Sécurité des systèmes d'exploitation

Authentification

Plan

- Principes
- Méthodes courantes
- Authentification sur des systèmes Linux
- Authentification sur des systèmes Windows
- Protocoles d'authentification réseau
  - NTLM
  - Kerberos

Principes

- Définition : L'authentification est la fonction de sécurité qui consiste à apporter et à contrôler la preuve de l'identité d'une personne, de l'émetteur d'un message, d'un logiciel, d'un serveur logique ou d'un équipement.
- Différent de l'identification
  - S'identifier consiste à donner/délivrer son identité

Principes

- 3 facteurs d'authentification principaux :
  - Ce que je connais (un secret) ;
  - Ce que je possède (carte à puce, *token* USB) ;
  - Ce que je suis (biométrie).
- 4è facteur :
  - Ce que je sais faire (signature manuscrite)
    - Listé dans le Référentiel Général de Sécurité (Annexe B3) de l'ANSSI

Principes

- Il est possible de combiner plusieurs de ces principes :
  - 2FA (Two-factor authentication) ou MFA (Multi-factor authentication)
- Authentification forte
  - Au moins 2 facteurs
  - Mais pas uniquement
    - un attaquant ne doit pas pouvoir facilement contourner, tromper ou casser le procédé d'authentification

Méthodes courantes

- Authentification par mot de passe
  - Méthode simple
  - Méthode peu sûre, un mot de passe peut se partager volontairement ou involontairement
  - Qualité du mot de passe ?

Méthodes courantes

- Le stockage des mots de passe pose de nombreux problèmes en cas de vol de données
  - Par exemple, un cas récent (novembre 2015) : http://www.net-security.org/secworld.php?id=19163
- Méthodes courantes de stockage :
  - En clair
  - Chiffré
  - « Hashé »
  - « Hashé » et salé
  - A l'aide de fonctions de dérivation de clé (KDF)

Méthodes courantes

- Techniques d'attaques sur les mots de passe
  - Recherche exhaustive (*brute force*)
    - Peut utiliser des techniques probabilistes (chaînes de Markov) pour gagner en efficacité
    - Besoins de performance : utilisation de GPU ou de VM louées (Cloud)
  - Attaque par dictionnaire
    - Des transformations peuvent être opérées sur le contenu du dictionnaire
    - Il existe de nombreux dictionnaires, souvent constitués suite à des intrusions sur des sites web
      - RockYou : 32M de mots de passe

Rank	Num of Occurrences	Password
1	290729	123456
2	79076	12345
3	76789	123456789
4	59462	password
5	49952	iloveyou
6	33291	princess
7	21725	1234567
8	20901	rockyou
9	20553	12345678
10	16648	abc123

Source : Reusable Security

Méthodes courantes

- Techniques d'attaques sur les mots de passe
  - Compromis temps-mémoire
    - Le calcul en force brute est long (temps)
    - Idée : constituer un dictionnaire hash/mot de passe une seule fois et le réutiliser
      - Approche naïve : stocker les hashs associés avec les mots de passe en clair
        - Problème : taille des données générés (mémoire)
    - Compromis trouvé avec un stockage optimisé : des informations sont retirées des tables car elles peuvent être retrouvées par calcul
      - Tables de Hellman (1980)
      - *Rainbow Tables*, Oechslin (2003)
    - La préparation des tables (phase de pré-calcul) peut être longue ; il existe des tables prêtes à l'emploi

Méthodes courantes

- Lutter contre les techniques d'attaques
  - Politique de mots de passe
    - Utilisation de mots de passe complexes
      - Taille, diversités des caractères utilisés
      - Changement régulier
    - Interdire les mot de passe connus (dictionnaires)
  - Selon le canal de l'attaquant
    - En ligne ou interactif
      - Mécanisme de verrouillage après échec : limiter le nombre de tentatives
    - Hors-ligne (récupération de bases de mots de passe protégés)
      - Utilisation d'algorithmes de stockage conçu pour ralentir la recherche exhaustive : SHA512Crypt, bcrypt, PBKDF2, scrypt
        - Dernier en date, Argon2 : https://password-hashing.net/

Méthodes courantes

Estimated cost of hardware to crack a password in 1 year.

KDF	6 letters	8 letters	8 chars	10 chars	40-char text
DES CRYPT	< $1	< $1	< $1	< $1	< $1
MD5	< $1	< $1	< $1	$1.1k	$1
MD5 CRYPT	< $1	< $1	$130	$1.1M	$1.4k
PBKDF2 (100 ms)	< $1	< $1	$18k	$160M	$200k
bcrypt (95 ms)	< $1	$4	$130k	$1.2B	$1.5M
scrypt (64 ms)	< $1	$150	$4.8M	$43B	$52M
PBKDF2 (5.0 s)	< $1	$29	$920k	$8.3B	$10M
bcrypt (3.0 s)	< $1	$130	$4.3M	$39B	$47M
scrypt (3.8 s)	$900	$610k	$19B	$175T	$210B

- Estimation réalisée en 2012 par Colin Percival (auteur de scrypt)

Méthodes courantes

- Utilisation de supports physiques (facteur « ce que je possède »)
  - mémoires non sécurisées : clé USB, carte SD ;
  - mémoire sécurisée avec un microprocesseur dédié à l'authentification : carte à puce, crypto-clé USB, puce NFC (Near Field Communication), boîtier à interface sonore et/ou visuelle (émet des sons, affiche des valeurs)
    - Repose généralement sur une IGC ou des mots de passe à usage unique

Méthodes courantes

- La biométrie repose sur des phases d'apprentissage et de reconnaissance
  - constituer un modèle d'une personne donnée à partir d'un ou de plusieurs enregistrements
  - comparer le signal mesuré par le capteur biométrique avec le modèle constitué
- Problèmes principaux
  - Performance : taux de faux rejet et taux de fausse acceptation
  - Protection des données biométriques
    - Risque de détournement, falsification ou contrefaçon
    - Un usager ne pas changer ses caractéristiques

Méthodes courantes

Biometric	Accuracy	Security	Usability
Fingerprint	Medium	Low	High
Iris	High	Medium	Medium
Retina	High	High	Low
Hand Geometry	Low	Medium	Medium
Face	Medium	Medium	Medium
Voice	Low	Low	Medium

Source : Porcullis

Méthodes courantes

- Exemple de problèmes rencontrés
  - Watch a 10-Year-Old's Face Unlock His Mom's iPhone X (novembre 2017)
    - https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/
  - Support Apple
    - *The probability that a random person in the population could look at your iPhone X and unlock it using Face ID is approximately 1 in 1,000,000 (versus 1 in 50,000 for Touch ID).*
    - *The statistical probability is different for twins and siblings that look like you and among children under the age of 13, because their distinct facial features may not have fully developed. If you're concerned about this, we recommend using a passcode to authenticate.*

