

INTRODUCTION À LA SÉCURITÉ INFORMATIQUE POT-POURRI

Marc-Olivier Killijian

UQAM, CNRS

INF4471

1. Devoir 2 : 11 nov 23h59-14 nov 23h59
similaire au Devoir 1 - 10 questions - S6-S8-S9-S10

2. Pourriels

3. Anti-pourriels

4. Authentification de messages

5. Sécurité des protocoles

POURRIELS

Marc-Olivier Killijian

UQAM, CNRS

INF4471

DÉFINITION (PAUL GRAHAM)

- « Je propose de définir le *spam* comme courriels **automatiques non-sollicités.** »
- « Les définitions juridiques du spam, probablement influencées par les lobbyistes, *tendent à exclure le courrier envoyé par des entreprises* qui ont une "relation existante" avec le destinataire. Mais acheter quelque chose à une entreprise, par exemple, n'implique pas que vous avez **sollicité un courrier électronique** continu de sa part. »

(Paul Graham: organisateur de la première conférence sur le spam, USA, 2003)

DÉFINITION (BRAD TEMPLETONS)

- « Je défini l'abus de courriel comme étant un courriel qui répond à ces trois critères :
 1. Il est **non-sollicité**
 2. Il fait partie d'un **envoi de masse**
 3. L'**émetteur est inconnu du destinataire.** (Pas de contact personnel désiré de la part du destinataire.) »

(Brad Templetons: founder of one of the first companies on Internet in 1989)

UN EXEMPLE DE SPAM ?

The screenshot shows a dark-themed email client window, likely Mac Mail, displaying a spam message. The window has a standard OS X title bar with icons for close, minimize, maximize, and navigation. The main area shows the following details:

Proposition de doctorat
À : Marco Killijian

Boîte de réception - UQAM2 19 août 2020 à 12:35 NA

Bonjour Monsieur,

Je m'appelle [REDACTED], titulaire d'un master en informatique; spécialité réseaux et systèmes distribués obtenu au sein de l'université de skikda- Algérie. je souhaiterai intégrer votre université du Québec à Montréal, pour poursuivre un doctorat en l'analyse des systèmes informatiques.

"L'identification des inconsistices dans les noms de classes, dans les projets Pharo en utilisant ClassNames Blueprint" était mon thème de projet de fin d'études en master, cette étude est basée sur le travail de Dr. Alidra et. al, veuillez trouver en pièce jointe l'étude faite par ces derniers. J'ai pu reconstruire l'application du ClassNames Blueprint en utilisant le langage de programmation Pharo, l'intégrer avec Moose- une plate forme pour l'analyse des données et logiciels, pour que mon application s'étende à analyser les projets Java autant que les projets Pharo. Ce fut mon premier projet avec le langage de programmation orienté-objet Pharo, sachant que tout mon cursus universitaire était basé sur Java.

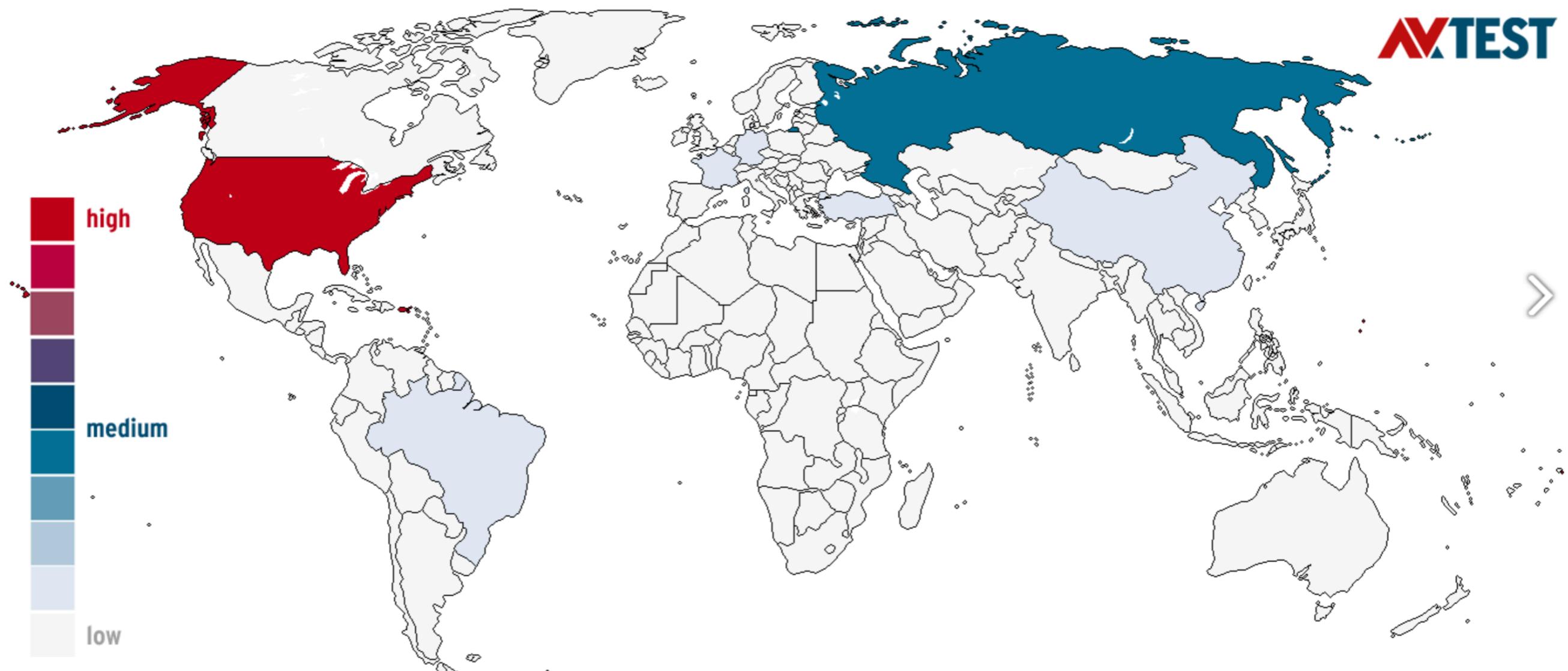
Je voudrais étendre cette étude à un niveau plus haut, découvrir de nouvelles façons pour déetecter les inconsistices dans les systèmes patrimoniaux ou les technologies en Big Data afin d'améliorer l'extraction des données, la compréhension, l'intégration de nouveaux services et par la suite la maintenance de ces systèmes.

Dans l'attente de votre réponse que j'espère favorable, je reste à votre disposition pour tout complément que vous souhaiteriez obtenir.

Mes respectueuses salutations.
[REDACTED]

document

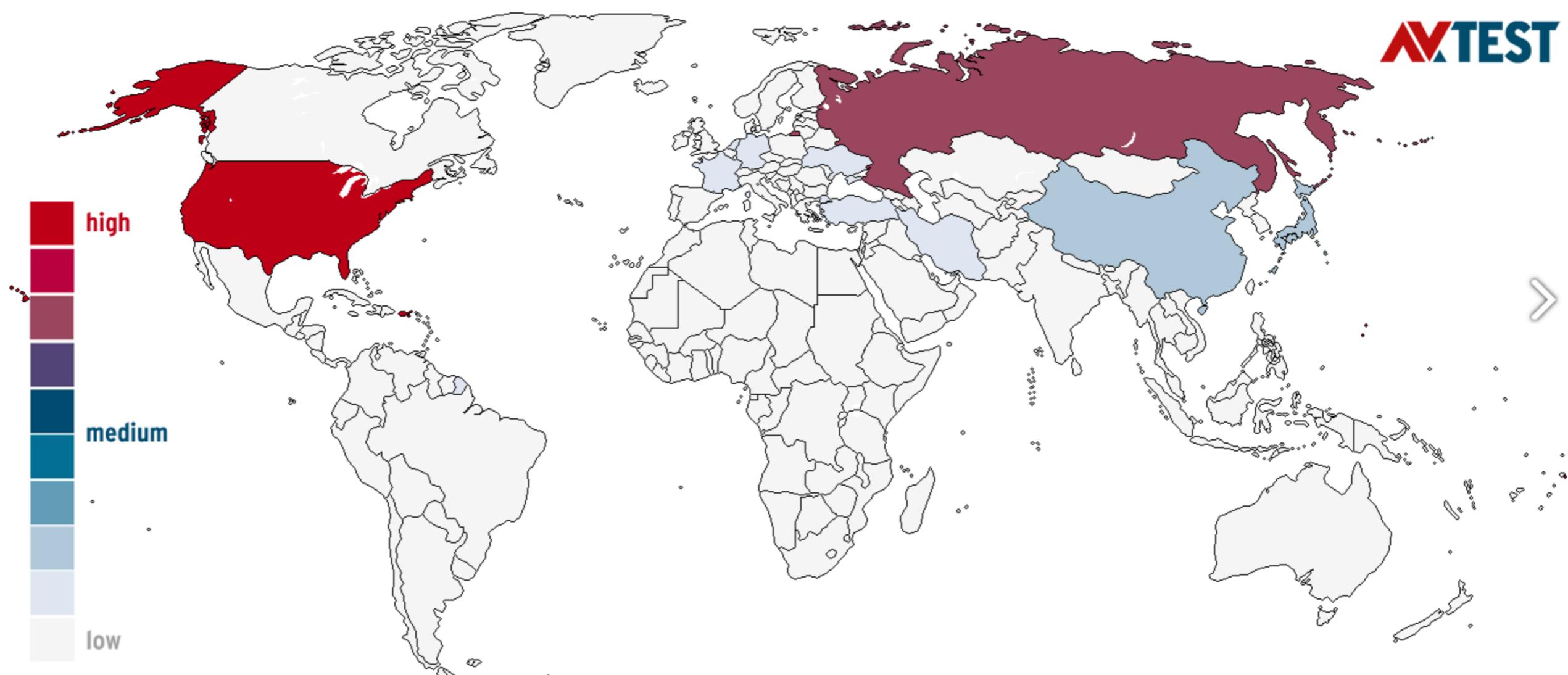
Origin of Spam per Country, last 180 days



Last update: October 23, 2020

Copyright © AV-TEST GmbH, www.av-test.org

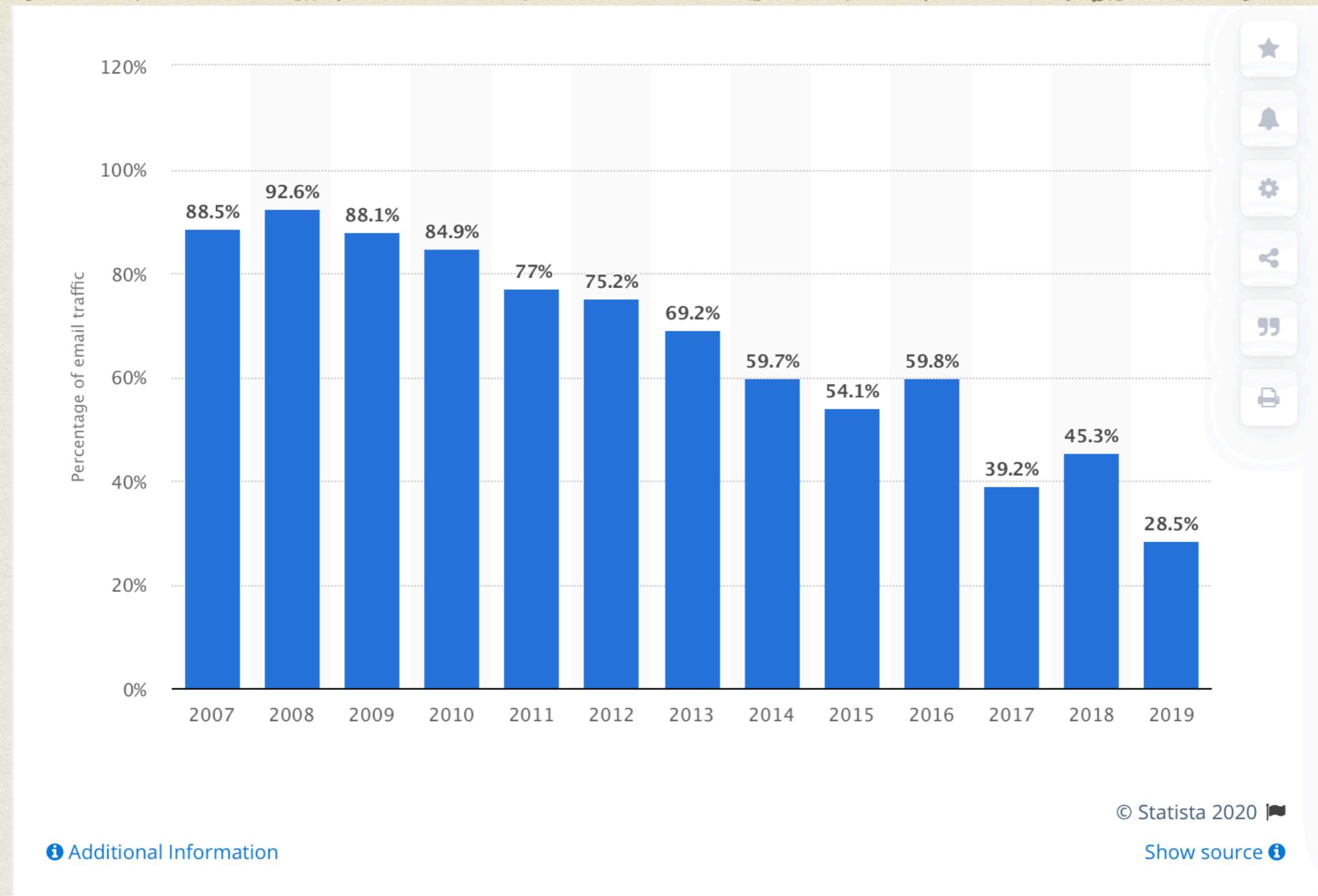
Origin of Spam per Country, last 14 days



