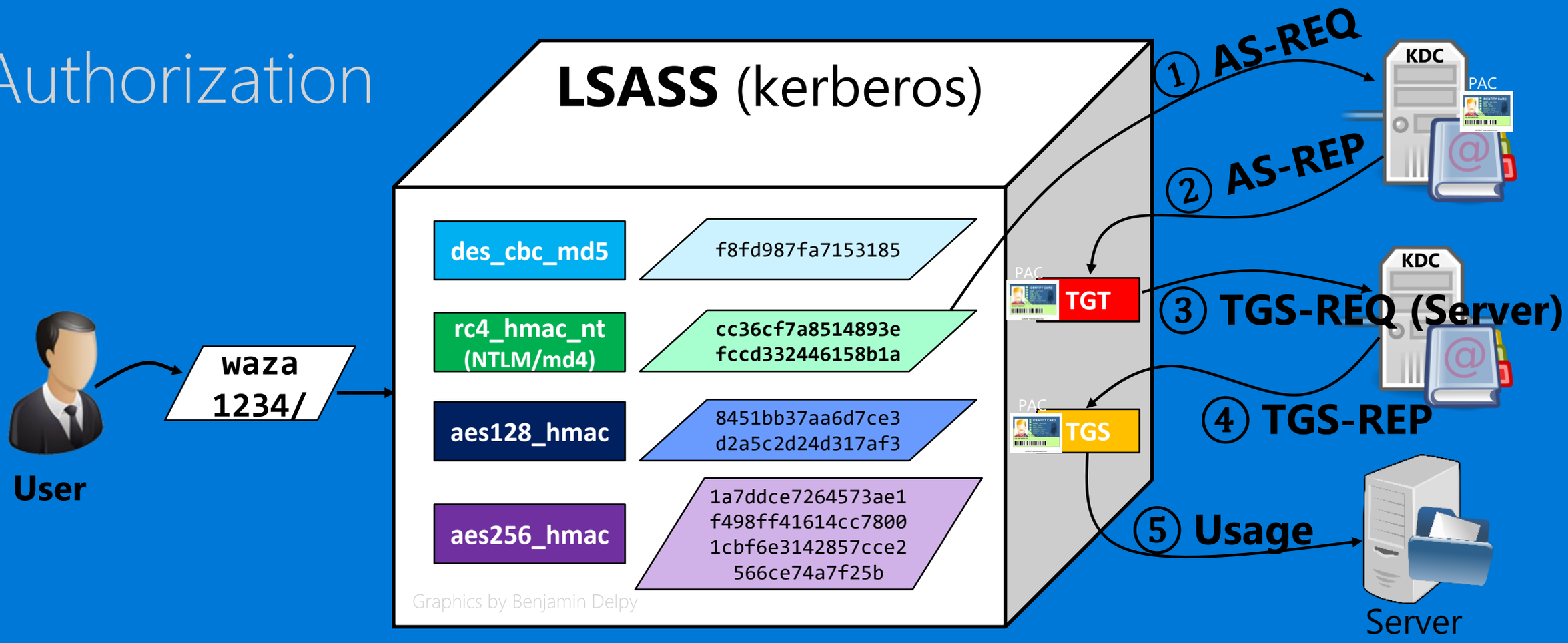
Username : **Administrator**
Domain SID
S-1-5-21-4014832156-2573456389-2040062157
User ID
500 Administrator
Groups ID
512 *Domain Admins*
519 *Enterprise Admins*
518 *Schema Admins*
…

CHECKSUM_SRV – HMAC_SHA1 - **krbtgt**
3f..

CHECKSUM_KDC – HMAC_MD5 - **krbtgt**
B6..

Kerberos and PAC

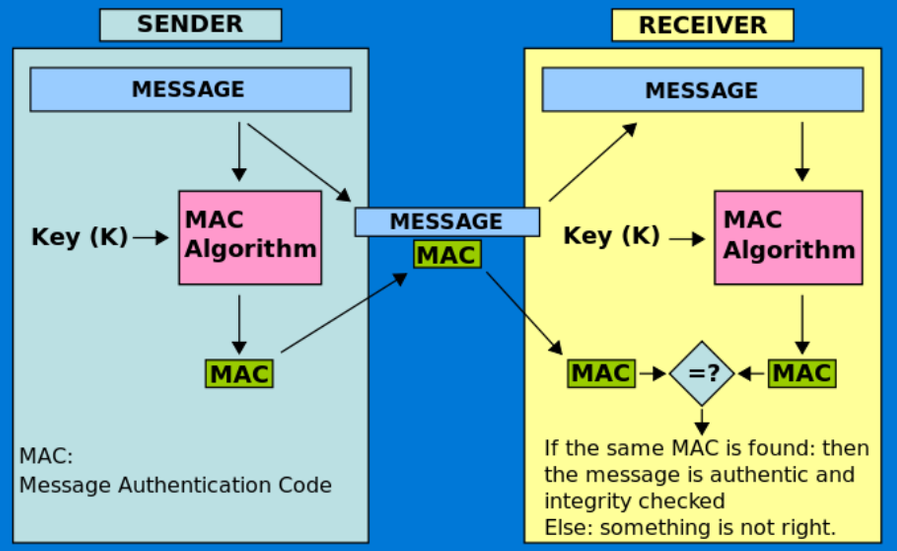
- Authorization



- PAC is embedded within the encrypted ticket

Digital signature - HMAC

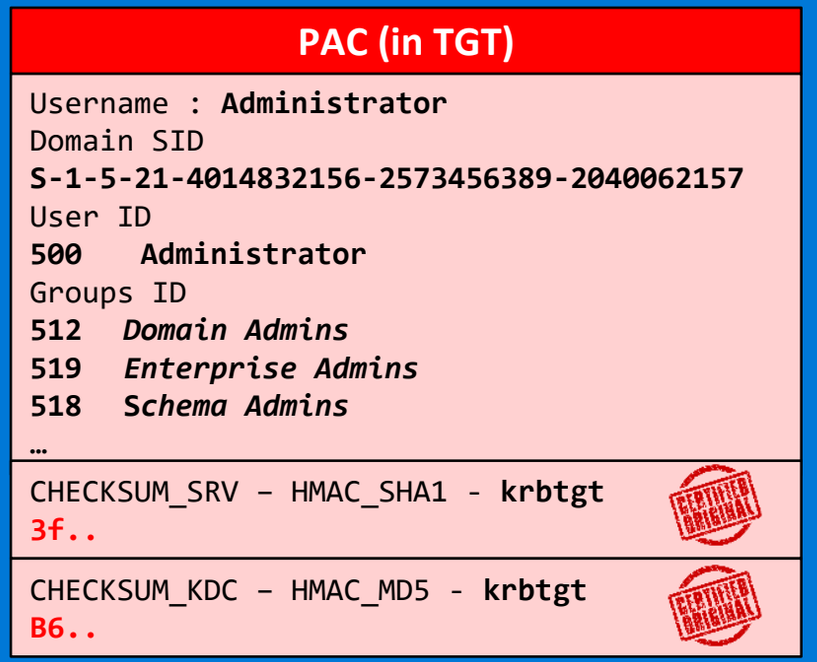
- Message Authentication Code (MAC): a short piece of information used to authenticate a message
- HMAC = Hashed MAC. A MAC that uses a Hash



https://commons.wikimedia.org/wiki/File:MAC.svg

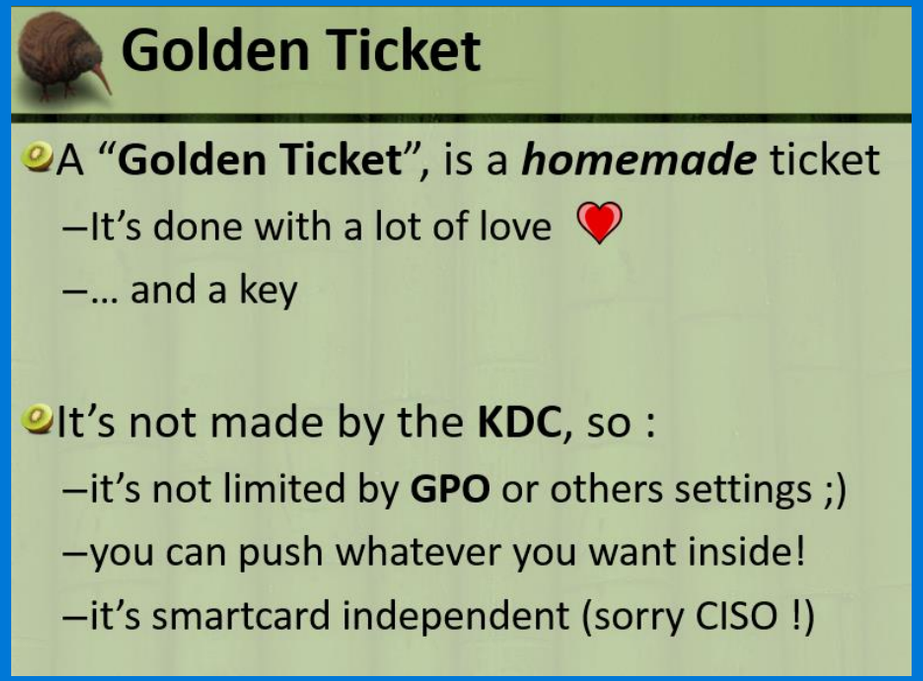
TGT Integrity

- 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?