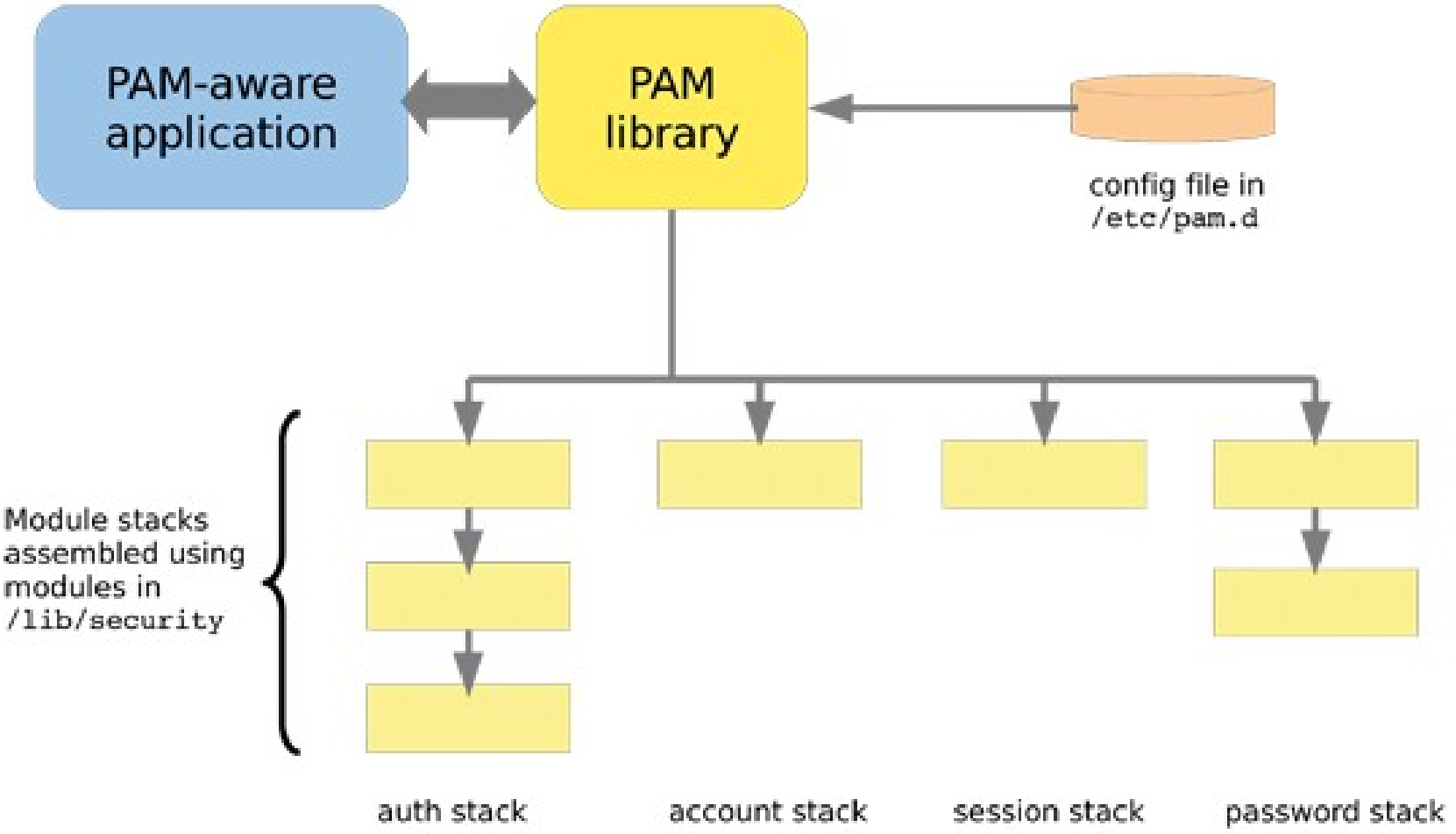
Authentification sur des systèmes Linux

- Un utilisateur est identifié par un UID (un entier)
  - La phase d'authentification permet de récupérer l'UID de l'utilisateur
- Peut être réalisée par plusieurs programmes, par ex. :
  - login
  - su
  - sshd
  - gdm, kdm, lightdm, ...
- Généralement, se traduit par la création d'un nouveau processus (par ex., un *shell*) avec l'UID de l'utilisateur authentifié

Authentification sur des systèmes Linux

- PAM (*Pluggable Authentication Modules)*
  - API générique d'ajout et de configuration de méthodes d'authentification
  - permet de définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification.
  - contrôler la manière dont les modules sont liés aux programmes en modifiant un fichier de configuration
    - configuration différente selon les programmes
- Les modules peuvent être empilés pour en utiliser plusieurs
  - MFA possible

Authentification sur des systèmes Linux



Source : TuxRadar

Authentification sur des systèmes Linux

- 4 types de modules PAM :
  - « auth », authentification réelle, par exemple en demandant et en vérifiant un mot de passe
    - définissent aussi des « certificats d'identité » tels que l'appartenance à un groupe ou des « tickets » Kerberos ;
  - « account », vérifie si l'accès est autorisé
    - compte non expiré, heure de la journée, ...
  - « password », changement des mots de passe
  - « session », mis en place d'éléments liés à la session de l'utilisateur
    - par exemple, en montant le répertoire personnel de l'utilisateur

Authentification sur des systèmes Linux

- Configuration stockée dans /etc/pam.d/
  - /etc/pam.conf est déprécié
- *Control flags*
  - *required* : échec authentification si échec du module
  - *requisite* : échec authentification si échec du module
    - Notification immédiate de l'échec
  - *sufficient* : résultat du module ignoré en cas d'échec
    - Si succès d'un module *sufficient* et qu'aucun des modules required précédents (dans la pile) n'a échoué, l'authentification réussie
  - *optional* : par défaut, résultat du module ignoré
    - Sauf s'il s'agit du seul module dans la pile

Authentification sur des systèmes Linux

- Fichier /etc/pam.d/su
  - Quel impact sur la commande su ?

```
#
# The PAM configuration file for the Shadow `su' service
#

# Maybe this line is not a good idea
auth       sufficient pam_permit.so

# This allows root to su without passwords (normal operation)
auth       sufficient pam_rootok.so

# Uncomment and edit /etc/security/time.conf if you need to set
# time restrainst on su usage.
# account    requisite  pam_time.so

# Sets up user limits according to /etc/security/limits.conf
# (Replaces the use of /etc/limits in old login)
session    required   pam_limits.so

# The standard Unix authentication modules, used with
# NIS (man nsswitch) as well as normal /etc/passwd and
# /etc/shadow entries.
@include common-auth
@include common-account
@include common-session
```

Authentification sur des systèmes Linux

- Quelques modules utiles pour la sécurité
  - Authentification
    - pam_tally2
      - Bloque l'accès après un nombre donné d'échecs
    - pam_wheel
      - Conditionne le succès à l'appartenance au groupe « wheel »
  - Qualité des mots de passe
    - pam_cracklib
      - Présence dans un dictionnaire ?
      - Critères additionels : longueur minimal, type de caractère (majuscule, minuscule, chiffre, autre) à utiliser, similarité avec le précédent, …
    - pam_passwdqc
      - Longueur minimale liée à la variété des types de caractère
      - Critères pour des phrases de passe

Authentification sur des systèmes Linux

- Les utilisateurs locaux sont définis dans le fichier /etc/passwd
  - Assure la correspondance nom/UID
  - Format des lignes : *name:password:UID:GID:GECOS:directory:shell*
    - par ex. : `util1:x:1001:1001::/home/util1:/bin/sh`
  - Le mot de passe n'est plus stocké dans ce fichier
  - Le GID désigne le groupe primaire de l'utilisateur
- UID 0 (root) désigne le super-utilisateur
  - Dispose de privilèges spéciaux
- L'attribution des UID > 0 dépend des distributions

Authentification sur des systèmes Linux

- « Mots de passe » stockés dans /etc/shadow
- 4 formats possibles (/etc/login.defs et PAM)
  - DES Crypt
    - ZIXt0E7AewSr2
  - MD5 Crypt
    - $1$0i9yM.4z$sCJbsmgAExKuAdvi9Qrp3.
  - SHA256 Crypt
    - $5$2eDph3cf$KDIGVA8NyRhV3zRs/pfdrcOdMNhU3Rj3CIGgmoHr4BB
  - SHA512 Crypt
    - 6r8.N6h/c$G/LQI25HZjjSjDLkuRtQCeLuF1A0yRxv/DjtU/KAjg84qxxOK9Q.IcDgHm7gj2wmxixgkW2wZmOabtWvbkd120