Last update: October 23, 2020

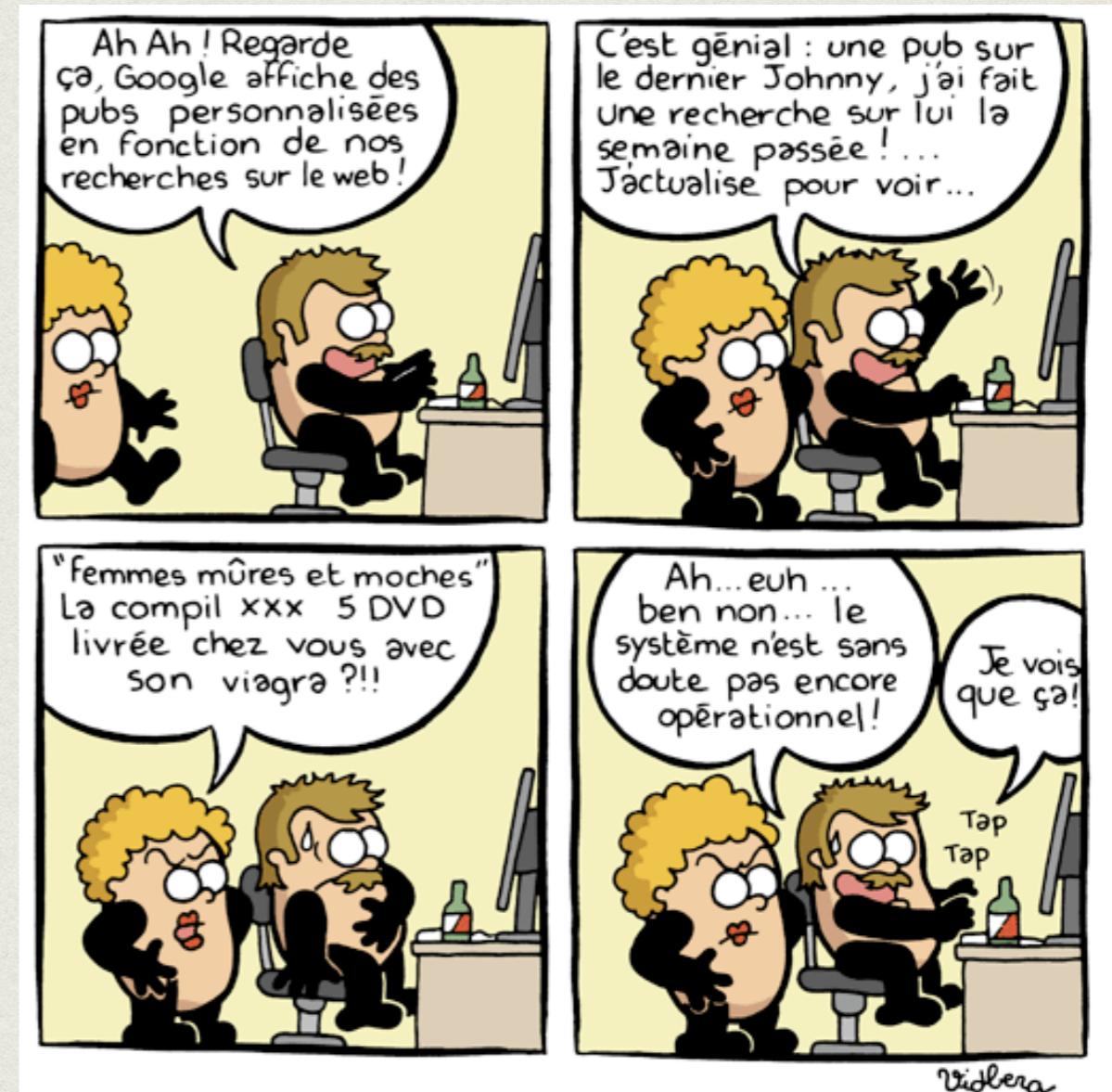
Copyright © AV-TEST GmbH, www.av-test.org

VOLUME DE SPAM



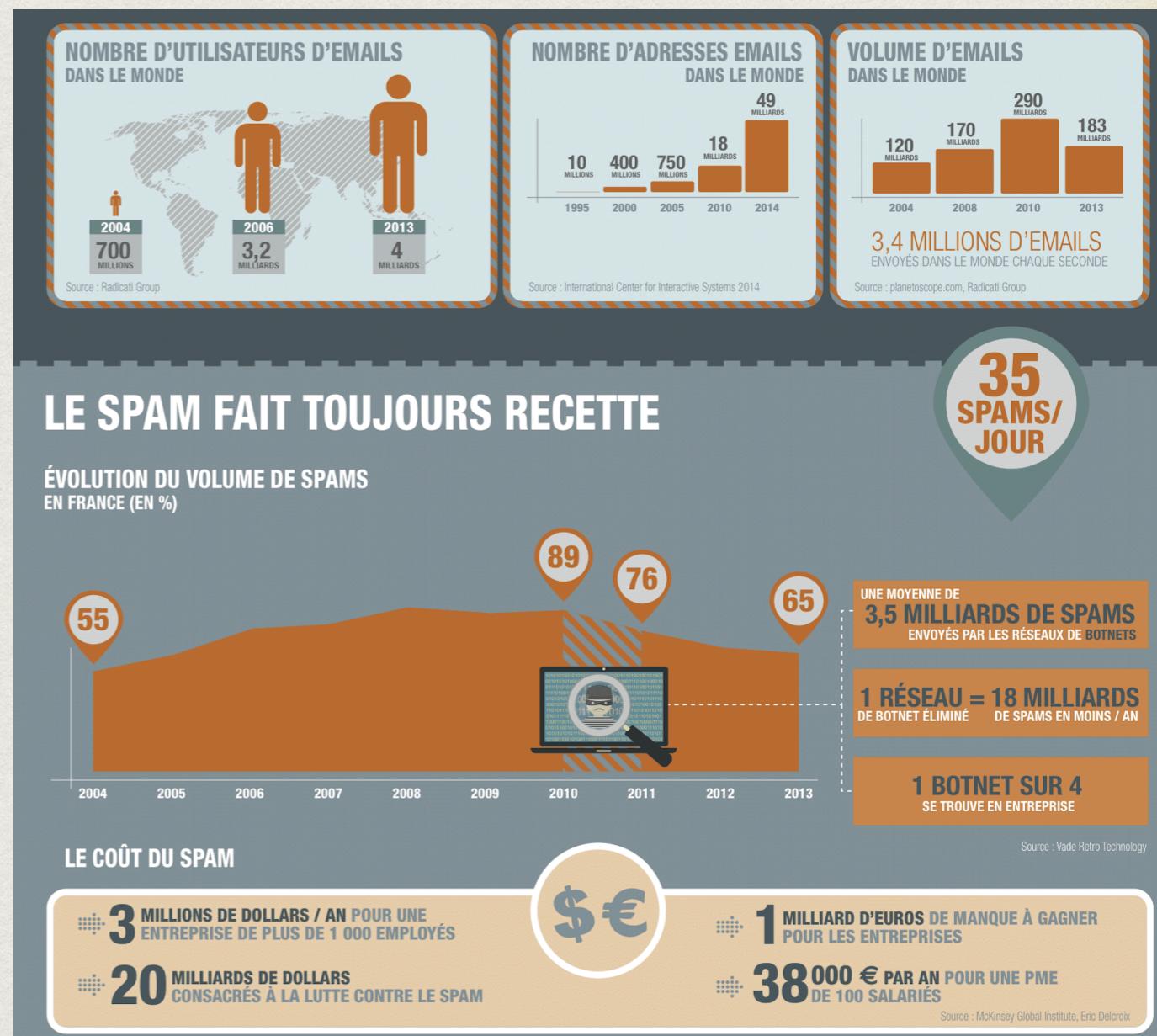
MODÈLE D'AFFAIRE

- Acteurs
 - Publicitaires
 - Spammers
 - Collecteurs d'adresse
- Sources de profits
 - Ventes, escroqueries
 - Partage des profits entre acteurs
 - Taille des listes d'adresse
 - Clics



MODÈLE D'AFFAIRE

- Acteurs
 - Publicitaires
 - Spammers
 - Collecteurs d'adresse
- Sources de couts
 - Traffic
 - Escroqueries
 - Temps-perdu
 - Lutte antispam