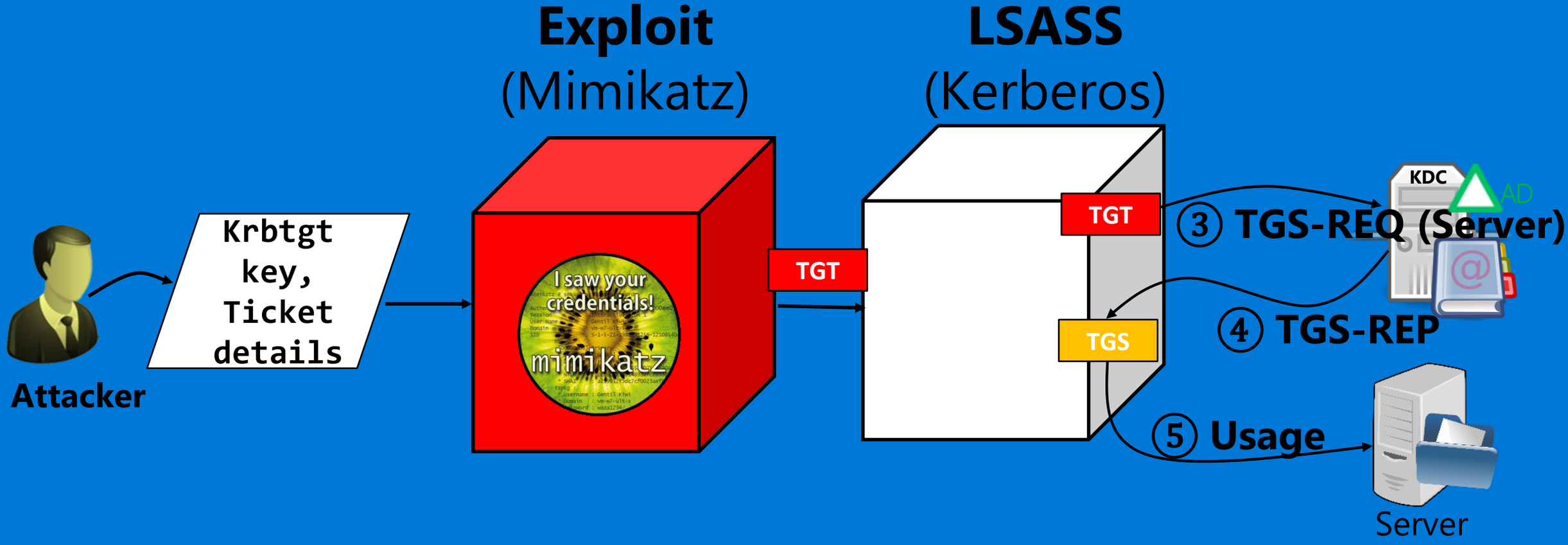


The Golden Ticket Attack

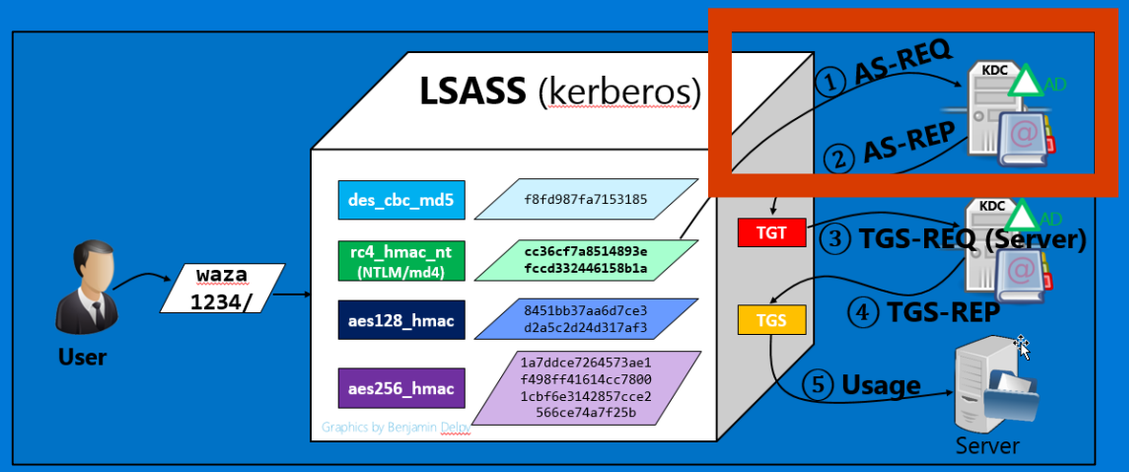
- Stealing KRBTGT key from AD allows the attackers to create arbitrary tickets
- In the words of its creator Benjamin Delpy (AKA gentilkiwi / Mimikatz):

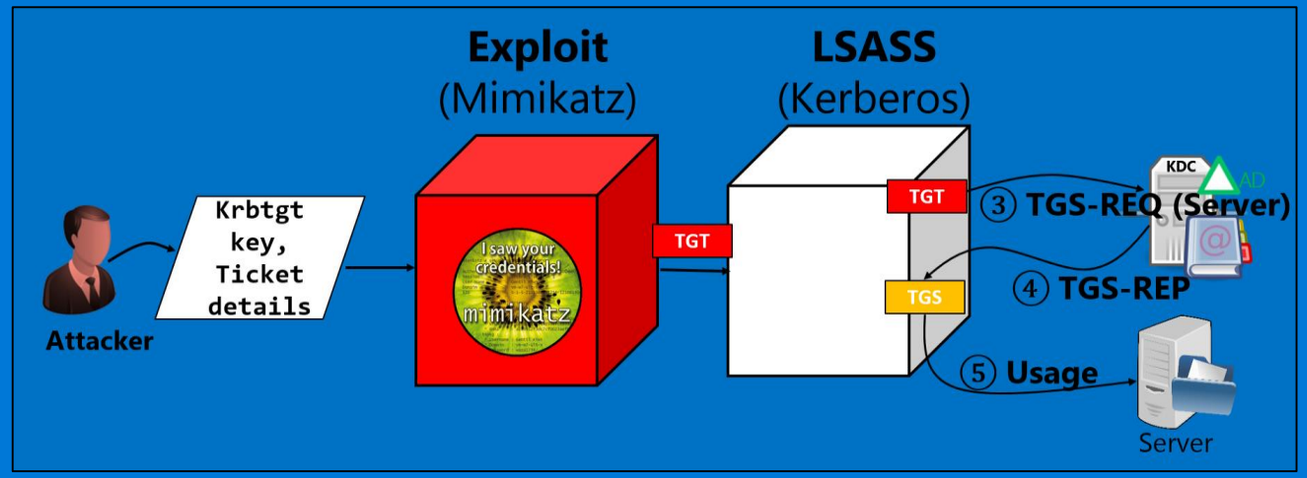


Golden Ticket Kerberos "Auth"



