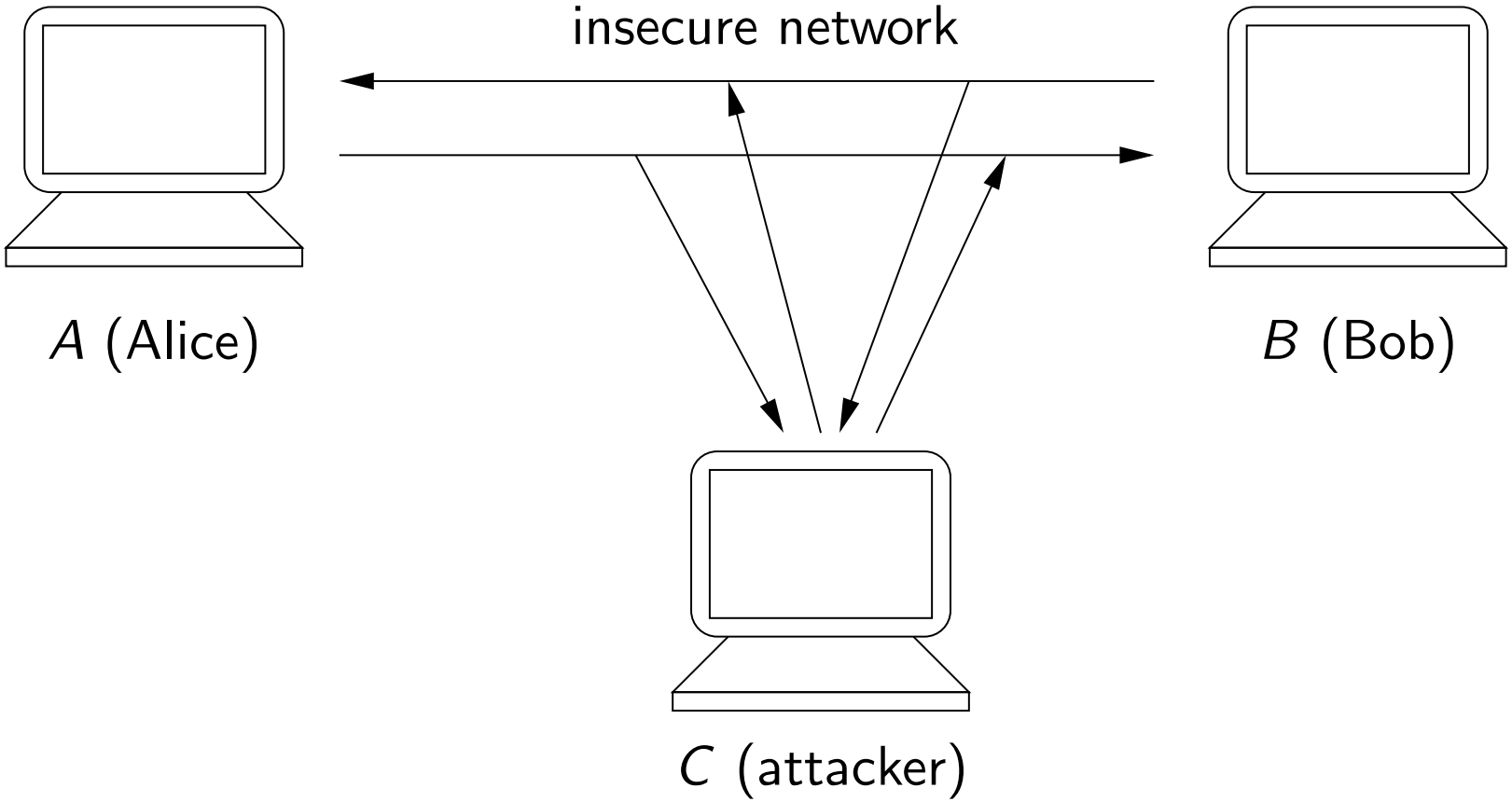
Protocoles cryptographiques: Attaques – Vérification

