La sécurité numérique et vous ?

Pascal Lafourcade

Chaire industrielle,
Confiance numérique

13 mai 2014

Objectifs de la Chaire de Confiance Numérique

Mise en place d'une activité de recherche traitant des aspects de la Confiance Numérique autour de la fiabilisation et de la sécurisation des systèmes et des services informatiques

- Pérenne
- Visible

Activité de recherche:

- Impulsée par almerys et la Caisse d'Epargne d'Auvergne et du Limousin via la Fondation de l'Université d'Auvergne
- Soutenue par le Région Auvergne
- Developpée au LIMOS

Objectifs de la Chaire de Confiance Numérique

- Recrutement d'un enseignant chercheur spécialiste du domaine qui sera le pivot nécessaire au démarrage et l'installation de cette activité
- Organisation d'une réflexion sur les actions de formation à mener des actions de dissémination et de transfert de technologies (Workshop, Projets ANR FUI,..)
- Mise en place et animation d'un groupe de réflexion et d'un séminaire pour échanger sur cette problématique

`http://confiance-numerique.clermont-universite.fr/`

Déjà plus de 30 séminaires (France, UK, Suisse, Espagne etc ...)

http://confiance-numerique.clermont-universite.fr/

- Chiffrement (compltement) homomorphe : de la théorie à la pratique
- Enjeux et impacts juridiques du chiffrement homomorphe
- Combinaison d'analyses statiques pour l'aide à la détection et à l'exploitabilité de vulnérabilités dans du code binaire
- Keep calm and change your password
- Authentication Using Pulse-Response Biometrics
- Security issues and Directions of Intelligent Transport Systems within limited-resources constraints
- IoT: Internet of (Insecure) Things
- Signature électronique et identité numérique : les ingrédients indispensables pour développer la confiance sur Internet.
- Primitives et constructions cryptographiques pour la confiance numérique.
- Je sais tout sur vous grâce au Wi-Fi!
- Vers un carte d'identité respectueuse de la vie privée.
- Identifiants et guesswork.
- Les nouvelles armes de James Bond.
- Virus dans une carte mythe ou (proche) réalité ?
- La confiance numérique, de l'autre côté du miroir...
- Comment avoir confiance dans les applications numériques ? Les méthodes formelles à la rescousse.
- Comment remettre l'internaute au centre des échanges ?

Séminaire Confiance Numérique

Prochain Séminaire

- Jeudi 5 Novembre 2015, 14h00 :

  E. Thomé **Menaces sur RSA et Diffie-Hellman: nouveaux algorithmes et nouveaux records.**

  S. Grzonkowski. **Symantec, Dublin, SMS spam: a holistic view.**

- Live et replay sur la web TV de l'UDA.
- Inscriptions : `pascal.lafourcade@udamail.fr`

FPS'15

8th International Symposium
on Foundations & Practice of Security

26, 27 et 28 Octobre 2015 Clermont-Ferrand

confiance-numerique.clermont-universite.fr/fps2015

Livre chez Dunod

Info Sup

Jean-Guillaume Dumas,
Pascal Lafourcade, Patrick Redon

Architectures PKI et communications sécurisées

Cet ouvrage s'adresse aux étudiants de master (mathématiques appliquées, informatique...), aux élèves-ingénieurs, aux enseignants-chercheurs et ingénieurs en sécurité numérique.

Son objectif est de fournir une approche compréhensible des techniques, technologies et enjeux liés aux **infrastructures de gestion de clefs publiques** (PKI, *Public Key Infrastructure*).

L'originalité de cet ouvrage est de présenter les **principes mathématiques et informatiques** qui fondent les PKI, mais aussi de donner une approche pratique de leur déploiement : il présente les dernières recommandations nationales (RGS) et européennes (e-IDAS) ainsi que de **nombreuses applications**, comme la gestion de la sécurité des navigateurs Internet et des systèmes d'exploitation ou encore de la monnaie électronique Bitcoin.

L'accent est mis sur une **présentation détaillée** et approfondie, alliant fondements théoriques, protocoles cryptographiques en vigueur et **standards les plus récents**.

