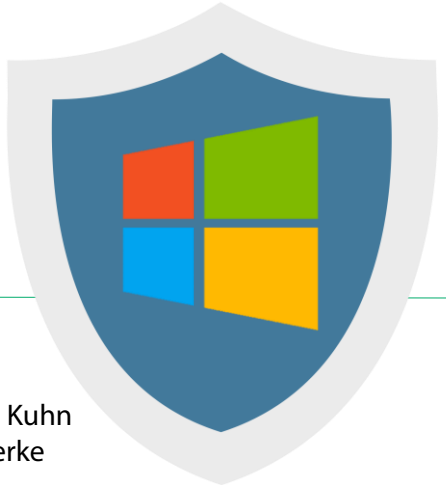
How to Efficiently Protect Active Directory from Credential Theft & Large Scale Compromise



An Approach Based on Real-World Expertise

Friedwart Kuhn, fkuhn@ernw.de

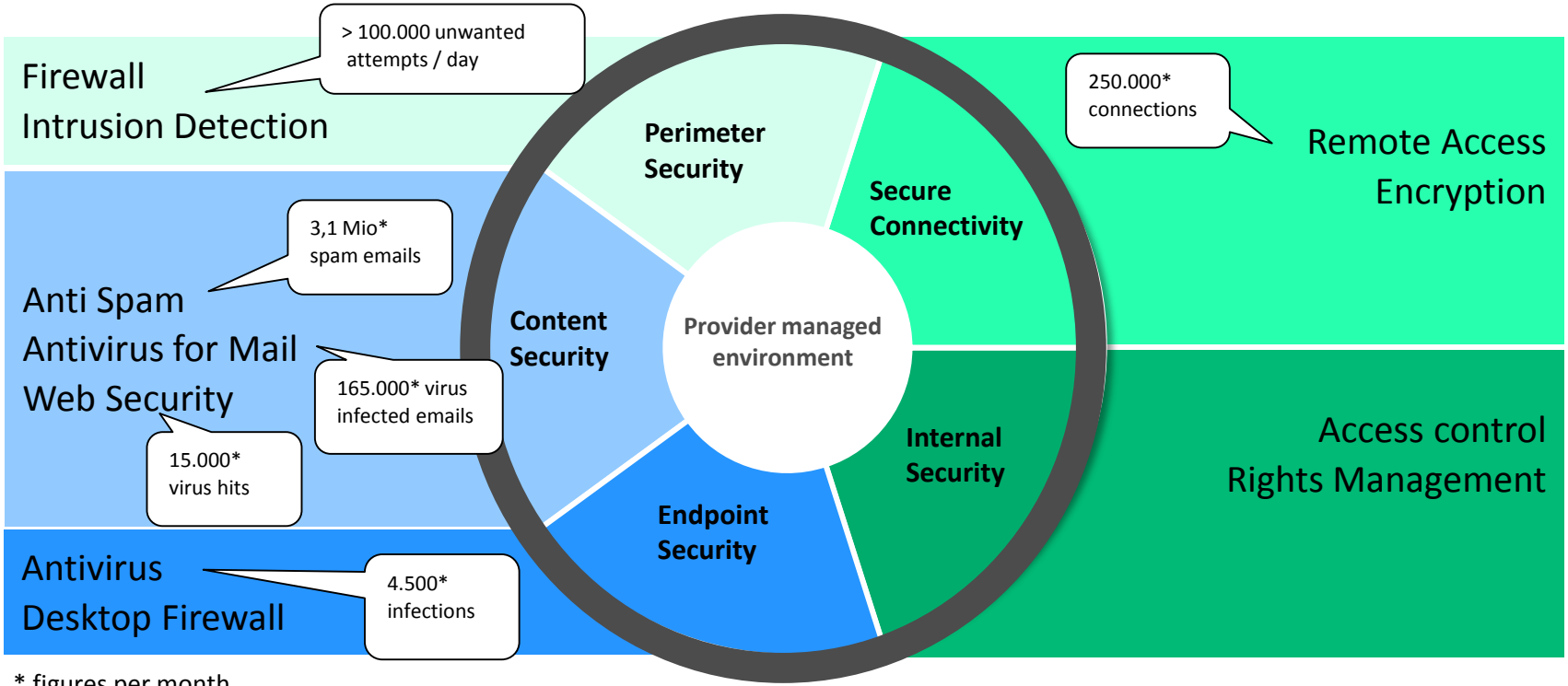
Agenda

- Introduction
- Windows Authentication
- Credential Theft, Reuse & Self-made Tickets
- Mitigations

ERNW
providing security.

Do you think you protected?

IT-Security @ Medium-Large Enterprises



* figures per month

ERNW
providing security.

Do you think it mig possible
that one of ya W systems in
Active Dire ry mpromised?

Do you think you are protected…

…against Pass-the-$ attacks?

Do you know about Golden Tickets?

IMAGINE AN ATTACKER WITH THE CAPABILITIES OF THE T-1000 FROM TERMINATOR 2

IMPERSONATION ...

ERNW
providing security.

BYPASSING SECURITY ...

ERNW
providing security.

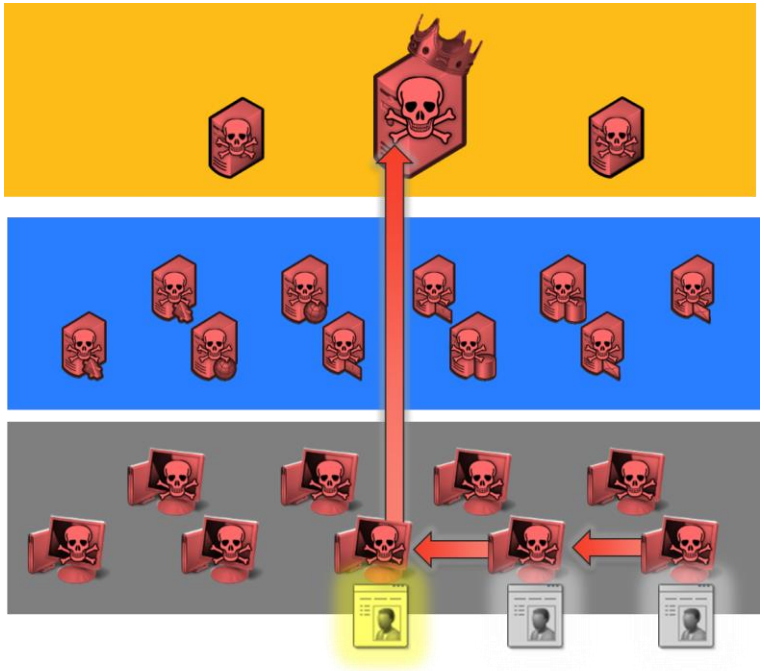
IS THIS THE FUTURE?

NO, IT ALREADY HAPPENED...

DO YOU SEE ANY LINK TO YOUR IT INFRASTRUCTURE...?

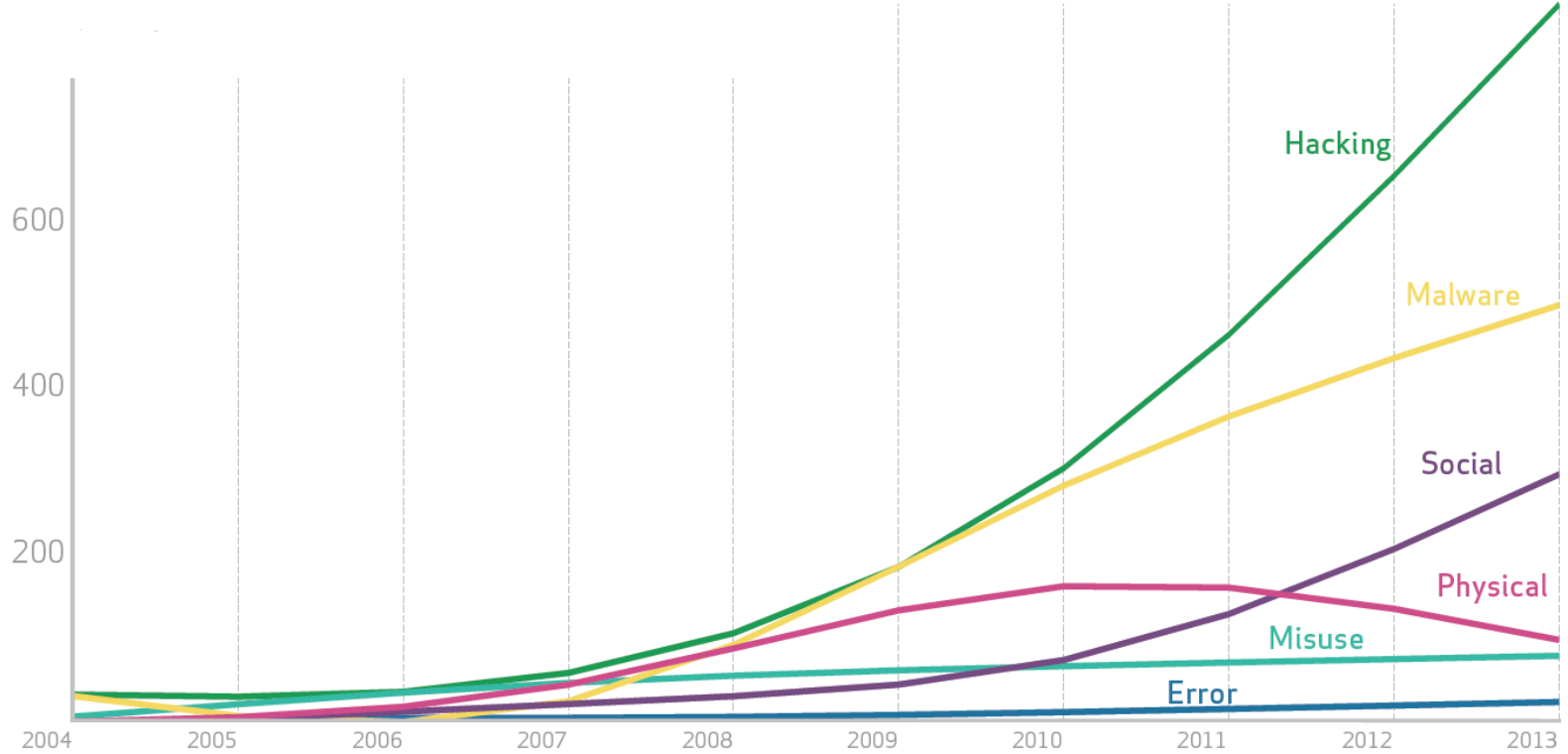
Pass the Hash in 48 hours (or less)