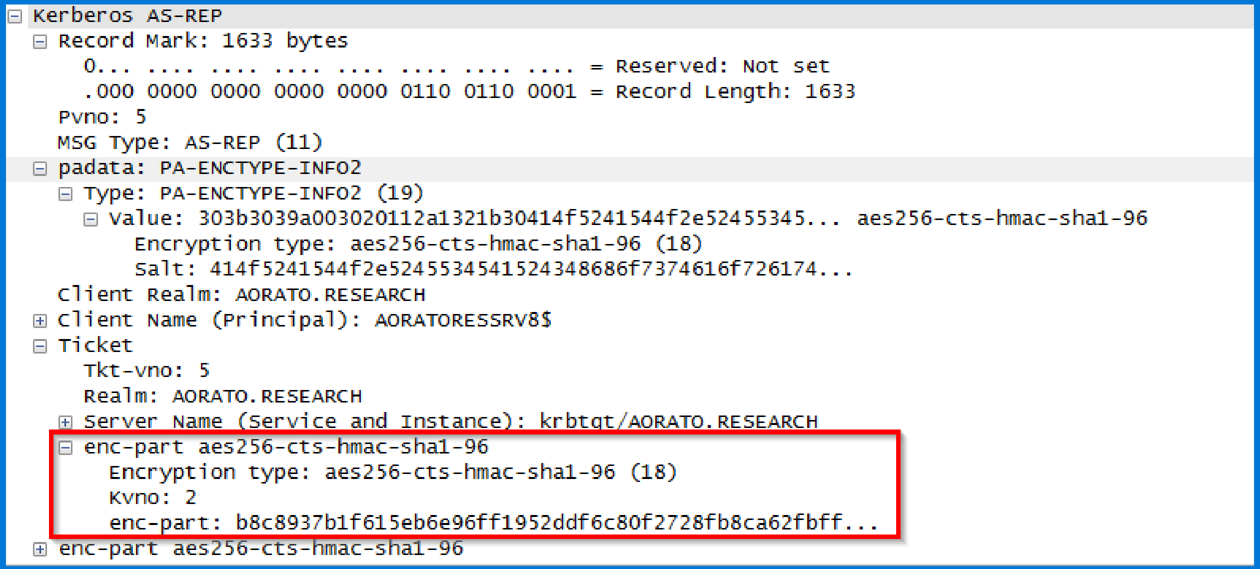
Let's Play Spot the Difference

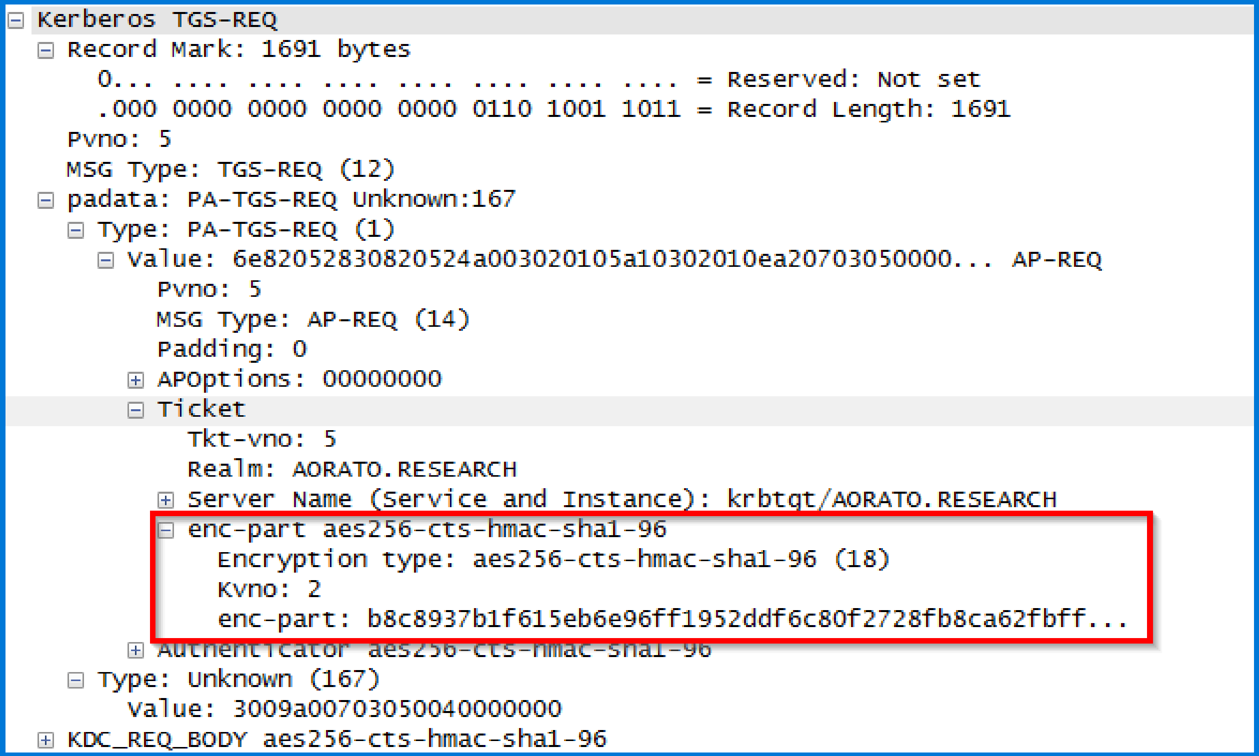




Can you spot the difference?

Over the network

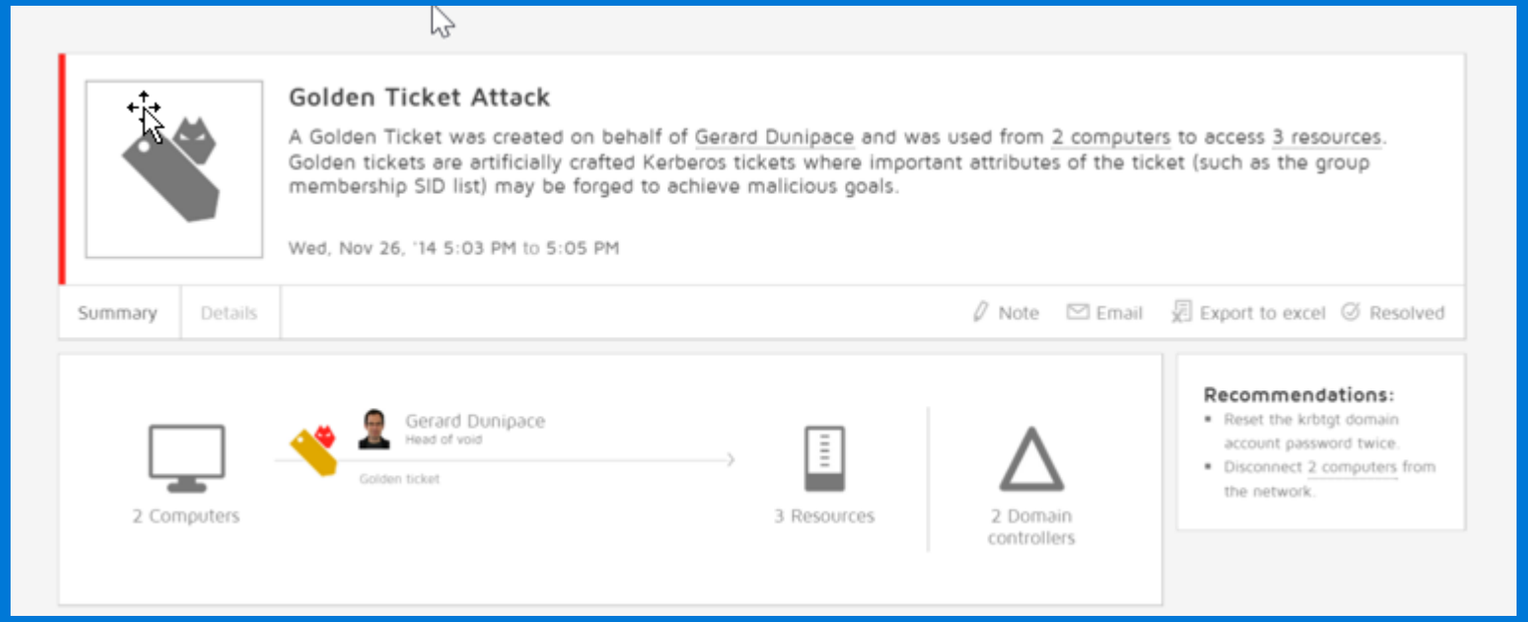




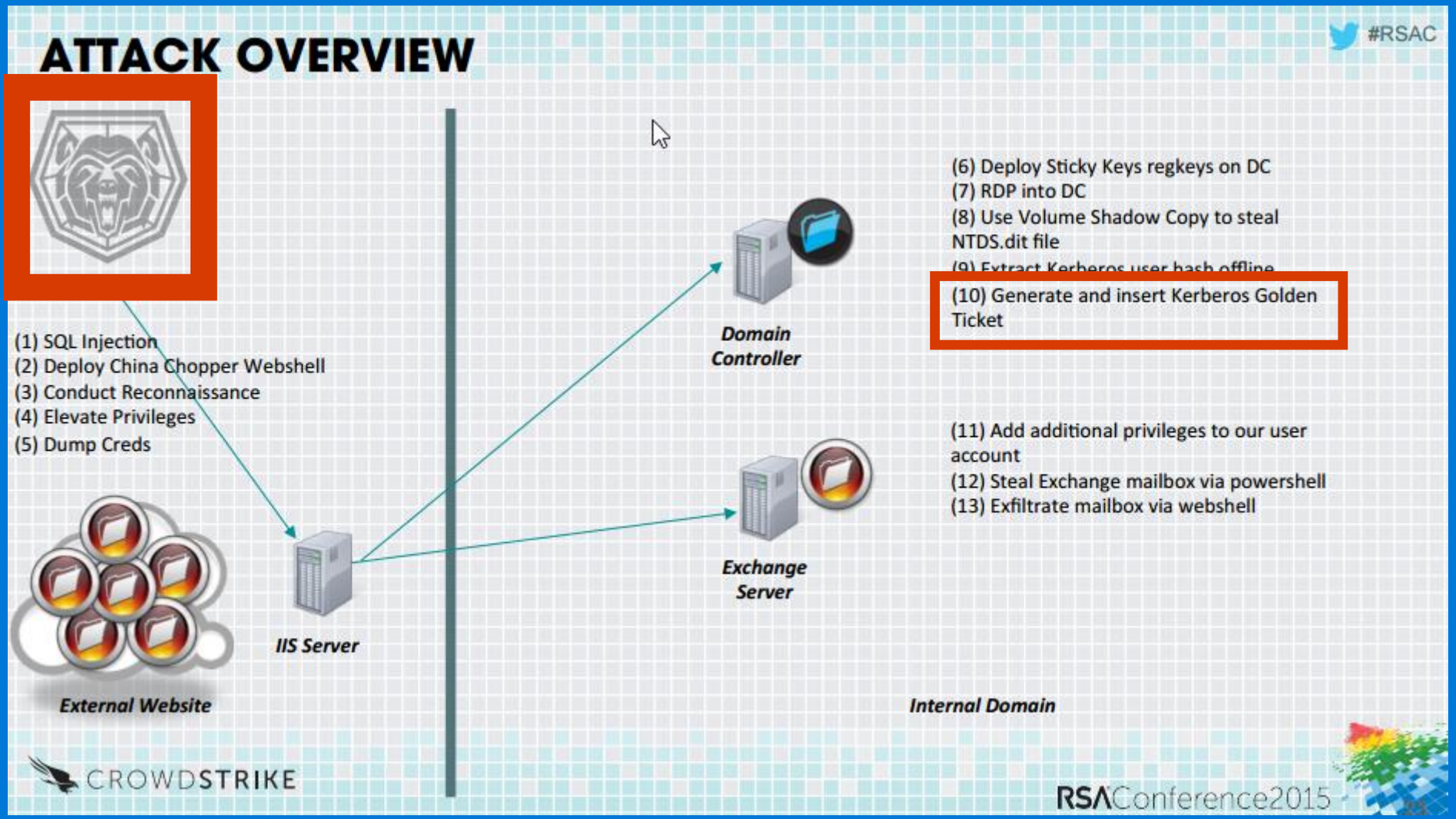
Source	Destination	Protocol	Info	enc-part
10.0.0.4	10.0.0.5	KRB5	AS-REP	b8c8937b1f615eb6e96ff1952ddf6c80f2728fb8ca62fbff...
10.0.0.5	10.0.0.4	KRB5	TGS-REQ	b8c8937b1f615eb6e96ff1952ddf6c80f2728fb8ca62fbff...
10.0.0.5	10.0.0.4	KRB5	TGS-REQ	b8c8937b1f615eb6e96ff1952ddf6c80f2728fb8ca62fbff...
10.0.0.5	10.0.0.4	KRB5	TGS-REQ	b8c8937b1f615eb6e96ff1952ddf6c80f2728fb8ca62fbff...
10.0.0.5	10.0.0.4	KRB5	TGS-REQ	b8c8937b1f615eb6e96ff1952ddf6c80f2728fb8ca62fbff...
10.0.0.5	10.0.0.4	KRB5	TGS-REQ	b8c8937b1f615eb6e96ff1952ddf6c80f2728fb8ca62fbff...