Cet ouvrage comporte également plus de **50 exercices corrigés originaux**.

RESSOURCES NUMÉRIQUES

Le **code source** des exemples est disponible en téléchargement à l'adresse suivante :
www.dunod.com/contenus-complémentaires/9782100726158

9 782100 726158

6244596
ISBN 978-2-10-072615-8

LICENCE MASTER DOCTORAT
1 2 3 4 5 6 7 8

Les actus du savoir

DUNOD
dunod.com

Jean-Guillaume Dumas
est professeur, il enseigne à l'université de Grenoble-Alpes dans les masters SAFE (Sécurité, audit, informatique légale) et SCCI (Sécurité, cryptologie et codage de l'information).

Pascal Lafourcade
est titulaire d'une chaire industrielle à l'université d'Auvergne. Il travaille sur la vérification de protocoles cryptographiques au Laboratoire informatique, modélisation et optimisation des systèmes (LIMOS) de Clermont-Ferrand.

Patrick Redon
est expert en sécurité des SI dans le secteur de la Défense, de la cybersécurité et de la protection des infrastructures critiques. Il enseigne dans le master SAFE de l'université de Grenoble-Alpes.

Info Sup

J.-G. Dumas
P. Lafourcade
P. Redon

Architectures PKI

Master • Écoles d'ingénieurs

Architectures PKI et communications sécurisées

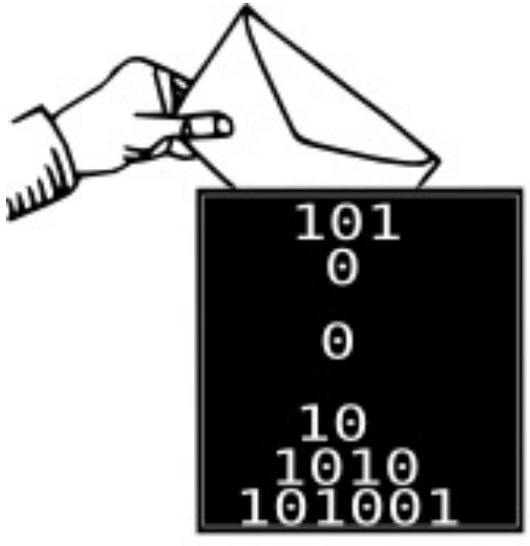
Jean-Guillaume Dumas
Pascal Lafourcade
Patrick Redon

DUNOD

Outline:

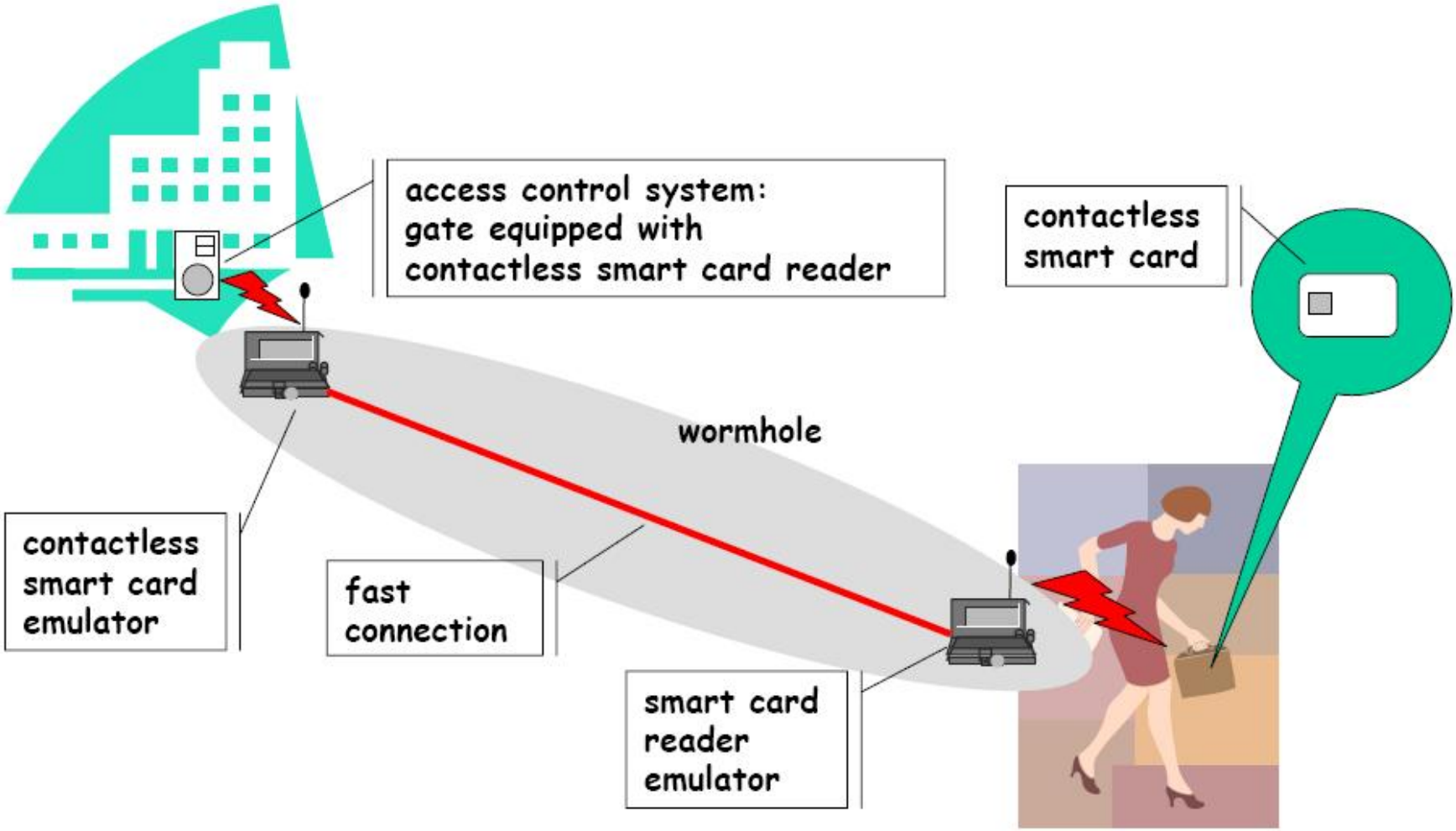
Outline

La sécurité est omniprésente !

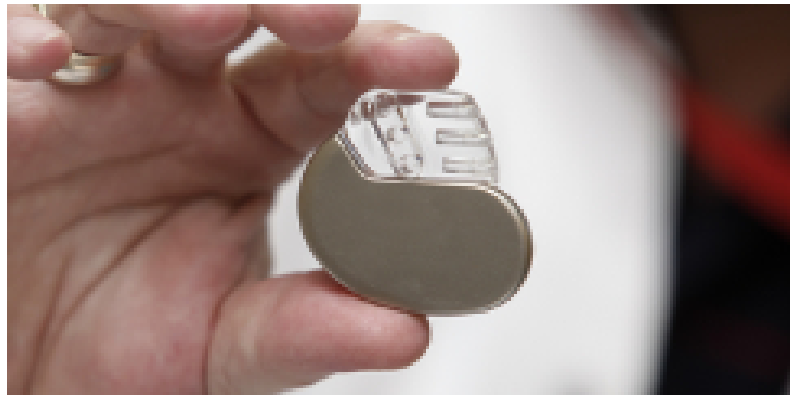


À cause du succés de l'informatique

“Wormhole Attack”