Authentification sur des systèmes Linux

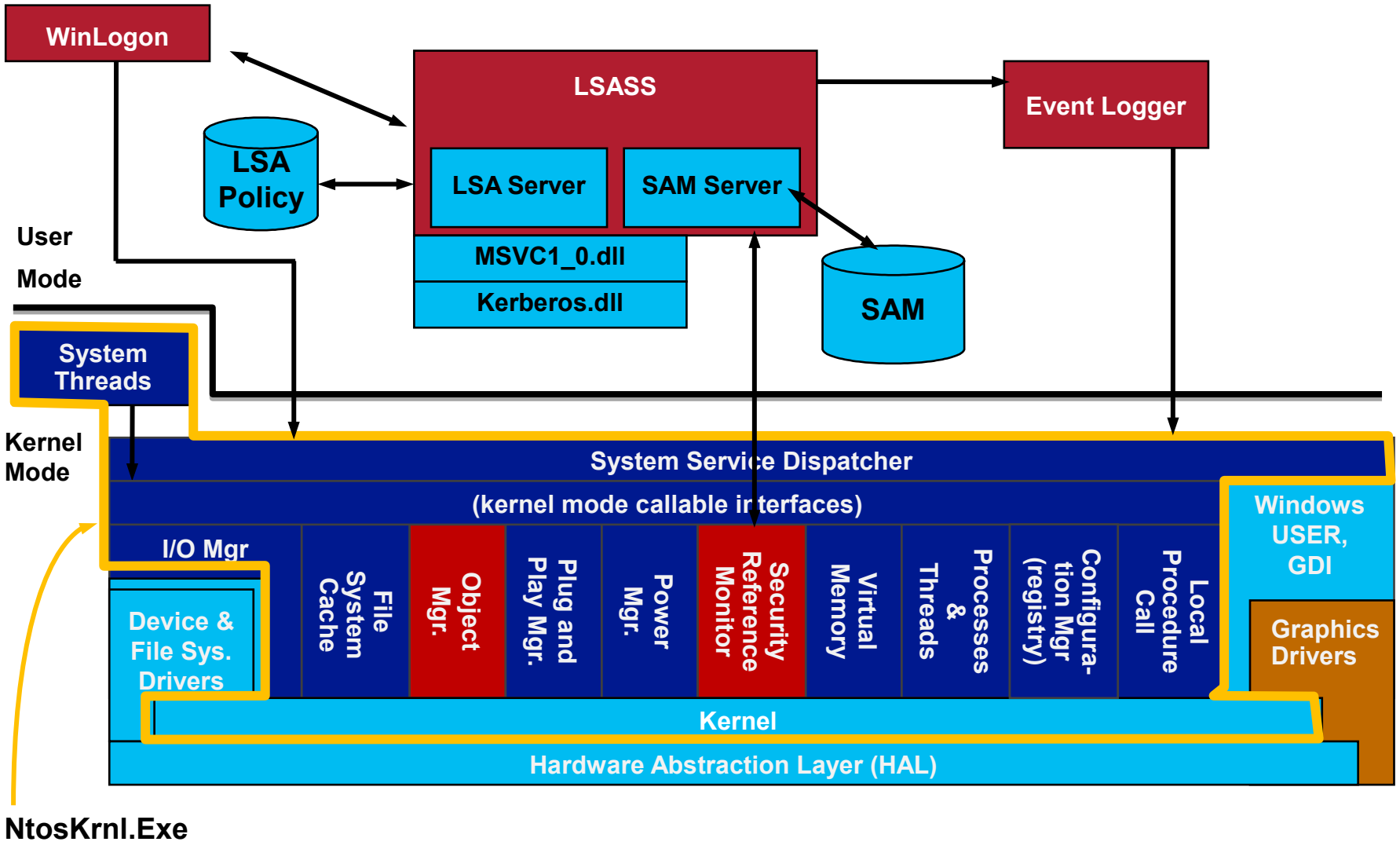
- Les utilisateurs peuvent appartenir à plusieurs groupes :
  - le groupe primaire ;
  - des groupes additionnels.
- La composition des groupes est définie par le fichier /etc/group
  - Format des lignes : group_name:password:GID:user_list
  - A noter, un groupe contient uniquement des utilisateurs

Authentification sur des systèmes Windows

- Ouverture de session
  - Le système authentifie l'utilisateur (par ex. sur la base du nom et du mot de passe) puis créer un jeton d'accès en cas de réussite
    - Implique que le compte utilisateur soit autorisé à ouvrir une session
  - Création d'un LUID (Logon Unique IDentifier).

Authentification sur des systèmes Windows

- Composants de sécurité Windows



Source : Microsoft

Authentification sur des systèmes Windows

- Le « Security reference monitor » (SRM) est un composant du noyau, en charge de :
  - définir les jetons d'accès ;
  - réaliser les contrôles d'accès sur les objets ;
  - manipuler les privilèges utilisateurs ;
  - générer des messages dans les journaux de sécurité.
- Le « Local Security Authority subsystem » (LSASS), est un processus, responsable de :
  - la politique de sécurité locale (définition des utilisateurs autorisés à se connecter, politique de mot de passe, attribution des privilèges aux utilisateurs et groupes, paramètres d'audit, …) ;
  - l'authentification des utilisateurs ;
  - générer des messages dans les journaux de sécurité.

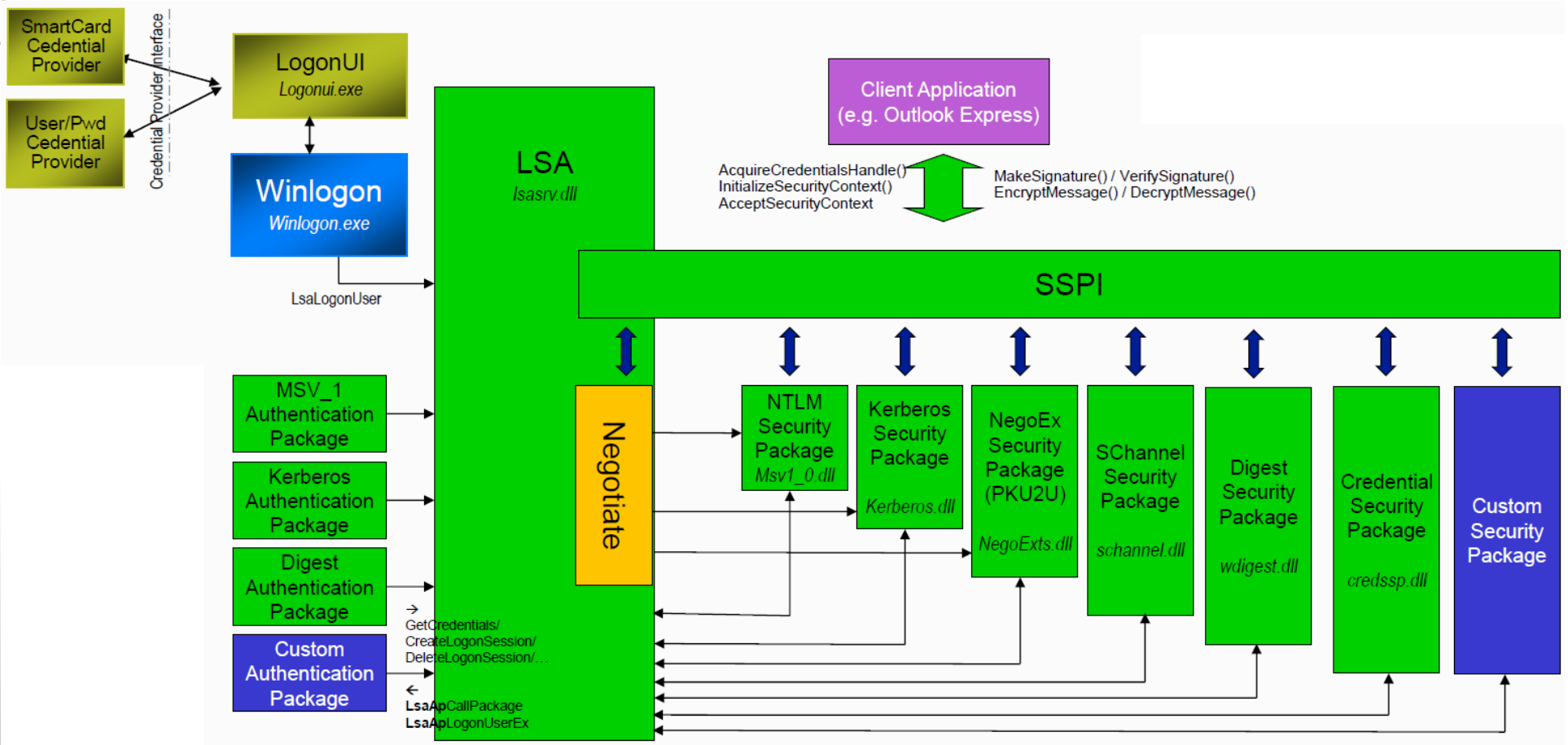
Authentification sur des systèmes Windows

- La « LSASS policy database » contient les paramètres de la politique de sécurité
  - stockée dans le registre (HKLM\SECURITY)
- Le « Security Accounts Manager » (SAM) est un service responsable de la gestion des utilisateurs et des groupes définis localement
- La base SAM contient les utilisateurs et des groupes définis localement avec leurs mots de passe et d'autres attributs
  - stockée dans le registre (HKLM\SAM)

Authentification sur des systèmes Windows

- Les *packages* d'authentification sont des bibliothèques (par ex. msv1_0.dll ou Kerberos.dll) chargées dans LSASS qui sont responsables de
  - l'authentification des utilisateurs ;
  - fournir les informations utilisées par LSASS pour générer un jeton.

