La sécurité, quelle confiance ? Une approche universitaire

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

FONDATION UNIVERSITÉ D'AUVERGNE

UdA

LIMOS

almerys innover pour la vie

CAISSE D'EPARGNE D'AUVERGNE ET DU LIMOUSIN

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 3 Septembre 2015, 14h00 :

  R. Sasse **ARPKI: Attack Resilient Public-Key Infrastructure.**

  P. Owezarski **Plateforme pour l'exécution contrôlée de logiciels malveillants**

- 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

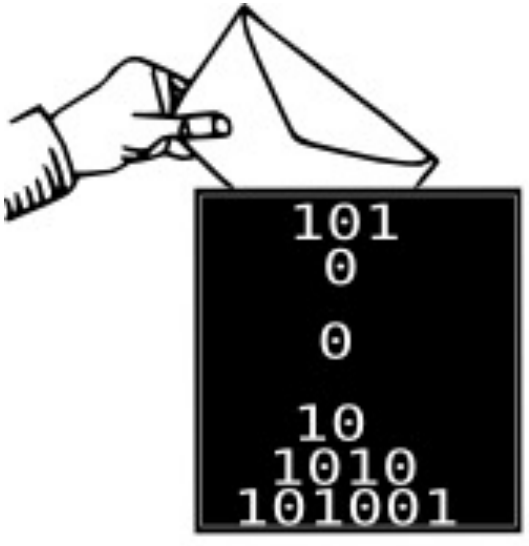
Master • Écoles d'ingénieurs

Architectures PKI et communications sécurisées

Jean-Guillaume Dumas
Pascal Lafourcade
Patrick Redon

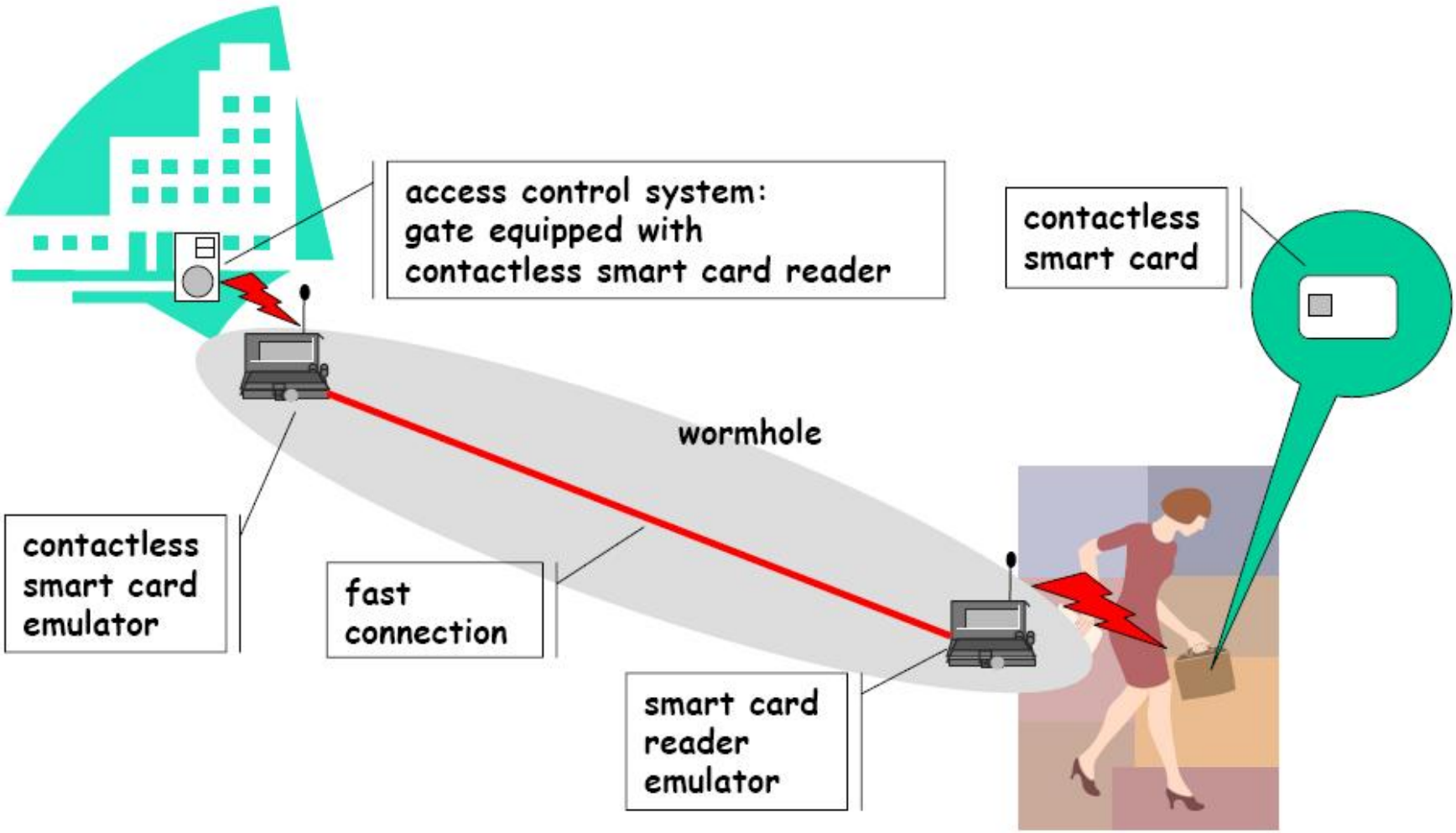
DUNOD

Nowadays Security is Everywhere!

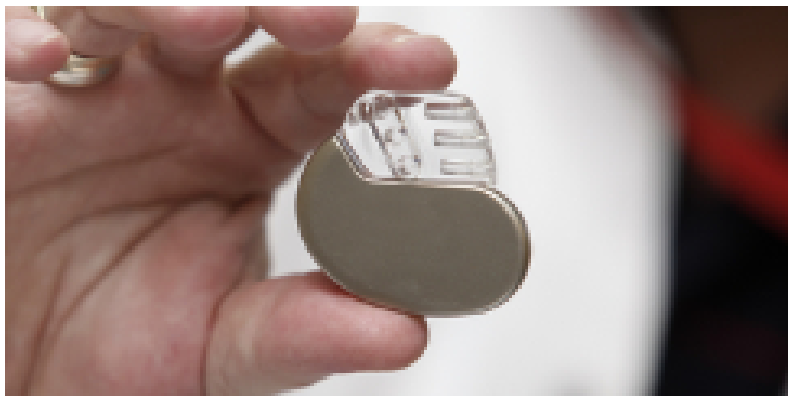


Due to the succes of Computer Science.