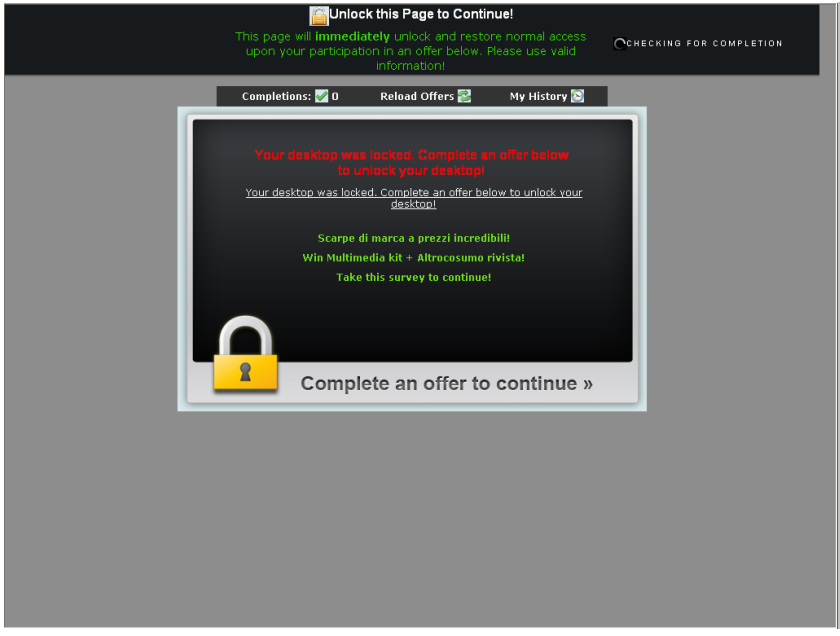
Hacking Pacemakers (2012)



5 Famillies of Cyber Criminality

- Ransomwares
- Phishing
- Botnets and zombies
- Espionnage
- Sabotage

Ransomwares



http://stopransomware.fr/

Hameçonnage (Phising)

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

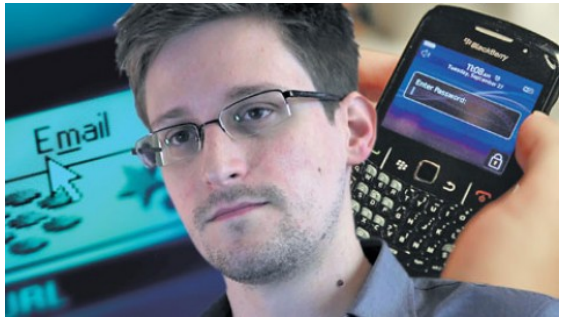
http://www.societegenerale.fr/espaceclient:
id=56452575711&res=lorem-ipsum-dolor&quux=2&lang=
frsessid=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMI
88.132.11.17

