Module de confiance de plate-forme

[Trusted Platform Module (TPM)]

Attaque; réparation; vérification

Mark D. Ryan
HP Labs, Bristol, UK *(invité)*
University of Birmingham, UK

Liqun Chen
HP Labs, Bristol, UK

Grenoble, mai 2009

Plan

- Informatique de confiance
  - Le passé controversé
  - La situation actuelle (TCG/TPM, et TCM)
- Le module de confiance de plate-forme [Trusted platform module (TPM)]
- Des détails techniques, et des défauts
  - Questions au sujet des mots de passe faibles.
  - Questions concernant le partage des mots de passe.
- Réparation des défauts, et la vérification de la réparation.

Informatique de confiance

- L'idée est que le matériel a des capacités protégés, qui peuvent être invoqués à distance.
  - Ces capacités ne peuvent pas être contournées par le propriétaire / utilisateur.
  - Le matériel a des clés cryptographiques, qui sont hors de contrôle de l'utilisateur.

Informatique déloyale

[Treacherous computing]

“Avec un plan qu'elles appellent informatique de confiance, les grandes sociétés de médias, en collaboration avec des sociétés informatiques telles que Microsoft et Intel, prévoient que votre ordinateur les obéisse, au lieu de vous obéir.”

L'intimidation commerciale, la guerre économique, et la censure politique

- “TC peut permettre la censure à distance . Dans sa forme la plus simple, les applications peuvent être conçues de manière à supprimer à distance le piratage de musique.

- “En mai 2010, le président Clinton aura deux boutons rouges sur son bureau – un qui envoie des missiles à la Chine, et l'autre qui permet de désactiver tous les ordinateurs en Chine.

Le *Trusted Computing Group*

- Un consortium industriel, comprenant
  - Microsoft, HP, Dell, Sony, Lenovo, Toshiba, Vodafone, Seagate, . . .
  - (environ 160 organisations au total)

- Le principal résultat est la spécification du TPM
  - La spécification est ***disponible au public***
  - Le TPM est un ***dispositif passif*** (il ne contrôle ni interdit quoi que ce soit; il accomplit des actions seulement si on lui demande)
  - Il a pour mandat d'être ***opt-in***, non opt-out
  - Il inclut des fonctionnalités permettant de respecter ***la vie privée***

TC peut fournir la sécurity et le *privacy*

L'anonymisation assistée par TPM

- Google n'aura pas ton adresse IP (et c'est plus éfficace que TOR)

TPM-supported p2p network

- TPMs help ensure honesty of other participants, without compromising privacy

TPMs in ticketing systems

No privacy

- Les TPMs du coté serveur aident a assurer conformité aux politiques securité-privé sur les données des passagers

Cloud computing

- ???

\end{speculation}

Le Module de Confiance de Plate-forme
[Trusted Platform Module, TPM]

- Une puce actuellement inclue dans 100M portables
  - HP, Dell, Sony, Lenovo, Toshiba . . .
  - Soldered onto the motherboard, on the LPC bus
  - HP tout seul vend 1M portables par mois avec TPM
- Spécifié par le *Trusted Computing Group*
  - Un consortium industriel comprenant Intel, HP, Microsoft, AMD, IBM, Sun, Lenovo. . . . et 130 autres
- Plusieurs fabricants
  - Atmel, Broadcom, Infineon, Sinosun, STMicroelectronics, and Winbond
- Supporting software to be rolled out over the next few years
  - MS BitLocker is the only mainstream application so far

Les fonctionalités du TPM

Le stockage sécurisé

- Creation des clés RSA (avec la partie privée connue seulement par le TPM)
- Chiffrement et déchiffrement des donnés avec ces clés