Authentification sur des systèmes Windows



Source : Microsoft

Authentification sur des systèmes Windows

- L'interface SSPI (Security Support Provider Interface) réalise l'abstraction du processus d'authentification client/serveur
  - Agnostique vis-à-vis de la couche réseau
    - Délivre des jetons opaques (différents des jetons d'accès)
  - Permet
    - D'établir l'identité de l'autre partie, sous réserve que le protocole d'authentification le supporte
    - Établie une clé de session partagée qui peut être utilisée par la couche application

Authentification sur des systèmes Windows

- Identifiant de sécurité (SID)
  - S-1-5-21-211353117-160123419-83662341-500

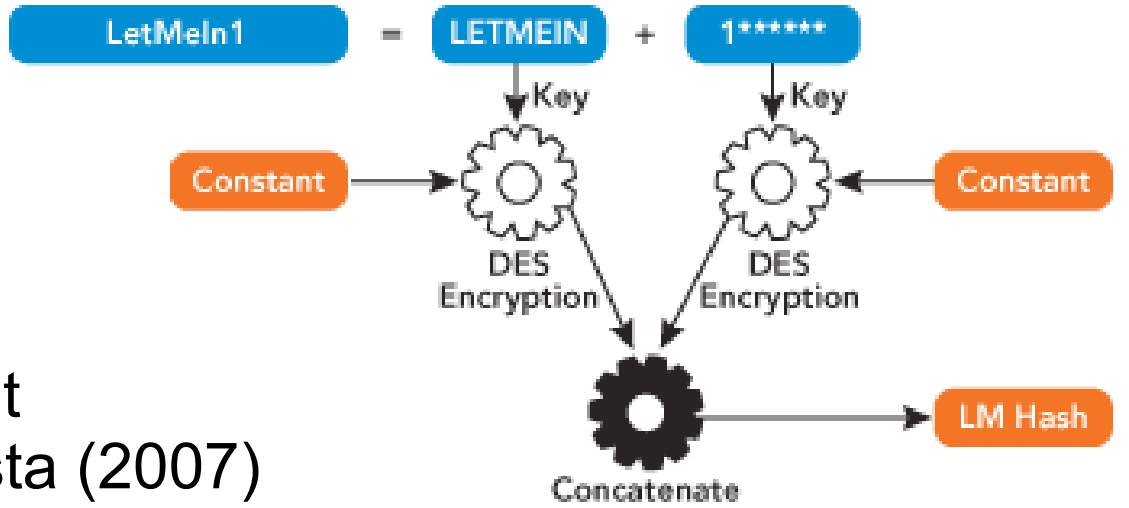
  - 5 est la valeur d'identifiant-autorité (ici SECURITY_NT_AUTHORITY)
  - L'identifiant d'autorité désigne une machine (ou un domaine Windows)
  - Le RID (Relative IDentifier) désigne un utilisateur ou un groupe de la machine (ou du domaine)
    - La valeur 500 est attribuée au compte d'administrateur initial
    - Les nouveaux utilisateurs ou groupes commencent à 1000

Authentification sur des systèmes Windows

- Il existe des SID pré-établis, par ex.
  - S-1-1-0 : groupe *Everyone*
  - S-1-5-11: groupe *Authenticated Users*
  - S-1-5-18 : compte *Local System*
  - S-1-5-32-544: groupe *Administrators*
- Consulter le SID de l'utilisateur et ceux des groupes dont il est membre
  - whoami /all

Authentification sur des systèmes Windows

- La base SAM stocke les mots de passe dans 2 formats
  - Hash LM (LAN Manager)
    - Utilisation du chiffrement DES
    - Mot de passe limité à 14 caractères (*)
    - Désactivé par défaut depuis Windows Vista (2007) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa : NoLmHash = 0x1



  - Hash NTLM (NT LAN Manager)
    - MD4(UnicodePassword)
    - Mot de passe limité à 127 caractères

Authentification sur des systèmes Windows

- Les hashs LM et NTLM ne sont ni salés, ni conçu pour ralentir une attaque exhaustive
- Syskey
  - Surchiffrement RC4 des hash LM et NTLM avec une clé de 128 bits qui peut être :
    - Stockée sur un support amovible ou sur le disque (!)
    - Dérivée d'un mot de passe saisie au démarrage
    - Stockée dans le registre dans la ruche HKLM\SECURITY
  - Protection peu efficace => depuis Windows 10 1709, l'utilitaire syskey.exe a été retiré du système
    - La base SAM est néanmoins chiffrée avec la clé stockée dans le registre