Botnets and Zombies

Espionnage

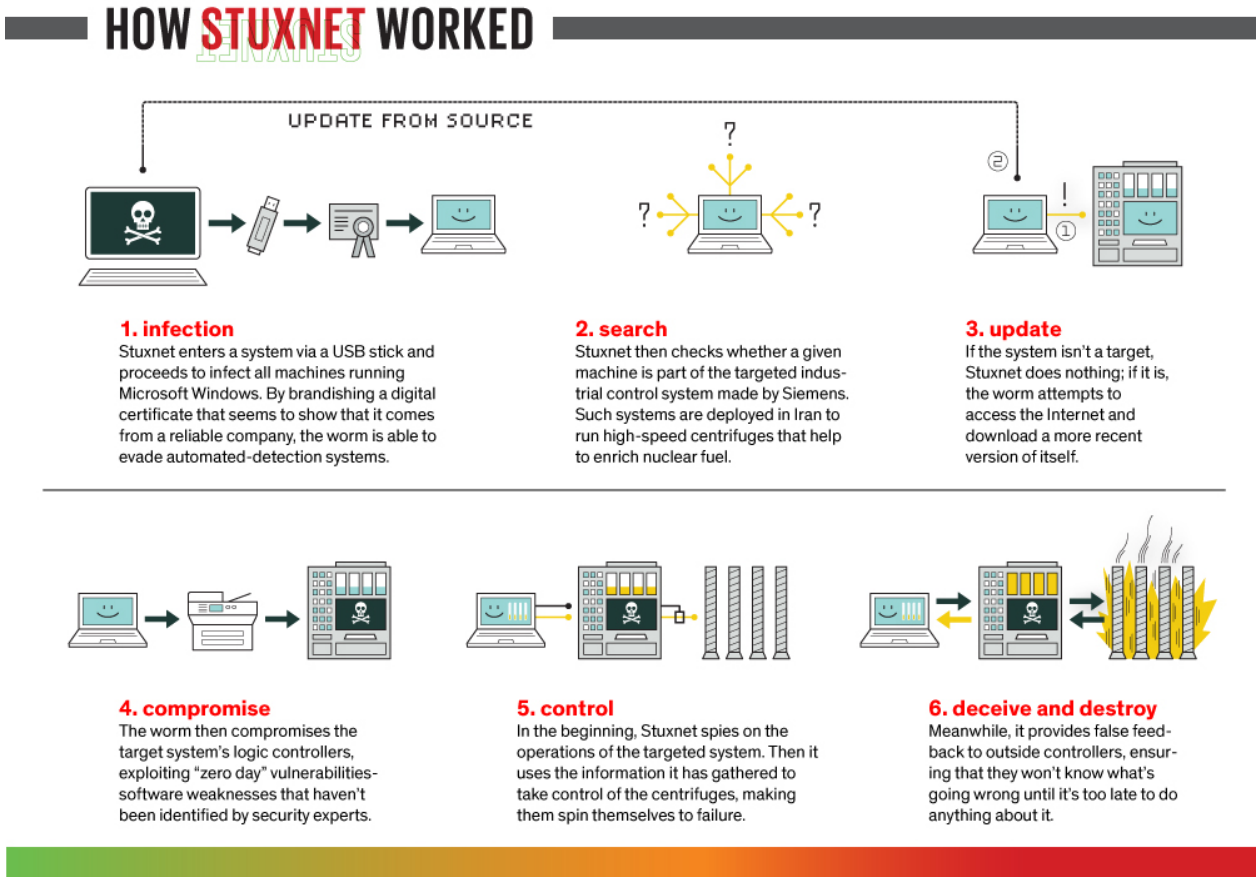
- Big Brother (Government)
- Medium Brother (Corporation)
- Little Brother (Individual)

Edward Joseph Snowden, 6th june 2013



Sabotage

Stuxnet, 2010



Saudi Aramco 30 000 PC effacés.

http://cybermap.kaspersky.com/

 Toggle Demo Mode

Pourquoi y-a-t-il de plus en plus d'attaques?

- Faisable à la maison
- Peu cher, self-service
- Rapide, large échelle, semi-automatique
- Fausse impression d'être anonyme

Pourquoi y-a-t-il de plus en plus d'attaques?

- Faisable à la maison
- Peu cher, self-service
- Rapide, large échelle, semi-automatique
- Fausse impression d'être anonyme

Internet a été conçu pour fonctionner pas pour être sûr !

Outline

La sécurité numérique est déjà là

Mais prendre de bonnes habitudes ça prend du temps ...

même quand c'est important

Devenir acteur de sa sécurité numérique

Devenir acteur de sa sécurité numérique

car la sécurité c'est pas automatique.