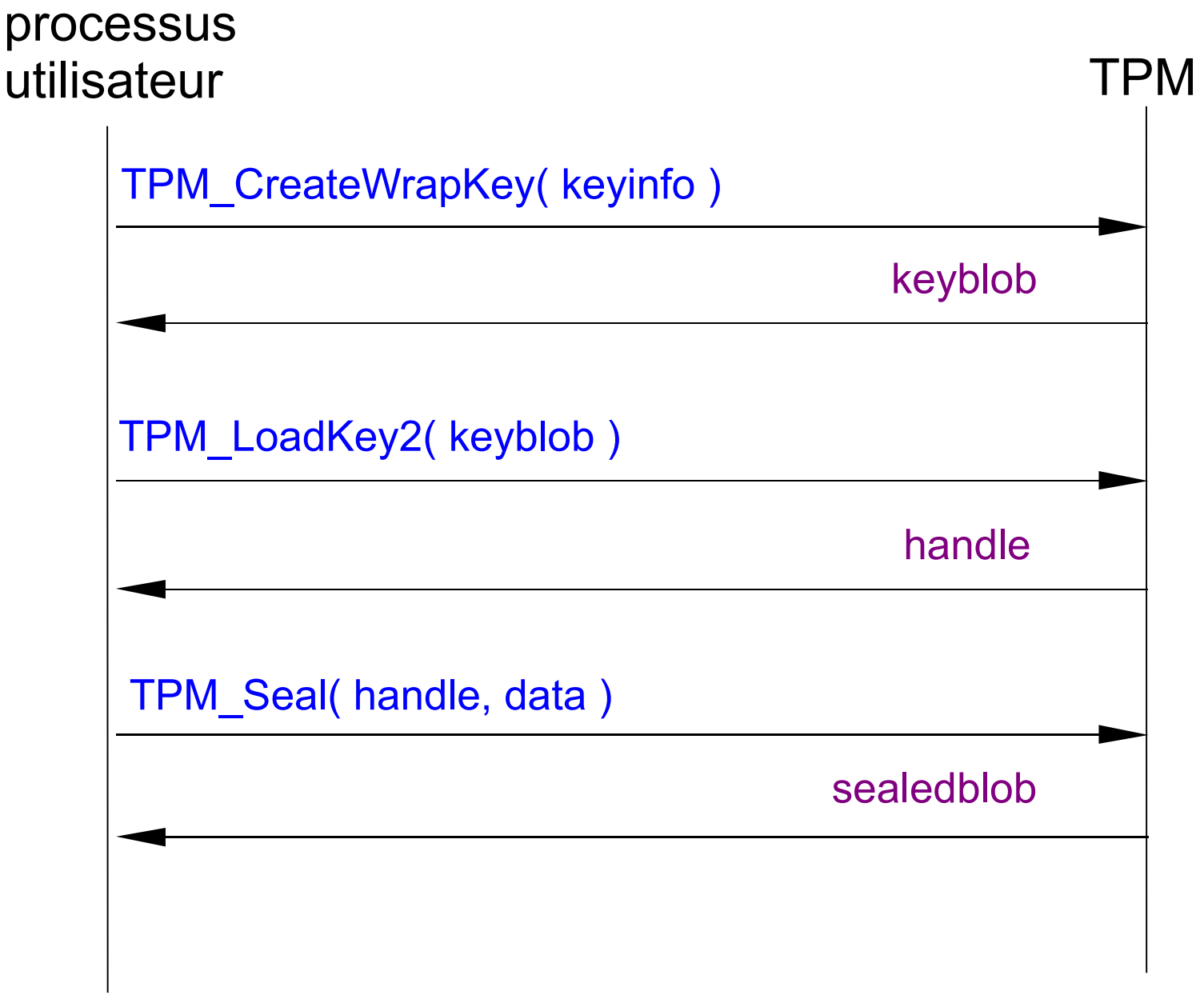
Le rapport d'intégrité de la plate-forme

- “Mesure” et rapport d'intégrité de la plate-forme; peut inclure la mesure du BIOS, du MBR du disque, du secteur de boot, du système d'exploitation, et du logiciel d'application.

L'authentification de la plate-forme

- Creation of *attestation identity keys (AIK)*, with anonymity guarantees (DAA)

Flux des commandes du TPM



Les mots de passe du TPM
[TPM authData]