Bruno Blanchet

INRIA Paris-Rocquencourt
Bruno.Blanchet@inria.fr

Juin 2014

Réseaux non sûrs



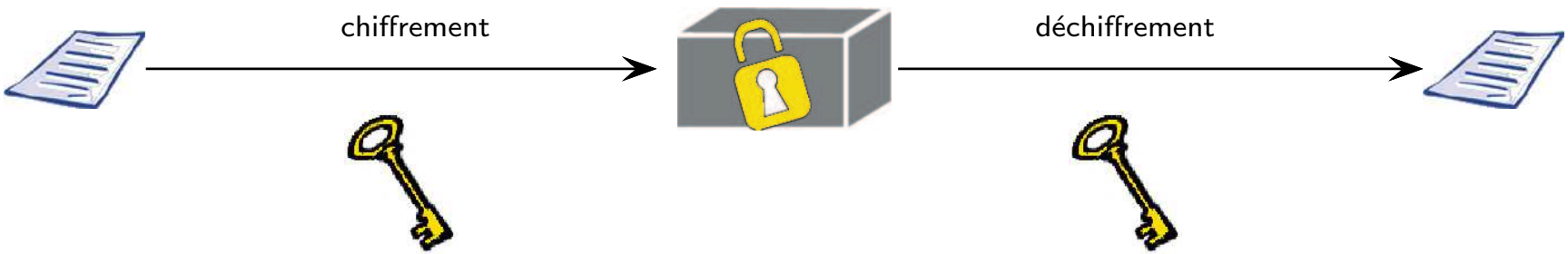
Un attaquant peut

- écouter les messages
- envoyer ses propres messages

Protocoles cryptographiques

- Utiliser la cryptographie pour sécuriser les communications
- Par exemple, chiffrer les données pour préserver le secret

Chiffrement symétrique



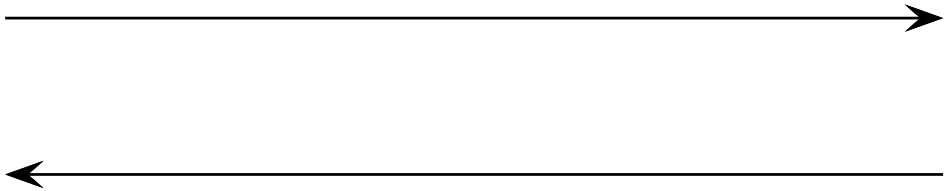
Les protocoles cryptographiques sont partout