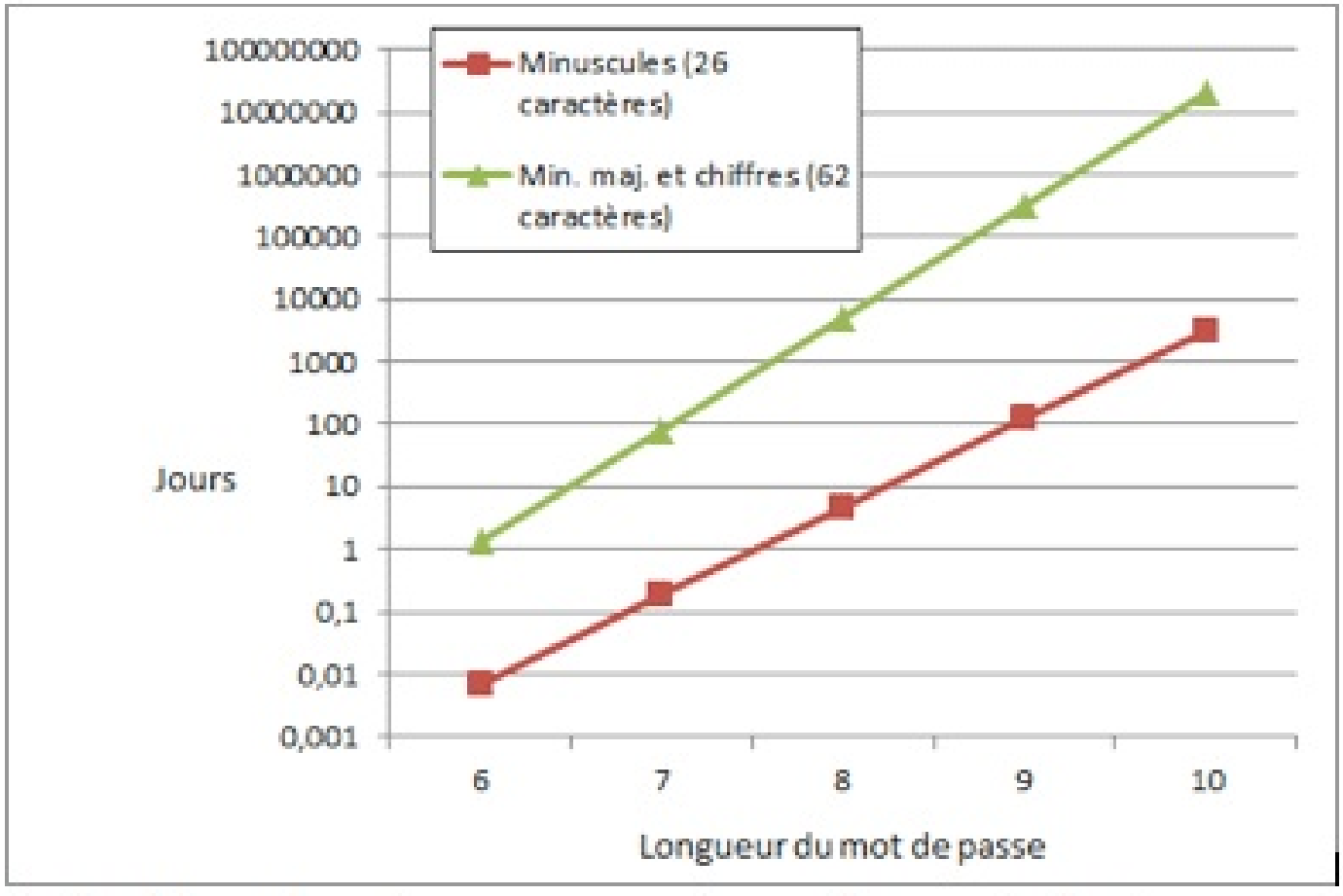
Sécurité de mes mots de passe

Sécurité de mes mots de passe

Top 25 en 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

Passwords: Brute force



Suite aux fuites ...

Suite aux fuites ...

... j'ai changé mes mots de passe !

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Outline

Octobre 2014

TED
Ideas worth spreading

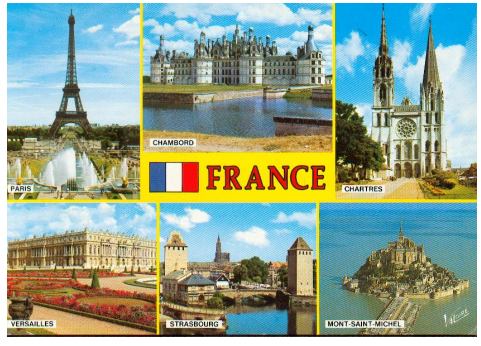
L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...