Wormhole Attack



Hacking Pacemakers:



Manufacturers are still not putting security first when designing implantable medical devices (2012)

Paypal Attack

"Model-Based Vulnerability Testing of Payment Protocol Implementations", Ghazi Maatoug, Frédéric Dadeau and Michael Rusinowitch, Hotspot 2014

You are the Data

Governmental Attacks

- April 2007: a serie of cyberattacks against Estonia
- January 2009: hackers attacked Israels internet infrastructure
- February 2011: hackers have infiltrated three canadian government departments and obtained classified information.
- Since August 2012: EDF is victim of a cyberattack (Phising)
- March 2013: South Korean financial institutions had their networks infected.

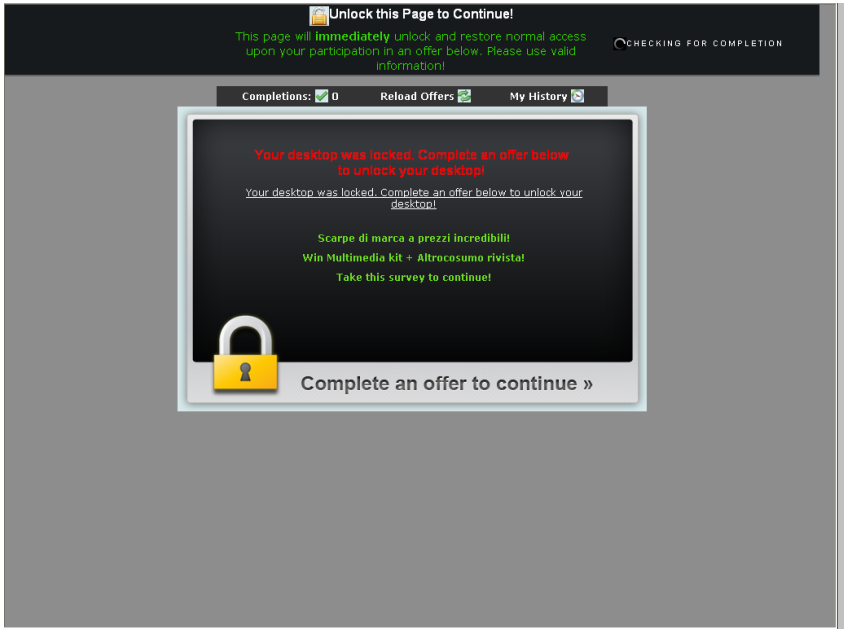
`http://www.defense.gouv.fr/content/download/135220/1336475/Dicod-Cyber-Attaque.swf`

