

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
- ▶ Développée 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 (complètement) 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 ?

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`

8th International Symposium
on Foundations & Practice of Security
26, 27 et 28 Octobre 2015 Clermont-Ferrand



confiance-numerique.clermont-universite.fr/fps2015



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 clés 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 (RCS) 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**.



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



9 782100 726158
6244566
ISBN 978-2-10-072615-8



Les actus
du savoir



DUNOD
dunod.com

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:

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

Conclusion

Outline

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

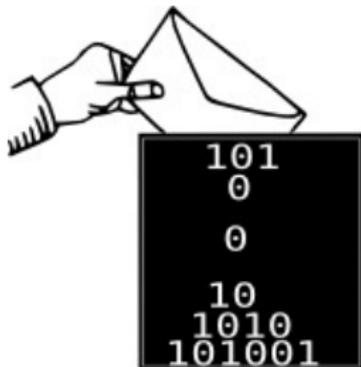
Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

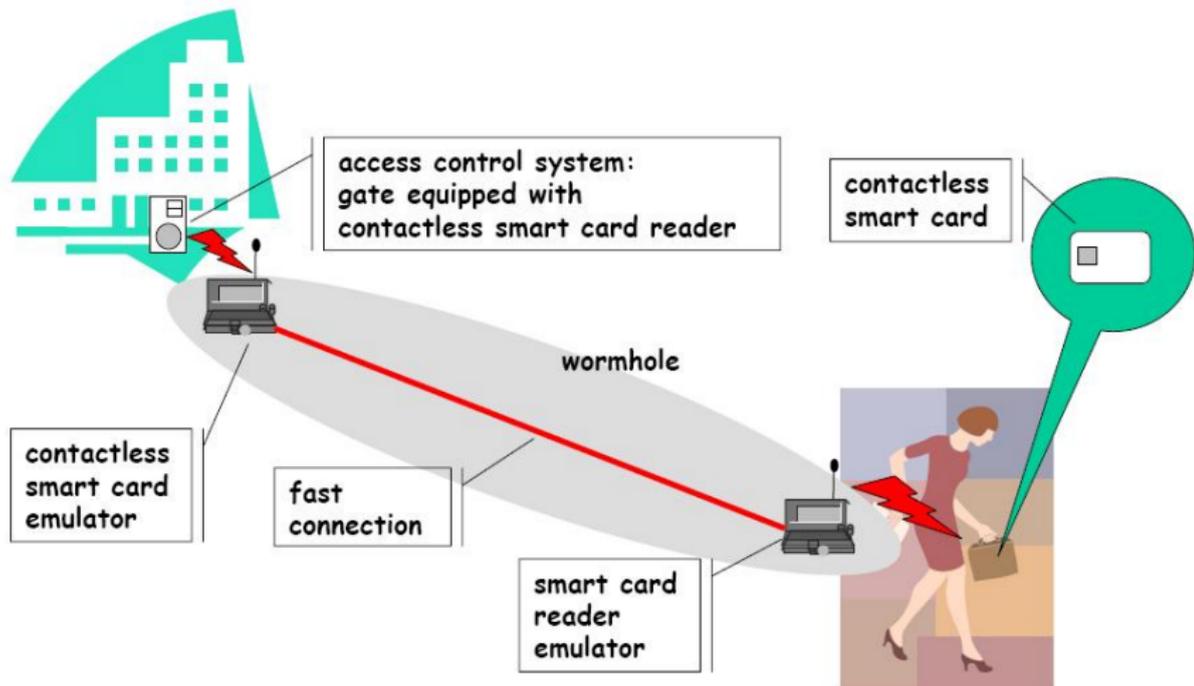
Conclusion

La sécurité est omniprésente !



À cause du succès de l'informatique

“Wormhole Attack”



Hacking Pacemakers (2012)



5 Families of Cyber Criminality

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



Ransomwares

Unlock this Page to Continue!

This page will immediately unlock once you restore normal access upon your participation in an offer below. Please use valid information. CHECKED FOR COMPLETION

Completed: 0 Refused Offers My History

Your desktop was locked. Complete an offer below to unlock your desktop!

Your desktop was locked. Complete an offer below to unlock your desktop!

Scame di meno a prezzi incredibili
Wie Malware da > Altruismus risistat
Take this server to ransom!

 Complete an offer to continue »

ATTENTION!