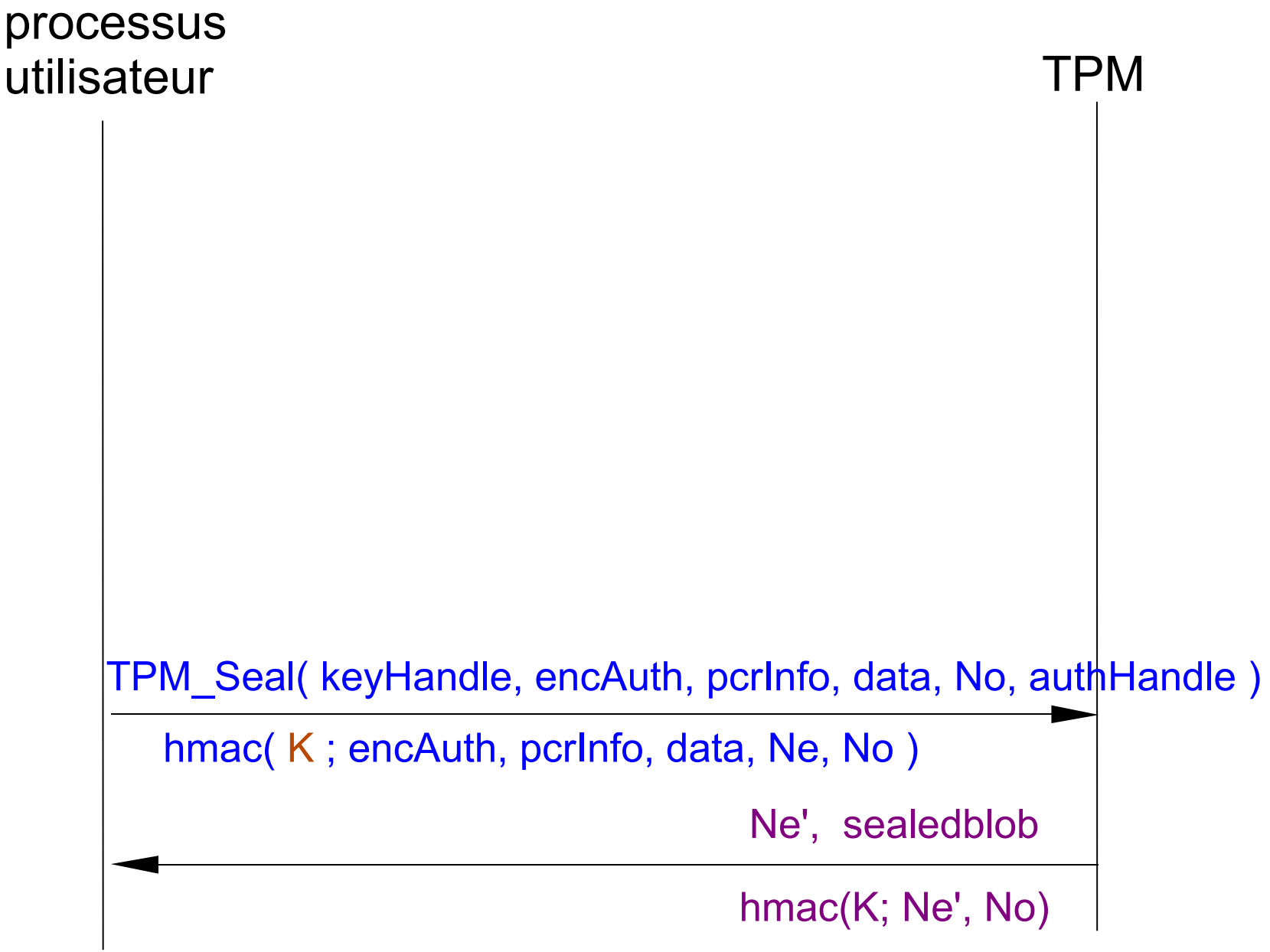
- Pour chaque objet ou ressource du TPM, on associe une valeur authData
  - Un secret de 160 bits partagé entre l'utilisateur et TPM
  - On peut y penser comme un mot de passe qui doit être cité à l'utilisation de l'objet ou de la ressource

Bank card PINs are examples only weak secrets. The ATM allows ona small number of incorrect guesses.