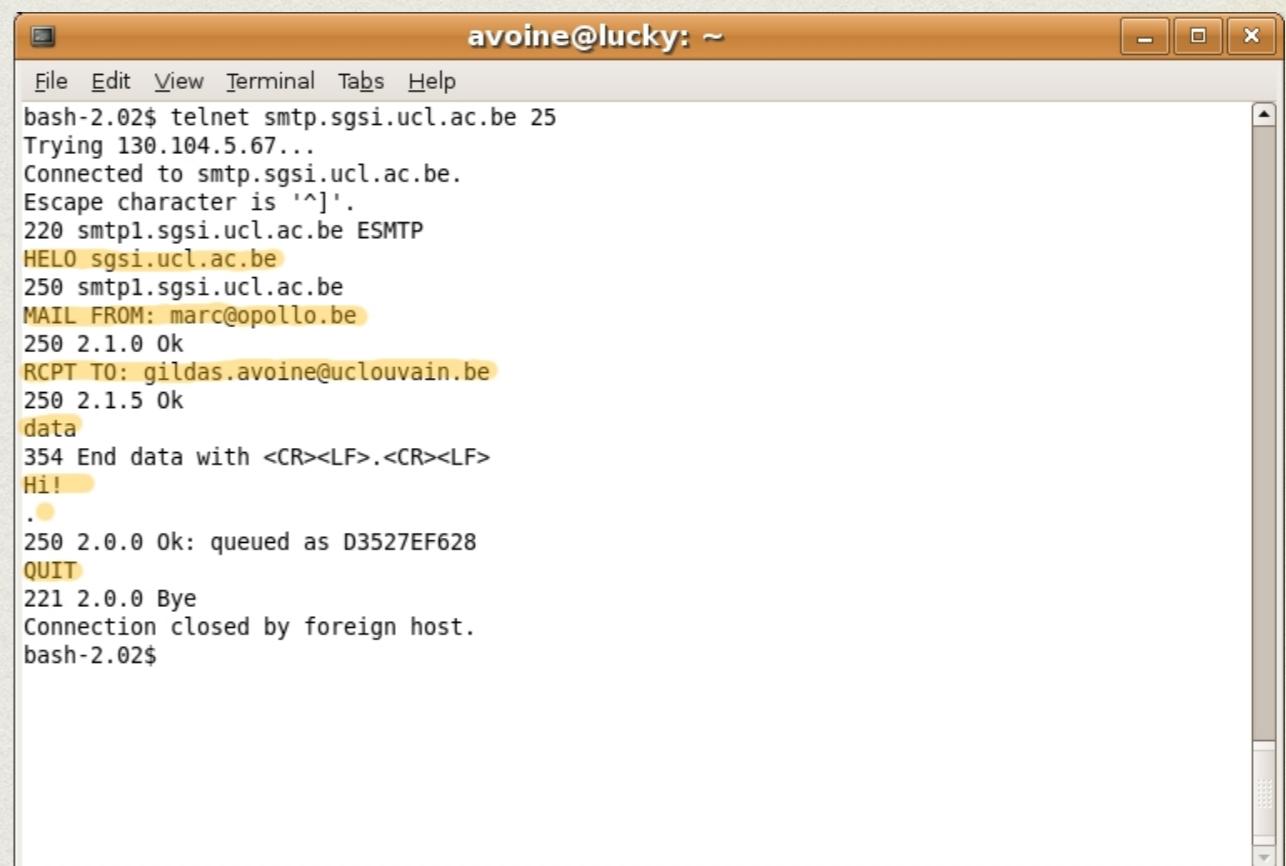


SOURCE DE TROUBLES

- Infrastructure
 - Bande passante
 - Couts de transferts
 - Equipement (pare-feus, stockage, serveurs, backups, etc.)
 - Maliciels: en 2013 ~4% des courriels contenaient un malware
 - Hameçonnage
- Productivité
 - Dérangé pendant le travail
 - Symantec (1000 utilisateurs) : 65% +10min/j ; 24% +20min/j
 - Perte de courriels utiles
 - Besoin de changer d'adresses
- Lois
 - Employés/compagnies
 - Utilisateurs/fournisseurs

TECHNIQUES DE SPAM (1)

- Méthode 1 : Utiliser son propre serveur SMTP (ou celui de son fournisseur)
 - La plupart du temps en forgeant l'adresse de l'émetteur pour se protéger de contre-attaques
- SMTP (Simple Mail Transfer Protocol), RFC 821, 1982
 - Connexion TCP sur le port 25, des commandes simples
 - HELO (annonce du serveur)
 - Mail From: (définition de l'émetteur)
 - Rcpt To: (destination)
 - Data: (contenu)



The screenshot shows a terminal window titled "avoine@lucky: ~". The window contains a transcript of an SMTP session:

```
File Edit View Terminal Tabs Help
bash-2.02$ telnet smtp.sgsi.ucl.ac.be 25
Trying 130.104.5.67...
Connected to smtp.sgsi.ucl.ac.be.
Escape character is '^].
220 smtp1.sgsi.ucl.ac.be ESMTP
HELO sgsi.ucl.ac.be
250 smtp1.sgsi.ucl.ac.be
MAIL FROM: marc@opollo.be
250 2.1.0 Ok
RCPT TO: gildas.avoine@uclouvain.be
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Hi!
.
250 2.0.0 Ok: queued as D3527EF628
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
bash-2.02$
```

TECHNIQUES DE SPAM

(2)

- Pas d'authentification avec SMTP: facile de forger des courriels
- Résultats identiques en modifiant le champs « from » de son logiciel de gestion des courriels
- Mais ... facile de retrouver l'auteur réel du message
 - contenu du HELO
 - @ IP de l'émetteur
 - Heure de réception
- Pour ne pas être détecter, besoin de lancer la connexion d'une machine qui ne fait pas de journaux de connexions

TECHNIQUES DE SPAM

(3)

- Méthode 2: utilisation de relais ouverts
 - certains serveurs SMTP sont ouverts (n'importe qui peut s'y connecter, sans compte sur la machine)
 - on s'y connecte pour envoyer un message à 1000+ destinations
 - ils relaient poliment le message à chaque destination
- 55% des serveurs SMTP étaient ouverts en 1998, plus que 1% en 2002
 - Dorénavant, l'émetteur ou récepteur soit être dans le domaine du serveur
 - Les serveurs ouverts sont rapidement black-listés

TECHNIQUES DE SPAM

(3)

- Méthode 3 : exploitation de comptes webmail
 - un robot ouvre de nombreux comptes webmail
 - les exploiter jusqu'à fermeture
- Méthode 4 : exploiter des ordinateurs personnels
 - maliciels -> botnets

COLLECTE D'ADRESSES

- Crawler le web
- Dictionnaires : générer des adresses pour un domaine
- Hacking : attaquer une base de données
- Malware : récupérer des carnets d'adresses
- Chaines de courriels, etc.

COLLECTE D'ADRESSES

- Crawling
 - Dictionary attack
 - Hacking
 - Malware
 - Chain
-
- The screenshot shows a website for a business database. At the top, it says "148 COUNTRIES BUSINESS DATABASE". On the left, there's a "Navigation" sidebar with links for Asia, Oceania, North America, Africa, Europe, South America, and Business Email List. The main content area has two tables. The first table, "World Wide", lists "World Wide Email List" with 1200+ Million records for \$650 USD and another with 900+ Million records for \$450 USD, both with "Buy Now" buttons. The second table, "Asia Business Database", lists various countries with their record counts and prices, each with a "Buy Now" button. The countries listed are United Arab Emirates, Afghanistan, Armenia, China, Hong Kong, Indonesia, Malaysia, Azerbaijan, Bahrain, Bangladesh, Bhutan, Brunei, Cambodia, Iran, Iraq, and Japan.
- | Region | Country | Records | Price | Action |
|------------------------|-----------------------|-----------------------|-------------------------|-------------------------|
| World Wide | World Wide Email List | 1200+ Million records | \$650 USD | Buy Now |
| | World Wide Email List | 900+ Million records | \$450 USD | Buy Now |
| Asia Business Database | United Arab Emirates | 1+ Million records | \$200 USD | Buy Now |
| | Afghanistan | 861 records | \$39.90 USD | Buy Now |
| | Armenia | 2574 records | \$58.90 USD | Buy Now |
| | China | 1180170 records | \$235.90 USD | Buy Now |
| | Hong Kong | 360000 records | \$125.00 USD | Buy Now |
| | Indonesia | 412251 records | \$274.90 USD | Buy Now |
| | Malaysia | 314132 records | \$294.90 USD | Buy Now |
| | Azerbaijan | 13864 records | \$78.90 USD | Buy Now |
| | Bahrain | 9905 records | \$176.90 USD | Buy Now |
| | Bangladesh | 15950 records | \$80 USD | Buy Now |
| | Bhutan | 1304 records | \$58.90 USD | Buy Now |
| | Brunei | 56741 records | \$137.90 USD | Buy Now |
| | Cambodia | 6458 records | \$78.90 USD | Buy Now |
| | Iran | 28727 records | \$196.90 USD | Buy Now |
| | Iraq | 1658 records | \$68.90 USD | Buy Now |
| Japan | 334721 records | \$294.90 USD | Buy Now | |

ANTI-POURRIELS

Marc-Olivier Killijian

UQAM, CNRS

INF4471

LEGALEMENT

- Envoyer des pourriels est puni par la loi
 - Jeremy Jaynes (2006 Virginie) 9 ans de prison. \$750000/mois avec 1M courriels/j
 - James McCalla (2006 Iowa) amende de 11.2Mds\$ pour avoir envoyé 280M courriels
 - 514-Billets (2018 Québec) amende de 100000CAD pour envoi de textos non-sollicités
- USA : CAN-SPAM Act - Controlling the Assault of Non-Solicited Ornography And Marketing Act of 20003
- Canada : LCAP - Loi Canadienne Anti Pourriel

TECHNIQUEMENT

- Il est facile de reconnaître un spam
 - Il devrait être facile de les filtrer automatiquement !
- Filtrage de spam basé sur le **contenu et le format**
 - **faux positifs et faux négatifs**
 - **SpamAssassin** - un des filtres les plus efficaces/répandu
 - Open source, basé sur des règles de score positif/négatif
 - Des centaines de règles (locales, réseau, Bayes)

TECHNIQUEMENT

	rawbody	Extra blank lines in base64 encoding	MIME_BASE64_BLANKS	0.001 0.001	Wiki
I	rawbody	Message text disguised using base64 encoding	MIME_BASE64_TEXT	0.001 0.001 0.001 1.741	Wiki
	body	Missing blank line between MIME header and body	MISSING_MIME_HB_SEP	0.001 0.001 0.001 0.001	Wiki
F	body	Multipart message mostly text/html MIME	MIME_HTML_MOSTLY	0.354 0.001 0.725 0.428	Wiki
	body	Message only has text/html MIME parts	MIME_HTML_ONLY	2.199 1.105 1.199 0.723	Wiki
	rawbody	Quoted-printable line longer than 76 chars	MIME_QP_LONG_LINE	0.001	Wiki
	body	MIME character set is an unknown ISO charset	MIME_BAD_ISO_CHARSET	1	Wiki
	body	IP to HTTPS link found in HTML	HTTPS_IP_MISMATCH	1	Wiki
	body	Message contained a URI which was truncated	URI_TRUNCATED	0.001	Wiki
	header	Passed through trusted hosts only via SMTP	ALL_TRUSTED	-1.000	Wiki
	header	Informational: message was not relayed via SMTP	NO_RELAYS	-0.001	Wiki
	header	NJABL: sender is confirmed open relay	RCVD_IN_NJABL_RELAY	0.1881 0 2.499	Wiki
	header	NJABL: sender is confirmed spam source	RCVD_IN_NJABL_SPAM	0.1466 0 1.249	Wiki
	header	NJABL: sent through multi-stage open relay	RCVD_IN_NJABL_MULTI	1	Wiki
	header	NJABL: sender is an open formmail	RCVD_IN_NJABL_CGI	1	Wiki
	header	NJABL: sender is an open proxy	RCVD_IN_NJABL_PROXY	0.0208 0 2.224	Wiki
	header	SORBS: sender is open HTTP proxy server	RCVD_IN_SORBS_HTTP	0.2499 0 0.001	Wiki
	header	SORBS: sender is open SOCKS proxy server	RCVD_IN_SORBS SOCKS	0.2443 0 1.927	Wiki
	header	SORBS: sender is open proxy server	RCVD_IN_SORBS_MISC	1	Wiki

TECHNIQUEMENT

- Listes Noires
 - Listes noires DNS (DNSBL) recensent les domaines connus pour leur envoi de spam, e.g. SpamHaus
 - utilisées par les filtres comme SpamAssassin
 - et par les serveurs pour filtrer le trafic entrant
- + : peu cher et facile à mettre en place
- - : de nombreux faux négatifs et besoin de gestionnaires de liste réactif

TECHNIQUEMENT

- Listes Blanches
 - Forcer l'acceptation de courriels issus d'émetteurs connus
 - + : peu cher et facile à mettre en place
 - - : beaucoup de faux positifs et besoin de connaître l'émetteur a priori
- SpamAssassin les utilise en partie pour attribuer un score positif

TECHNIQUEMENT

- Listes de Spam
 - Base de données qui recense le contenu de courriels identifiés comme spam
 - Vérifier que le contenu d'un message n'est pas dans cette BDD
 - + : BDD partagée, peu de faux positifs
 - - : variantes non-déetectées, besoin de serveurs de BDD, nombreux faux négatifs

TECHNIQUEMENT

- Listes grises : bloquer un courriel si le serveur de l'émetteur a un comportement anormal
 - Création d'une base de données de triplets
<IP serveur; @emetteur; @destinataire>
 - Cette BDD sert de liste blanche
 - Les messages qui ne sont pas dans la liste blanche sont **grisés**
 - un message d'erreur est renvoyé au serveur émetteur qui doit ré-essayer 30 minutes plus tard s'il respecte RFC2821
 - si c'est le cas le message est dé-grisé, et délivré puis un triplet est créé, sinon -> spam
 - + : pas ou peu de faux négatifs
 - - : délais introduit par le processus

TECHNIQUEMENT

- Autres pistes
 - Authentification plus forte
 - Challenge/réponses pour être ajoutés à une liste-blanche
 - Hashcash (*proof-of-work à la blockchain*)
 - etc.