`http://jenairienacacher.fr/`

La sécurité des emails par défaut

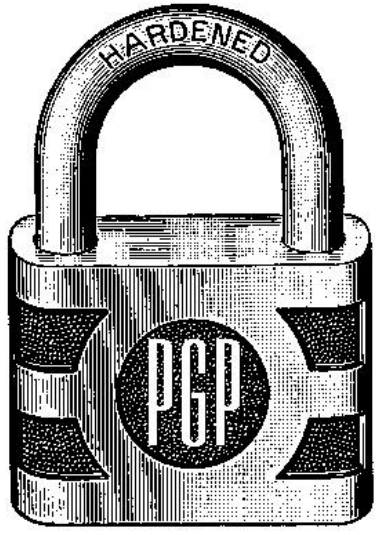


Première demande d'E. Snowden ...

... utiliser PGP

Pretty Good Privacy

Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991.

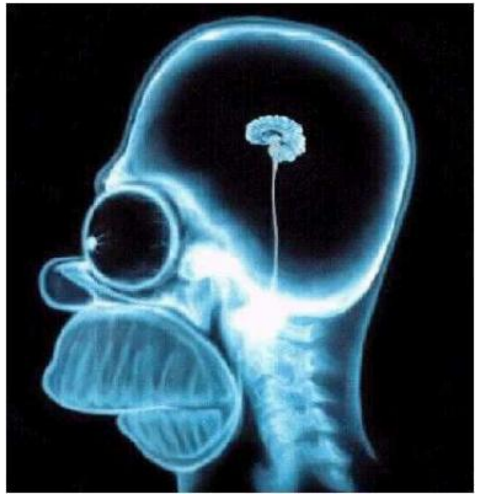


Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.

If privacy is outlawed, only outlaws will have privacy

Est-ce si difficile ?

1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs $\geq$ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



Outline

Principales propriétés de sécurité

- Confidentialité ou Secret
- Authentification
- Intégrité
- Disponibilité

Authentification

"On the Internet, nobody knows you're a dog."

Mécanismes pour l'authentification

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

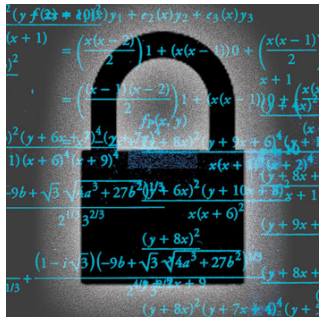
Other security properties

- Perfect Forward Secrecy
- Non-repudiation
- Équité
- Privacy

Outline

Formal Verification Approaches

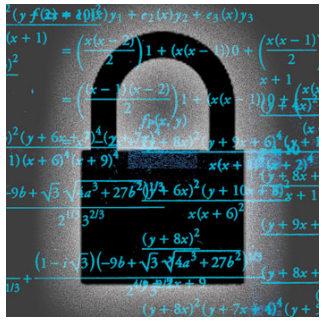
Designer



Attaquant

Formal Verification Approaches

Designer

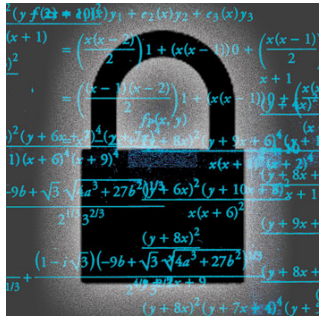


Attaquant

Équipe de Sécurité

Formal Verification Approaches

Designer



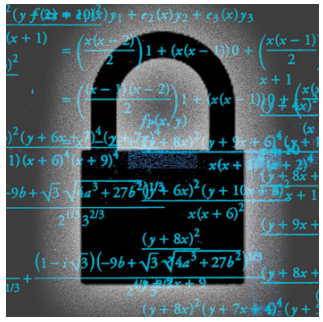
Attaquant

Donner une preuve

Équipe de Sécurité

Formal Verification Approaches

Designer



Attaquant

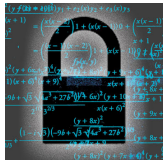
Donner une preuve

Trouver une attaque

Équipe de Sécurité

Sécurité basée sur la cryptographie ?

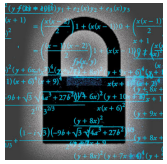
Cryptographie:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocoles: Algorithmes distribués

Sécurité basée sur la cryptographie ?