`http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm`

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=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMk
88.132.11.17
```

Botnets and Zombies

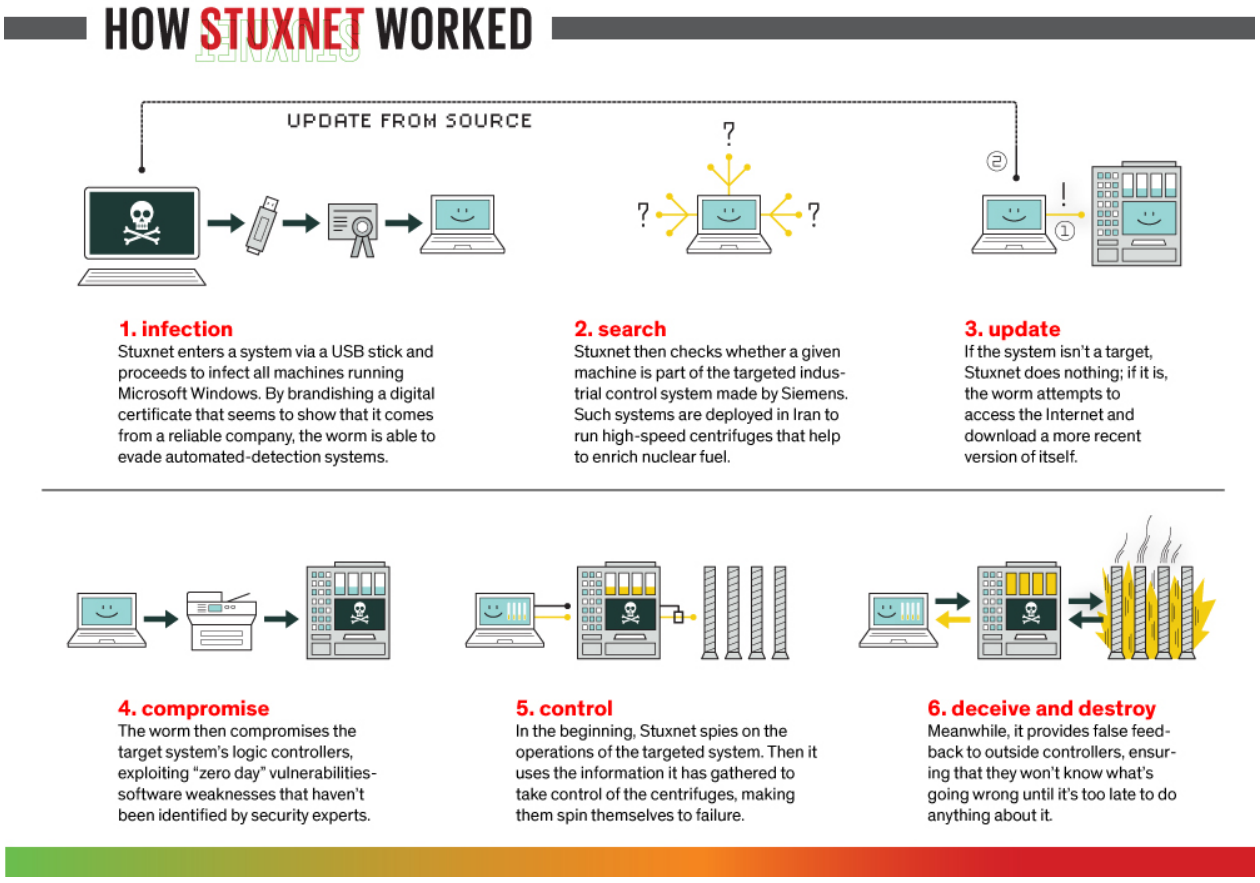
Espionnage

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

Edward Joseph Snowden, 6th june 2013

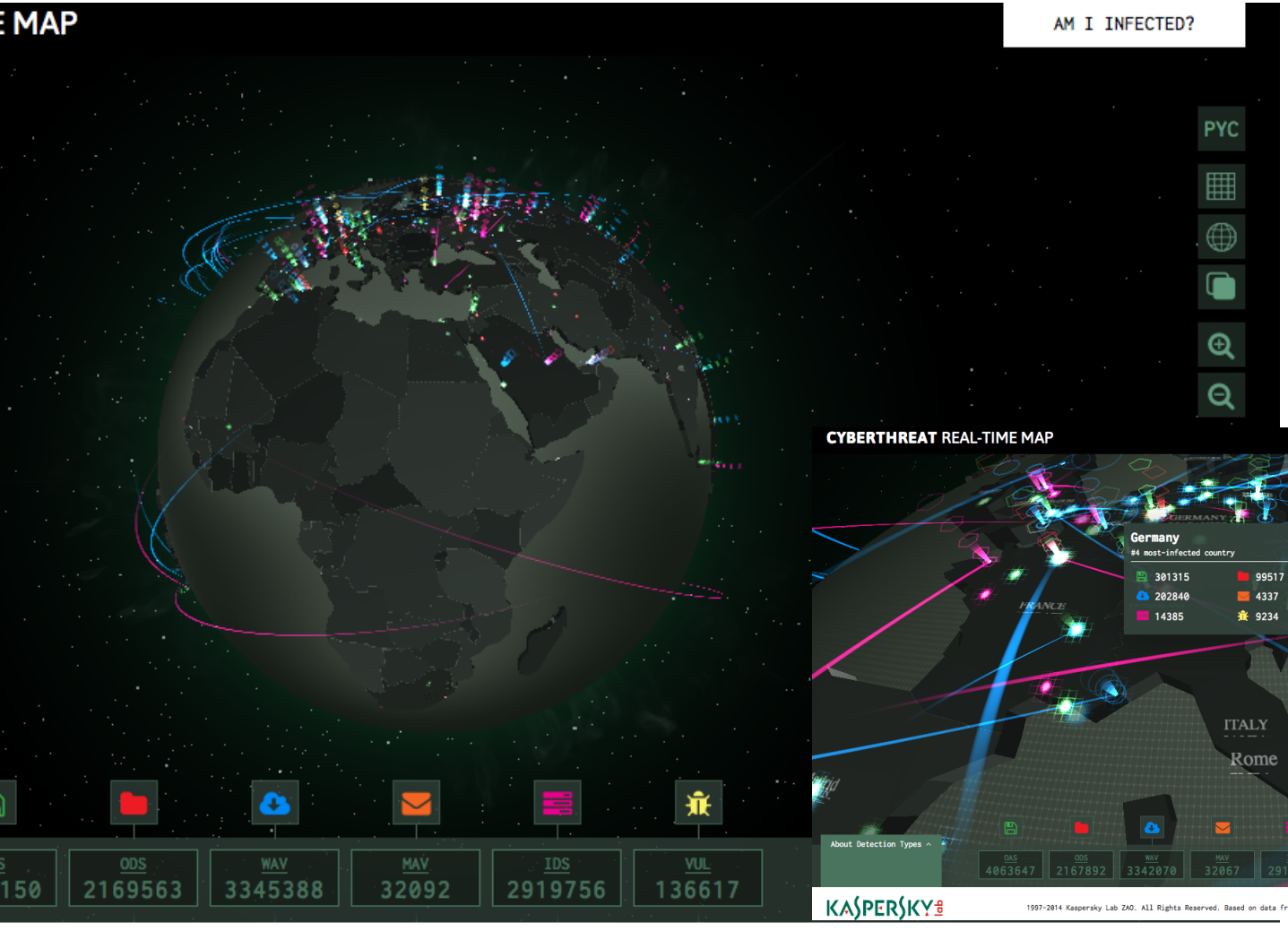
Sabotage

Stuxnet, 2010



Saudi Aramco 30 000 PC and servers have been deleted.

http://cybermap.kaspersky.com/

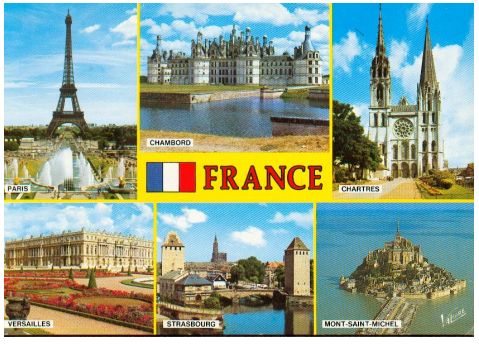


Why is there an explosion of computer security attacks?

- You can do it at home
- You do not need expensive material, self-service
- It is automatic, fast, and large scale
- You think you are anonymous