1. Attacker targets workstations en masse
2. User running as local admin is compromised, attacker harvests credentials
3. Attacker uses credentials for lateral movement or privilege escalation
4. Attacker acquires domain admin credentials
5. Attacker exercises full control of data and systems in the environment

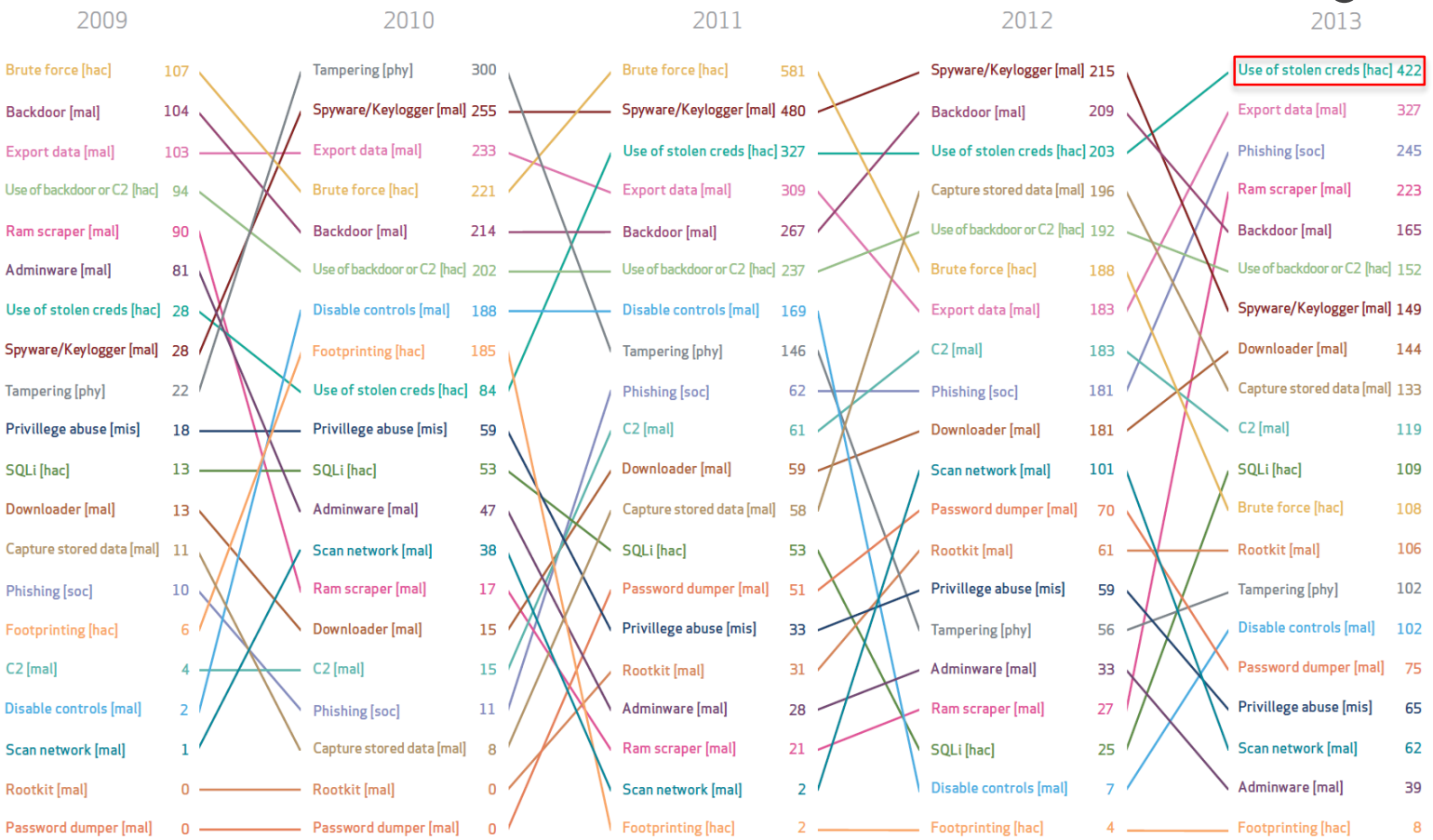


Source: Mark Simos, Nicholas DiCola; "TWC: Pass-the-Hash and Credential Theft Mitigation Architectures"

Number of breaches per threat action category over time



[1]: DBIR 2014

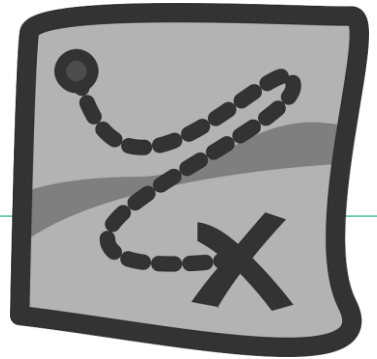

2009
Brute force [hac] 107
Backdoor [mal] 104
Export data [mal] 103
Use of backdoor or C2 [hac] 94
Ram scraper [mal] 90
Adminware [mal] 81
Use of stolen creds [hac] 28
Spyware/Keylogger [mal] 28
Tampering [phy] 22
Privillege abuse [mis] 18
SQLi [hac] 13
Downloader [mal] 13
Capture stored data [mal] 11
Phishing [soc] 10
Footprinting [hac] 6
C2 [mal] 4
Disable controls [mal] 2
Scan network [mal] 1
Rootkit [mal] 0
Password dumper [mal] 0
2010
Tampering [phy] 300
Spyware/Keylogger [mal] 255
Export data [mal] 233
Brute force [hac] 221
Backdoor [mal] 214
Use of backdoor or C2 [hac] 202
Disable controls [mal] 188
Footprinting [hac] 185
Use of stolen creds [hac] 84
Privillege abuse [mis] 59
SQLi [hac] 53
Adminware [mal] 47
Scan network [mal] 38
Ram scraper [mal] 17
Downloader [mal] 15
C2 [mal] 15
Phishing [soc] 11
Capture stored data [mal] 8
Rootkit [mal] 0
Password dumper [mal] 0
2011
Brute force [hac] 581
Spyware/Keylogger [mal] 480
Use of stolen creds [hac] 327
Export data [mal] 309
Backdoor [mal] 267
Use of backdoor or C2 [hac] 237
Disable controls [mal] 169
Tampering [phy] 146
Phishing [soc] 62
C2 [mal] 61
Downloader [mal] 59
Capture stored data [mal] 58
SQLi [hac] 53
Password dumper [mal] 51
Privillege abuse [mis] 33
Rootkit [mal] 31
Adminware [mal] 28
Ram scraper [mal] 21
Scan network [mal] 2
Footprinting [hac] 2
2012
Spyware/Keylogger [mal] 215
Backdoor [mal] 209
Use of stolen creds [hac] 203
Capture stored data [mal] 196
Use of backdoor or C2 [hac] 192
Brute force [hac] 188
Export data [mal] 183
C2 [mal] 183
Phishing [soc] 181
Downloader [mal] 181
Scan network [mal] 101
Password dumper [mal] 70
Rootkit [mal] 61
Privillege abuse [mis] 59
Tampering [phy] 56
Adminware [mal] 33
Ram scraper [mal] 27
SQLi [hac] 25
Disable controls [mal] 7
Footprinting [hac] 4
2013
Use of stolen creds [hac] 422
Export data [mal] 327
Phishing [soc] 245
Ram scraper [mal] 223
Backdoor [mal] 165
Use of backdoor or C2 [hac] 152
Spyware/Keylogger [mal] 149
Downloader [mal] 144
Capture stored data [mal] 133
C2 [mal] 119
SQLi [hac] 109
Brute force [hac] 108
Rootkit [mal] 106
Tampering [phy] 102
Disable controls [mal] 102
Password dumper [mal] 75
Privillege abuse [mis] 65
Scan network [mal] 62
Adminware [mal] 39
Footprinting [hac] 8

[1]: DBIR 2014

How do you comm u e management?

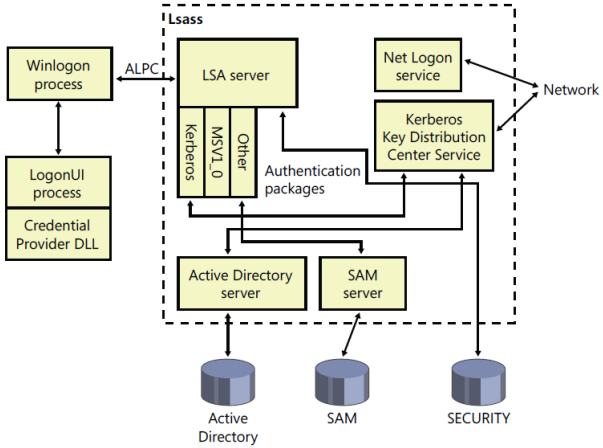
ERNW
providing security.