Network-Based Detection

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



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
DEPARTURE GATE
A22
BOARDS AT
3:15PM
SEPT 01 2010
BOARDING ZONE
2
1ST LEG
0018A
AIRLINES INC
NO SMOKING
UNITED BOARDING PASS
UNITED FLIGHT D3048
SEAT NUMBER
23A
Coach
LAST NAME, FIRST NAME
RAPID CITY SD TO DENVER CO
RAP TO DEN
DEPARTS
3:40PM
UNITED
31
12

PILOT


SC MAGAZINE
FOR IT SECURITY PROFESSIONALS
> SC US
SC UK
NEWS
PRODUCTS
BLOGS
RESOURCES
VIDEOS
SC Magazine > News > Duqu2.0 knocks Kaspersky and security peers
Tom Reeve, senior report, SC Magazine UK
June 11, 2015
Duqu2.0 knocks Kaspersky and security peers
Andromeda botnet used to distribute new point-of-sale malware
Ohio inmate caught with pris
administrative
login credentials

PAC (Privilege Attribute Certificate)

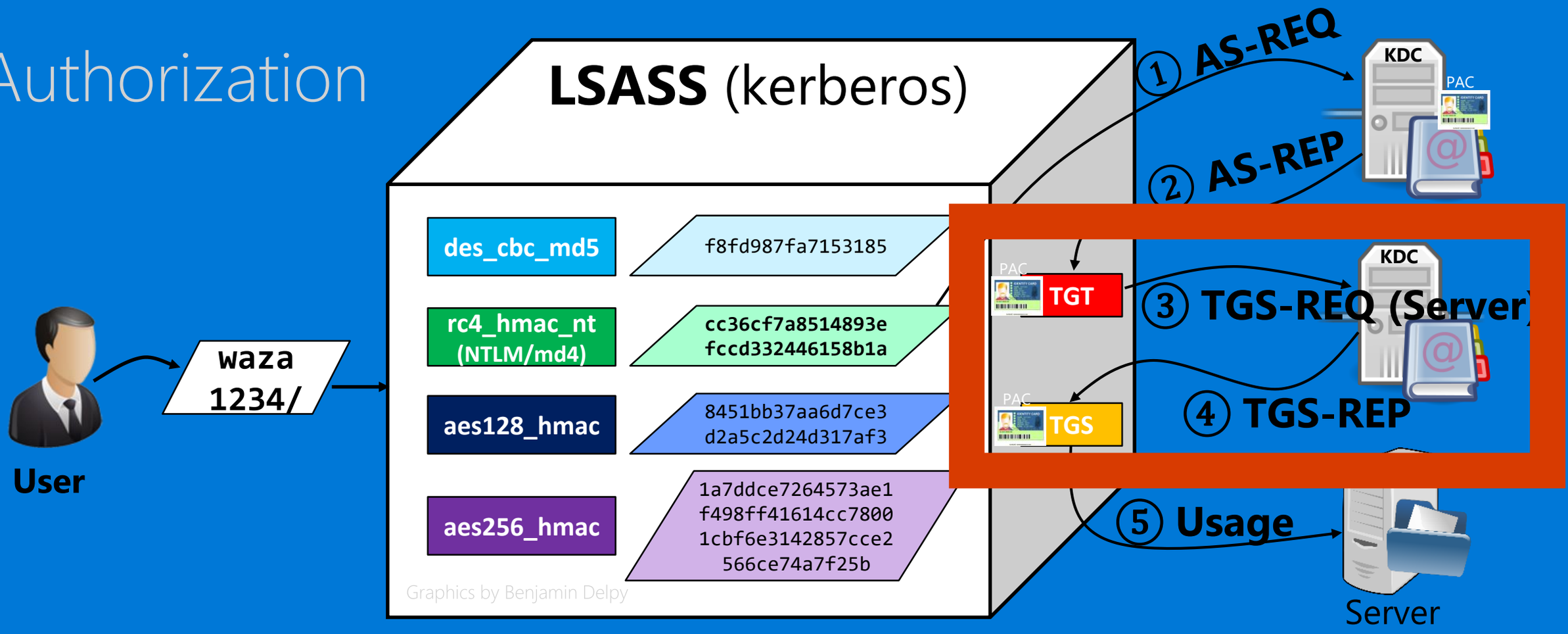
- MS Specific [MS-PAC]
- Authorization Data
- Signed by the KRBTGT key

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

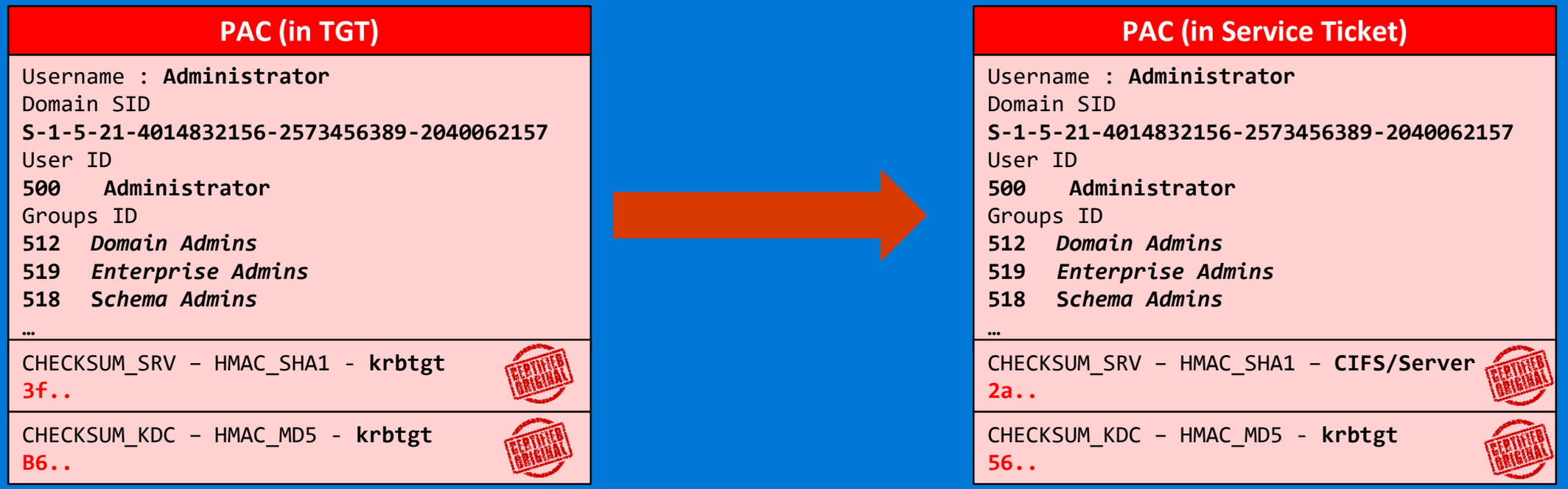
- Authorization



- PAC is embedded within the encrypted ticket

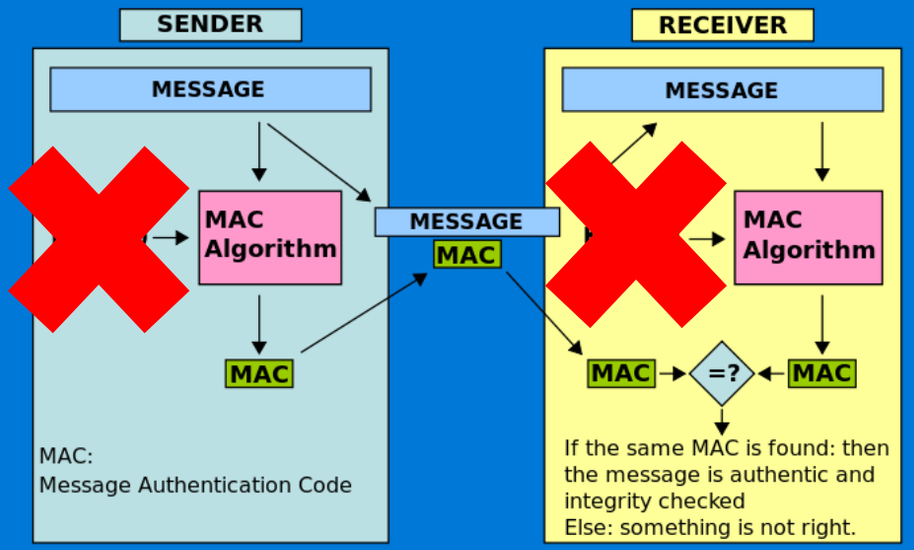
TGT to Service Ticket

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



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”!