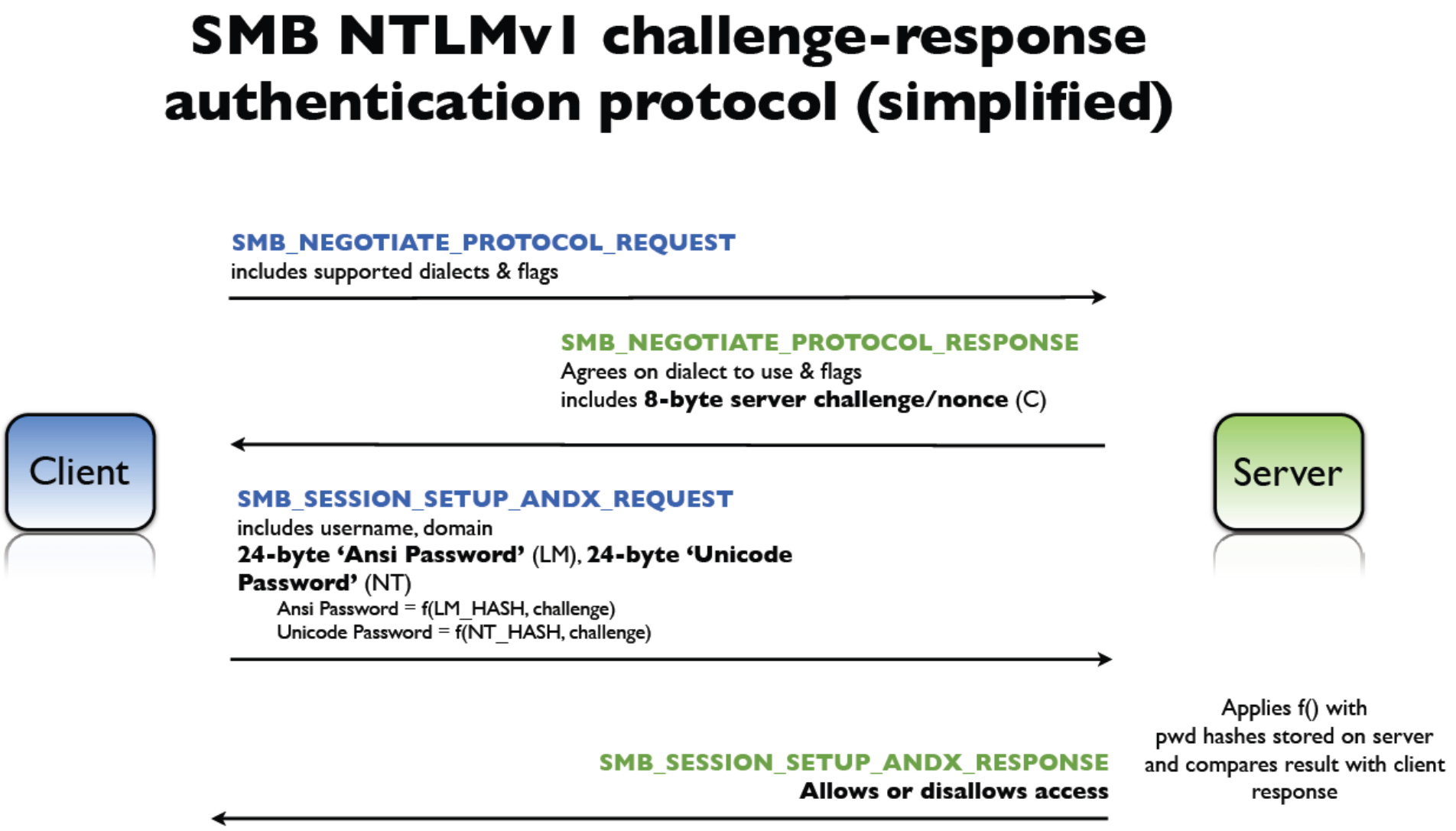
Protocoles d'authentification réseau

- Cas d'usage
  - Ouverture de session à l'aide d'une base d'utilisateur délocalisée sur des serveurs
  - Accès à des ressources sur une machine distante
- Protocoles étudiés
  - NTLM : natif Windows, supporté sur les systèmes Linux avec SAMBA
  - Kerberos : natif depuis Windows 2000, supporté sur les systèmes Linux (MIT Kerberos ou Heimdall)

Protocoles d'authentification réseau

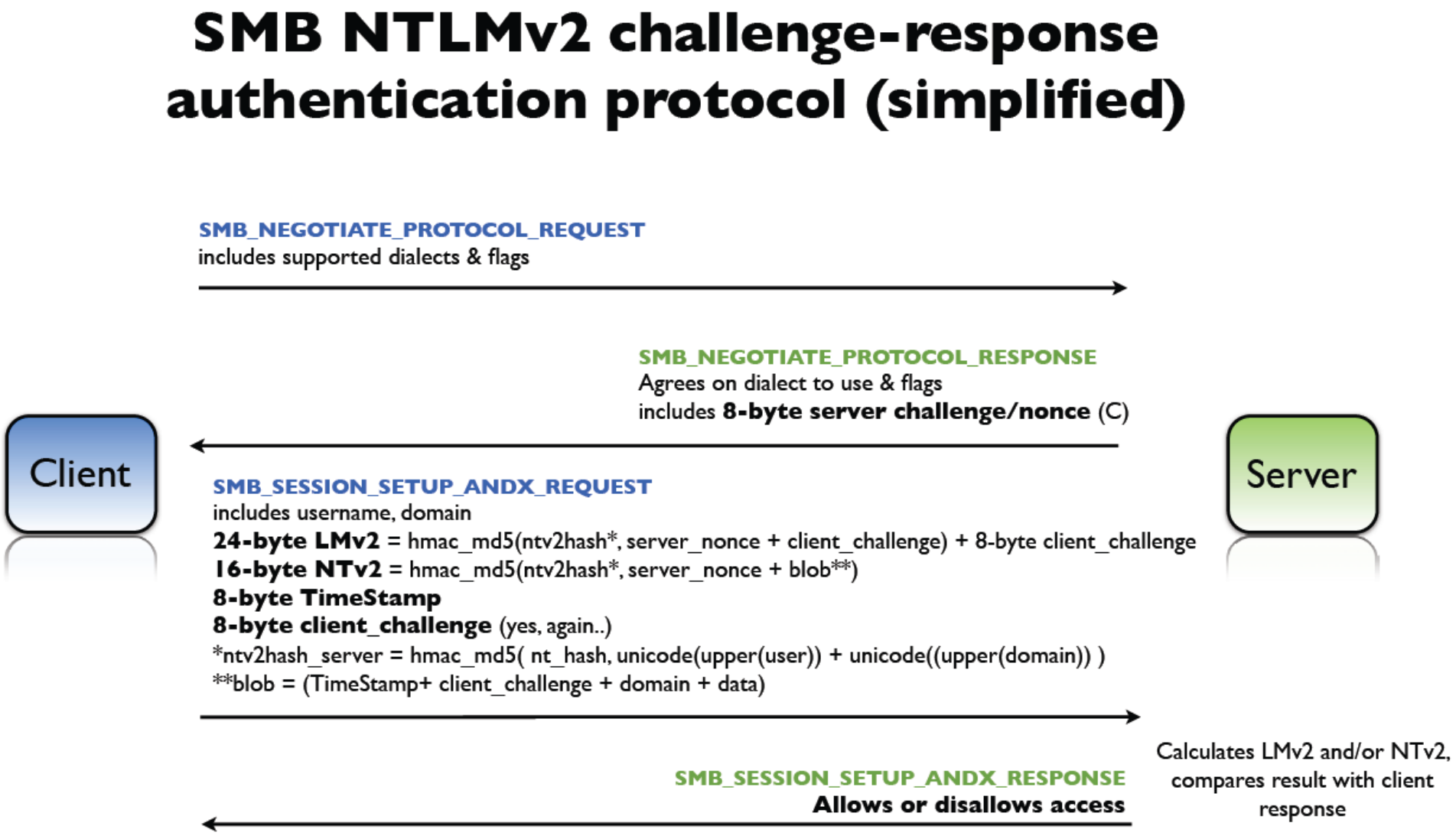
- NTLM est un protocole de type défi/réponse
  - Repose sur l'existence d'un secret partagé, le hash du mot de passe de l'utilisateur
- Évolution du protocole LM
  - Utilisation du hash NTLM au lieu du hash LM
- Dernière version majeure : NTLMv2 (1998)
- Attaque Pass-The-Hash
  - L'authentification nécessite la connaissance du hash, pas du mot de passe