So, let's start ;-)



Authentication in Windows

Security Subsystem Architecture



- Ensures authentication and authorization
- Components run in the context of the lsass.exe
- Includes
  - Kerberos v5 authentication protocol
  - NTLM authentication protocol
  - LSA Server service
  - And others

LSA Protection Mechanisms

- Cryptomaterial (credentials, keys, etc.) in memory is encrypted, but in a reversible fashion
- Encryption is symmetric, keys are also in memory in the LSASS process
- Of particular interest:
  - Password hashes
  - Encryption keys
  - Kerberos tickets

Local LM/NTLM Authentication

Kerberos

- Authentication protocol for mutual authentication between client/server or server/server
- Used to access a service on a remote system
- Three integral parts:
  - Key Distribution Center (KDC)
  - Client user
  - Server with the desired service/resource
- KDC part of the Domain Controller; performs two service functions:
  - Authentication Service (AS)
  - Ticket-Granting Service (TGS)
- Three different symmetric encryption keys are relevant in the process

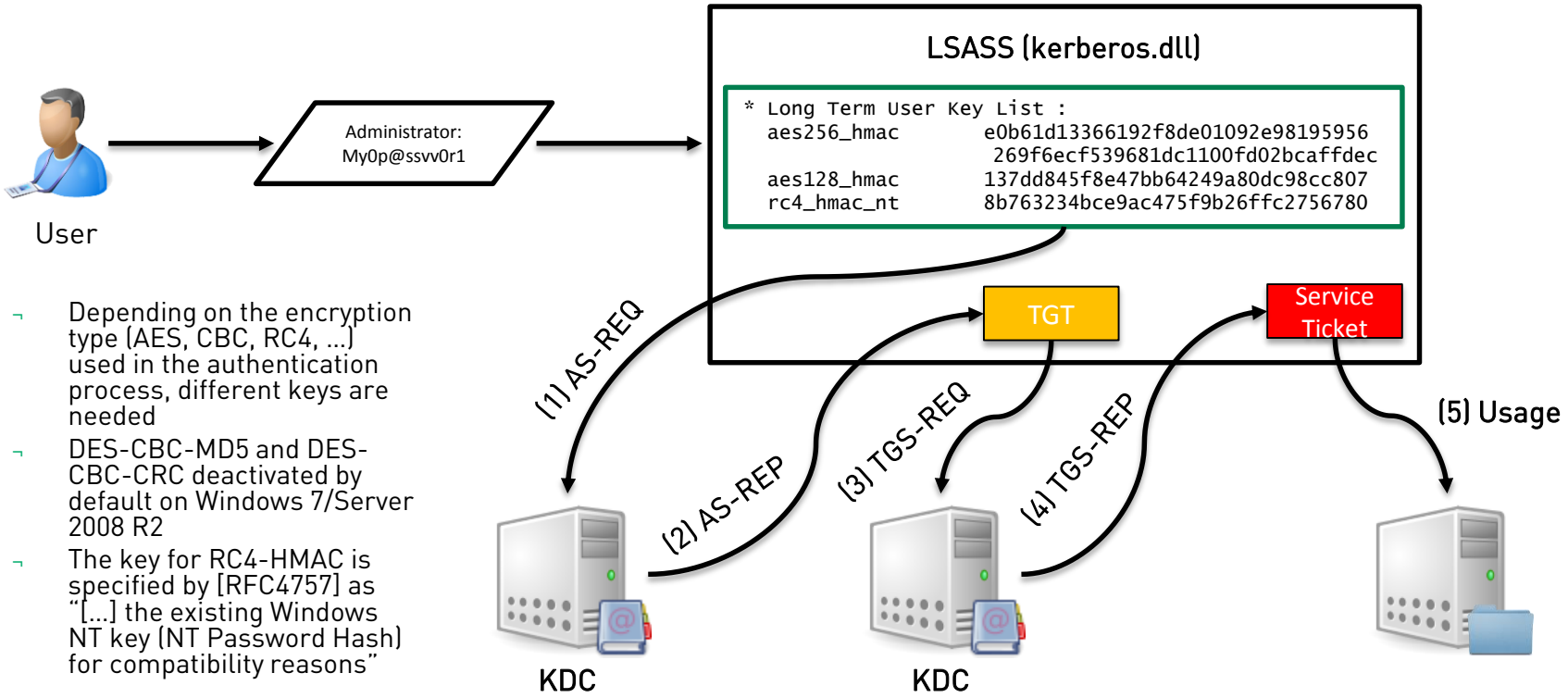
Kerberos Keys

- KDC long-term key (Domain key)
  - Derived from **krbtgt** account password
  - Usage:
    - Ticket-Granting Ticket (**TGT**) encryption
    - Sign token information, the so called **PAC**
- Client long-term key
  - Derived from user/computer account password
  - Usage:
    - AS-REQ time stamp encryption
    - Session key encryption
- Server/service long-term key
  - Derived from computer account password
  - Usage:
    - **Service Ticket** encryption
    - Countersign **PAC** in Service Ticket

Microsoft Kerberos PAC

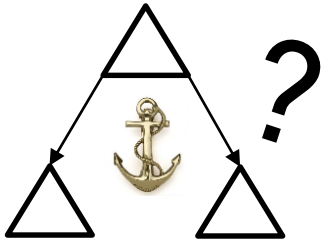
- Privileged Account Certificate (PAC)
- Extension element of the authorization-data field in Kerberos tickets
- Contains authorization-related information for Windows security principles:
  - SIDs and RIDs
  - Group membership
  - User profile information (home directory or logon scripts)
  - Password credentials
  - Security privileges
- Signed with the KDC long-term key and the service long-term key

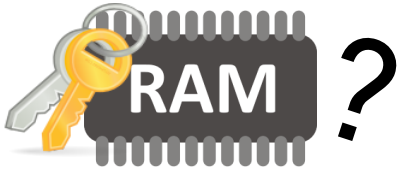
Kerberos Authentication Overview



- Depending on the encryption type (AES, CBC, RC4, …) used in the authentication process, different keys are needed
- DES-CBC-MD5 and DES-CBC-CRC deactivated by default on Windows 7/Server 2008 R2
- The key for RC4-HMAC is specified by [RFC4757] as "[…] the existing Windows NT key (NT Password Hash) for compatibility reasons"

2 Important Conclusions

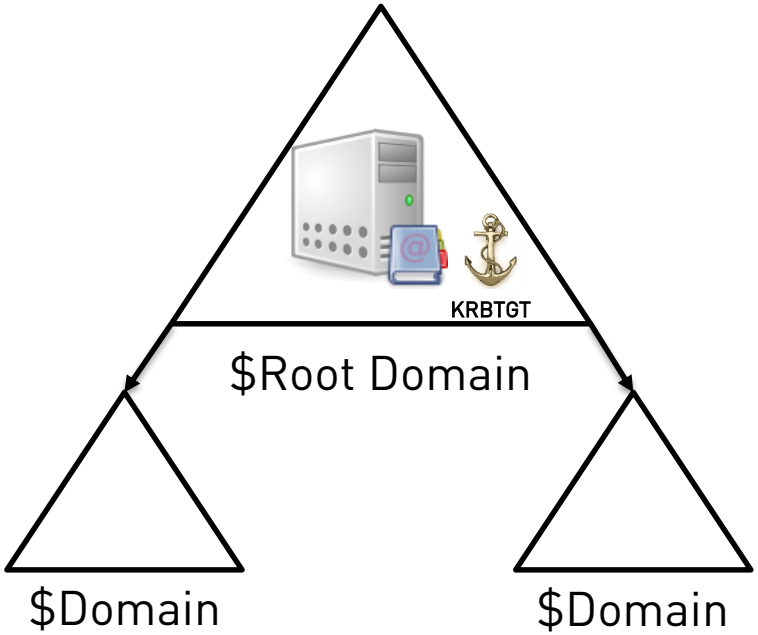




1. Who is the trust anchor in Active Directory

2. Which credentials are in which way stored/accessible in Windows memory

The Trust Anchor



- **Remember:** the KDC creates the PAC (contains information about how powerful the user is (his privileges, group memberships etc.) and signs it with the KRBTGT's NTLM hash
- → KRBTGT's NTLM hash
  = central trusted token "stamping authority"
  = trust anchor of the domain
- Keep this in mind, we will come back to this later… ;-)

Credentials/Credential Material in LSASS

ERNW providing security.

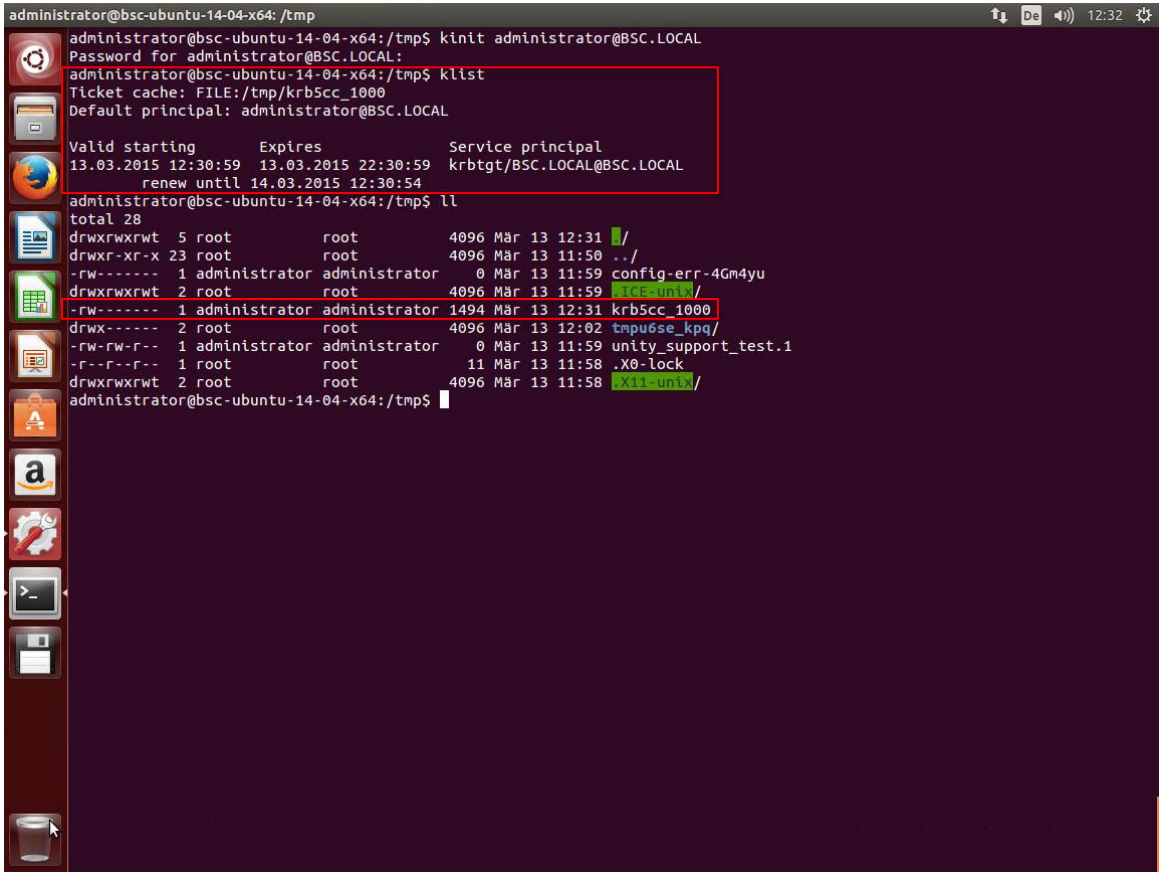
	Primary			CredentialKeys				tspkg		wdigest		kerberos				livessp	ssp	dpapi	credman 6
	LM	NTLM	SHA1	NTLM	SHA1	Root	DPAPI	off	on	off	on	pass 1	PIN 4	tickets	eKeys				
Windows XP/2003																			
Local Account								2											
Domain Account								2					5						
Windows Vista/2008 & 7/2008r2																			
Local Account																			
Domain Account																			
Windows 8/2012																			
Microsoft Account																			
Local Account																			
Domain Account																			
Windows 8.1/2012r2																			
Microsoft Account									3		3								
Local Account									3		3	7							
Domain Account									3		3								
Domain Protected Users									3		3								