cliquer ici pour accéder à la
signature de votre déclaration

Employé nomade

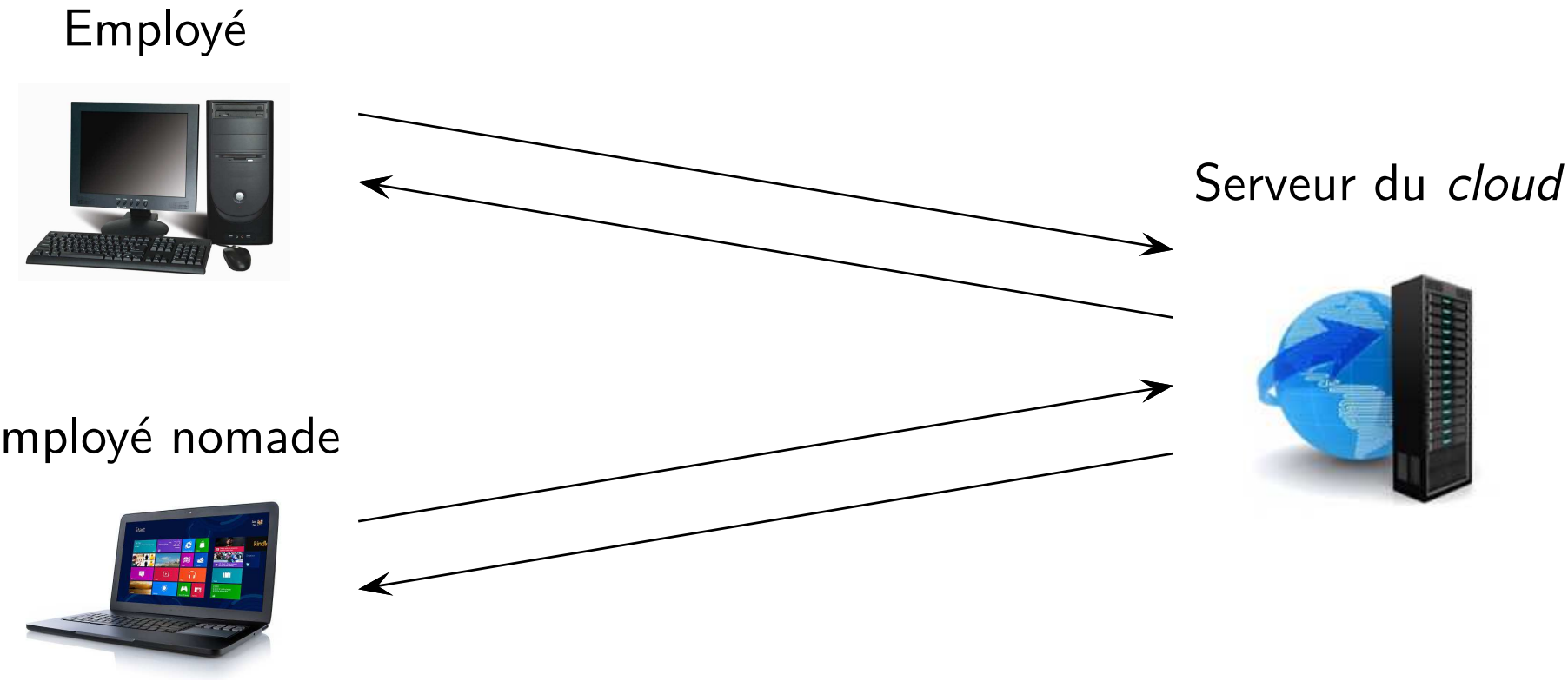
Serveur d'entreprise

Employé nomade



Protocoles habituels : TLS (`https://`) ou IPsec (VPN)

Stockage sur le *cloud*



On fait confiance au fournisseur du *cloud* pour :

- ne pas regarder les données de ses clients ;
- protéger les clients les uns des autres.

Sinon, il faut chiffrer les données avant de les envoyer au *cloud*.

Les protocoles cryptographiques sont difficiles à concevoir

- Des erreurs peuvent apparaître à différents niveaux :
  - primitives
  - protocole
  - implémentation
- Les erreurs de sécurité apparaissant seulement en présence d'un attaquant.
  - Elles ne sont pas détectées par les tests.

$\Rightarrow$ Beaucoup d'attaques sont découvertes contre des protocoles cryptographiques.

Une attaque récente et grave

Le Monde Technologies

TECHNOLOGIES | Jeux vidéo | Hits Playtime | Libertés numériques | Téléphonie mobile | Droit d'auteur | Rése

Faille Heartbleed : les sites pour lesquels il est conseillé de changer son mot de passe

Le Monde.fr | 11.04.2014 à 04h48 • Mis à jour le 14.04.2014 à 15h08 |

Par Michaël Szadkowski

Abonnez-vous à partir de 1 € | Réagir | Classer | Partager

Recommander | Partager | 14 010 personnes le recommandent.

Le changement de son mot de passe est conseillé pour tous les sites qui ont annoncé avoir fait une mise à jour de sécurité, après la découverte du bug qui affecte le protocole OpenSSL. | REUTERS/PAWEL KOPCZYNSKI

Deux jours après la révélation d'une faille de sécurité au sein du protocole OpenSSL, baptisée « Heartbleed », cette dernière est décrite par certains comme *« le pire cauchemar »* qui puisse arriver concernant la sécurité des échanges sur Internet.

LECTURE ZEN

Le logiciel libre OpenSSL est installé sur les serveurs de très nombreux sites pour établir des connexions chiffrées et sécurisées entre ce dernier et ses utilisateurs. De très nombreux sites Internet utilisent OpenSSL pour sécuriser leurs échanges.

Une attaque récente et grave

M TechLesEchos.fr

NEWS BOURSE PATRIMOINE BUSINESS T

TECHNOLOGIES Jeux vidé

FRANCE INTERNATIONAL INDUSTRIE-SERVICES TECH MÉDIAS FINANCE-MARCHÉS RÉG

Faille H
lesquel
son mo

Le Monde.fr | 11.04

Par Michaël Szad

Abonnez-vous à partir de 1 €

Recommander

Le changemen
annoncé avoir f
affecte le proto

Deux jours après
OpenSSL, baptis
« le pire caucher
Internet.