Protocoles d'authentification réseau



Source : Amplia Security

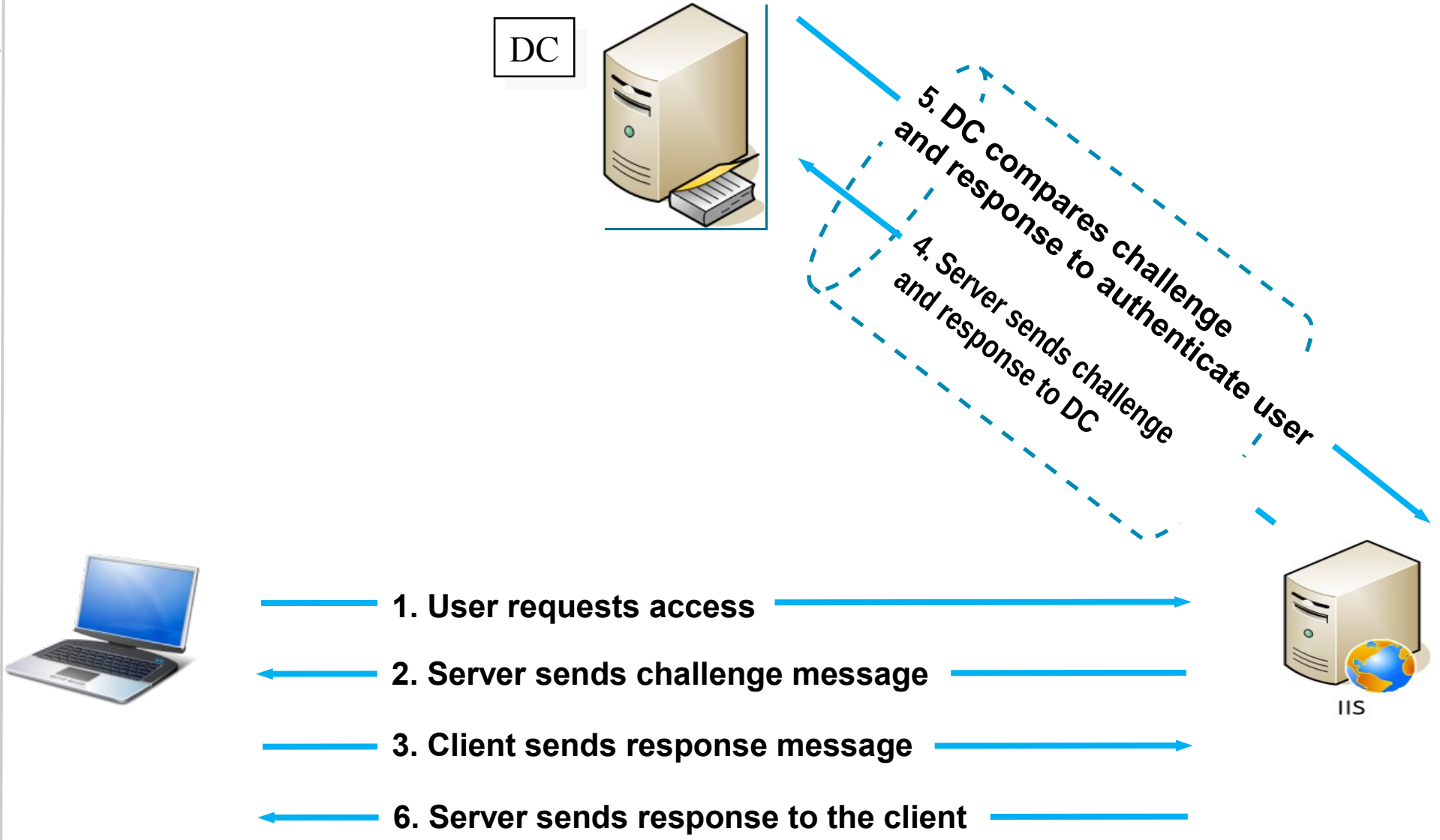
Protocoles d'authentification réseau



Source : Amplia Security

Protocoles d'authentification réseau

- Mécanisme de SSO (*Single Sign-On*)



Protocoles d'authentification réseau

- Kerberos
  - Développé par le MIT dans les années 80 au sein du projet Athena
  - Version 5 publiée en 1993 (RFC1510)
    - Spécification à jour RFC4120 (2005)
  - Conçu pour fonctionner sur un réseau non sûr
  - Repose sur une tierce partie de confiance
  - Utilisation d'algorithmes de chiffrement symétrique
- Basé sur 3 composants : un client, un serveur et une autorité auxquels les 2 font confiance, le KDC (*Key Distribution Center*)

Protocoles d'authentification réseau

- Un utilisateur, un client, un serveur sont des « principaux » Kerberos, il en existe 2 types :
  - UPN (User Principal Name)
    - user@realm.test
  - SPN (Service Principal Name)
    - CIFS/FS1@REALM.TEST
- Un « royaume » Kerberos :
  - est une organisation logique composée d'un ensemble de machines
    - Dans le monde Windows, on parle de domaine et le rôle de KDC est porté par un « contrôleur de domaine »
  - est capable d'authentifier les principaux déclarés sur ses KDC

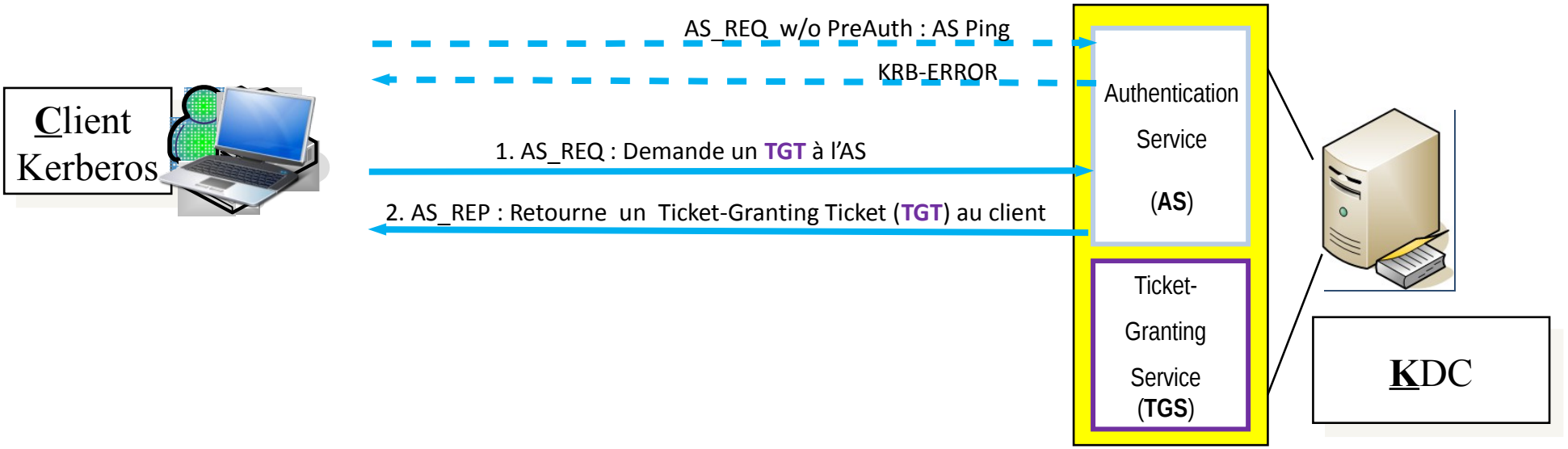
Protocoles d'authentification réseau

- Notion de ticket
  - Un ticket est une structure de données constituée d'une partie chiffrée et d'une partie claire.
  - Les tickets servent à authentifier les requêtes des principaux
  - Deux type de tickets :
    - *Ticket Granting Ticket* (TGT)
    - *Service Ticket* (ST)
  - Les tickets sont « signés » par le KDC
    - Les TGT sont également chiffrés par le KDC
      - Dans le monde Windows, le hash d'un compte spécial nommé krbtgt est utilisé comme clé secrète du KDC
  - Les tickets ont une durée de vie limitée

Protocoles d'authentification réseau

- Service Kerberos
  - Deux types de services sont requis :
    - *Authentication Service* (AS)
    - *Ticket Granting Service* (TGS)
- Le KDC génère des secrets partagés à partir des hashs des mots de passe
  - Clés de sessions pour les échanges de tickets
- Authentification mutuelle
  - Le client présente un ticket du KDC que le serveur peut déchiffrer avec sa clé privée
  - Le serveur renvoie des informations que le client peut déchiffrer

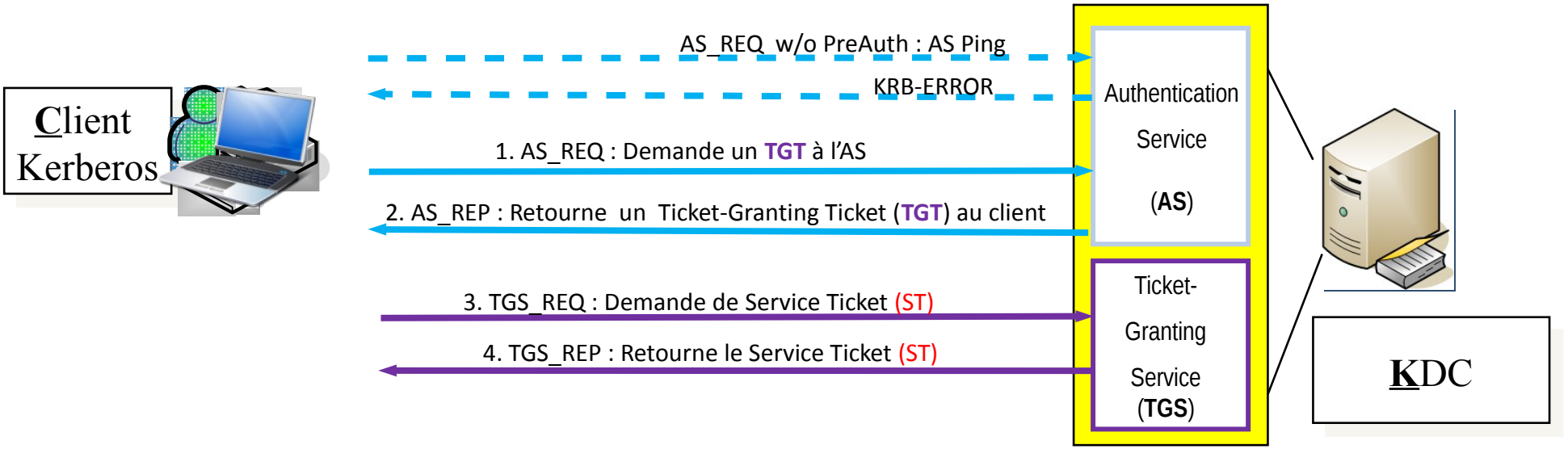
Protocoles d'authentification réseau



1. Le client calcule le hash du mot de passe utilisateur (secret partagé entre le client et l'AS) et utilise ce hash comme clé pour chiffrer une estampille temporelle (*timestamp*)
→ la fourniture de l'estampille temporelle est imposée par la phase de pré-authentification