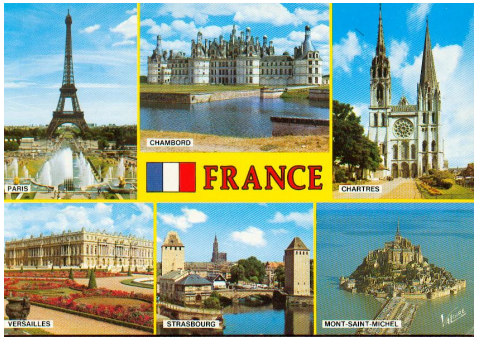
Why is there an explosion of computer security attacks?

- You can do it at home
- You do not need expensive material, self-service
- It is automatic, fast, and large scale
- You think you are anonymous



Why is there an explosion of computer security attacks?

- You can do it at home
- You do not need expensive material, self-service
- It is automatic, fast, and large scale
- You think you are anonymous



Internet has been designed to work and not to be secured !

Computer Science Security Agencies

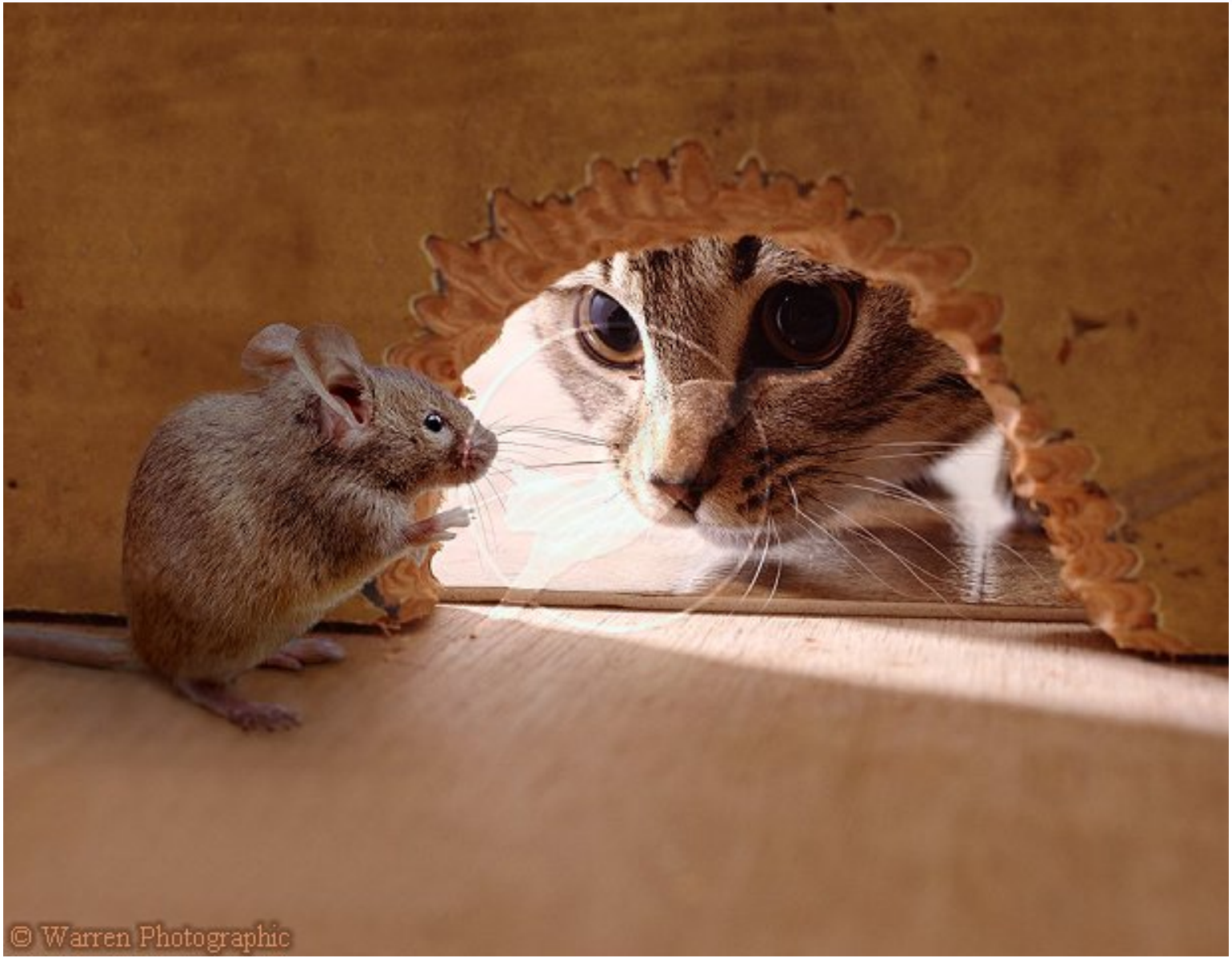
ANSSI Agence nationale de la sécurité des systèmes d'information

- 2000,
- 2002, first security team
- 2007, French government proposed : http://www.securite-informatique.gouv.fr/