AUTHENTIFICATION DE MESSAGE

Marc-Olivier Killijian

UQAM, CNRS

INF4471

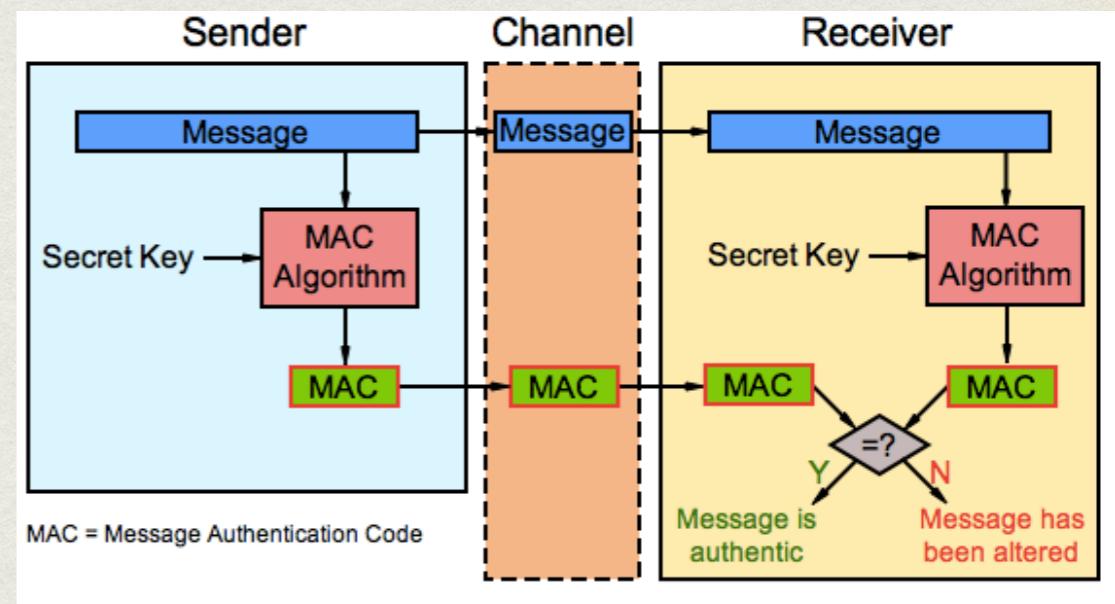
AUTHENTIFICATION DE MESSAGE

- Comment Bob peut s'assurer qu'un message a bien été envoyé par Alice et pas Eve ?
- Assurer l'**intégrité** (et **authenticité**) d'un message
- Confidentialité $\not\Rightarrow$ Intégrité



CODE D'AUTHENTIFICATION DE MESSAGE

- CAM ou MAC (Message Auth Code) : système d'authentification à partir d'une **clé secrète partagée**
- Empêcher Eve de forger des messages en impersonnant Alice ou Bob
- Algorithme d'authentification :
 $s = S_k(m)$
- Algorithme de vérification :
 $V_k(s, m) : \text{si } s = S_k(m) \text{ alors accept sinon reject}$



PROPRIÉTÉS

- Sans la clé, on ne peut forger un message valide (qui n'a pas été préalablement authentifié par son émetteur légitime)
 - On ne peut donc modifier un message sans être détecté
 - un message peut être confidentiel sans être intégrer (ex: 2TP)
 - un message peut être intégrer sans être confidentiel (ex: on envoie $(m, S_k(m))$ en clair)

FRAICHEUR D'UN MESSAGE

- Intégrité $\not\Rightarrow$ message récent
- Attaque par rejeu est possible
 - Alice envoie à Bob ($m = \text{« rendez vous ce soir au restaurant à 20h »}, S_{k_{alice}}(m)$)
 - Eve, jalouse, écoute et enregistre $(m, S_{k_{alice}}(m))$
 - Eve peut renvoyer $(m, S_{k_{alice}}(m))$ à Bob sans rejet du message

FRAICHEUR D'UN MESSAGE

- Contre-mesures
 - Index : les messages sont indexés
 - Détection de rejeux et de la perte (accidentelle ou malveillante) de messages
 - Etiquette temporelle : les messages sont estampillés avec la date d'envoi; les messages trop anciens sont refusés
 - Permet malgré tout les rejeux rapides

FONCTION DE HACHAGE CRYPTOGRAPHIQUE

- Rappel: h est une fonction de hachage crypto si
 - $h : \{0,1\}^* \rightarrow \{0,1\}^k$
 - h peut être calculé efficacement
 - difficile de calculer $h^{-1}(s) = m$
 - difficile de trouver une collision tq $h(x) = h(y)$, $x \neq y$
 - k doit être choisi suffisamment grand pour rendre la fouille exhaustive impossible en pratique

HMAC

- Hash-based MAC : génère un CAM à partir d'une fonction de hachage cryptographique (IpSec et SSL)
- $S_k(m) = h((k \oplus opad) || h((k \oplus ipad) || m))$
- $V_k(m, s) : si \ h((k \oplus opad) || h((k \oplus ipad) || m)) = s \ alors \ accept \ sinon \ reject$
- $opad = 0x5c5c\dots5c$ et $ipad = 0x3636\dots36$ de la taille de k choisis avec une grande distance de Hamming
- tailles de clé de 128 ou 160 bits

RECHERCHE DE COLLISION

- Paradoxe de l'anniversaire: $p(n) = 1 - \frac{365!}{365^n(365 - n)!}$ et donc $n \geq 23 \Rightarrow p(n) > 50\%$
- Recherche de collision avec mémorisation de tous les essais : tant que pas de collision, je mémorise le résultat et continue la recherche
 - En moyenne $2^{k/2}$ essais avec k le nb de bits de sortie de h
- Selon la fonction de hachage, il peut exister des attaques plus efficaces
- Choisir un k suffisamment grand, au moins 128 bits !

ATTAQUE PAR PRÉ-IMAGE

- Pré-image de premier ordre
 - à partir d'un haché z chercher une pré-image x tq
$$h(x) = z$$
- Pré-image de second ordre
 - à partir d'un message x chercher un message y tq
$$h(x) = h(y)$$

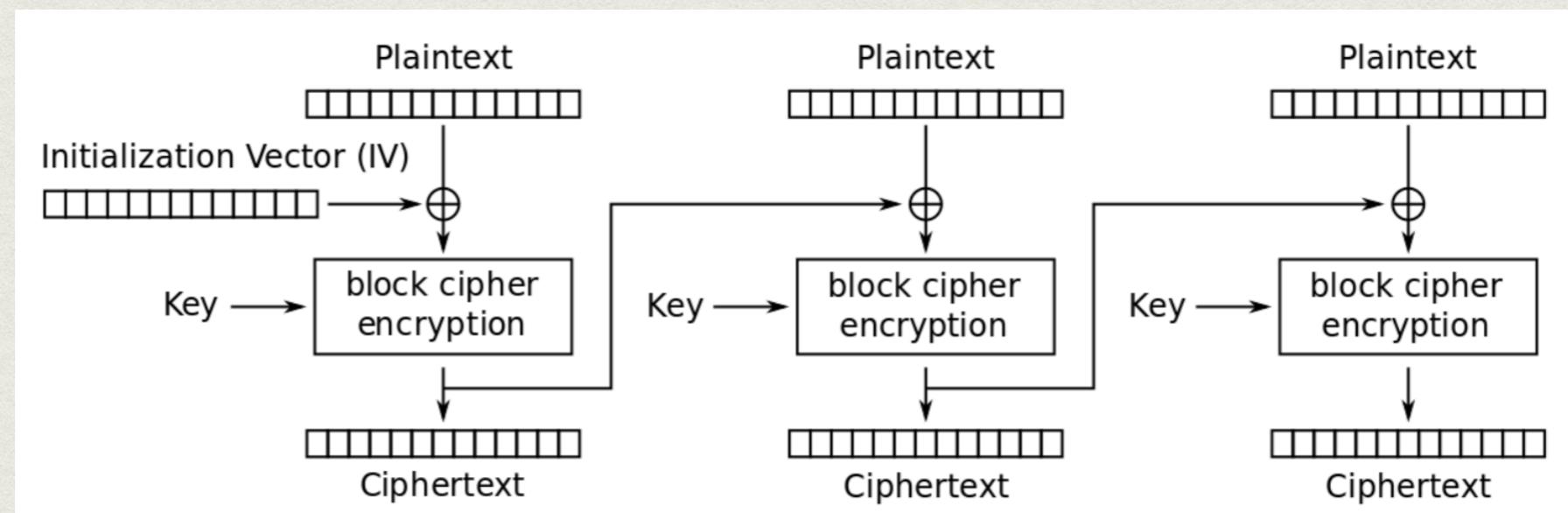
ETAT DES LIEUX

- existe t'il des fonctions de hachage à collision difficile ?

Hash function	Security claim	Best attack	Publish date	Comment
MD5	2^{64}	2^{18} time	2013-03-25	This attack takes seconds on a regular PC. Two-block collisions in 2^{18} , single-block collisions in 2^{41} .
SHA-1	2^{80}	$2^{61.2}$	2020-01-08	Paper by Gaëtan Leurent and Thomas Peyrin ^[2]
SHA256	2^{128}	31 of 64 rounds ($2^{65.5}$)	2013-05-28	Two-block collision. ^[3]
SHA512	2^{256}	24 of 80 rounds ($2^{32.5}$)	2008-11-25	Paper. ^[4]
SHA-3	Up to 2^{512}	6 of 24 rounds (2^{50})	2017	Paper. ^[5]
BLAKE2s	2^{128}	2.5 of 10 rounds (2^{112})	2009-05-26	Paper. ^[6]
BLAKE2b	2^{256}	2.5 of 12 rounds (2^{224})	2009-05-26	Paper. ^[6]

CBC-MAC

- DES ou AES en mode CBC peut être utilisé pour authentifier des messages
 - on chiffre $m = (m_0, m_1, \dots, m_{n-1})$ en CBC et on prend c_{n-1} comme CAM
- même efficacité que le mécanisme de chiffrement (taille de clés, temps de calcul)



SÉCURITÉ DES CBC-MAC

- Aussi sécuritaire que la méthode de chiffrement
 - si les messages sont de taille fixe
 - sinon problème du *padding*
 - Avec des 0 : possibilité de faire des faux messages en ajoutant ou enlevant des 0
 - Avec un 1 suivi de 0 : évite l'attaque ci-dessus mais il en existe d'autres
 - Avec la taille du message en tête puis des 0 en queue : ok

STANDARDS ISO POUR CBC-MAC

- 6 standards ISO dont
 - SMAC : CBC-MAC de base
 - EMAC : CBC-MAC + chiffrement de l'empreinte (avec une clé supp)
 - Sûr si clés assez longues mais sujet à une attaque similaire au double DES donc utiliser AES
 - ARMAC : chiffrement/déchiffrement supp du dernier bloc (avec 2 clés supp)

CHIFFREMENT AUTHENTIFIÉ

- chiffré-et-authentifié? ($c = \text{ENC}_{k_1}(m), s = S_{k_2}(m)$)
 - non-sûr, s peut révéler de l'information sur m
- authentifié-puis-chiffré (à la SSL)? ($c = \text{ENC}_{k_1}(m \parallel S_{k_2}(m))$)
 - non-sûr pour certain schémas car c n'est pas authentifié
- chiffré-puis-authentifié? ($c = \text{ENC}_{k_1}(m), s = S_{k_2}(c)$)
 - sûr si les schémas ENC et S sont sûrs

SÉCURITÉ DES PROTOCOLES

Marc-Olivier Killijian
UQAM, CNRS
INF4471

PROTOCOLES CRYPTOGRAPHIQUES

- Protocoles qui utilisent de la crypto pour construire des fonctions de plus haut niveau
 - Échange de clés
 - Authentification
 - ...
- Peuvent être attaqués par
 - Primitives crypto si mal utilisées, implémentées, paramétrées, ...
 - Du point de vue logique, à cause d'une mauvaise conception du protocole