2. L'AS déchiffre l'estampille temporelle. Si celle-ci est correcte, cela démontre que le client connaît bien le mot de passe de l'utilisateur.
L'AS renvoie alors une clé de session (client/KDC) et le TGT chiffrés avec une clé connue du TGS

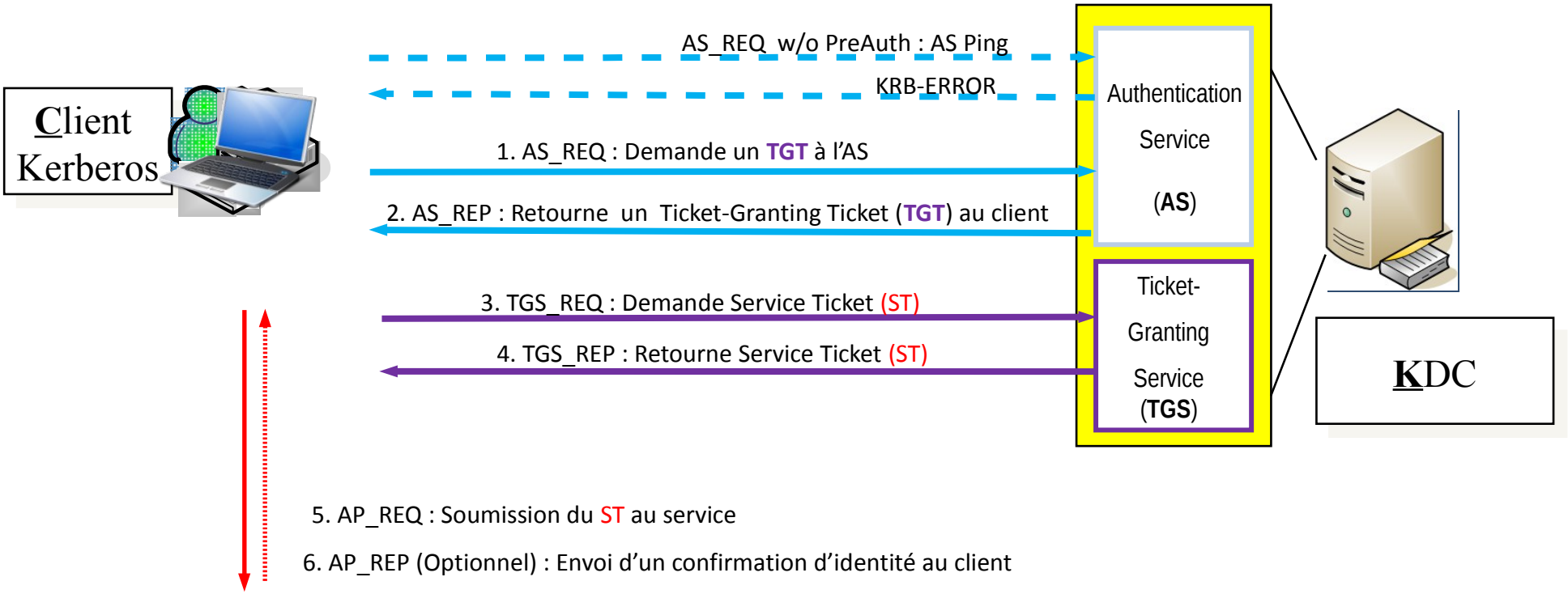
Protocoles d'authentification réseau



3. Le client construit une requête ciblant un principal particulier (ici le serveur IIS) en utilisant la clé de session (client/KDC). Le client envoie sa requête, accompagnée du TGT, au TGS.

4. Le TGS décode le TGT et la requête. Si celle-ci est approuvée, le TGS génère une réponse contenant 2 parties :
- une partie pour le serveur (le ST), chiffrée avec la clé secrète du serveur, contenant des informations sur le client
- une partie pour le client, chiffrée avec la clé de session (client/KDC), contenant une clé de session (client/serveur)

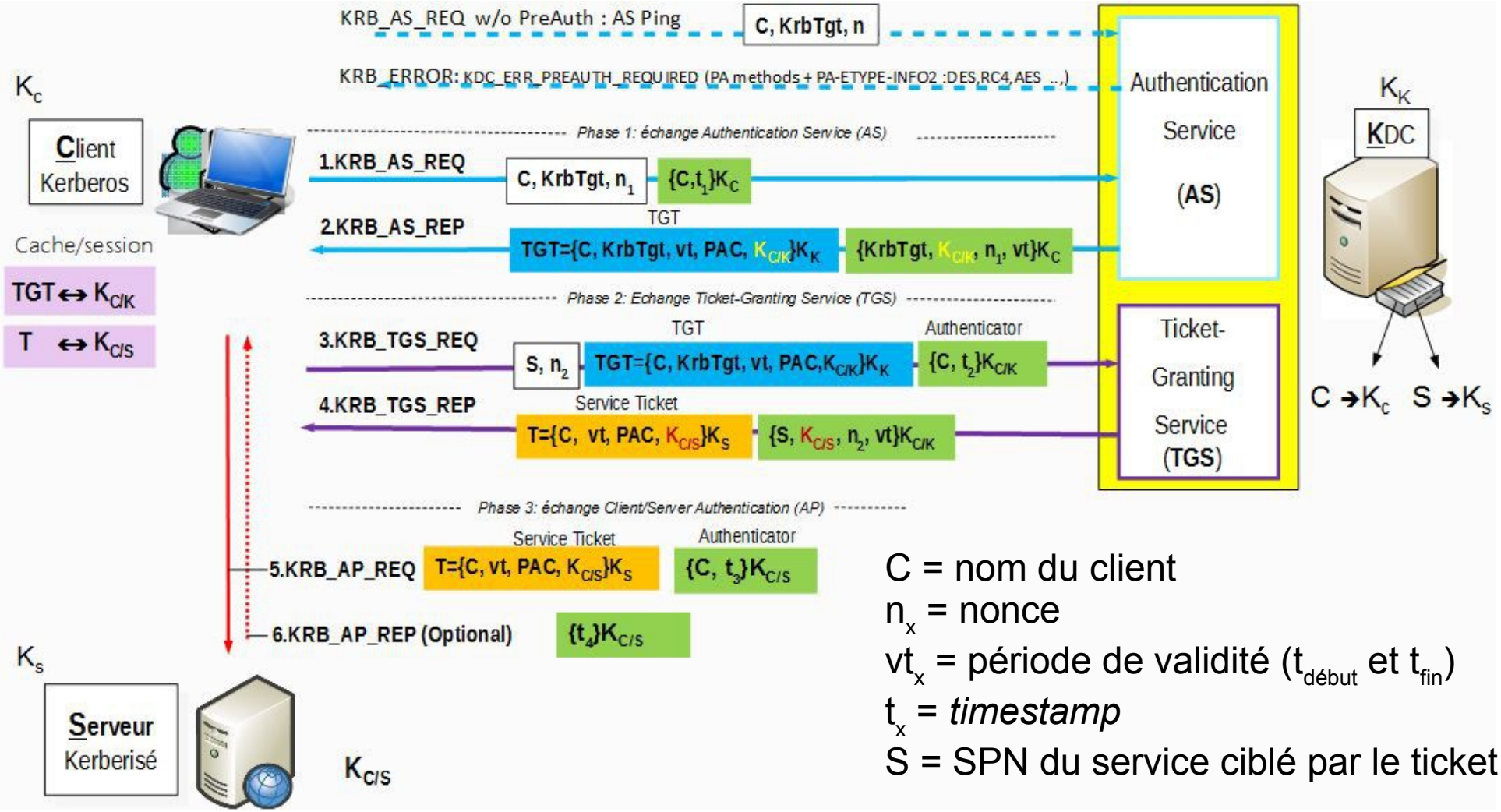
Protocoles d'authentification réseau



5. Le client envoie sa requête, accompagnée du ST, au serveur.

Le serveur accepte le ticket de service sans communication directe avec le KDC puisque le ST est chiffré avec sa clé secrète du serveur.