Votre ordinateur est bloqué en raison du DMIT de la loi de la France

En réalisant les visiteurs suivants:
• le fait d'une prise de main du site. Inscription ou le transfert des documents du contenu personnalisé avec la participation des visiteurs, le programme système en raison des archives, de la sécurité et des autres systèmes en un seul-coucoune les archives. La punition est prévue par l'article 227-17) du Code pénal de la France. Cela est puni par une sanction pénale de 2 à 5 ans.
• l'exploitation du logiciel avec le violation des droits d'auteur. La punition est prévue par l'article 323-2) du Code pénal de la France. Cela est puni par une sanction pénale de 1 à 3 ans.
• l'envoi des données multiples avec la violation des droits d'auteur. La punition est prévue par l'article 323-2) du Code pénal de la France. Cela est puni par une sanction pénale de 1 à 3 ans.

Pour un délit contre l'indivisibilité, il sera fait usage l'ensemble conformément par la législation française dans le montant de 100 euros aux 2 jours à partir. La punition est prévue par l'article 227-17) du Code pénal de la France. Cela est puni par une sanction pénale de 2 à 5 ans.
• l'exploitation du logiciel avec le violation des droits d'auteur. La punition est prévue par l'article 323-2) du Code pénal de la France. Cela est puni par une sanction pénale de 1 à 3 ans.
• l'envoi des données multiples avec la violation des droits d'auteur. La punition est prévue par l'article 323-2) du Code pénal de la France. Cela est puni par une sanction pénale de 1 à 3 ans.

Da puis-je acheter un voucher Ukash?

Acheter Ukash dans plus de 25 000 points de vente en France. Vous pouvez acheter Ukash dans des centaines de milliers de points de vente dans le monde entier, sur Internet, des distributeurs, magasins DPE, et comptés 60 bureaux de poste, Pharmacies et 60000 services.

 **Take money** - Ukash est disponible dans des milliers de points de vente.

 **Yoursite** - Ukash est maintenant disponible dans les Cadeaux de Noël.

www.ukash.com  **Banking** - Ukash est en ligne 24/7 avec Visa / MasterCard ou Carte Bancaire.

payer une amende de 100 €



<http://stopransomware.fr/>

Hameçonnage (Phishing)



Dear valued customer of TrustedBank,

We have received 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 discrepancy. We are happy you have chosen us to do business with.

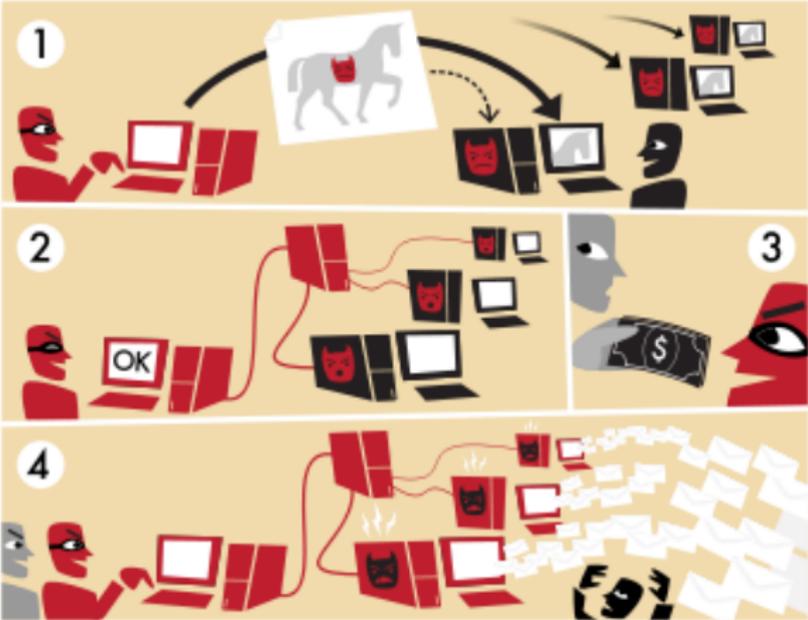
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

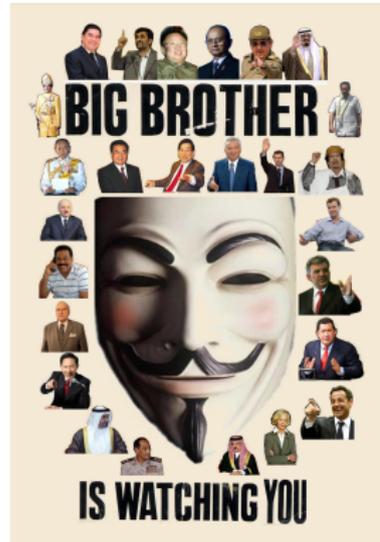


`http://www.societegenerale.fr/espaceclient:
id=56452575711&res=lorem-ipsu-
m-dolor&quux=2&lang=
frsessid=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMF
88.132.11.17`

Botnets and Zombies



Espionnage



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

Edward Joseph Snowden, 6th june 2013



Sabotage

Stuxnet, 2010

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Saudi Aramco 30 000 PC effacés.