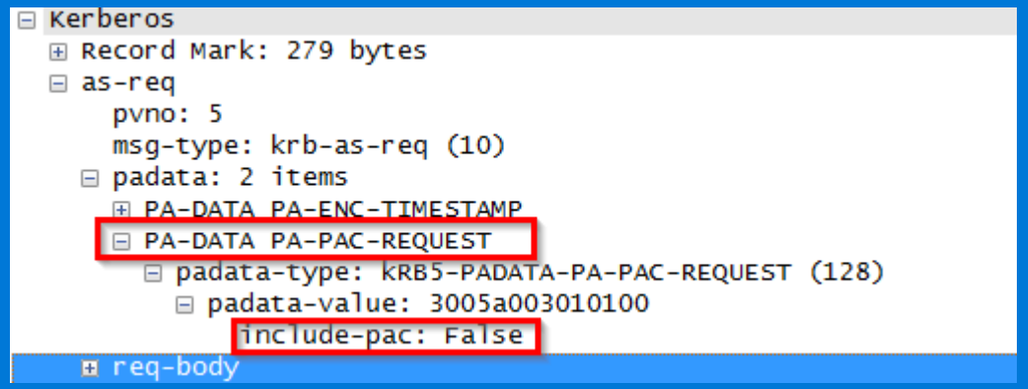
https://commons.wikimedia.org/wiki/File:MAC.svg

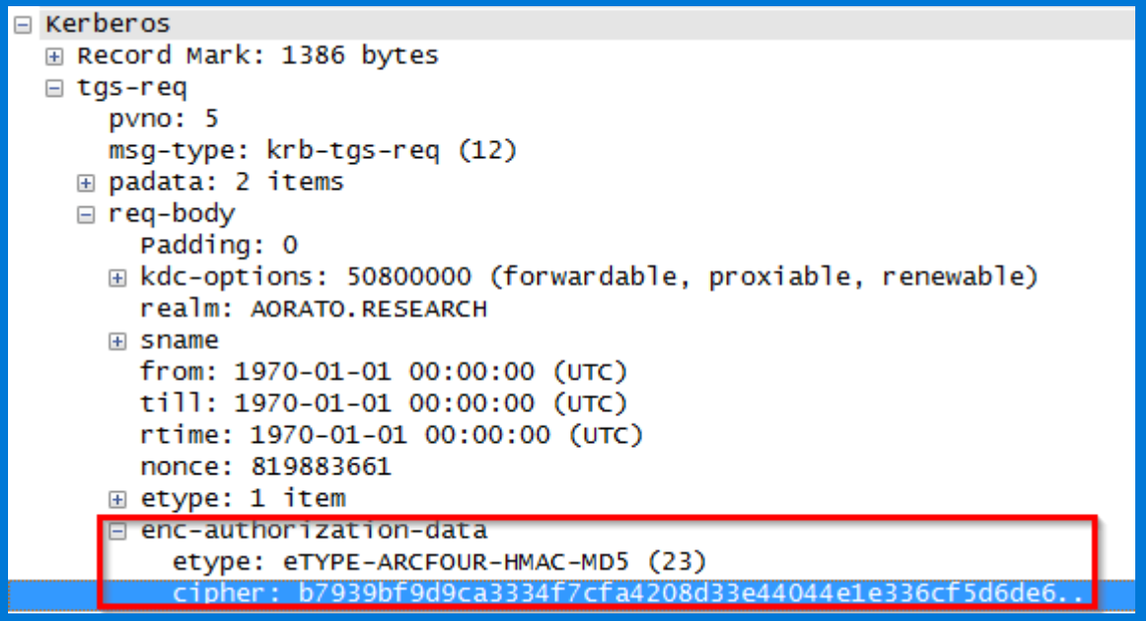
But is this Vuln Exploitable?

- 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? ☺

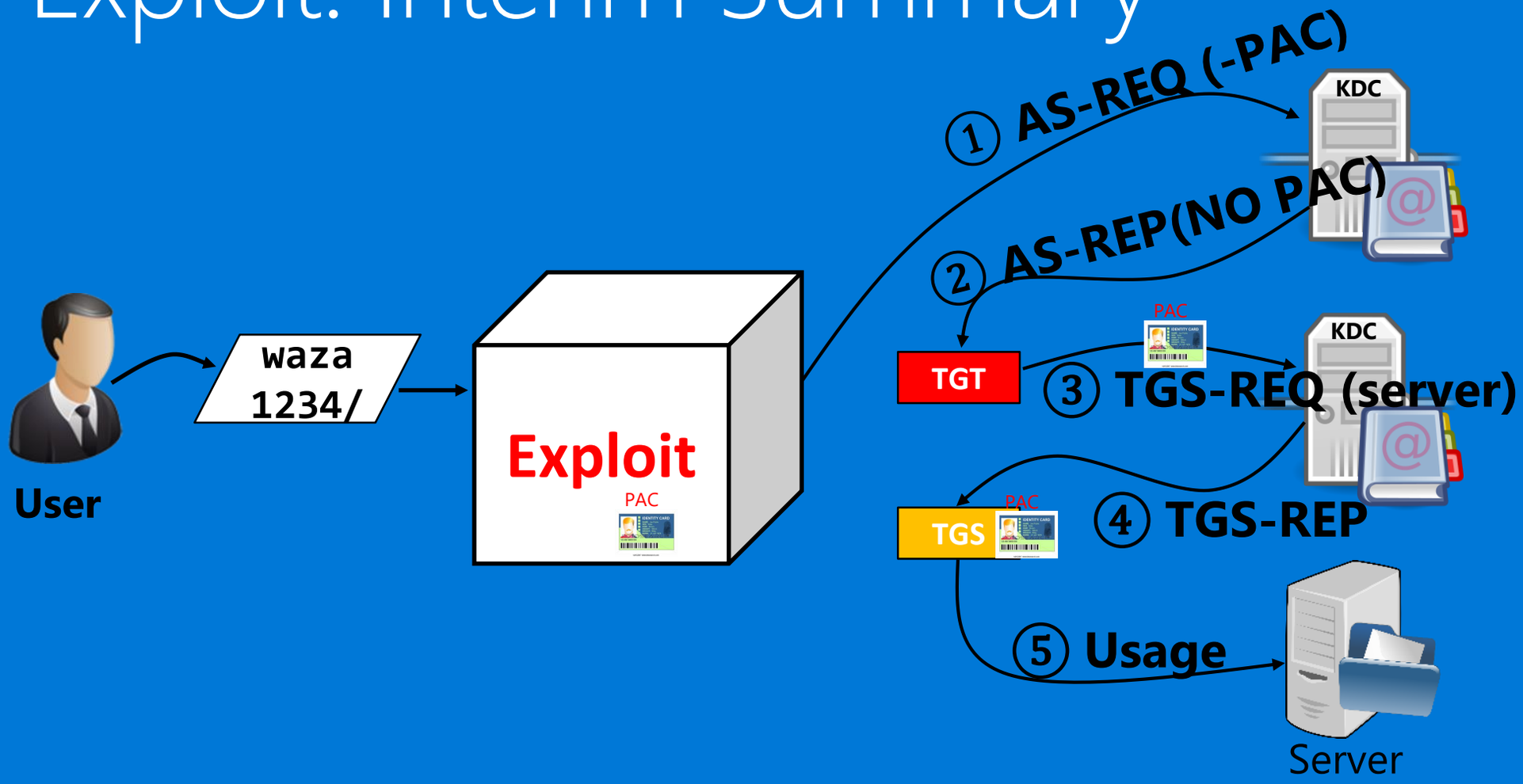
The Exploit

- 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)