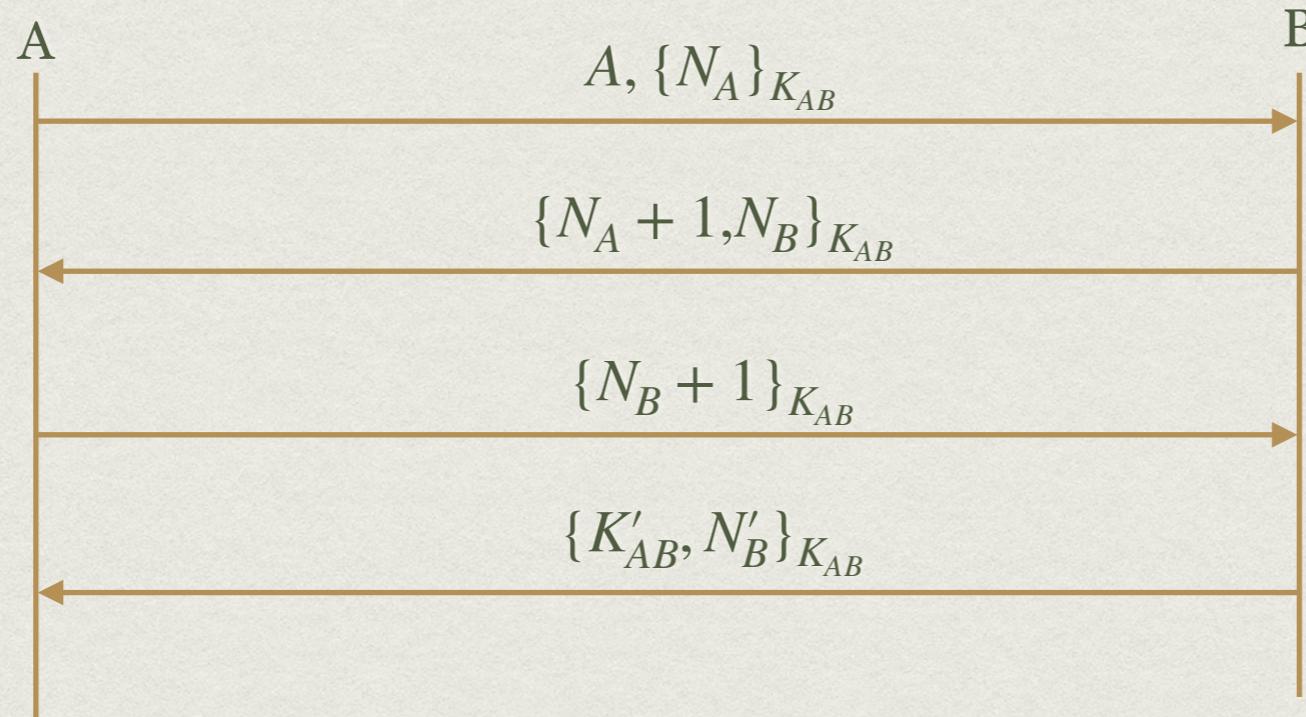
AUTHENTIFICATION D'ENTITÉ

- Comment m'authentifier auprès d'une entité ?
- Unilatéralement : comment authentifier une entité auprès d'une autre ?
- Mutuellement : comment deux entités peuvent s'authentifier ?
 - en option: et générer une clé de session ?



EXAMPLE: ANDREW SECURE RPC

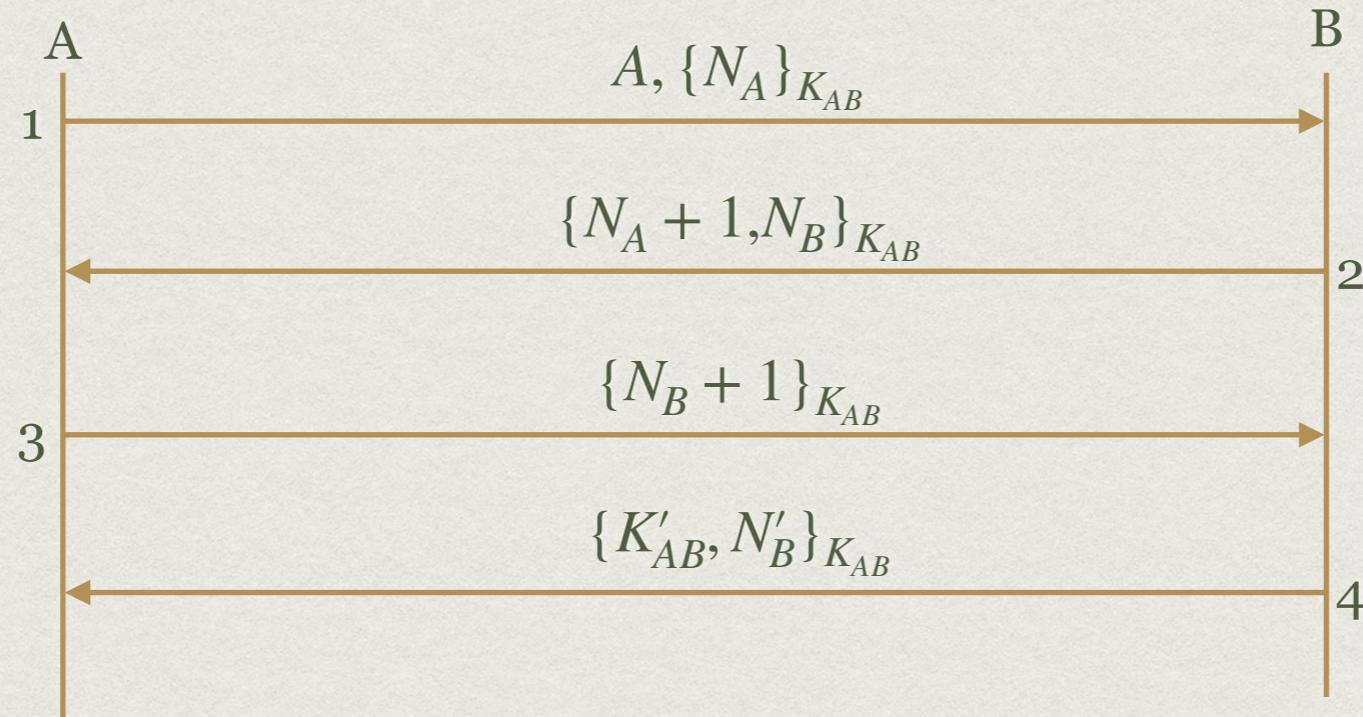
- Génération d'une nouvelle clé k'_{AB} à partir de k_{AB} secret partagé



- Questions fondamentales
 - Ce protocole atteint-il les objectifs de sécurité attendus
 - Attaques possibles ?
 - Si oui, comment modifier le protocole pour les éviter ?

EXAMPLE: ANDREW SECURE RPC

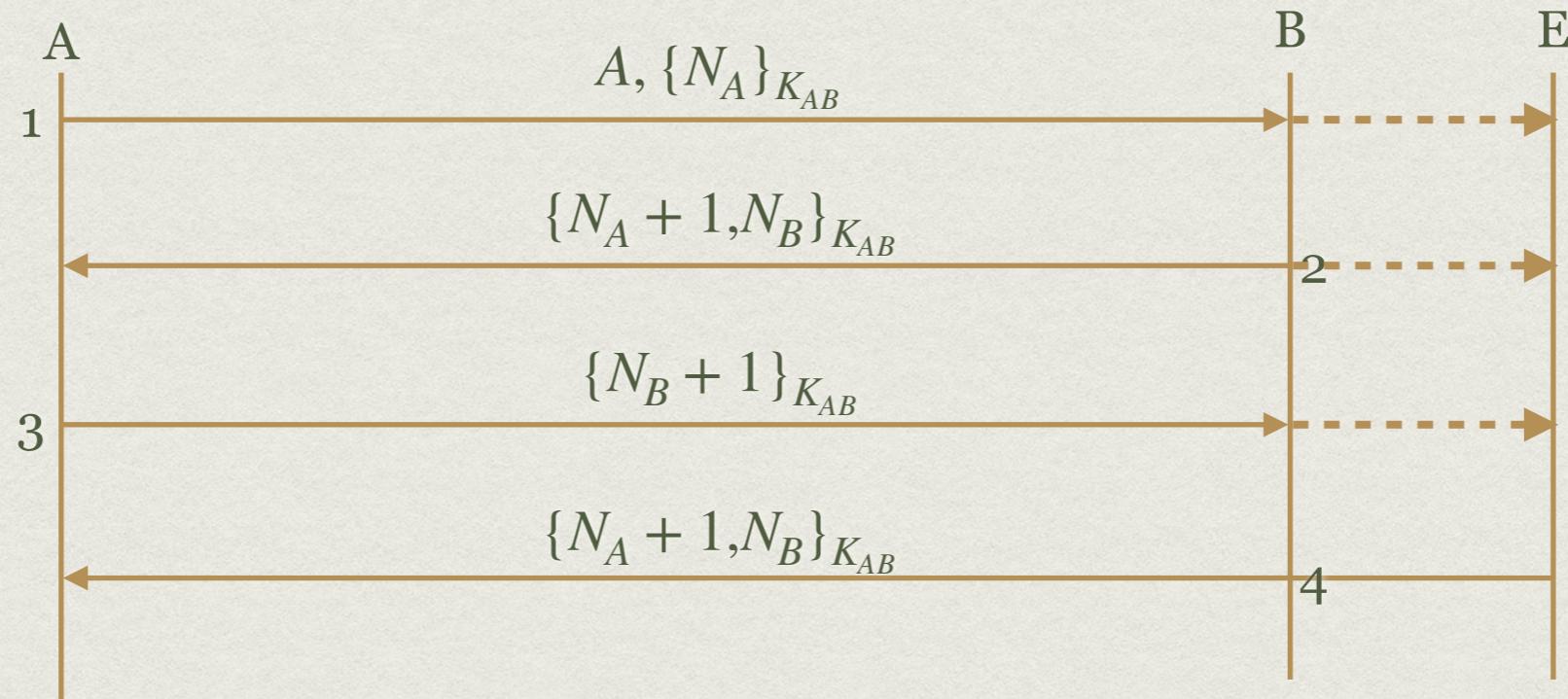
- Génération d'une nouvelle clé k'_{AB} à partir de k_{AB} secret partagé



- A la fin de l'étape 3, A et B sont authentifiés (les msg 2 et 3 dépendent des msg précédents)
 - le msg 4 ne dépend pas des précédents (problème de fraicheur)
- Rejeu : Eve peut remplacer le message de l'étape 4 par un msg où elle contrôle la nouvelle clé (par exemple en rejouant le msg 2)