<http://cybermap.kaspersky.com/>

AM I INFECTED?

PYC

CYBERTHREAT REAL-TIME MAP

Germany
#1 most-infected country

381315	99017
282848	4337
14385	5234

150 ODS 2169563 MAV 3345388 MAV 32092 IDS 2919756 VUL 136617

KASPERSKY

1997-2014 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab. [Toggle Demo Mode](#)

f t g+ in

1997-2014 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab. [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

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

Conclusion

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



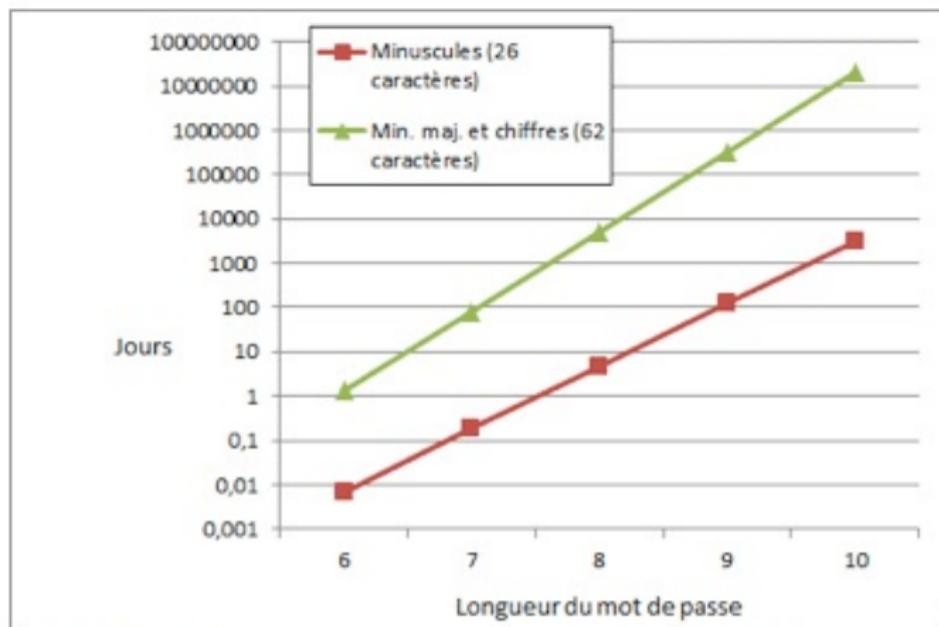
Sécurité de mes mots de passe



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 ...

rockyou

New RockYou Password

Retype Password

I agree to the [Terms of Service](#).

Year of Birth

Sex

Country

Zip/Postal

```
79985232 | -- | - @fbi.gov | -+ujciL90fBni0xG6CatHBw== | -anniversary | --
185089730 | -- | - gon@ic.fbi.gov | -9nCgb38RHiw= | -band | --
188684532 | -- | - burn@ic.fbi.gov | -EQ7fipT71/Q= | -numbers | --
83041678 | -- | - v | -hRwtmq98mKzioxG6CatHBw== | - | --
94038395 | -- | - n@ic.fbi.gov | -MreVpEovY17ioxG6CatHBw== | -eod date | --
116097938 | -- | - | -Tur7wt2zH5CwIIHfjvcHKQ= | -SH? | --
83310434 | -- | - c.fbi.gov | -NLupdfyYrsM= | -ATP_MIDDLE | --
113389790 | -- | - v | -iMhaearHXjPioxG6CatHBw== | -w | --
113931981 | -- | - @ic.fbi.gov | -lTmosXxYnP3ioxG6CatHBw== | -See MSDN | --
114081741 | -- | - lom@ic.fbi.gov | -ZcDbLLvCad0= | -fuzzy boy 26 | --
106145242 | -- | - @ic.fbi.gov | -xc2KumNGzYfioxG6CatHBw== | -4s | --
106437837 | -- | - i.gov | -adIewKvmJEsFqx0HFoFrxx== | - | --
96649467 | -- | - ius@ic.fbi.gov | -lsYw5KRKNT/ioxG6CatHBw== | -glass of | --
96678195 | -- | - .fbi.gov | -X4+k4uhyDh/ioxG6CatHBw== | - | --
105095956 | -- | - =earthlink.net | -ZU2tTFIzq/ioxG6CatHBw== | -socialsecurity# | --
108260815 | -- | - r@genext.net | -MuKhZ7KtsiHioxG6CatHBw== | -socialsecurity | --
83508352 | -- | - h 3hotmail.com | -ADEcoaN2oUM= | -socialsecurityno | --
83823162 | -- | - k 590@aol.com | -9HT+kVHQfs4= | -socialsecurity name | --
80331688 | -- | - b .edu | -nliwEcoZTBmXrIXpAZiRHQ= | -ssn# | --
```

Suite aux fuites ...

rockyou

New RockYou Password

Retype Password

I agree to the [Terms of Service](#).