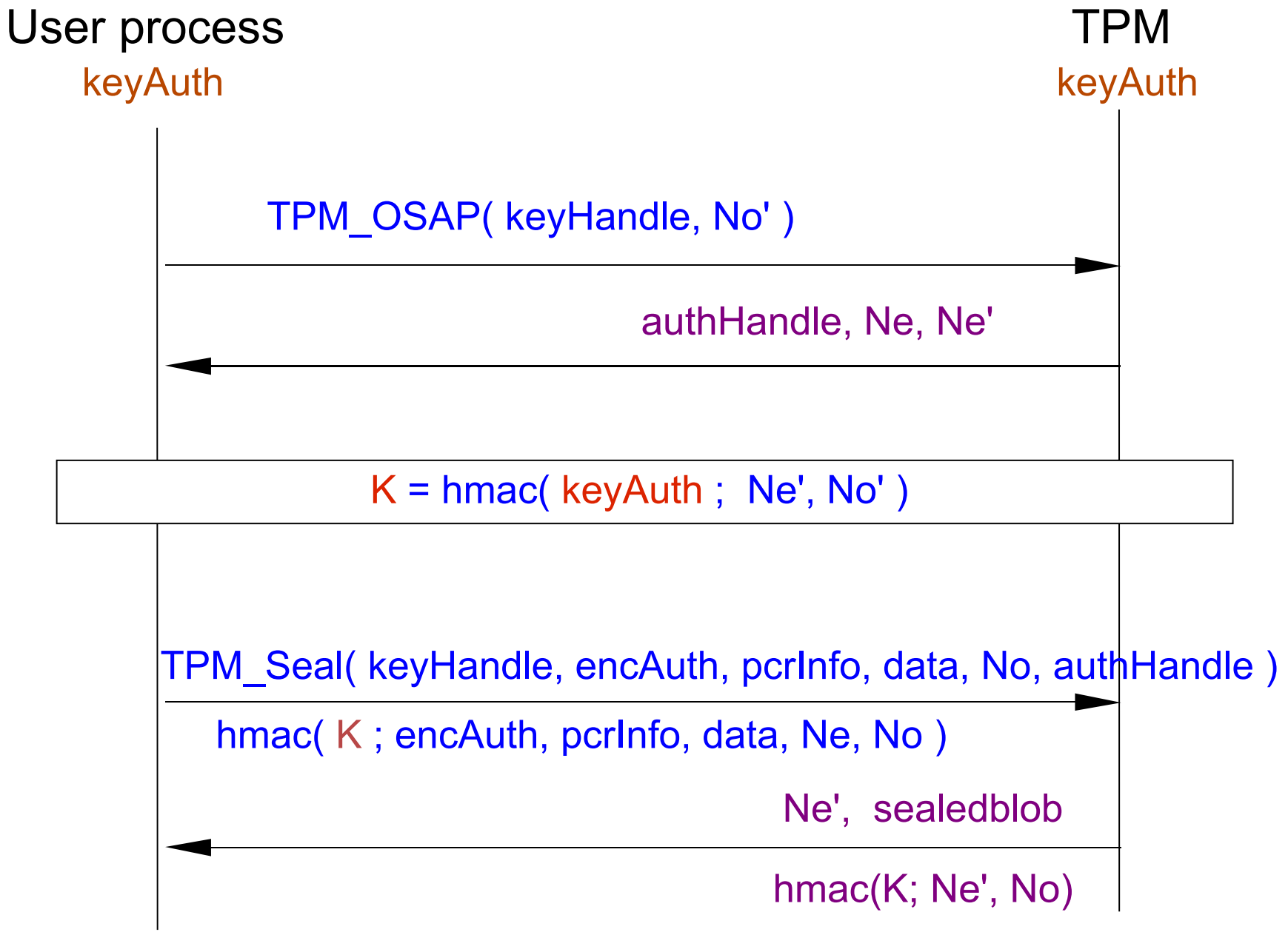
- Le authData peut être un secret faible
  - E.g., basé sur un mot de passe connu par l'utilisateur; e.g. Microsoft Bitlocker.
- Le TPM résiste aux attaques par dictionnaire en ligne; il refuse les utilisateurs qui font de nombreuses erreurs.
  - Les détails sont laissés au fabricant