Le logiciel libre C
établir des conne
De très nombreu

LECTURE ZEN

tech-medias • actu

Lesechos.fr • Le 24 avril 2014

Faille informatique « Heartbleed » : les leçons à tirer

La faille informatique baptisée Heartbleed est maintenant réparée. Mais les entreprises ont beaucoup à apprendre de ce malheureux épisode. La confidentialité des données de leurs clients a été mise en danger.

L'hémorragie est arrêtée. Entre mars 2012 et le 7 avril 2014, **la faille informatique Heartbleed (« coeur qui saigne », en anglais) a concerné un très grand nombre de sites Internet, des réseaux sociaux en passant par les banques en ligne et les plates-formes de e-commerce**. Le comble est que le danger provient justement du système chargé de sécuriser l'accès aux services sensibles comme le paiement en ligne...

L'alerte n'intervient que dans les premiers jours d'avril 2014. Jusqu'ici personne n'avaient constaté de péril. Le risque : des cyber-criminels pouvaient facilement retrouver les informations personnelles d'internautes utilisateurs de ces sites, dans la mémoire des serveurs informatiques. Noms et mots de passe en premier lieu. Quelques jours après la

Une attaque récente et grave

L'IMPACT DE LA FAILLE HEARTBLEED S'ÉTEND BIEN AU-DELÀ D'INTERNET

Recommander 6 | g+1 0 | 11/04/14

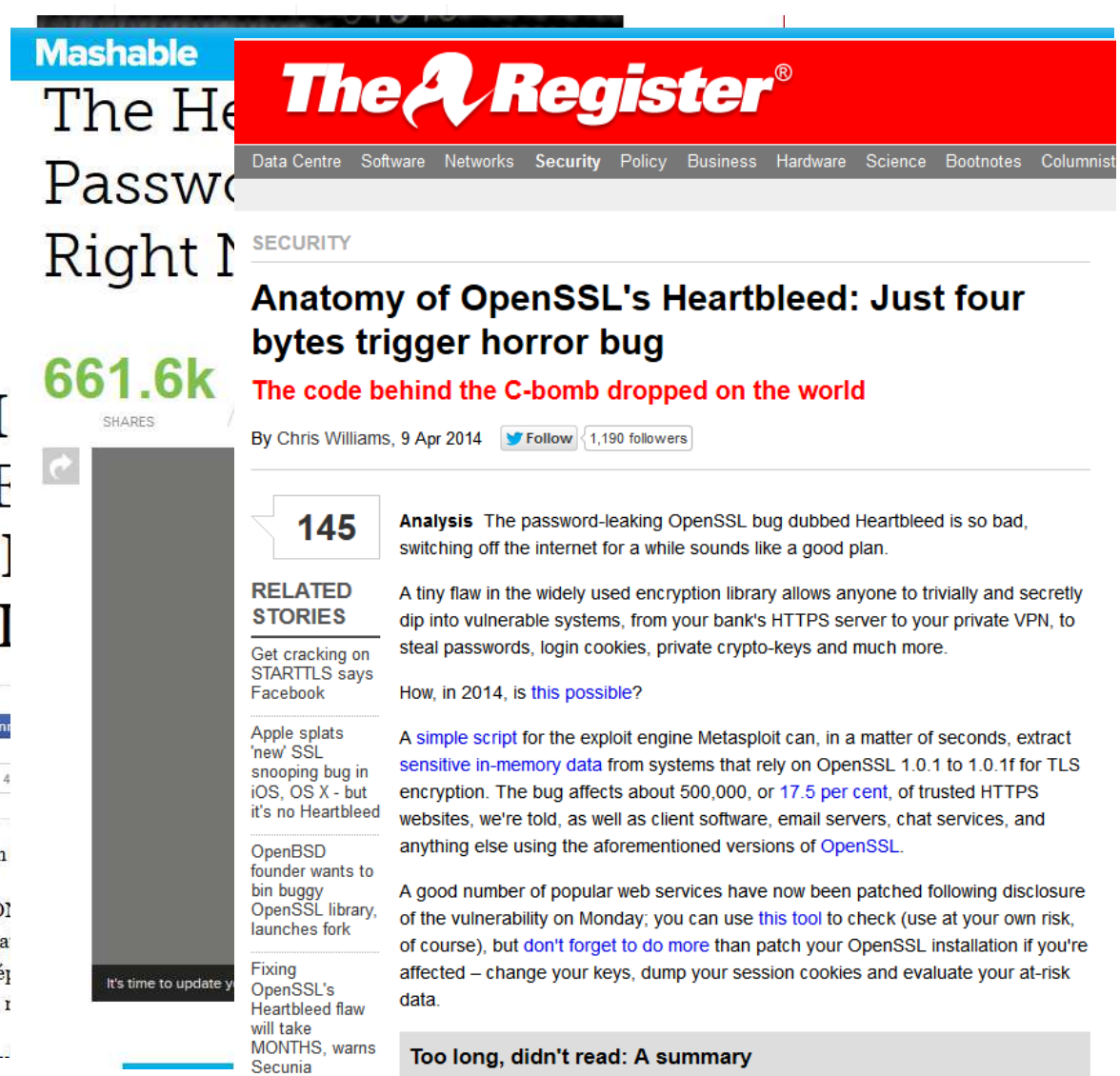
4 | 1 | 0 | 0 | 0 | Réagir 0

par Jim Finkle

BOSTON (Reuters) - La faille de sécurité "Heartbleed" pourrait permettre à des pirates informatiques d'accéder à des boîtes mail, de contourner des pare-feu, voire de pirater des téléphones portables, selon des spécialistes en informatique qui ont prévenu jeudi que les risques pourraient s'étendre au-delà des seuls serveurs internet.