Year of Birth

Sex

Country

Zip/Postal

```
79985232 | -- | -@fbi.gov | -+ujciL90fBni0xG6CatHBw== | -anniversary | --
185089730 | -- | -gon@ic.fbi.gov | -9nCqB38R4iw= | -band | --
188684532 | -- | -burn@ic.fbi.gov | -EQ7f1P71/Q= | -numbers | --
83041678 | -- | -v | -hRwtmq98mKz10xG6CatHBw== | - | --
94038395 | -- | -n@ic.fbi.gov | -MreVpEovY1710xG6CatHBw== | -eod date | --
116097938 | -- | - | -Tur7wt2zH5CwIIHfjvcHKQ== | -SH? | --
83310434 | -- | -c.fbi.gov | -NLupdfyYrsM= | -ATP_MIDDLE | --
113389790 | -- | -v | -lMhaearHXjP10xG6CatHBw== | -w | --
113931981 | -- | -@ic.fbi.gov | -lTmosXxYnP310xG6CatHBw== | -See MSDN | --
114081741 | -- | -lom@ic.fbi.gov | -ZcDbLlvCad0= | -fuzzy boy 26 | --
106145242 | -- | -@ic.fbi.gov | -xc2KumNGzYfioxG6CatHBw== | -4s | --
106437837 | -- | -i.gov | -adIewKvmJESFqx0HFoFrXg== | - | --
96649467 | -- | -ius@ic.fbi.gov | -lsYw5KRKNT/10xG6CatHBw== | -glass of | --
96678195 | -- | -.fbi.gov | -X4+k4uhyDh/10xG6CatHBw== | - | --
105095956 | -- | -earthlink.net | -ZU2tTFIzq/10xG6CatHBw== | -socialsecurity# | --
108260815 | -- | -r@genext.net | -MuKhZ7Kts1H10xG6CatHBw== | -socialsecurity | --
83508352 | -- | -hotmail.com | -ADEcoaN2oUM= | -socialsecurityno. | --
83823162 | -- | -k590@aol.com | -9HT+kVHQfs4= | -socialsecurity name | --
89331688 | -- | -b.edu | -nliwEcoZTBmXrIXpAZiRHQ== | -ssn# | --
```

... 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

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

Conclusion

Octobre 2014



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



Pretty Good Privacy

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

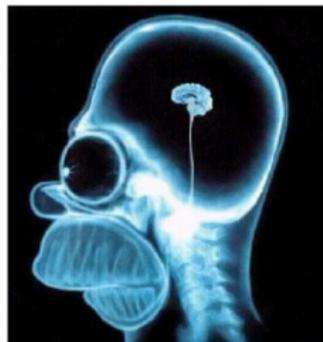


*Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.*

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 ≥ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



Outline

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

Conclusion

Principales propriétés de sécurité

- Confidentialité ou Secret
- Authentification
- Intégrité
- Disponibilité

Authentication



Mécanismes pour l'authentification

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

Other security properties

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

Outline

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

Conclusion

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
- ▶ Authentication,
- ▶ 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**



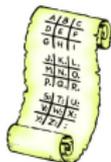
Securité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?



Sécurité des protocoles cryptographiques

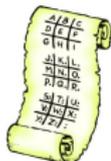
Comment se convaincre qu'un protocole est sûr?





Sécurité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?

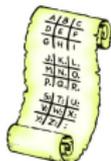


- **Prouver** qu'il n'y a pas d'attaque sous certaines hypothèses.



Sécurité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?

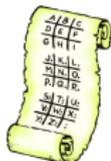


- ▶ **Prouver** qu'il n'y a pas d'attaque sous certaines hypothèses.
 - ▶ faire les preuves c'est difficile,
 - ▶ et sujetes aux erreurs.



Sécurité des protocoles cryptographiques

Comment se convaincre qu'un protocole est sûr?



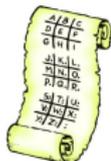
- ▶ **Prouver** qu'il n'y a pas d'attaque sous certaines hypothèses.
 - ▶ faire les preuves c'est difficile,
 - ▶ et sujetes aux erreurs.

Comment se convaincre qu'une preuve est correcte?



Sécurité 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.

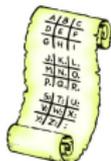
Comment se convaincre qu'une preuve est correcte?





Sécurité 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 est correcte?



Computer-Aided Security

Mes sujets de recherche

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

Outline

Introduction

Cybercriminalité une réalité

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Vérification formelle

Conclusion

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 ?