EXAMPLE: ANDREW SECURE RPC

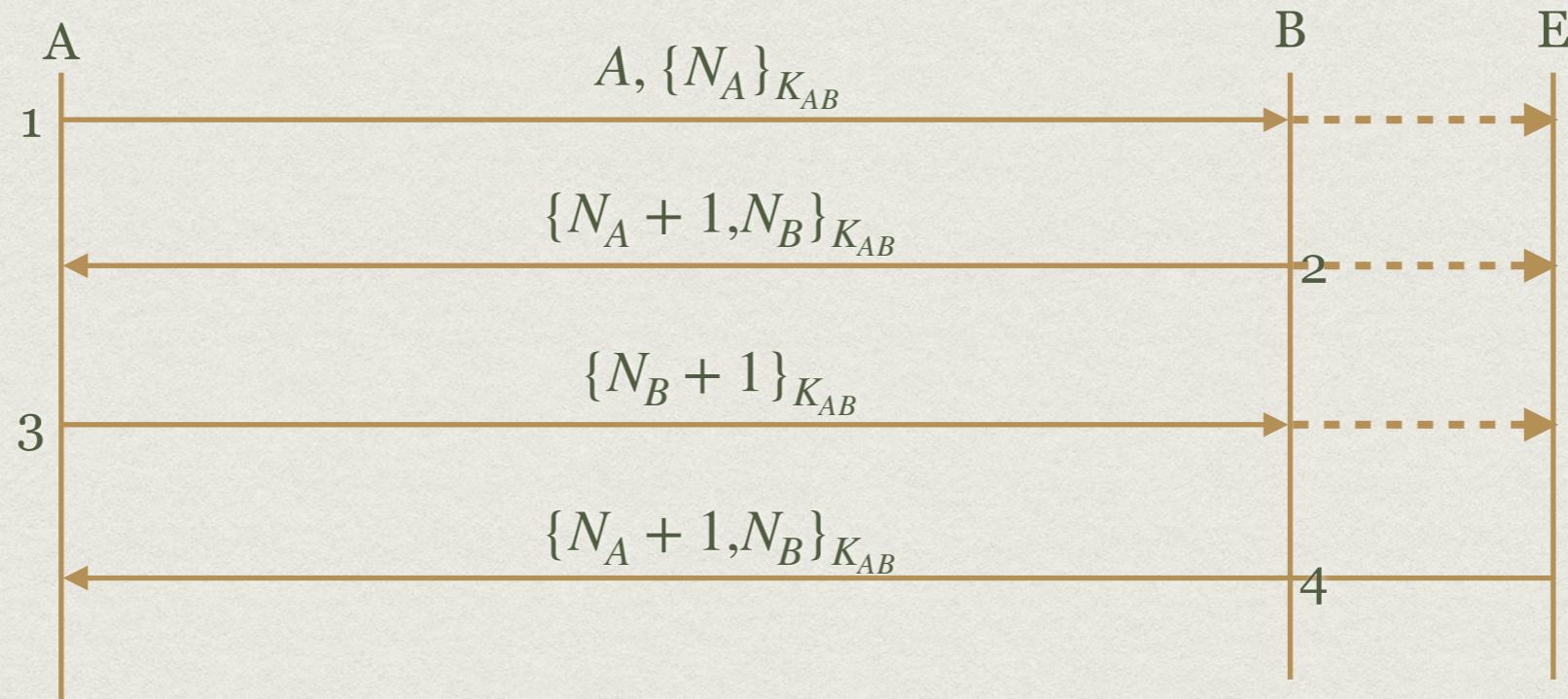
- Génération d'une nouvelle clé k'_{AB} à partir de k_{AB} secret partagé



- A la fin de l'étape 3, A et B sont authentifiés (les msg 2 et 3 dépendent des msg précédents)
 - le msg 4 ne dépend pas des précédents (problème de fraicheur)
- Rejeu : Eve peut remplacer le message de l'étape 4 par un msg où elle contrôle la nouvelle clé (par exemple en rejouant le msg 2)

EXAMPLE: ANDREW SECURE RPC

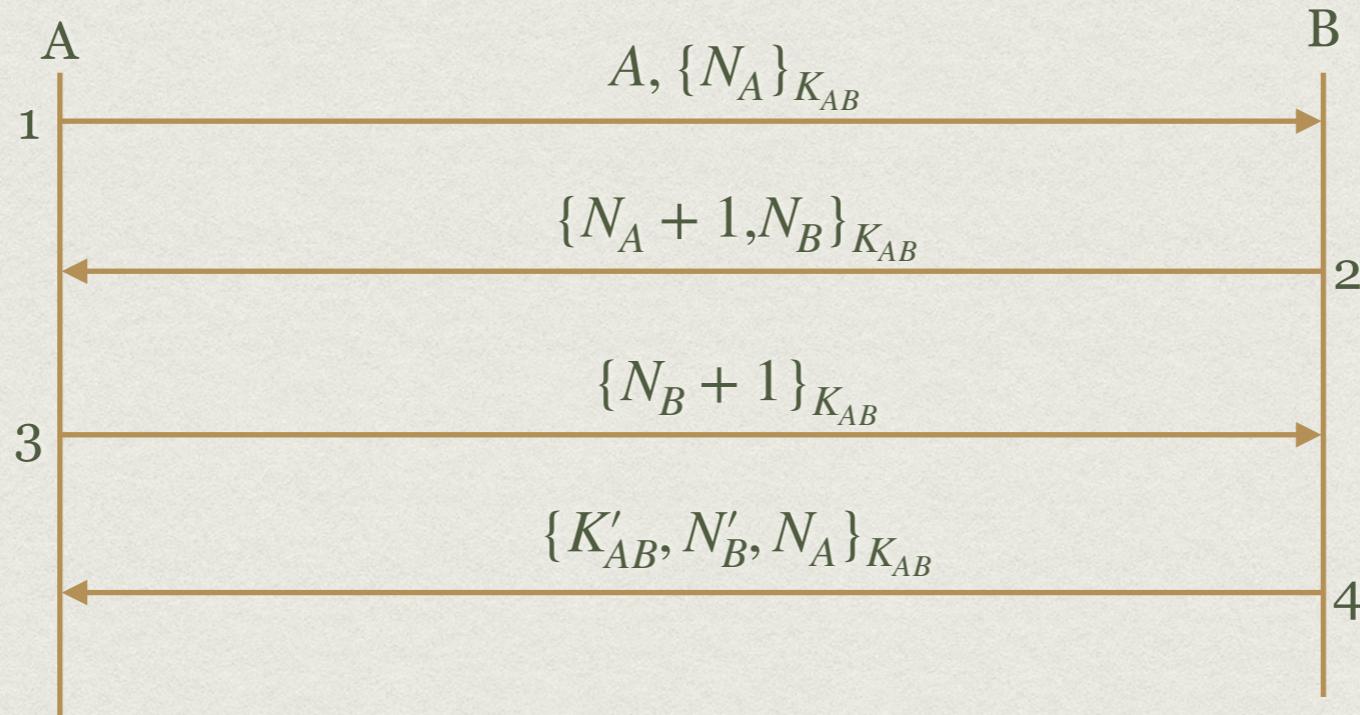
- Génération d'une nouvelle clé k'_{AB} à partir de k_{AB} secret partagé



- Une attaque par rejeu (replay attack) consiste à renvoyer un message précédemment observé
- On l'évite typiquement en liant chaque message aux précédents, par un numéro de séquence, ou par un secret spécifique issu de la session d'échange de messages

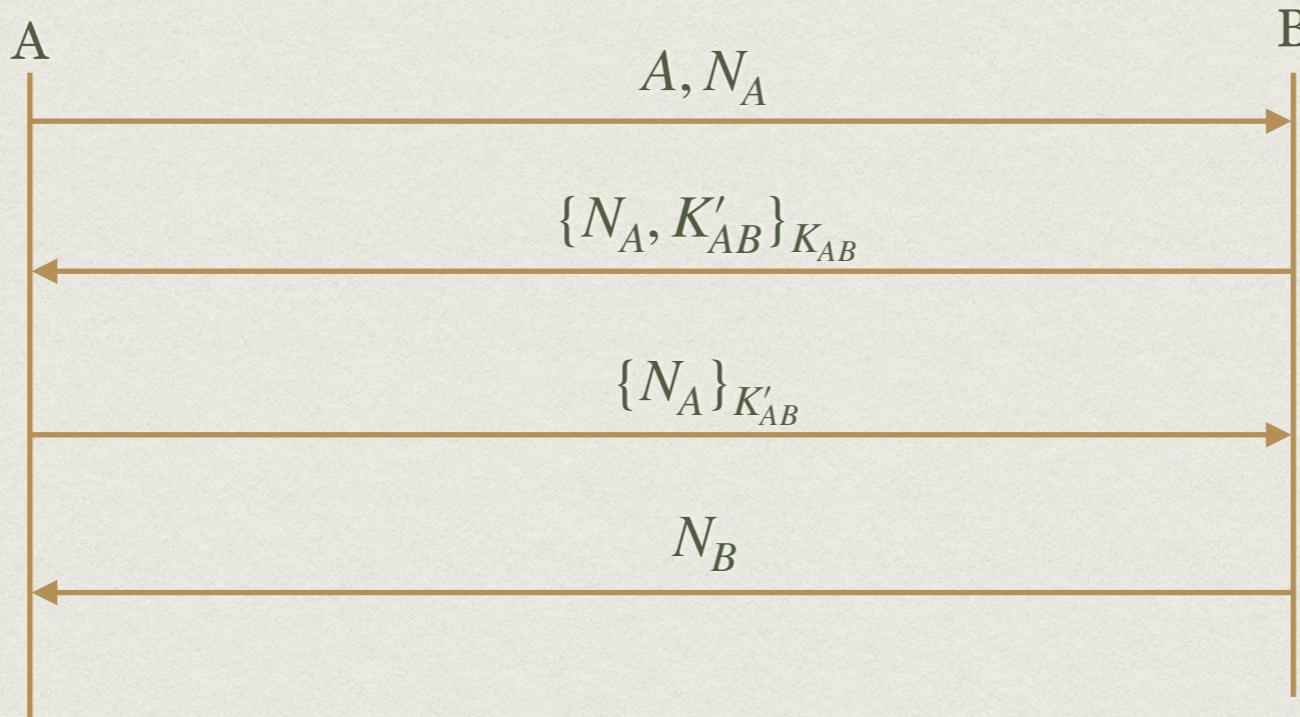
ANDREW SECURE RPC CORRIGÉ

- On lie le msg 4 à la session en y ajoutant N_A



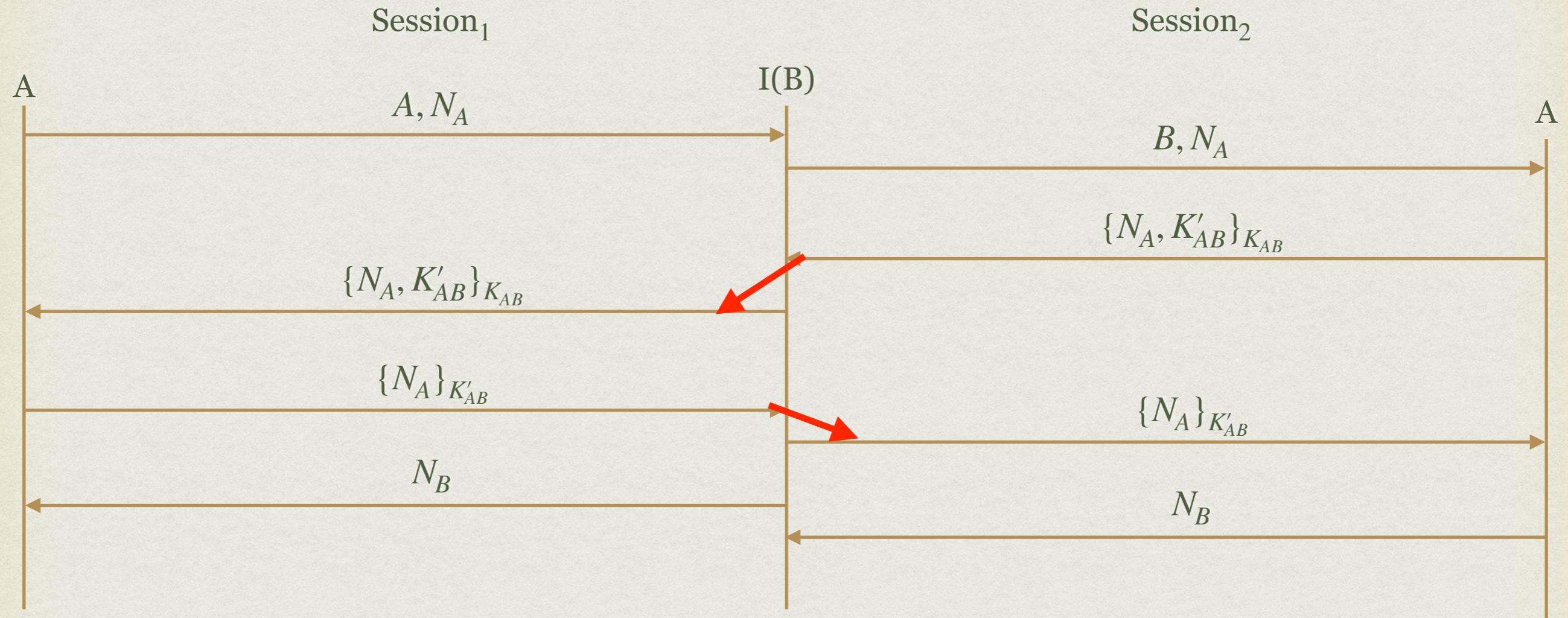
EXAMPLE: MODIFIED ANDREW SECURE RPC

- Génération d'une nouvelle clé k'_{AB} à partir de k_{AB} secret partagé mais avec moins de chiffrement