Problème 1:
Le authdata faible

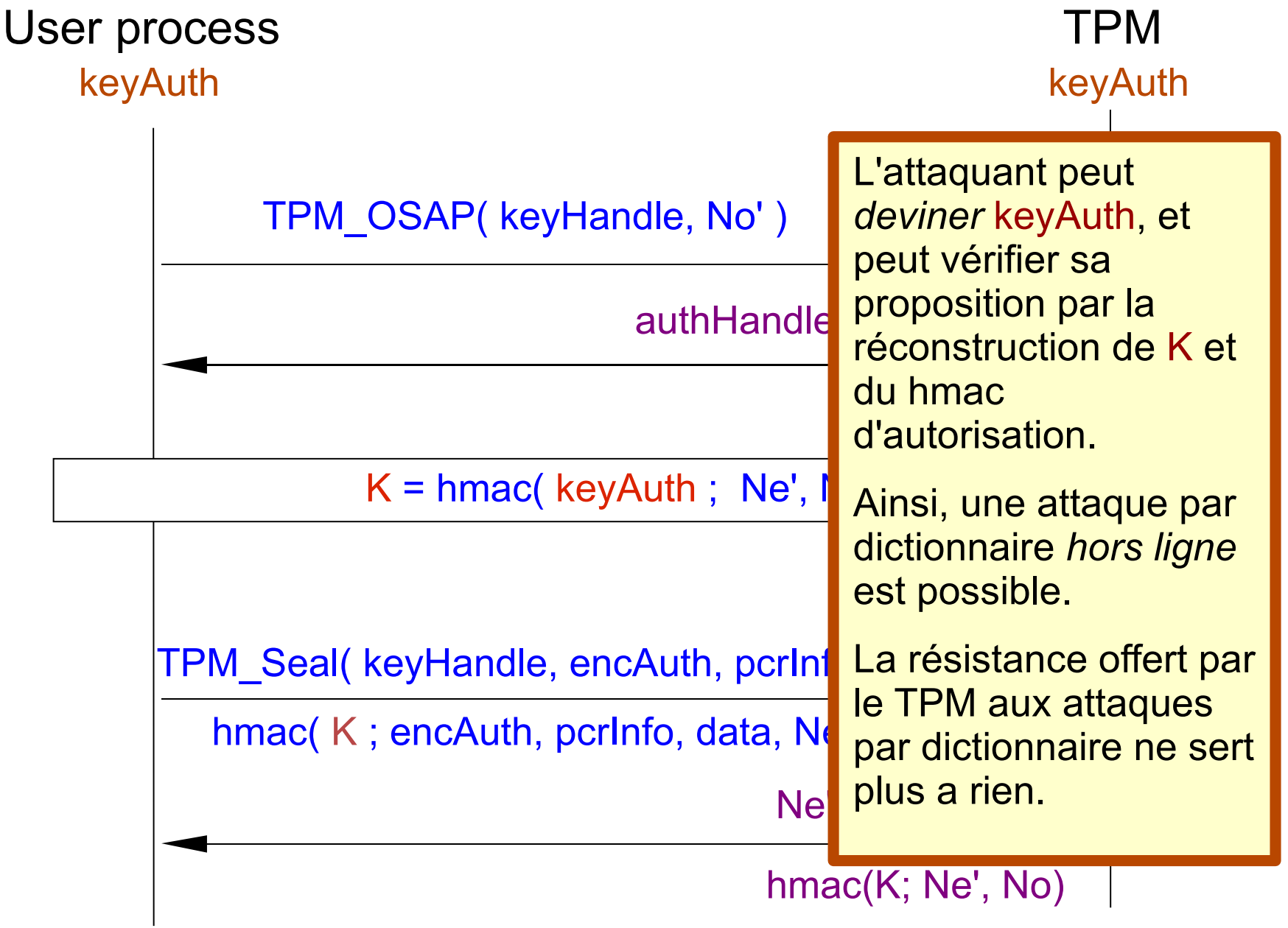
TPM_Seal


processus
utilisateur
TPM
TPM_Seal(keyHandle, encAuth, pcrInfo, data, No, authHandle)
hmac(K ; encAuth, pcrInfo, data, Ne, No)
Ne', sealedblob
hmac(K; Ne', No)

TPM_Seal en plus de détail



Le authdata faible: l'attaque



Conséquences

- L'authdata compromis implique que l'attaquant peut usurper l'identité d'un utilisateur légitime
  - E.g., le propriétaire du TPM
- L'authdata compromis implique que l'attaquant peut usurper l'identité du TPM
  - E.g.,, l'attaquant peut créer sa propre clé, et peut forger la réponse du TPM à la commande TPM_CreateWrapKey. Ainsi, l'utilisateur va chiffrer ses données avec la clé de l'attaquant.

Des scénarios pour l'attaque de l'authdata faible

Carte à puce

- L'authdata est stocké sur une carte à puce, qui fournit les HMACs d'autorisation à la demande du logiciel de l'utilisateur

L'utilisation à distance du TPM

- Le TPM d'une plate-forme est accedé a distance, e.g., par sysAdmin.
- L'utilisateur de la plate-forme peut lancer l'attaque par dictionnaire sur l'authdata du sysAdmin.

Le TPM dans un serveur

- Les clients se servent de la fonctionalité du TPM installé sur un serveur.
- Le propriétaire du serveur peut lancer l'attaque sur l'authdata des clients.

Les sessions transports chiffrées
[Encrypted transport sessions]