	Windows 8.1 vault for user's authentication				
	PIN		Picture		Fingerprint
	code	pass	gestures	pass	pass
Microsoft Account					
Local Account					

	not applicable
	data in memory
	no data in memory

1. can need an unlock on NT5, not available with smartcard
2. tspkg is not installed by default on XP, not available on 2003
3. tspkg is off by default (but needed for SSO with remoteapps/ts), wdigest too
   http://technet.microsoft.com/library/dn303404.aspx
4. PIN code when SmartCard used for native Logon
5. PIN code is NOT encrypted in memory (XP/2003)
6. When accessed/used by owner
7. When local admin, UAC and after unlock

Source: Benjamin Delpy, http://1drv.ms/1fCWkhu

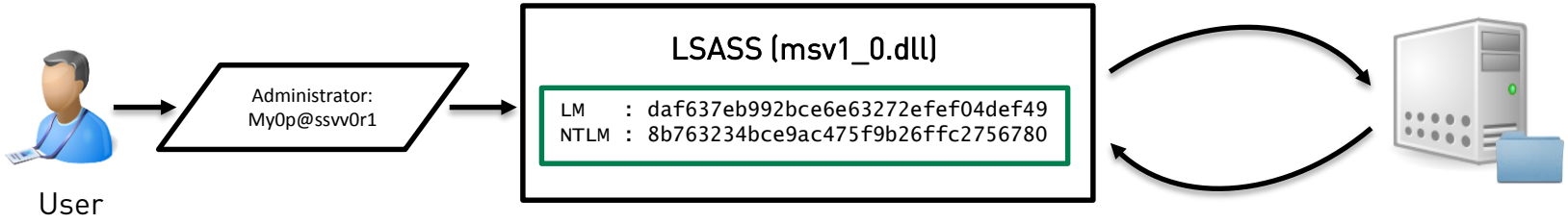


Ubuntu Kerberos Client (MIT)

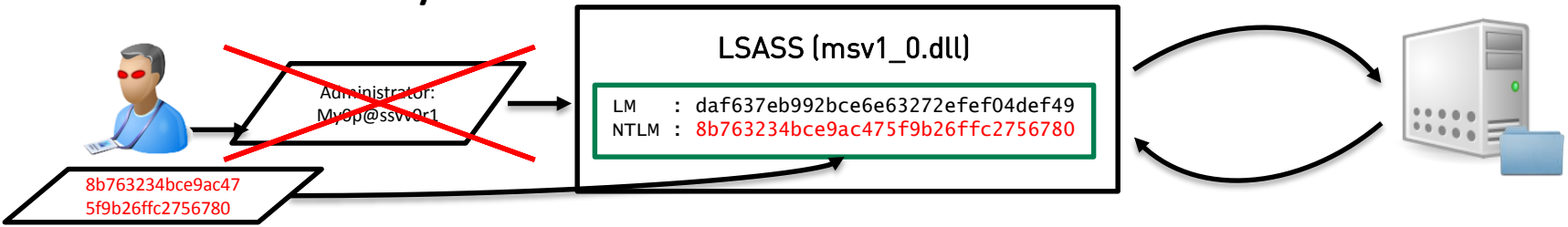
- Client caches tickets in a file
  - In /tmp
- One file per user
- User has full access to all his tickets
  - In Windows users cannot export their tickets by default
- Root user has access to all ticket caches of all users
- Tickets can be easily extracted an reused in e.g. mimikatz

Credential Theft and Reuse

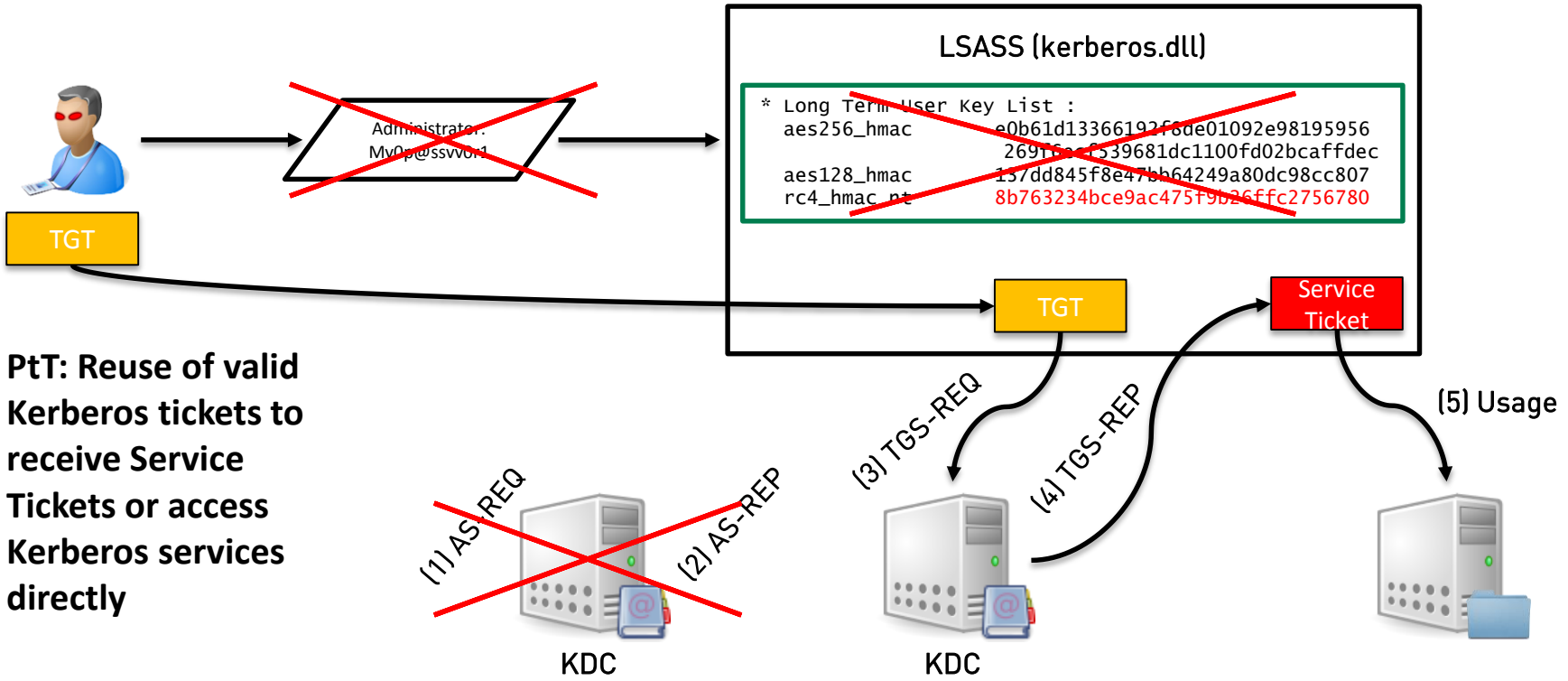
Pass-the-Hash LM/NTLM Authentication



PtH: Reuse of valid password hashes as a credential equivalent to authenticate to a remote server/service