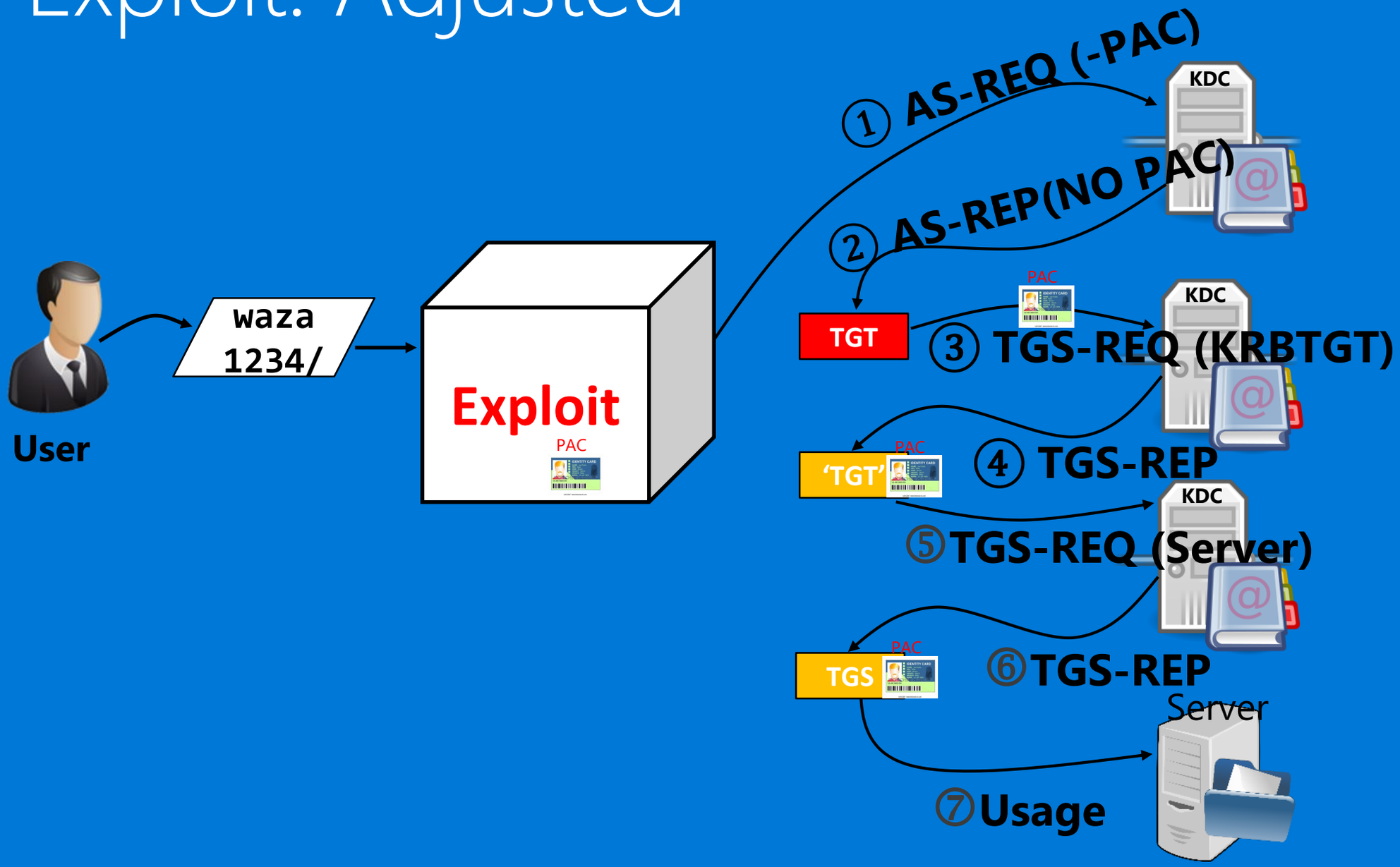
The Exploit: Interim Summary



Problem (for the attacker)

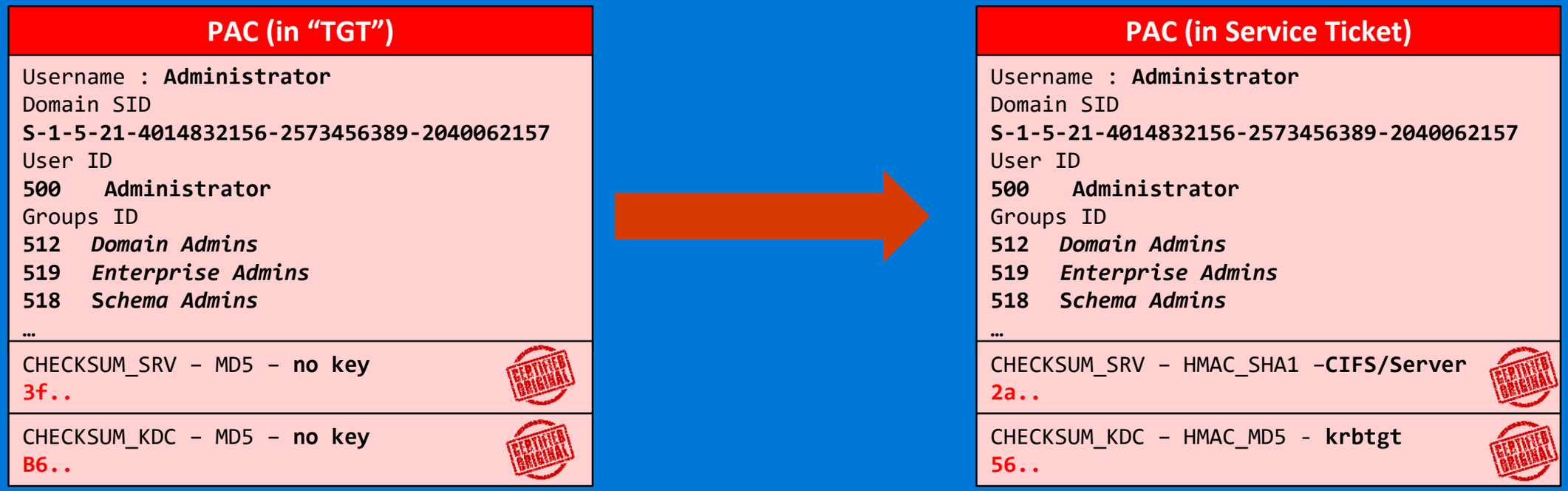
- MS11-013 fixed key-less hash signatures issue
  - For clients and servers
  - Not for KDC!

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

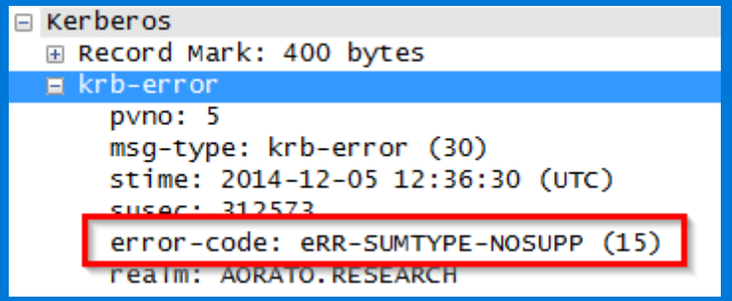



Gavin Millard @gmillard · 11h
MS14-068 in the real world.
"Welcome Captain. Would you like a coffee before you take off"
#infosec
PiLOT
UNITED FLIGHT D3048
RAP - DEN
DEPARTURE GATE
A22
BOARDS AT
3:15PM
SEPT 01 2010
BOARDING ZONE
2
SEAT NUMBER
23A
Coach
LAST NAME, FIRST NAME
RAPID CITY SD TO DENVER CO
RAP TO DEN
DEPARTS
3:40PM
NO SMOKING
UNITED BOARDING PASS
UNITED
31
12

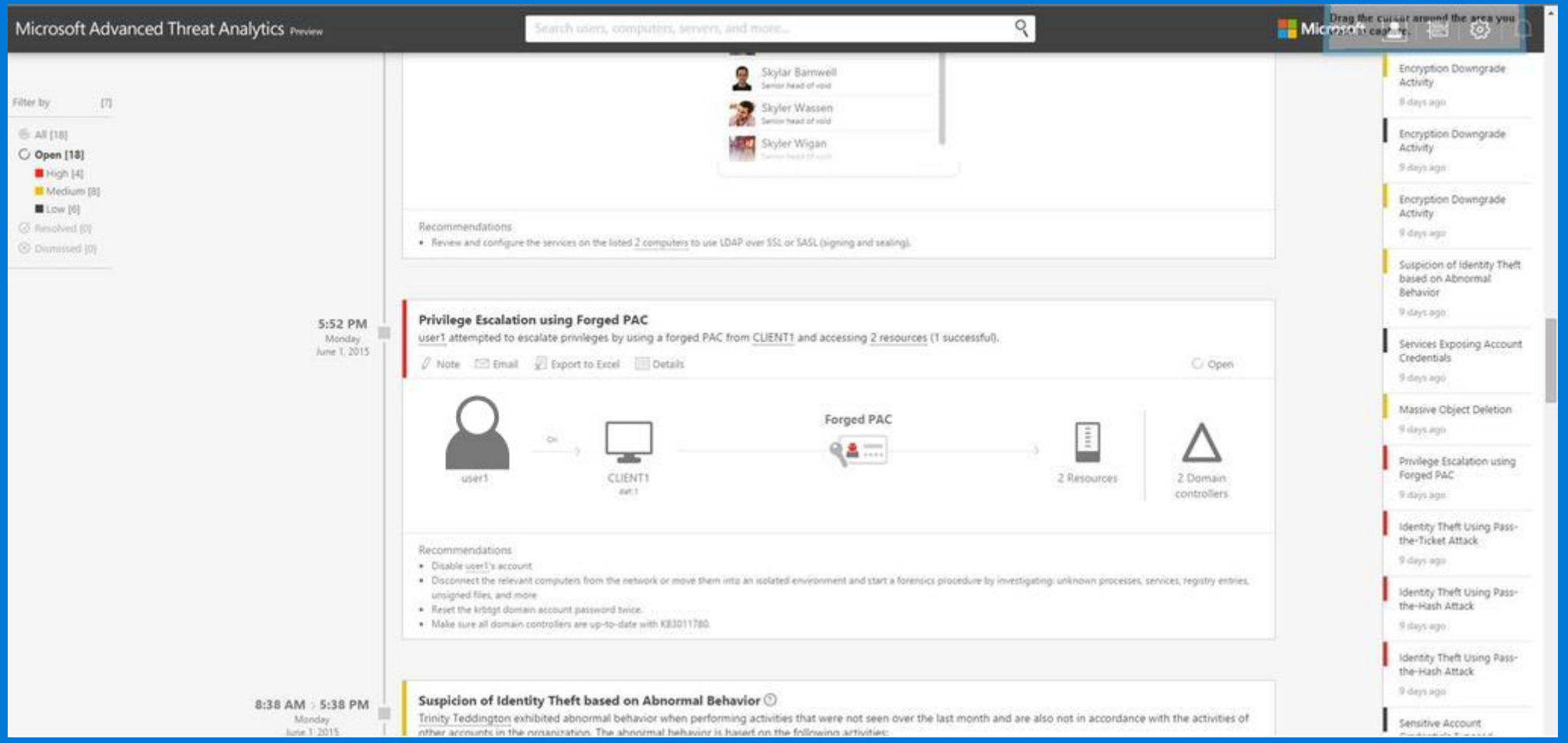

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS
> SC US
SC UK
NEWS
PRODUCTS
BLOGS
RESOURCES
VIDEOS
SC Magazine > News > Duqu2.0 knocks Kaspersky and security peers
Tom Reeve, senior report, SC Magazine UK
June 11, 2015
Duqu2.0 knocks Kaspersky and security peers
Andromeda botnet used to distribute new point-of-sale malware