Protocoles d'authentification réseau



C = nom du client
n_x = nonce
vt_x = période de validité ($t_{début}$ et t_{fin})
t_x = *timestamp*
S = SPN du service ciblé par le ticket

K_C = clé secrète du client
K_S = clé secrète du service
K_K = clé secrète du KDC
$K_{C/K}$ = clé de session Client/KDC
$K_{C/S}$ = clé de session Client/Service

PAC = Privilege Attribute Certificate (champ spécifique à l'implémentation Microsoft)

KrbTgt = SPN du TGS (nom codé en dur dans l'implémentation Microsoft)

Protocoles d'authentification réseau

- Chiffrement supporté par défaut dans l'implémentation Microsoft
  - Des-cbc-crc → déprécié par la RFC6649 !
  - des-cbc-md5 → déprécié par la RFC6649 !
  - rc4-hmac
    - L'utilisation de RC4 a été introduite par Microsoft pour utiliser le hash NTLM (128 bit) comme clé secrète
      - Un attaquant qui peut faire une attaque Pass-The-Hash NTLM peut aussi s'authentifier avec Kerberos !
  - rc4-hmac-exp → déprécié par la RFC6649 !
  - aes128-cts-hmac-sha1-96 et aes256-cts-hmac-sha1-96
    - Clé secrète = PBKDF2(motdepasse)

Protocoles d'authentification réseau

- Quelques attaques sur Kerberos
  - Golden Ticket
    - Forgeage d'un TGT sans passer par la phase d'authentification (KRB_AS_REQ & KRB_AS_REP)
      - Généralement avec l'UPN d'un compte à privilèges
    - Permet de s'adresser à un TGS pour obtenir des ST
    - Nécessite d'avoir la clé secrète du TGS (par ex., le hash NTLM du compte krbtgt pour un KDC Microsoft)
  - Pass-The-Ticket
    - Nécessite d'avoir la clé de session $K_{C/K}$ et le TGT du client (sous Windows, peut se faire avec Mimikatz)
    - Permet de s'adresser à un TGS pour obtenir des ST

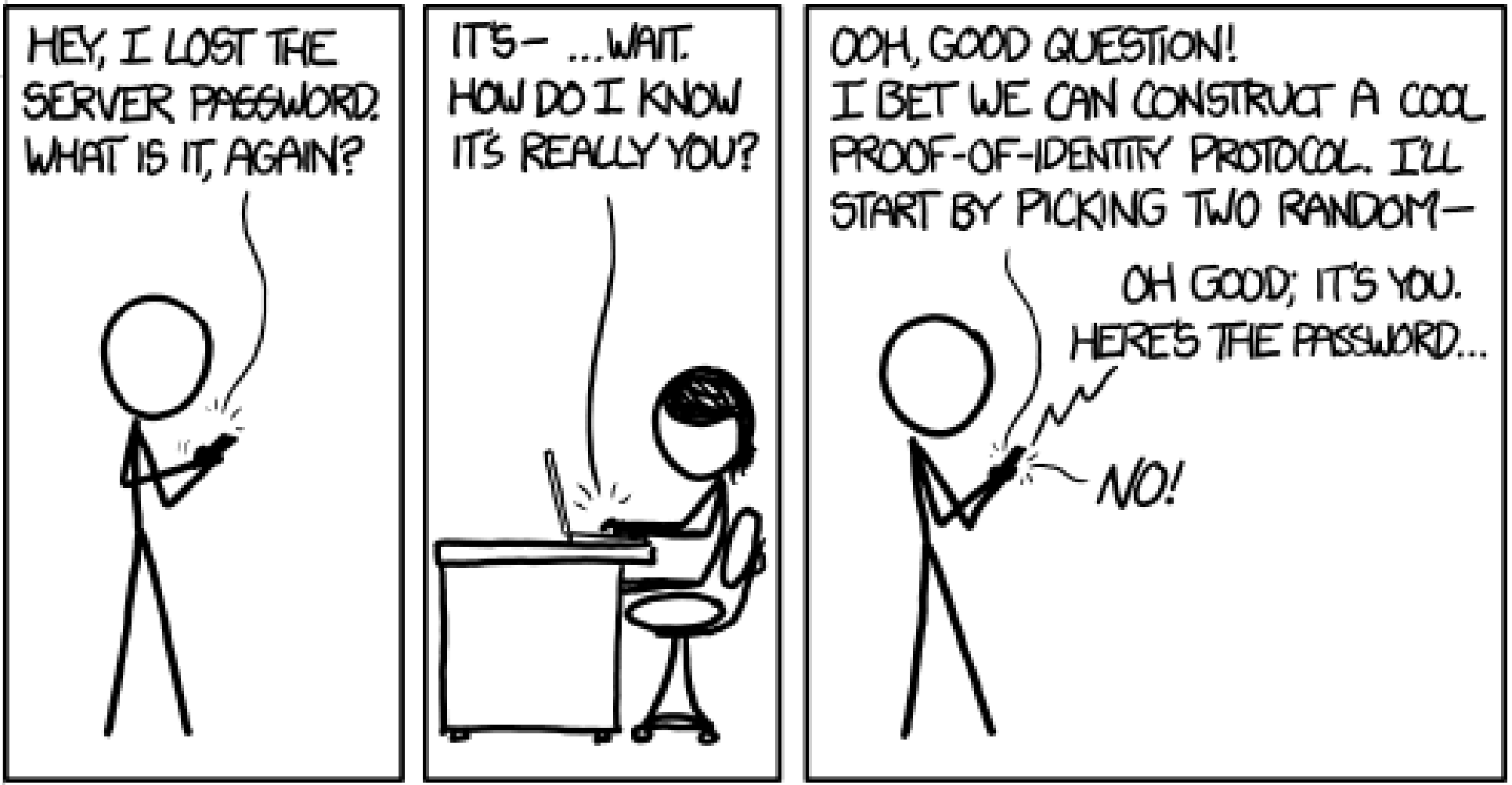
Protocoles d'authentification réseau

- attaques sur Kerberos (suite)
  - Silver Ticket
    - Forgeage d'un ticket TGS valide pour un service sur un serveur donné
      - Permet d'obtenir des ST pour se connecter à ce service
    - Nécessite d'avoir le *hash* d'un compte de service configuré avec un SPN
      - Ce *hash* correspond à K_S
    - Spécifique Microsoft
      - le PAC décrit des informations de sécurité (utilisées pour créer le jeton d'accès) comme l'appartenance aux groupes
      - la plupart des services ne vérifie pas l'intégrité du PAC auprès du KDC
      - le PAC peut être forgé pour réaliser une élévation de privilèges sur le serveur ciblé (appartenance à un groupe privilégié)

Pour aller plus loin

- Password Security: past, present, future, Openwall, Passwords^12
- NIST Special Publication 800-63B, Digital Identity Guidelines : Authentication and Lifecycle Management
- Secrets d'authentification épisode II : Kerberos contre-attaque, Aurélien Bordes, SSTIC 2014
- Red vs. Blue: Modern Active Directory Attacks, Detection, and Protection, Sean Metcalf, Black Hat USA 2015

Questions ?


HEY, I LOST THE SERVER PASSWORD. WHAT IS IT, AGAIN?
IT'S— ...WAIT. HOW DO I KNOW IT'S REALLY YOU?
OOH, GOOD QUESTION! I BET WE CAN CONSTRUCT A COOL PROOF-OF-IDENTITY PROTOCOL. I'LL START BY PICKING TWO RANDOM—
OH GOOD; IT'S YOU. HERE'S THE PASSWORD...
NO!