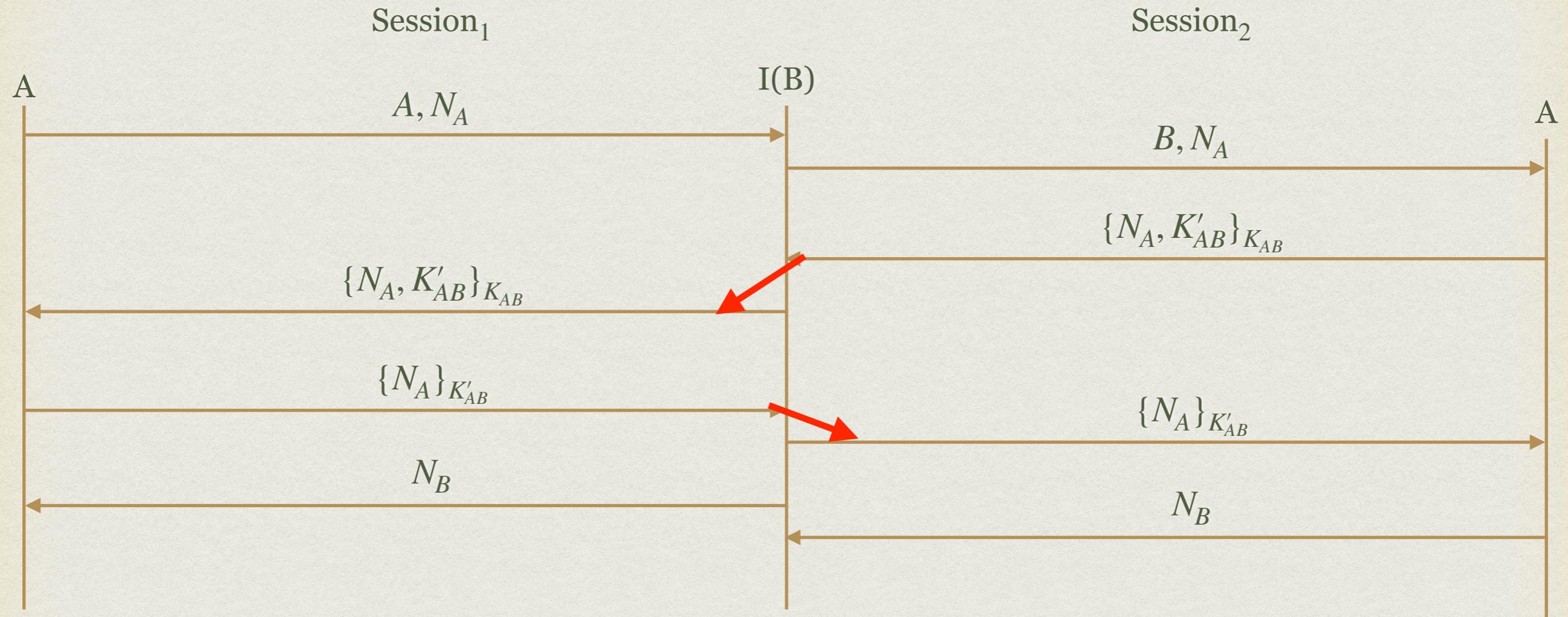
- Ce protocole atteint il les objectifs de sécurité attendus
- Attaques possibles ?

ATTAQUE PAR SESSION PARALLÈLE



- I se fait passer pour B auprès de A dans la session 2

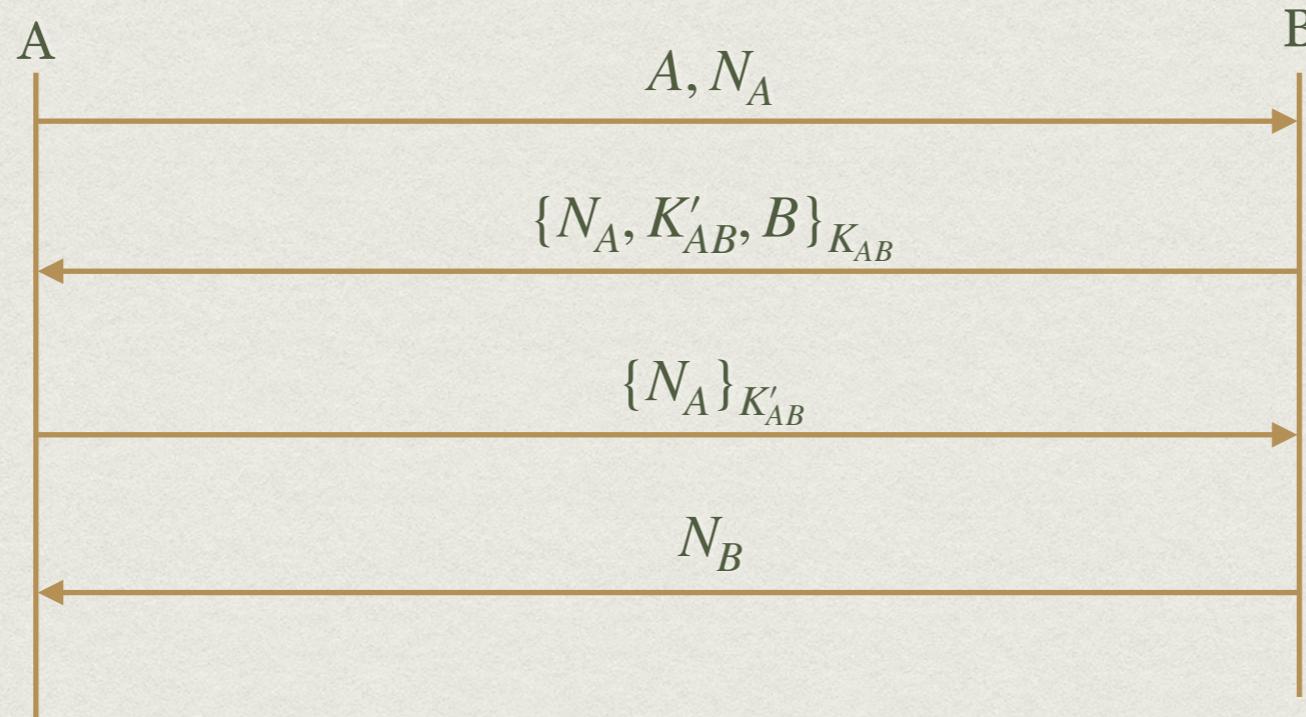
ATTAQUE PAR SESSION PARALLÈLE



- Une attaque par session parallèle consiste à engager deux sessions et rejouer les messages de l'une dans l'autre

MODIFIED ANDREW SECURE RPC CORRIGÉE

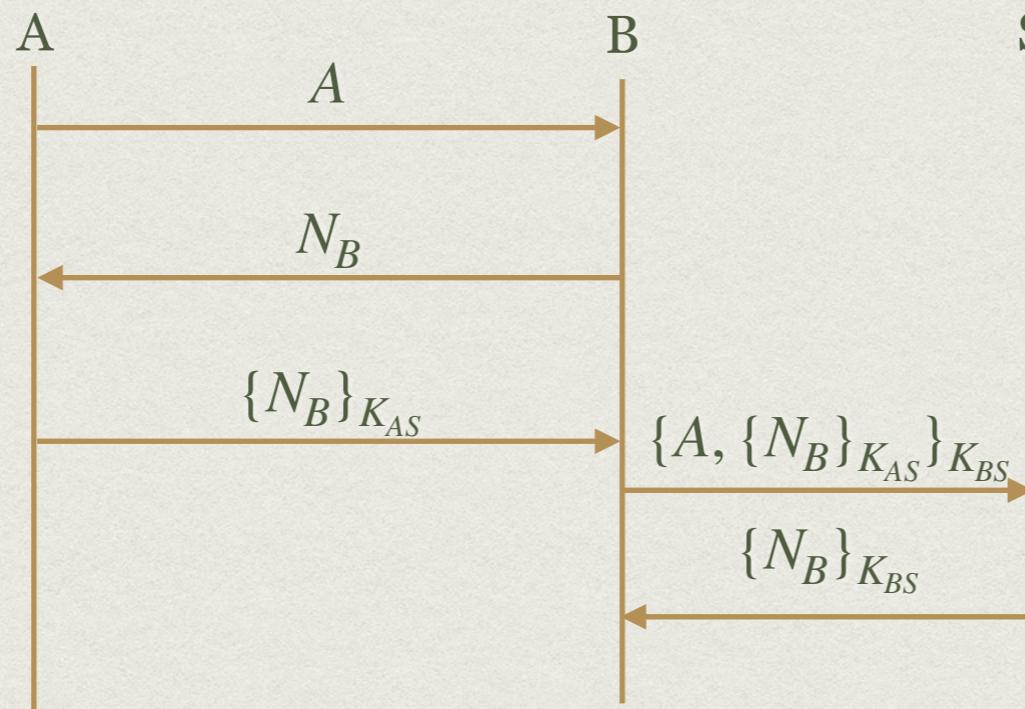
- Génération d'une nouvelle clé k'_{AB} à partir de k_{AB} secret partagé mais avec moins de chiffrement



- On empêche les attaques par sessions parallèles en rendant impossible le rejeu de messages inter-session, ici en rendant le message 2 unidirectionnel

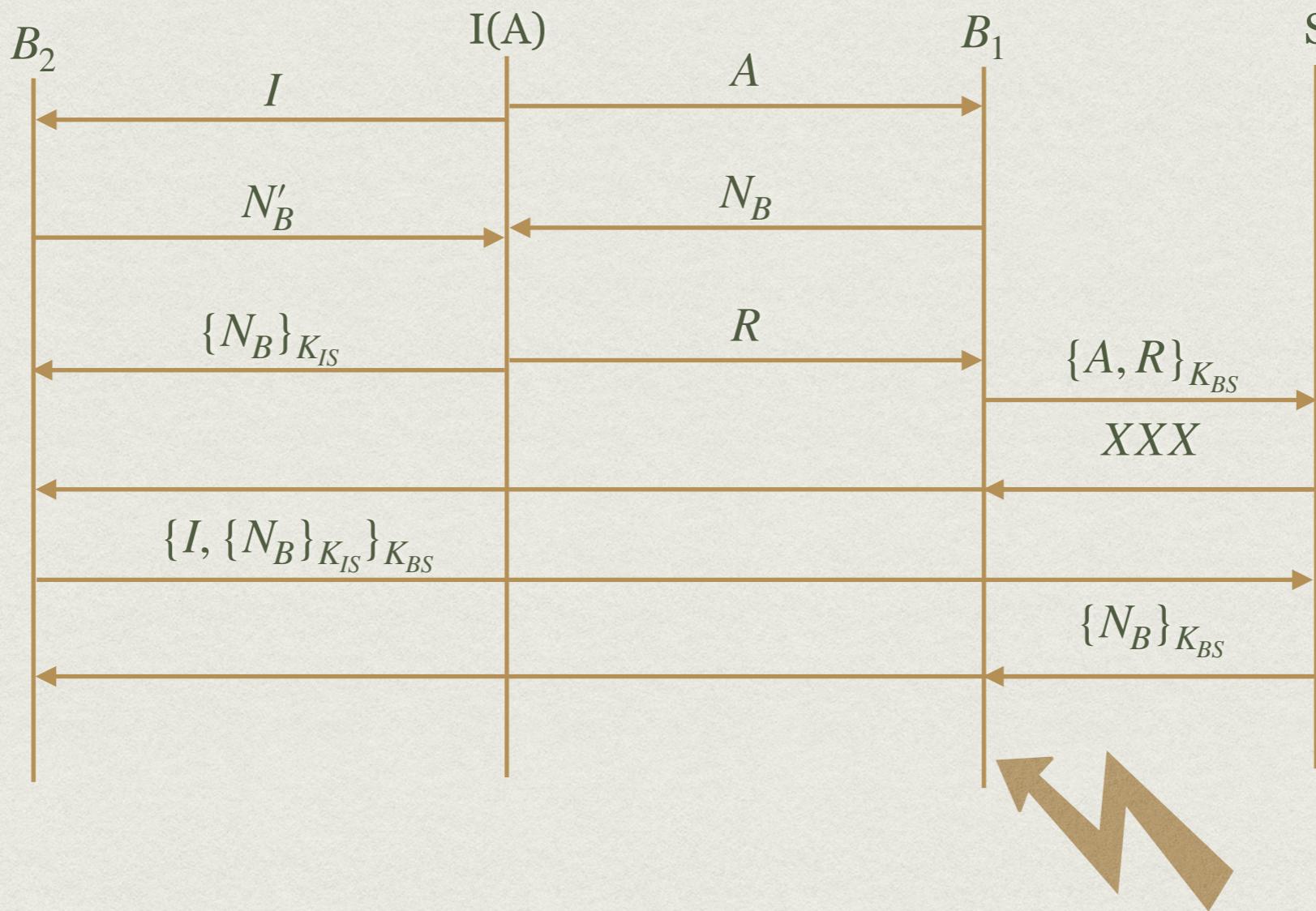
EXAMPLE: AUTHENTIFICATION VIA UN SERVEUR

- k_{AS} et k_{BS} secrets partagés entre (Alice, Bob) et un serveur



- Authentification unilatérale ou mutuelle ?
- Attaques possibles ?