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



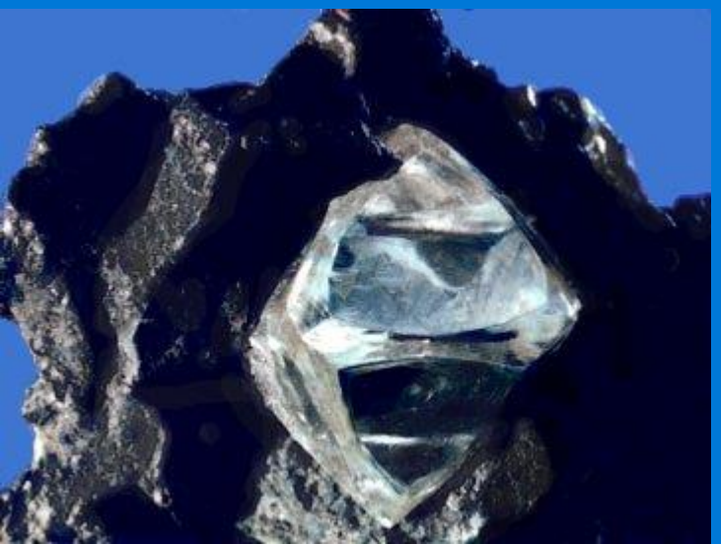
Network–based Detection



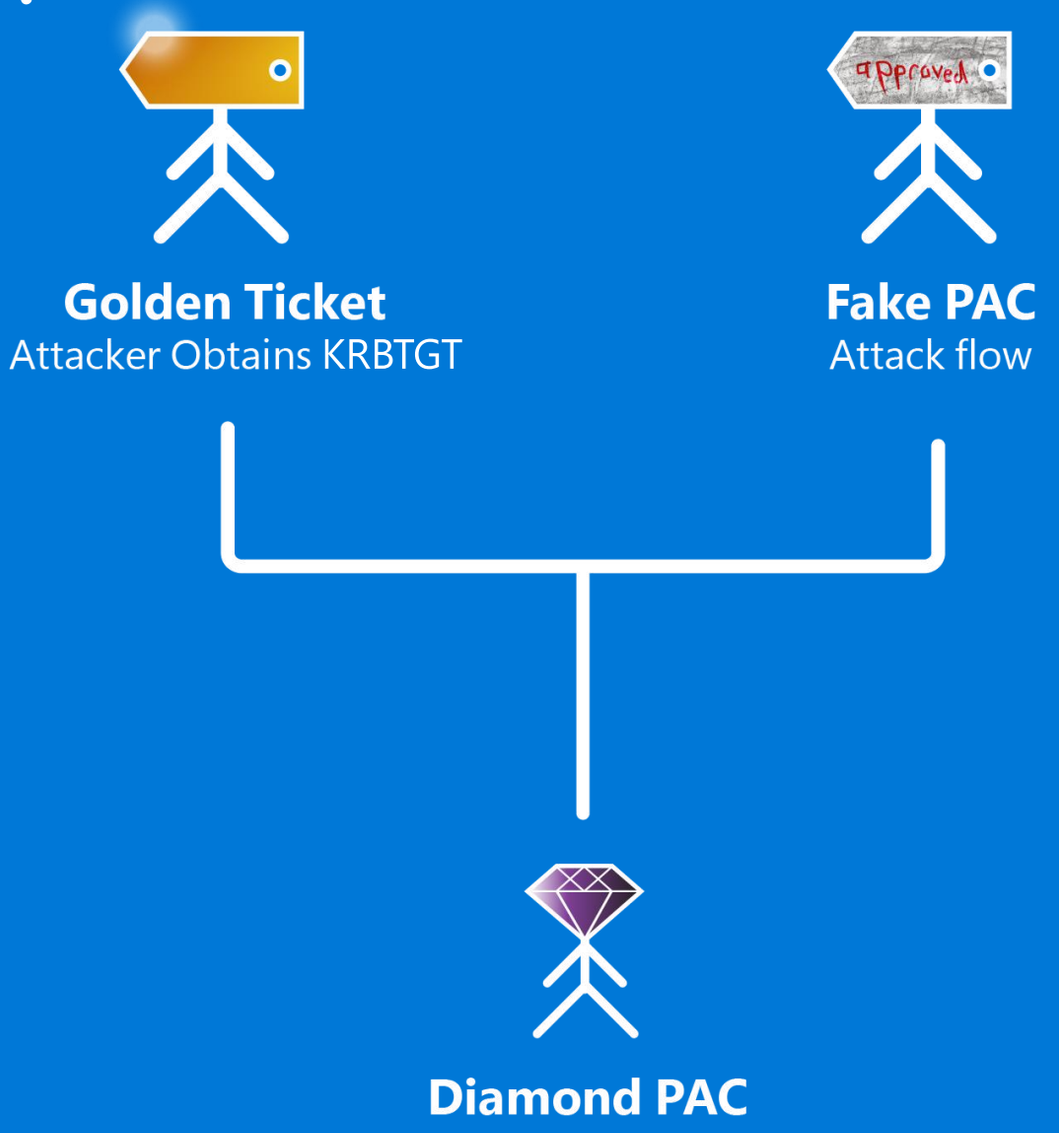
Forged PAC: Diamond PAC

What is a Diamond PAC?

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



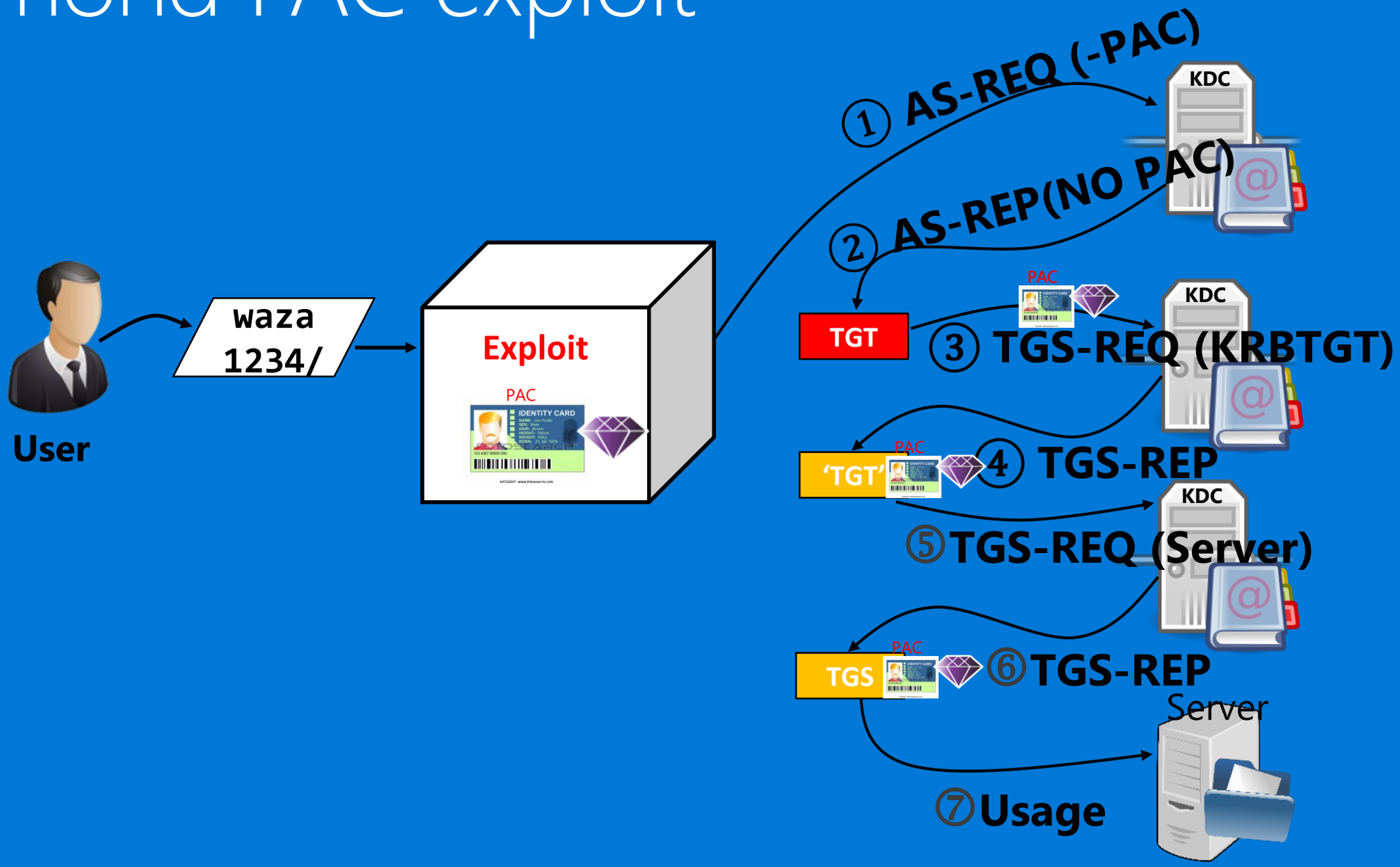
Diamond Photograph courtesy of the U.S. Geological Survey