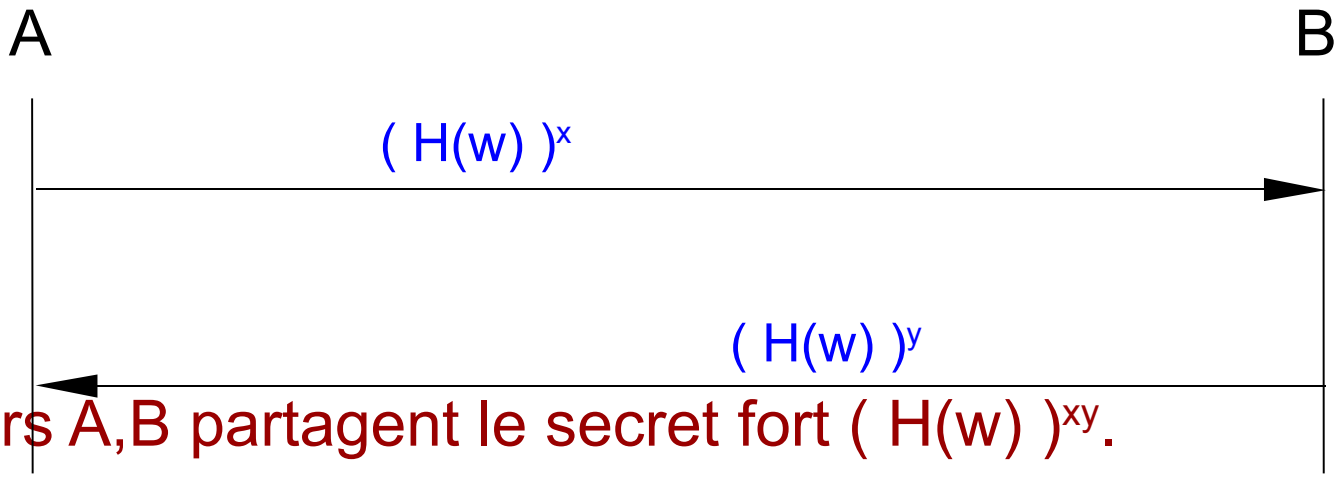
- TPM supports a notion of *encrypted transport session*
  - Commands are wrapped, and *some* of the data parameters are encrypted
- Unfortunately, the high-entropy values (rolling nonces) are not encrypted! They are still sent in plaintext.
- Encrypted transport sessions make guessing attacks a bit harder (a few more low-entropy values to guess), but do not solve it.

Solution pour éviter l'attaque sur l'authdata faible

- Objectifs
  - Éviter les attaques de dictionnaire hors ligne
  - Continuer à permettre la possibilité de l'authData faible
  - Changer la spécification du TPM aussi peu que possible
    - minimiser les modifications au structure des commandes
    - minimiser le besoin de memoire supplementaire dans le TPM
    - minimiser les exigences computationelles supplémentaires
- Idée
  - Etablir un secret de session fort à partir du authdata faible, et se servir du secret fort pour authentifier les commandes

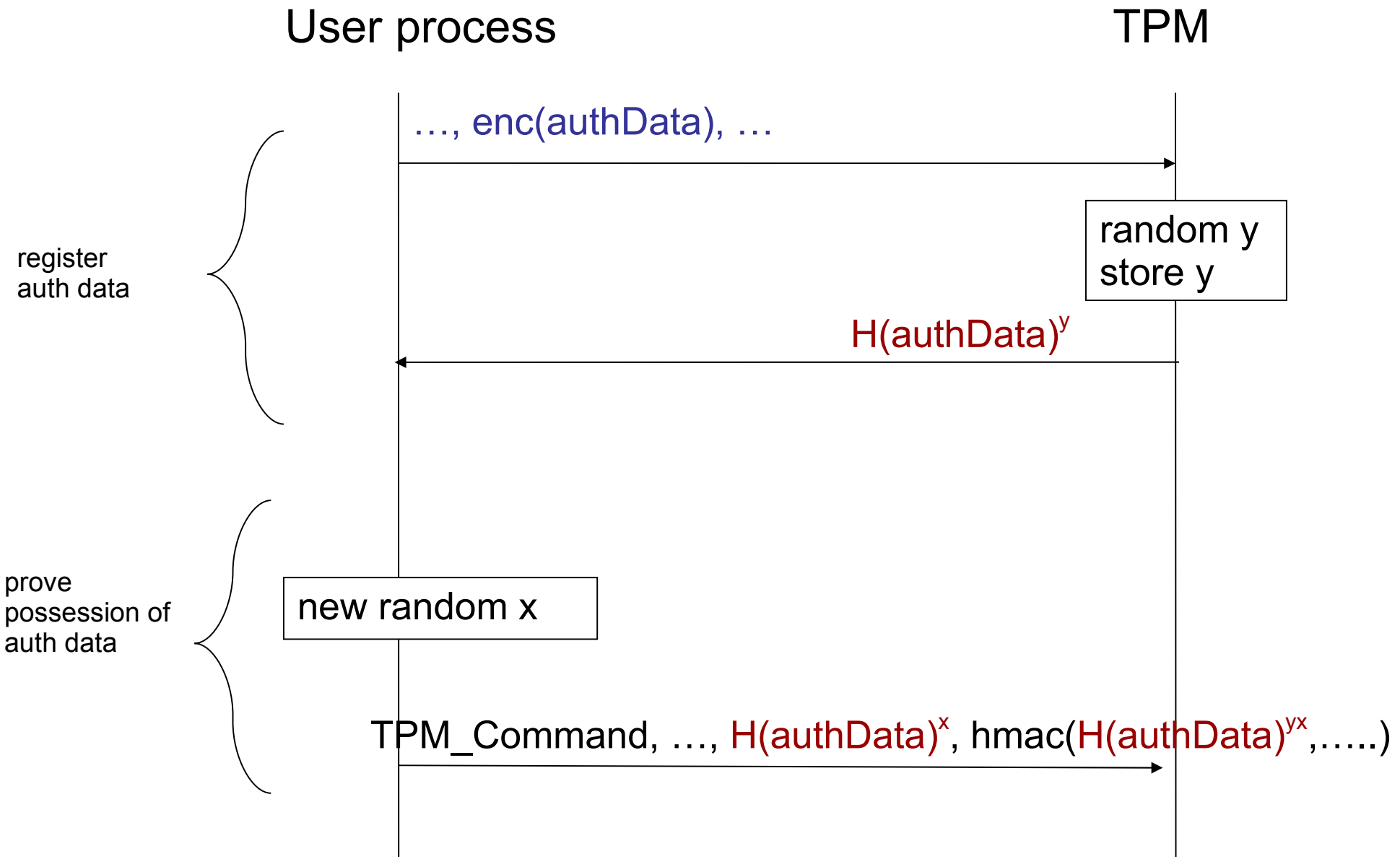
Simple Password Exponential Key Exchange (SPEKE) [Jablon 1996]