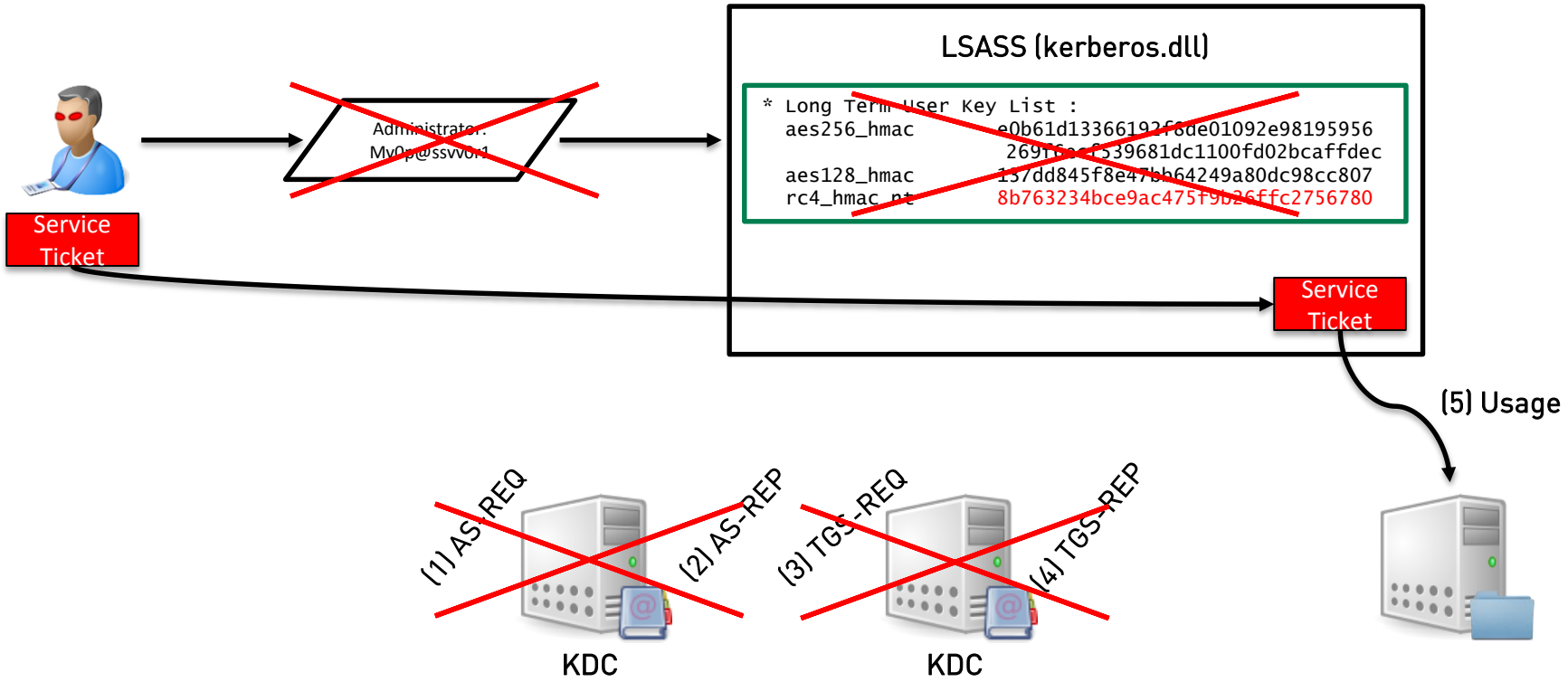


Pass-the-Ticket: TGT

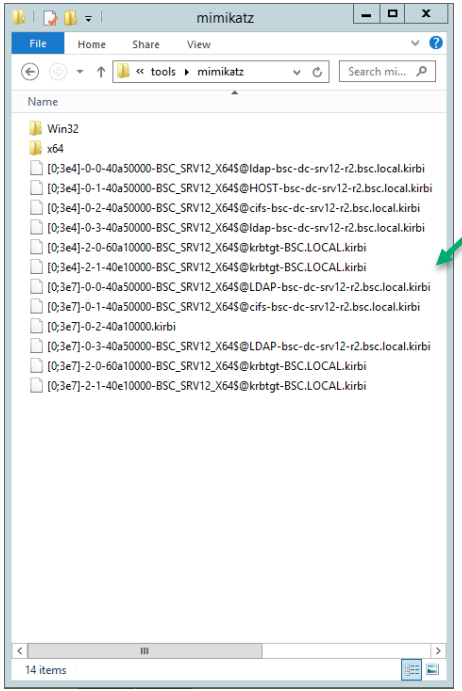


PtT: Reuse of valid Kerberos tickets to receive Service Tickets or access Kerberos services directly

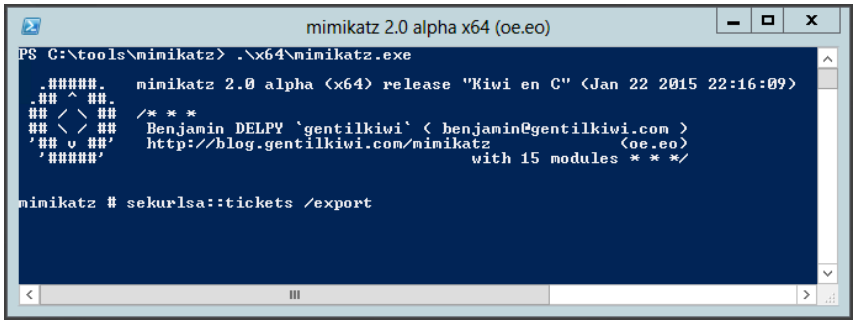
Pass-the-Ticket: Service Ticket



Export Kerberos Tickets



They can be used ;-) (for 10h)



Summary Pass-the-Ticket

- Several ways to obtain Kerberos tickets
- Can be used to impersonate other users
- **TGT** and **Service Ticket** both have time restrictions
  - Full impersonation of a user for up to 10 hours (default lifetime of **TGTs**)
  - Access to a service for up to 10 hours (default lifetime of **Service Tickets**)

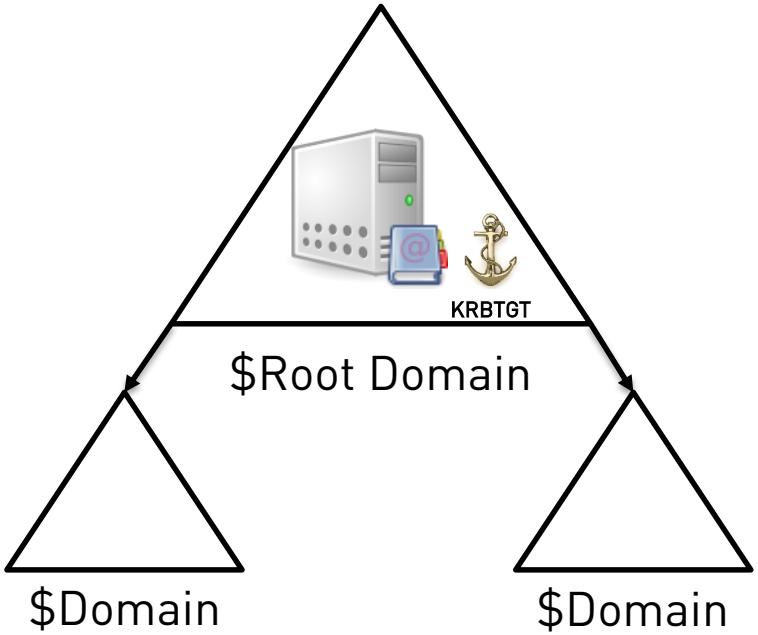
- ... so, why not create our own tickets?

Self-made Kerberos Tickets

Golden Ticket

- Self-made Ticket Granting Ticket (TGT)
  - “It’s done with a lot of love <3” (Credit goes to Benjamin ;-))
- Requires the KDC long-term key (**krbtgt key/hash**) from the Domain Controller
- _NOT_ made by the KDC
  - Variable life time (e.g. 10 years)
  - Not limited by security settings (e.g. Group Policy settings)
  - PAC can have arbitrary attributes (e.g. User name, user RID, group membership)
  - Smart card independent

Remember… ;-)



- The **KDC long-term key** (krbtgt key) is the **primary trust anchor** in a Kerberos environment
  - Compromise of the krbtgt means compromise of the whole Domain
- **Krbtgt key** is generated once and **does not change automatically**
  - Only changes during an upgrade of the Domain Functional Level from NT5 -> NT6
    - Windows Server 2000/2003 to Server 2008/2012
    - An upgrade from Server 2008 to 2012 does _NOT_ change the value
    - Previous krbtgt key is also valid!

Golden Ticket Prerequisites

- **KDC long-term key**, RC4 (NTLM hash) or AES
  - Available through different tools/techniques:
    - Online: From DC memory with mimikatz (see example)
    - Offline: From ntds.dit dump, task manager lsass.exe dump
- **Domain SID**
- **Domain Name**

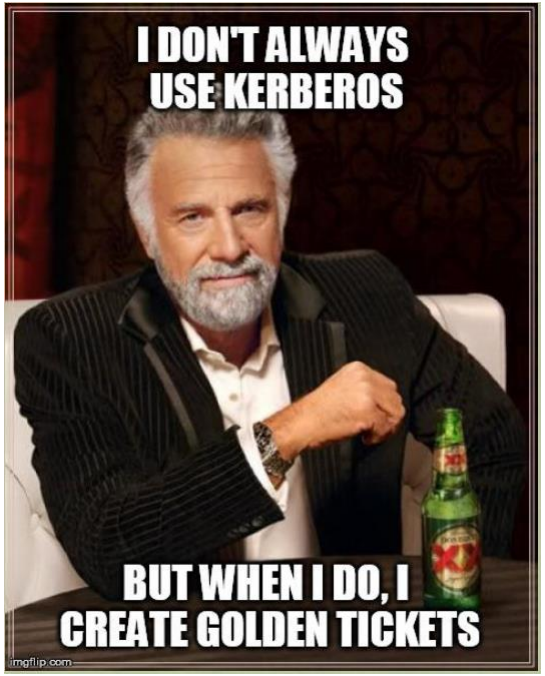
```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : BSC / S-1-5-21-2935009051-1024133711-517063756

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    LM   :
    NTLM : 14057bb953e6252fed3184484b3f8190

 * Kerberos-Newer-Keys
    Default Salt : BSC.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 16f13f49a9918f0f516280928791994c
                                 dba8ed2d2727efa1d946cfe9bfb53b95
      aes128_hmac       (4096) : f15a9b2cbb40e81a09bda8a039e83181
      des_cbc_md5       (4096) : 6dd3c101292ca154
```

Capabilities of Golden Tickets

- Create **TGTs** for:
  - Existing user accounts with valid group membership
    - Impersonate any user on the domain
  - Existing user accounts with arbitrary group membership
    - Impersonate any user on the domain and join any domain group (e.g. Domain Admins)
  - Non-existing user accounts with arbitrary group membership
    - User “Eve” as Domain Administrator
  - Existing but disabled user accounts

- Be creative ;)

I like this one ;-)
Thx, Benjamin ::



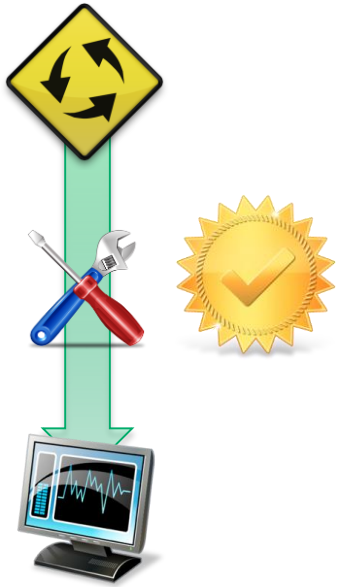
And now???