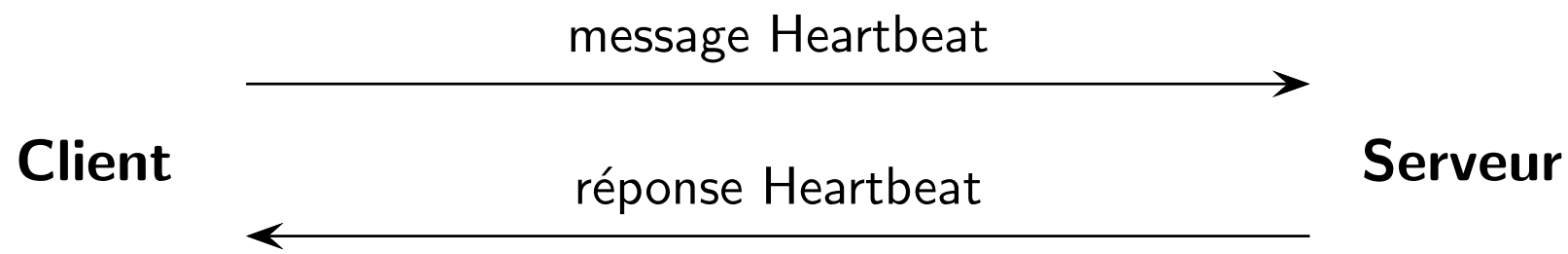
Une attaque récente et grave

Une attaque récente et grave



Heartbleed expliqué

- SSL/TLS : protocole utilisé pour les pages web `https://`.
- Heartbeat : une extension de TLS qui vérifie juste qu'un serveur est vivant.
  - Le client envoie un packet au serveur.
  - Le serveur répond au client avec le même paquet.



- L'attaque :
  1. Un client malhonnête envoie un octet mais dit qu'il a envoyé 65535 octets.
  2. Le serveur répond avec 65535 octets : l'octet du client et les 65534 octets suivants de sa mémoire.

Vérification

Pour détecter ces attaques, il faut vérifier les protocoles formellement.
Plusieurs niveaux :

- Primitives cryptographiques
- Spécification du protocole : description formelle du protocole
- Implémentation : le programme qui implémente le protocole
- Niveau physique : carte à puce, . . .

Modèles des protocoles

	Modèle symbolique	Modèle calculatoire
Messages	Termes $\texttt{encrypt}(M, K)$	Chaînes de bits 0100011
Primitives	Symboles de fonction `encrypt`	Fonctions sur les chaînes de bits
Attaquant	Restreint à n'utiliser que les primitives	N'importe quel algorithme

Conclusion

- Penser tôt à la sécurité
  - Quand il y a une attaque, il est trop tard !
- Utiliser les outils disponibles, ne pas chercher à recréer ses propres protocoles
- Faire des mises à jour régulières
- Les méthodes formelles peuvent servir
  - miTLS, une implémentation de référence vérifiée de TLS, `www.mitls.org`