- A et B partagent un secret faible w
- Setup:
  - Soit G un champ fini d'ordre prime q and et modulus prime p, où q est au moins 160 bits, et p est au moins 1024 bits, tel que $q \mid p - 1$.
  - Soit H une fonction de hash sur $H : \{0, 1\}^* \rightarrow G$. On suppose que les valeurs q, p et la fonction H sont connues à A et B (ce ne sont pas des secrets)



Alors A,B partagent le secret fort $(H(w))^{xy}$.

Integrating SPEKE: password-based proof of knowledge



Problème 2:
L'authdata partagé

L'authdata partagé

- TCG permet aux utilisateurs de partager l'authdata
  - C'est quand l'autorisation d'une clé doit être partagée. Par exemple, on peut supposer que SRKauth est une valeur bien connue.
- Par conséquent
  - La connaissance de SRKauth permet à n'importe qui d'usurper la réponse du TPM
  - L'attaquant qui connait l'authdata d'une clé parente peut créer des clés avec l'aide d'un logiciel, et les présenter comme des vraies clés du TPM.
- La solution SPEKE ne résout pas ce problème.

Des scenarios pour l'attaque de l'authdata partagé

SysAdmin

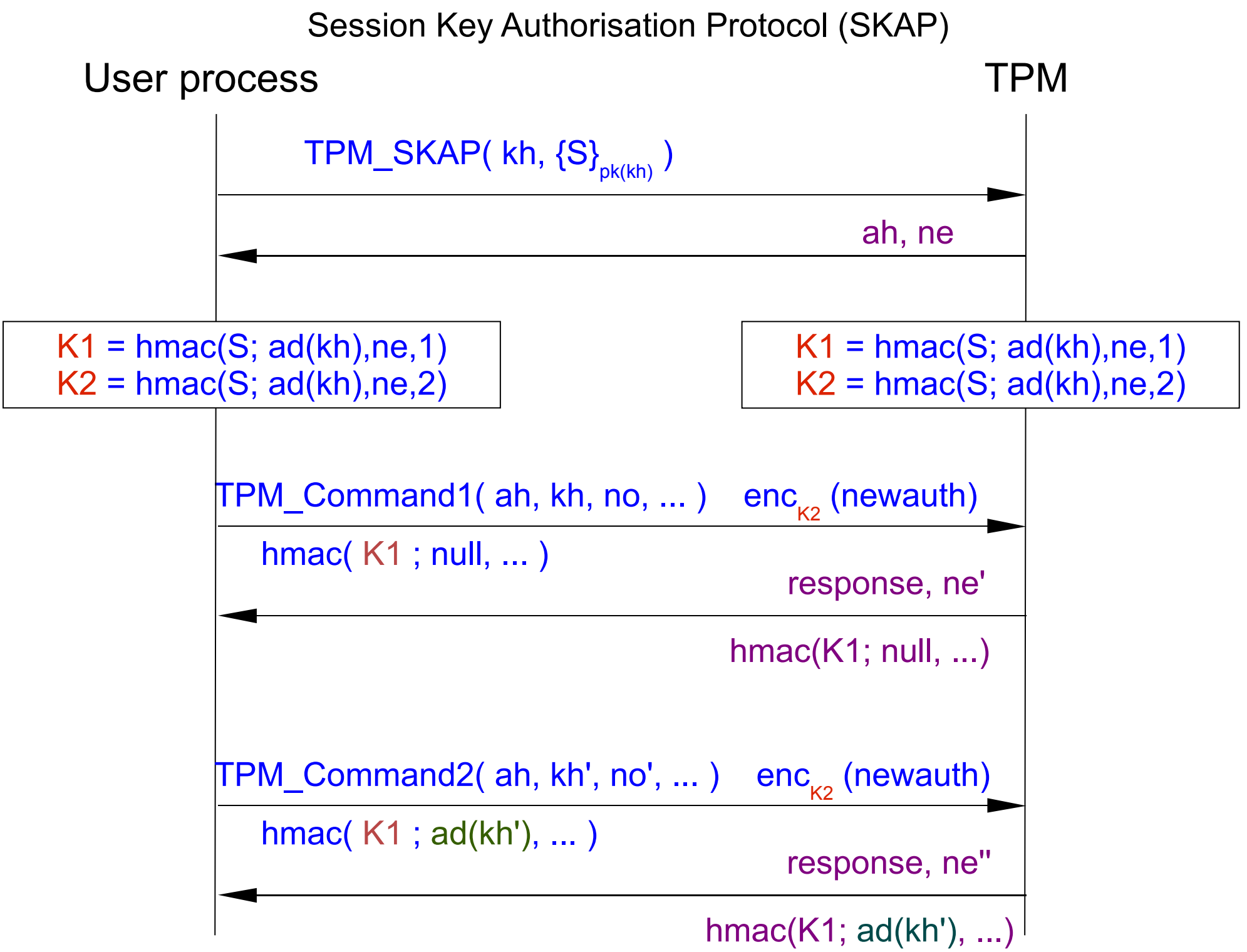
- Le sysAdmin prend possession du TPM avant de le donner à l'employé
- Le sysAdmin malveillant installe le logiciel qui intercepte le trafic du TPM, et qui répond à la place du TPM.