Mitigations

So what to do…?

- To prevent/mitigate credential theft and PtH in your environment
  - The short version
  - The more comprehensive version

Mitigations --The 2-Slider ;-) (1/2)



In 3 major steps :

- Reorganization of administrative practice /management of Active Directory and business critical services
- Complement reorganization of Active Directory management with some PtH-specific controls
- Implement appropriate Active Directory security logging & monitoring

Comparably small investment in new hardware and software

(2/2)

- This will _not_ require spending money for additional $Hardware & $Software

The small print:

But you will most probably need more administrative /operational resources…

That's it!

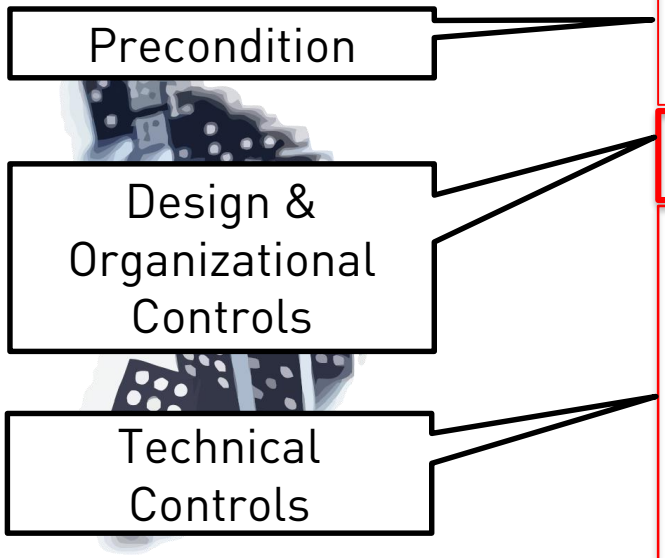
You are done ;-)

- Management will understand this?
- At least, they will understand the second slide.
  - So don't forget the small print.
- Remember what Haroon said about information asymmetry…
- Easy task?

Mitigations…

…the More Comprehensive Version ;-)

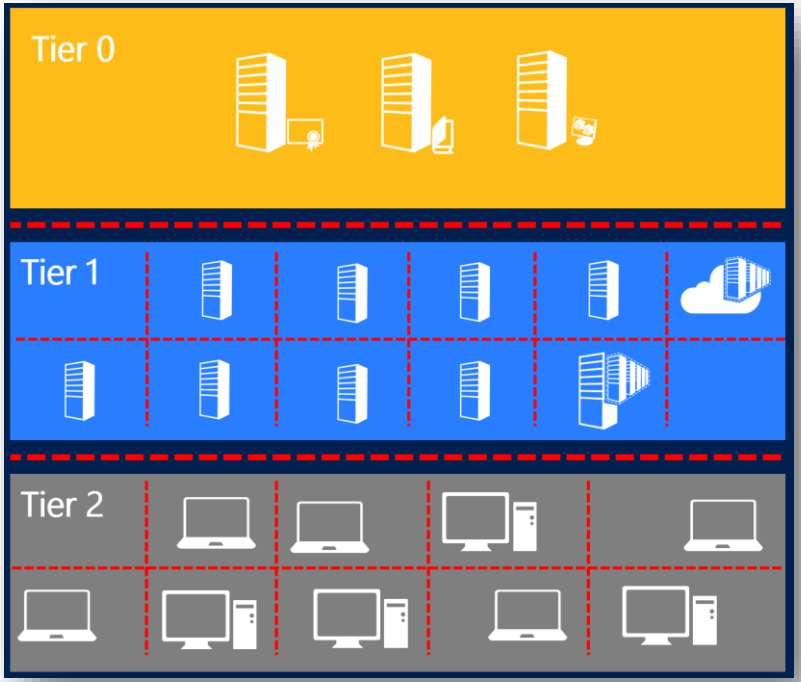
Mitigations Overview



- High level steps

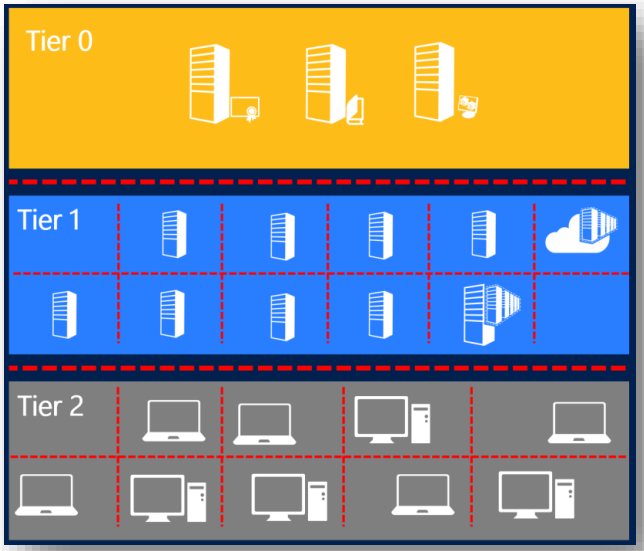
1. Identify business critical systems & applications and services
2. Have processes in place (patch mgmt & so on…)
3. Design & implement administration model & tiers
4. Implement ESAE forest
5. Implement secure Domain Controllers
6. Implement secure domain members
7. Implement MARS
8. Implement technical controls to prevent
   a. Credential theft
   b. Unauthorized credential use
9. Implement Active Directory security logging & monitoring

Design & Implement Administration Model and Tiers



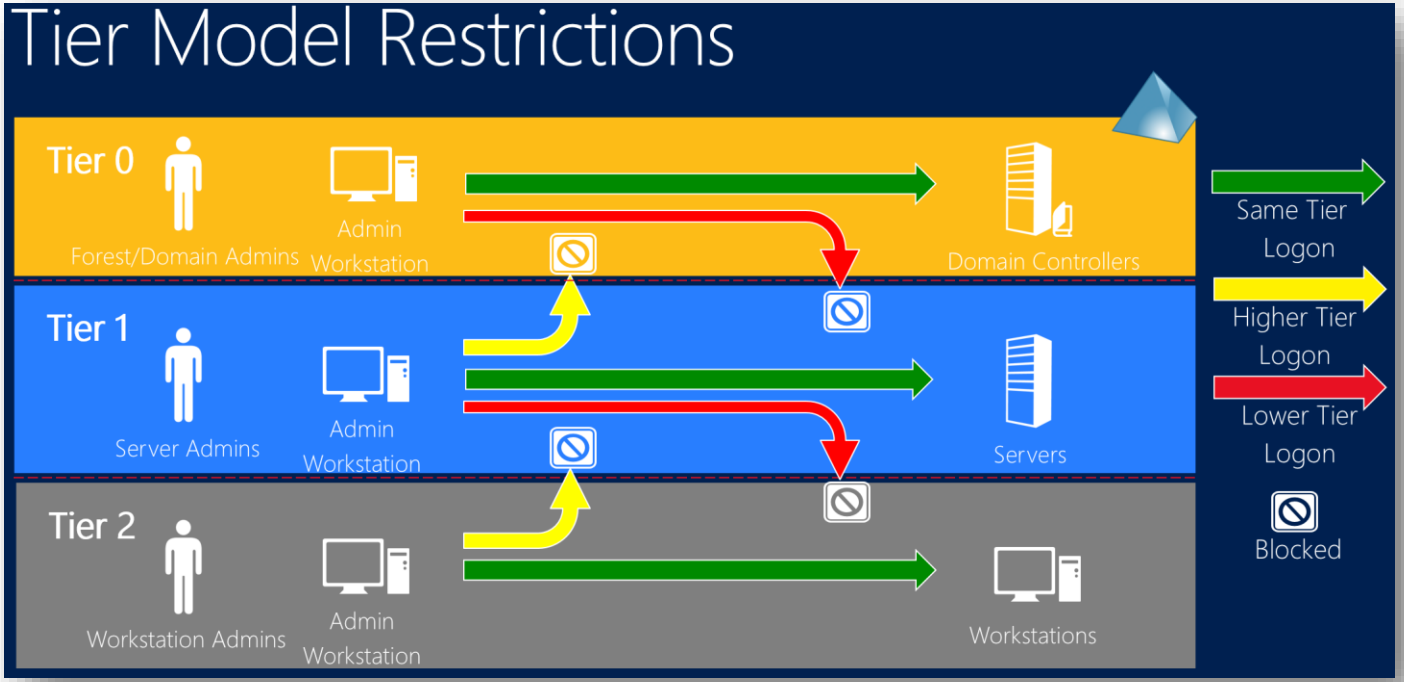
See [3]

Design & Implement Administration Model and Tiers



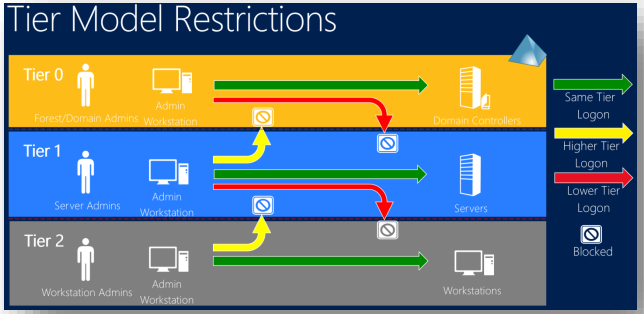
- Considerations (might be recommendations):
  - Implement at least 3 tiers
    - Domain Controllers
    - Servers with compartments between business critical services/server and other member servers
    - Clients
  - Each tier might have more than one compartment
  - **Separate internal Active Directory (forest) from DMZ Active Directory (forest)**