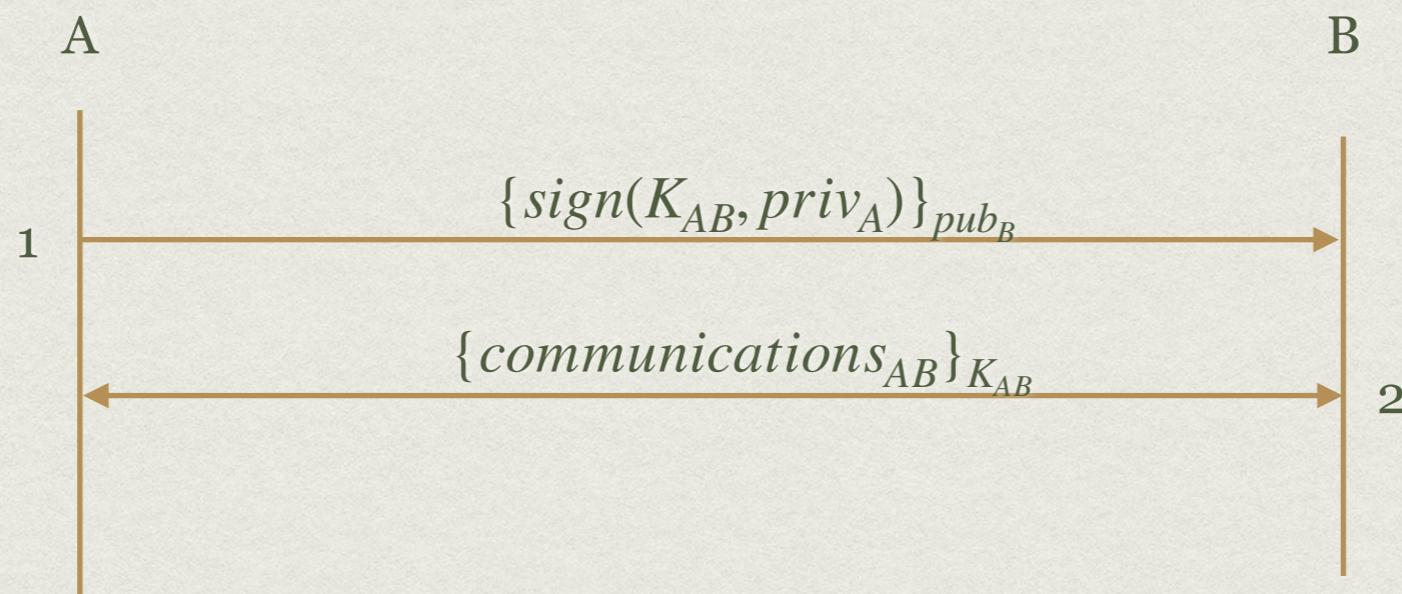
ATTAQUE PAR SESSIONS PARALLÈLES



- I se fait passer pour A auprès de B dans la session 1

PROTOCOLE D'ÉTABLISSEMENT DE CLÉS

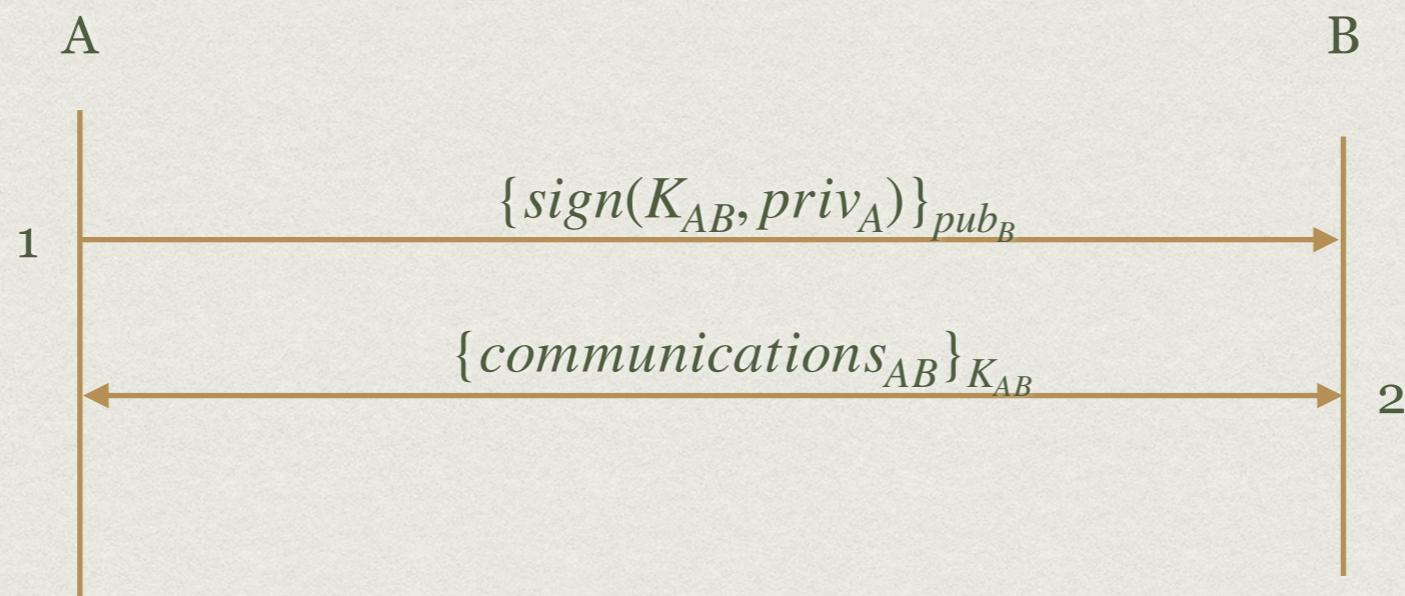
- Objectif : établir une clé symétrique entre Alice et Bob
- Ex.: protocole de Denning Sacco (1981) - simplifié



- Simple et efficace ?

PROTOCOLE D'ÉTABLISSEMENT DE CLÉS

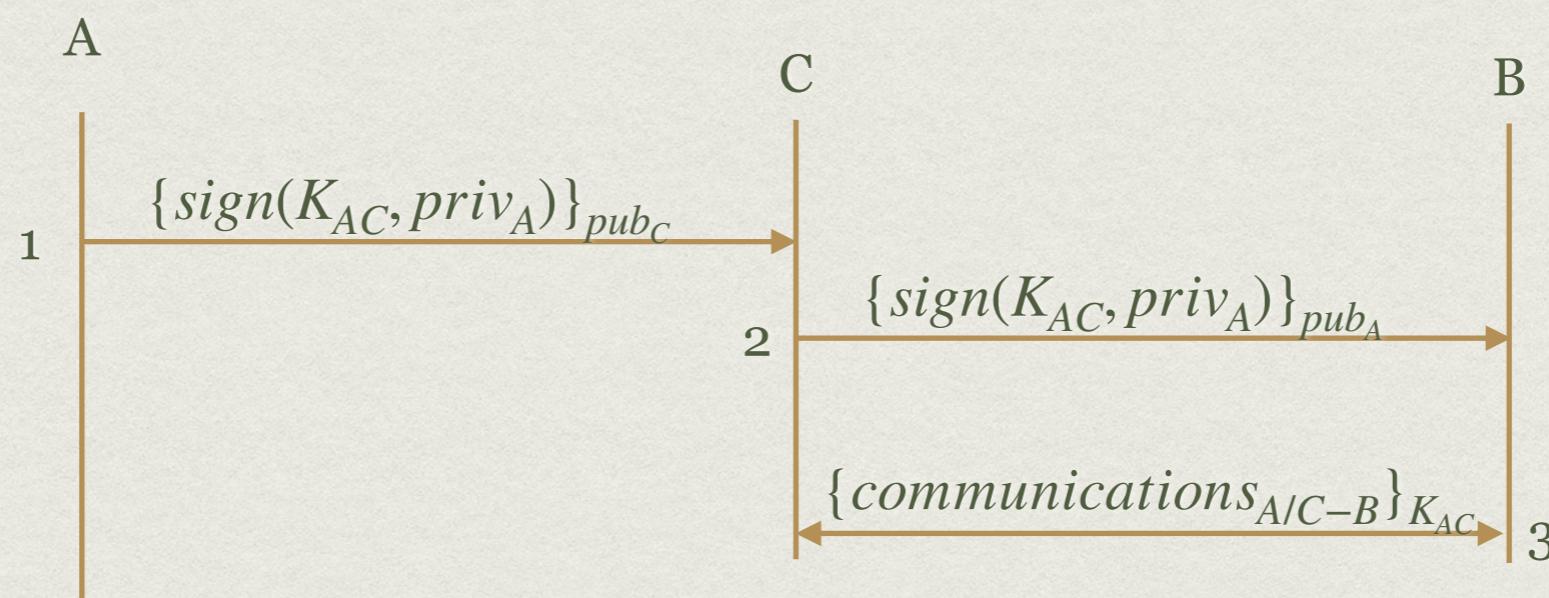
- Objectif : établir une clé symétrique entre Alice et Bob
- Ex.: protocole de Denning Sacco (1981) - simplifié



- Non, C peut impersonner A auprès de B par une attaque dite de l'homme du milieu

PROTOCOLE D'ÉTABLISSEMENT DE CLÉS

- Objectif : établir une clé symétrique entre Alice et Bob
- Ex.: protocole de Denning Sacco (1981) - simplifié



- Non, C peut impersonner A auprès de B en rejouant une partie du message

ATTAQUES LOGIQUES

- Protocoles cryptographiques « faciles » à écrire
- Facile à « casser », par une attaque logique
 - Attaques par rejeu, session //, homme-du-milieu
 - Même en présence de chiffrement parfait
 - Subtiles et difficiles à déceler

ATTAQUES LOGIQUES EXEMPLES RÉELS

- Google Apps - A. Armando et al. 2011
 - Possibilité d'accéder aux différents comptes d'un utilisateur (Gmail, Google calendar, etc.)
 - Créer une application malhonnête; faire en sorte que l'utilisateur y accède connecté à son compte Google; « voler » ses credentials
- Connexion HTTPS - Barghavan et al. 2015
 - Attaque de type MITM permet de faire revivre un vieux mode de chiffrement (taille de clé faible) et ainsi accéder aux données de l'utilisateur
 - Encore plus de 10% des sites https vulnérables (dont canadiantire.ca)

SE PROTÉGER DES ATTAQUES LOGIQUES

- Utiliser des portefeuilles qui bloquent les RF
- Mettre à jour ses logiciels
- Ne pas développer de nouveaux protocoles
- Prouver les protocoles, les applications