L'utilisation à distance du TPM

- Le TPM d'une plate-forme est accedé à distance, e.g., par sysAdmin.
- L'utilisateur d'une plate-forme peut usurpe la réponse attendue du TPM.

Session Key Authorisation Protocol (SKAP)

- Il generalise les protocoles OIAP et OSAP, fournissant un type de session qui a les avantages des deux.
  - Peut cacher un secret de session pour éviter d'avoir à demander l'authdata à plusieurs reprises (comme OSAP).
  - Il permet l'utilisation des objets differents dans une même session (comme OIAP).
- C'est une session de longue vie.
  - Il n'est pas necessaire de la terminer quand on introduit du nouveau authdata.
- Permet aux utilisateurs de partager l'authdata.
  - Authentification du TPM fourni par les clés TPM, non par authdata
- N'expose pas l'authdata faible aux attaques par dictionnaire hors ligne.


Session Key Authorisation Protocol (SKAP)
User process
TPM
TPM_SKAP(kh, {S}pk(kh))
ah, ne
K1 = hmac(S; ad(kh),ne,1)
K2 = hmac(S; ad(kh),ne,2)
K1 = hmac(S; ad(kh),ne,1)
K2 = hmac(S; ad(kh),ne,2)
TPM_Command1(ah, kh, no, ...)
enc K2 (newauth)
hmac(K1 ; null, ...)
response, ne'
hmac(K1; null, ...)
TPM_Command2(ah, kh', no', ...)
enc K2 (newauth)
hmac(K1 ; ad(kh'), ...)
response, ne''
hmac(K1; ad(kh'), ...)

Vérification de SKAP

Le modèle Dolev-Yao Needham-Schroeder

- L'attaquant contrôle tout sauf la crypto, qui est supposée parfaite

Le pi calcul appliqué

- Un language pour décrire les protocoles et les analyser dans le modele DY-NS
- Peut exprimer les propriétés de secret, de correspondance, et d'équivalence.

ProVerif

- Un outil developpé à l'ENS Paris pour l'analyse des protocoles décrits dans le pi calcul appliqué.

La propriété de correspondance pour SKAP

- Si l'utilisateur pense qu'il a completé SKAP avec le TPM, alors c'est bien le cas (il n'a pas été usurpé).

Conclusions

Les problèmes du TPM

- L'authdata faible
- L'authdata partagé
- Les sessions transports chiffrées

Notre solution

- Un nouveau protocole d'autorisation, SKAP, qui répare les deux problèmes.
- SKAP résout aussi plusieurs difficultés avec les sessions d'autorisation actelles.

Vérifcation

- ProVerif a vérifié que SKAP est sur contre les deux attaques.
- Le TPM est un sujet interessant pour la vérification.