Design & Implement Administration Model and Tiers



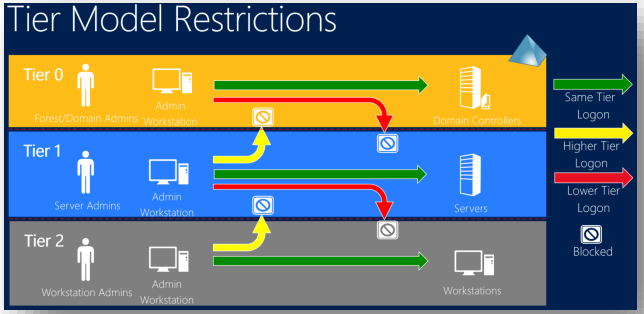
See [3]

How the Model Works



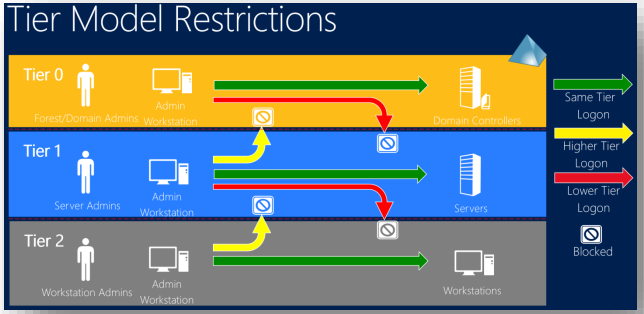
- Each administrative resource (group, account, servers, workstation, Active Directory object, or application) has to be classified as belonging to only one tier.
- Personnel with responsibilities at multiple tiers must have separate administrative accounts created for each required tier.
  - Any account that currently logs on to multiple tiers must be split into multiple accounts, each of which fits within only one tier definition.
  - These accounts must also be required to have different passwords.

How the Model Works



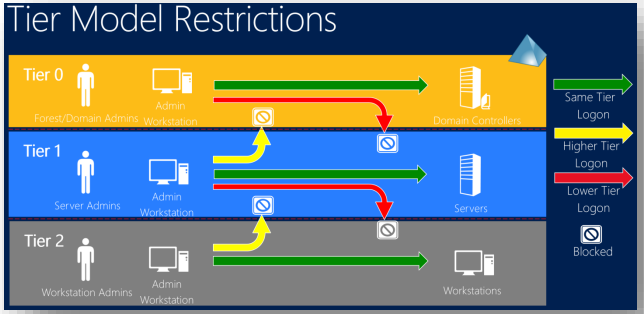
- Administrative accounts may not control higher-tier resources through administrative access. Accounts that control a higher tier may not log on to lower-tier computers.
- Administrative accounts may control lower-tier resources as required by their role, but only through management interfaces that are at the higher tier and that do not expose credentials.
  - Example: domain admin accounts (tier 0) managing server admin Active Directory account objects (tier 1) through Active Directory mmc consoles on a domain controller (tier 0).

How the Model Works



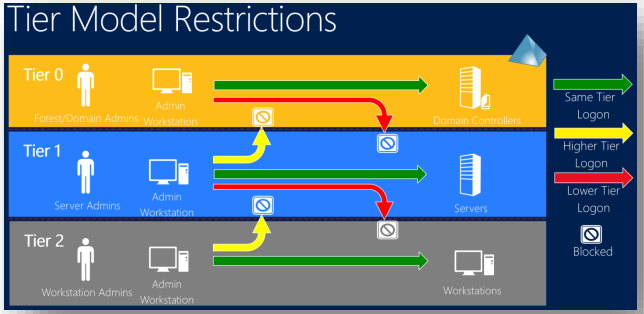
- Limit the number of administrative accounts, especially in tier 0.
  - The schema admin group should have members only on demand.
- Limit the number of hosts on which administrative credentials are exposed.
- Limit administrative role privileges to the minimum required.

How the Model Works



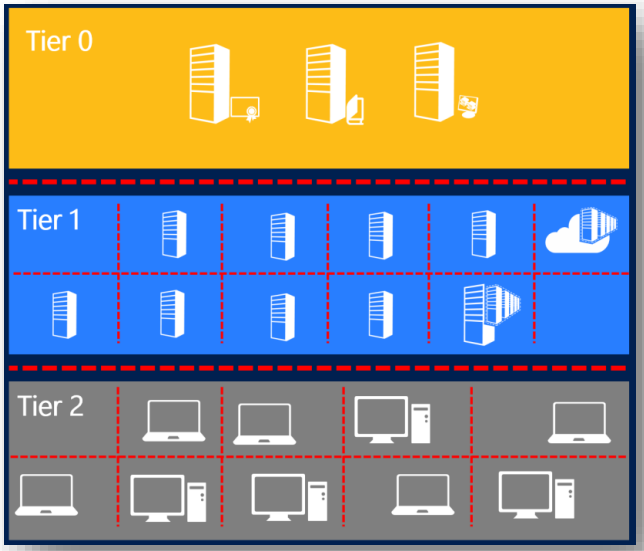
- Create a special group with the debug privilege and grant membership to this group only on demand.
  - Administrative accounts should not be member of this group by default.
- Restrict and protect high privileged domain accounts, so that:
  - Domain admins (tier 0) cannot log on to enterprise servers (tier 1) and standard user workstations (tier 2).
  - Server administrators (tier 1) cannot log on to standard user workstations (tier 2).
  - (users, computers) so that they can not be delegated

How the Model Works



- Restrict and protect local accounts with administrative privileges from being used for PtH
  - Enforce local account restrictions for remote access
  - Deny network logon to all local accounts
  - Create unique passwords for privileged local accounts or use a 3rd-party vendor solution for local account management.

A Simple Proposal…



- Define admin tiers for
  1. DCs
  2. Servers. With admin “compartments” for:
     1. Business critical systems
     2. Windows-based servers
     3. Linux/UX servers in AD
  3. Desktops /Laptops

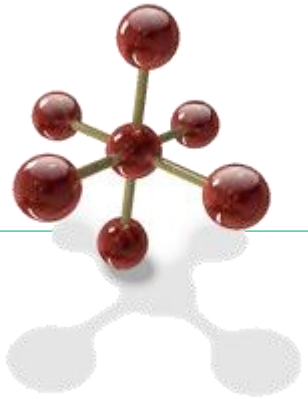
Administrative Tier Model at Your Org.

- Pre-condition
  - Re-org. of AD administration
  - Identification of business critical systems & applications
- Pro
  - Best security benefit
  - Future (Windows) administration model
- Challenges
  - Requires modification in admin mindset
  - Admins will have more accounts and hence higher operational effort
  - Services with domain admin privileges undermine admin tiering
- Alternatives
  - **none**

Build it by your own.
Don't buy it.

(Haroon Meer, Troopers 2015)

ESAE Forest

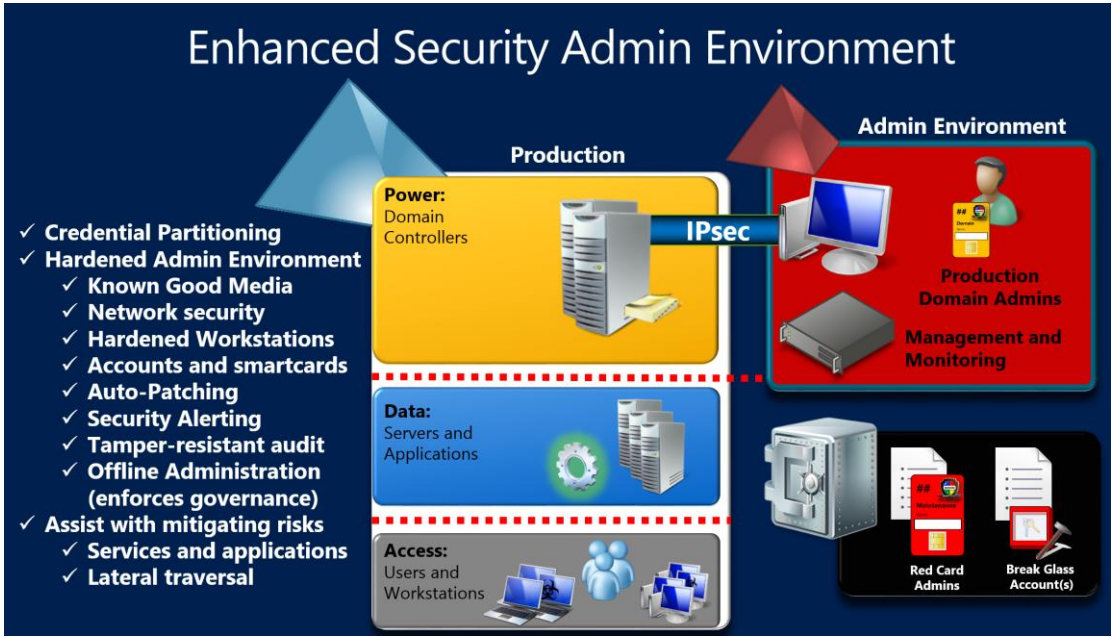


ESAE Forest

You might be willing to implement an ESAE forest.

Service offered by Microsoft.

From [5]



ESAE Forest

- Pre-condition
  - Re-org. of AD administration
  - Implementation of administrative tiers
- Pro
  - Additional layer of security for high privileged admin accounts
  - SCOM monitoring with special package for monitoring of changes of authentication packages on DCs in the production domain
- Cons
  - Supposes that the trust anchor of a forest are the Admins.
  - Does not add an additional layer of security for the KRBTGT account.
  - Adds administrative and operational complexity

Secure DCs & Domain Members

Security best practices for domain members

- Have OS _and_ application software up-to-date (patch & vulnerability management)
- I won´t speak about passwords… You know that one ;-) (but keep them long an complex anyway…)
- Have special look at service accounts
- Have UAC enabled at least at its default configuration
- Have DEP enabled & EMET deployed on as much systems as possible
  - At least on clients and DCs and IIS (Web servers)
- Have a look on additional NTFS permissions
- Implement restricted groups for privileged local accounts
- Don´t give admins by default the debug privilege

Valuable Recommendations…

…on **Service Accounts.**

Read this (https://community.rapid7.com/docs/DOC-2881).