Cryptographie:



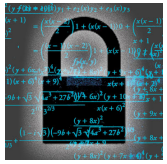
- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocoles: Algorithmes distribués

Propriétés:

- Secret
- Authentification,
- Privacy ...

Sécurité basée sur la cryptographie ?

Cryptographie:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocoles: Algorithmes distribués

Propriétés:

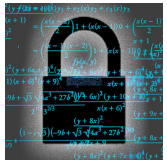
- Secret
- Authentification,
- Privacy ...

Intruders:

- Passif
- Actif
- CPA, CCA ...

Sécurité basée sur la cryptographie ?

Cryptographie:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocoles: Algorithmes distribués

Propriétés:

- Secret
- Authentification,
- Privacy ...

Intruders:

- Passif
- Actif
- CPA, CCA ...

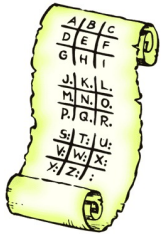
Proposer des protocoles cryptographiques **sûrs**, c'est **difficile**

Securité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?

Securité des protocoles cryptographiques

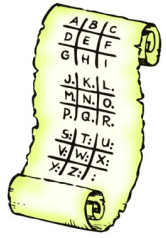
Comment se convaincre qu'un protocole est sûr?





Securité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?

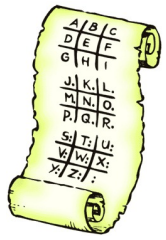




- Prouver qu'il n'y a pas d'attaque sous certaines hypothèses.

Securité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?

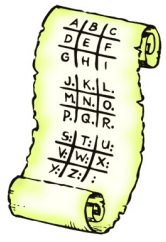




- Prouver qu'il n'y a pas d'attaque sous certaines hypothèses.
  - faire les preuves c'est difficile,
  - et sujetes aux erreurs.

Securité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?



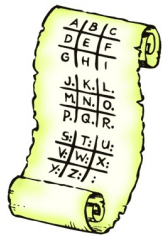


- Prouver qu'il n'y a pas d'attaque sous certaines hypothèses.
  - faire les preuves c'est difficile,
  - et sujetes aux erreurs.

Comment se convaincre qu'une preuve esr correcte?

Securité des protocoles cryptographiques

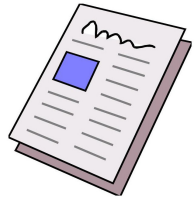
Comment se convaincre qu'un protocole est sûr?



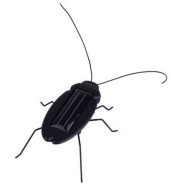


- Prouver qu'il n'y a pas d'attaque sous certaines hypothèses.
  - faire les preuves c'est difficile,
  - et sujetes aux erreurs.

Comment se convaincre qu'une preuve esr correcte?

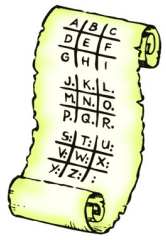






Securité des protocoles cryptographiques

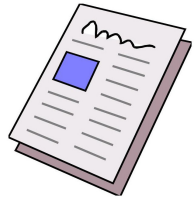
Comment se convaincre qu'un protocole est sûr?



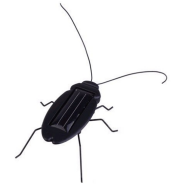


- Prouver qu'il n'y a pas d'attaque sous certaines hypothèses.
  - faire les preuves c'est difficile,
  - et sujetes aux erreurs.

Comment se convaincre qu'une preuve esr correcte?







Computer-Aided Security

Mes sujets de recherche

- Preuve automatique de cryptosystèmes
- e-services : e-voting, e-auction, e-reputation, e-cash, e-exam
- Stoackages Anonymes
- WSN, NFC

Outline

En résumé

- La sécurité est omniprésente
- **Sécurité = Cryptographie + Propriétés + Adversaires**
- Devenez acteur de votre sécurité

  PASSWORDS + CHIFFRER/SIGNER VOS EMAILS

- Sécurité assistée par ordinateur.

Merci pour votre attention.

Questions ?