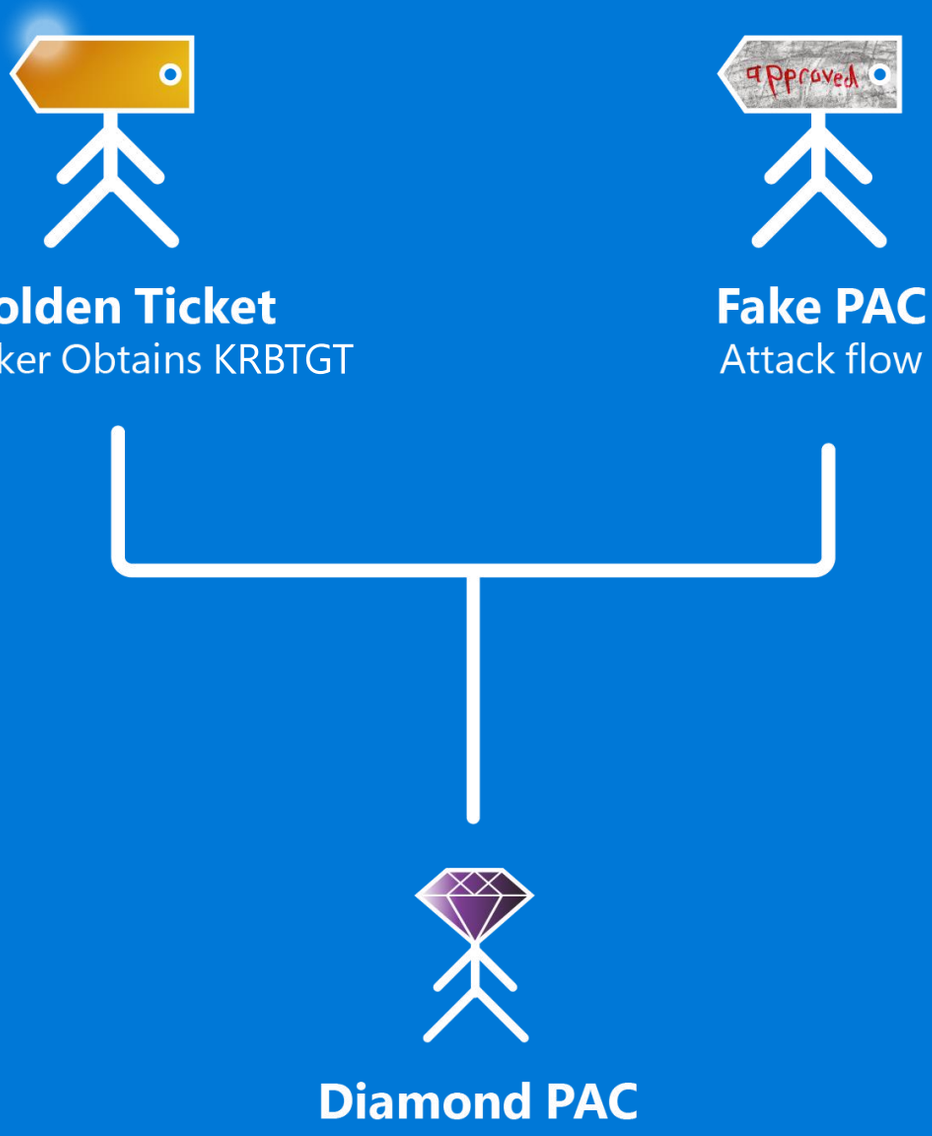
Diamond PAC exploit

- 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



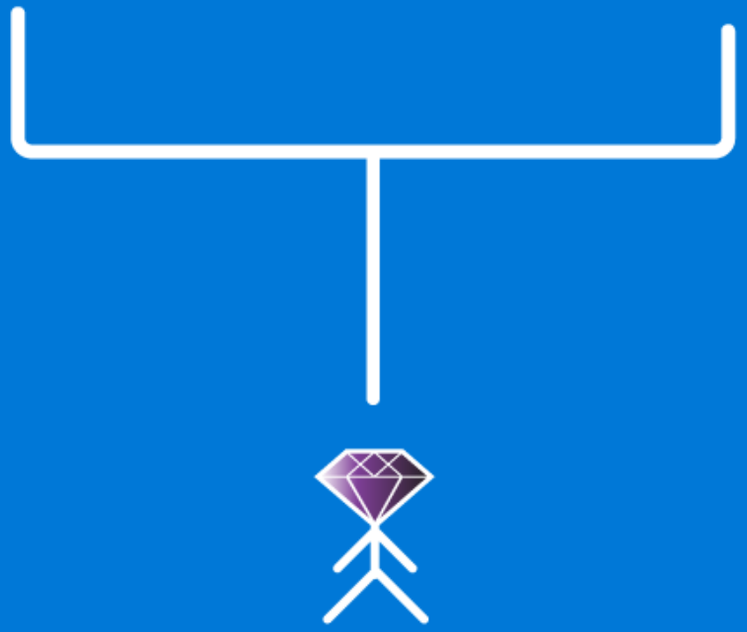
Why use the son if you can use its parents

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

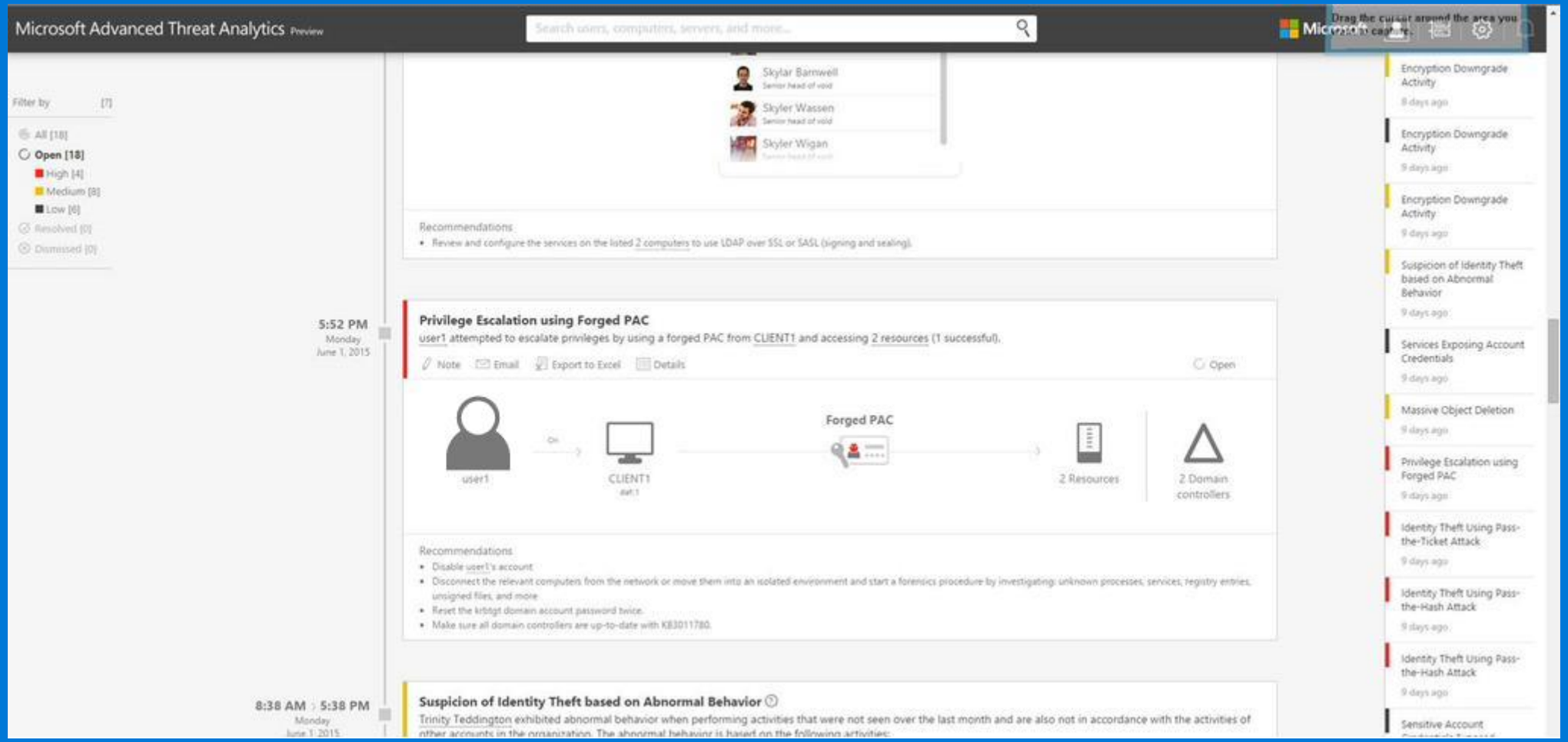
But legit

- 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



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?