Mitigating Service Account Credential Theft on Windows

Disclaimer

Authors

HD Moore	Joe Bialek	Ashwath Murthy
Rapid7	Microsoft	Palo Alto Networks

PtH /PtT /Golden Ticket Mitigations

PtH /PtT /Golden Ticket Mitigations

http://blogs.microsoft.com/cybertrust/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/

- There is not so much to do extra ;-)

1. Do the stuff already mentioned
   - Orga & technique
2. Reset KRBTGT account on a regular basis
3. Do Active Directory security monitoring

Overall Evaluation Table of Mitigations

Mitigation	Comment	Security Benefit	Operational Feasibility	Mitigates Cred. Theft	Mitigates Cred. Use	Mitigates Priv. Esca.	Mitigates Lat. Movement	Effective against mimikatz	Facilitates Sec. Monitoring	Must Have	Recommended
				Mitigation ≠ Prevention	Mitigation ≠ Prevention	Mitigation ≠ Prevention	Mitigation ≠ Prevention				
Admin Tiering /Credential Partitioning	**Req.1: Restrict & protect high privileged domain accounts from logon to lower tiers**: deny logon locally, deny logon as a batch job, deny log on as a service; account is sensitive and cannot be delegated. **Req.2: Restrict & protect local accounts with admin privileges from being used for PtH**: Enforce local account restrictions for remote access, Deny network logon to all local accounts, Create unique passwords for privileged local accounts.	excellent	low	no	yes	yes	yes (requires compartments within tier)	no	yes	yes	
ESAE Forest	Makes only sense together with Admin Tiering	high	medium	yes	no	yes	no	no	yes		yes
Secure Administration Hosts	Secure administration hosts are possible even without admin tiering, but full benefit requires admin tiering.	high	medium	yes	no	yes	no	no	a little bit ;-)	for DC tier	for server (& workstation tier)
Periodical KRBTGT Reset		high	Should be low, but little experience	no	yes (against existing GTs)	yes (against existing GTs)	yes (against existing GTs)	no (but restricts GT use)	yes	yes (assume breach)	

There's never enough time…

THANK YOU…

…for yours!

Disclaimer

All products, company names, brand names, trademarks and logos are the property of their respective owners!

Backup

An Overall Evaluation of Controls

For PtH/PtT/Golden Ticket-specific Attacks

Implement Technical Controls …

…to prevent credential theft & unauthorized credential use

- To be discussed or evaluated in your Org.:
  - Each control has to be evaluated with reference to:
    - Security benefit
    - Operational feasibility
    - User acceptance
- Cost estimate

PtH/PtT Specific Controls Short Version

For a 2008 R2- /Win 7-based infrastructure with DLF 2008 R2.

(Newer OS versions might be part of the domain and take advantage of some mitigations that require Server 2012 R2 /Windows 8.1)

- Implement Admin Tiering with
  - Logon restrictions for high privileged domain accounts & local accounts with admin privileges & well known SIDs
- Implement secure admin hosts
- Use remote management tools that do not place reusable creds in remote computers memory
- Implement services hardening
- Reset KRBTGT account

- Enforce credential removal after logoff
- Remove LM Hashes from LSASS
- Remove plaintext creds from LSASS for domain accounts
- LSA Protection
- Restrict debug privilege

PtH/PtT Specific Controls Short Version

For a relative homogeneous environment with:

- **Windows Server 2012 R2 & Windows 8.1**
- **DLF = Windows Server 2012 R2**

Implement additionally

- Protected Users security group
- Authentication Policy and Authentication Policy Silos

Conclusion on the Technical Controls…

…to prevent credential theft & unauthorized credential use

- Pre-condition
  - Classic DC/server/client hardening etc.
- Pro
  - Some technical controls with security benefit (e.g. logon restrictions f. privileged accounts)
- Challenges
  - Some controls require big evaluation effort (e.g. deactivation of NTLMv1) or are useless (Restricted Admin Mode for RDP)

How You Might Communicate ALL this

- With a risk analysis

&

- High level benefits summary

Risk Assessment – Current Risks Evaluated

Threat	Vulnerability (Description)	Primary Security Concern	Probability	Vulnerability	Impact	Risk
Disclosure of confidential and pii data (= personenbezogenen Daten im Sinne des BDSG) allover rated (not only a certain type of data)		C	4	4	5	80
Disclosure of arbitrary user mails	No admininistrative boundaries between DC administration, server administration and client administration	C	4	4	5	80
Disclosure of arbitrary Classified Person mails	No admininistrative boundaries between DC administration, server administration and client administration	C	4	4	5	80
Disclosure of Classified Person data (PowerPoint, Excel, Word, PDF etc.)	No admininistrative boundaries between DC administration, server administration and client administration	C	4	4	5	80
Disclosure of encrypted mails of Classified Person	No admininistrative boundaries between DC administration, server administration and client administration	C	3	4	5	60
Identity theft and use (pretend being a Classified Person via: mail, digital signature)	No admininistrative boundaries between DC administration, server administration and client administration	I	3	4	5	60
Disclosure of classified or stricktly confidential data (patents, strategy plans, finance etc.)	No admininistrative boundaries between DC administration, server administration and client administration	C	4	4	5	80

Risks Before and After Admin Tier Model + AD Hardening

Main Technical Threat	Threat	Vulnerability (Description)	Risk	Mitigated Risk
Vertical privilege escalation	Disclosure of confidential and pii data (= personenbezogenen Daten im Sinne des BDSG) allover rated (not only a certain type of data)		80	20
Vertical privilege escalation	Disclosure of arbitrary user mails	No admininistrative boundaries between DC administration, server administration and client administration	80	20
Vertical privilege escalation	Disclosure of arbitrary Classified Person mails	No admininistrative boundaries between DC administration, server administration and client administration	80	20
Vertical privilege escalation	Disclosure of Classified Person data (PowerPoint, Excel, Word, PDF etc.)	No admininistrative boundaries between DC administration, server administration and client administration	80	20
Vertical privilege escalation	Disclosure of encrypted mails of Classified Person	No admininistrative boundaries between DC administration, server administration and client administration	60	15
Vertical privilege escalation	Identity theft and use (pretend being a Classified Person via: mail, digital signature)	No admininistrative boundaries between DC administration, server administration and client administration	60	15
Vertical privilege escalation	Disclosure of classified or stricktly confidential data (patents, strategy plans, finance etc.)	No admininistrative boundaries between DC administration, server administration and client administration	80	20

Benefits

- Robust and industry standard like organization of operation:
  - Secure operation of Active Directory and business critical services
  - Sustainable operation on a long-term basis
  - Leading by example

Questions & Answers

Literature

[1] http://www.microsoft.com/en-gb/download/details.aspx?id=36036

[2] http://www.microsoft.com/en-gb/download/details.aspx?id=36036

[3] http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/DCIM-B213#fbid

[4] Microsoft Solutions for Security and Compliance. Windows Server 2003 Security Guide, 2006, *http://www.microsoft.com/en-us/download/details.aspx?id=8222*

[5] Mitigating Service Account Credential Theft on Windows, https://community.rapid7.com/docs/DOC-2881

[6] KRBTGT reset script & information: https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

[7] Protection from Kerberos Golden Ticket: http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf

Literature

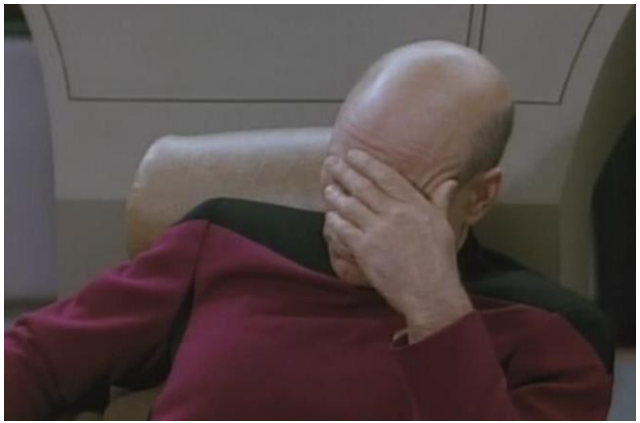
- [1]: 2014 Data Breach Investigations Report (DBIR), http://www.verizonenterprise.com/de/DBIR/

Recommendations from Microsoft

From their PtHv2 paper, see [2]

FEATURE	THEFT	USE
Logon restrictions with new well-known security identifiers (SIDs)		✓
Enforce credential removal after logoff	✓	
Remove LAN Manager (LM) hashes from LSASS	✓	
Remove plaintext credentials from LSASS for domain accounts	✓	
Restricted Admin mode for Remote Desktop	✓	
Protected Users security group	✓	
Authentication Policies and Silos	✓	✓
LSA protection-theft	✓	
Disable Automatic Restart Sign-on (ARSO) Routine	✓	

Microsoft Backpedals…



- “The default behavior for Restricted Admin mode changed in Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1. **By default, Restricted Admin mode is now turned off**, and you have to enable it again after you install update 2973351 or 2975625 if it is required. **Previously, Restricted Admin mode was turned on by default.** “

- Source: http://support.microsoft.com/de-de/kb/2975625/en-us

Mitigation against a Golden Ticket

- Recovering from a Golden Ticket is very difficult, if possible at all (because rebuilding your complete AD wouldn't be an option, right?)

Mitigation against a Golden Ticket

Reset KRBTGT's password

- Possible implications
  - TGTs get invalidated, so that:
    - End-users including smart-card users will be automatically requested to authenticate to receive a new valid ticket
    - Services and applications that require manual startup with a password and use Kerberos may stop working properly until next manual restart.
  - Requesting new TGTs may cause some load on the DC
  - The exact impact level will depend on the criticality of the related users, services and applications
  - Until now, little known experience about this, but following the right procedure, it shouldn't have a great impact.

Mitigation against a Golden Ticket

- Resetting procedure
  - Microsoft recently released a script with some additional information, see [6].
  - Detailed information is provided as well by the CERT-EU, see [7].