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

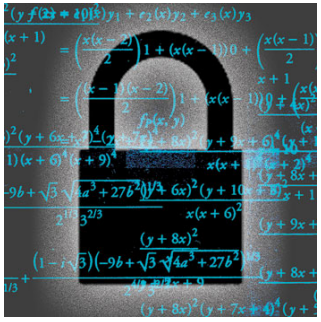
GCHQ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ


© Warren Photographic

Formal Verification Approaches

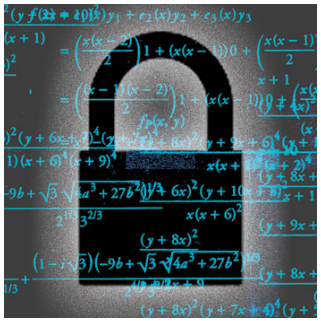
Designer



Attacker

Formal Verification Approaches

Designer

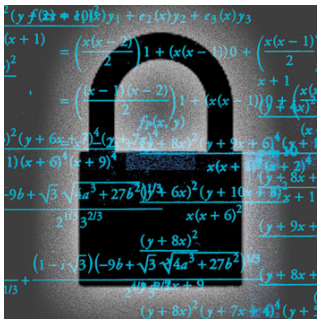


Attacker

Security Team

Formal Verification Approaches

Designer



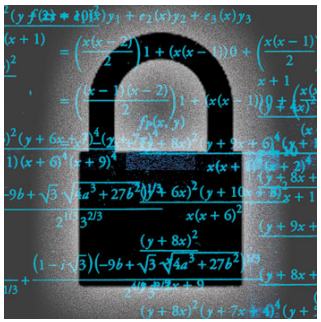
Attacker

Give a proof

Security Team

Formal Verification Approaches

Designer



Attacker

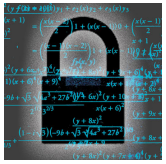
Give a proof

Find a flaw

Security Team

What is cryptography based security?

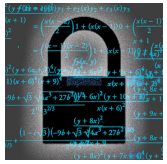
Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

What is cryptography based security?

Cryptography:



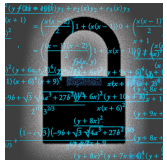
- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy ...

What is cryptography based security?

Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy ...

Intruders:

- Passive
- Active
- CPA, CCA ...

What is cryptography based security?

Cryptography:

- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy ...

Intruders:

- Passive
- Active
- CPA, CCA ...

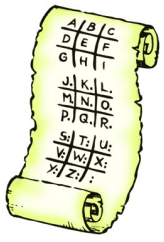
Designing **secure** cryptographic protocols is **difficult**

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?

Security of Cryptographic Protocols

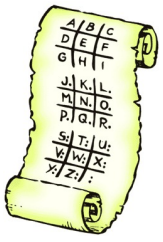
How can we be convinced that a protocols is secure?





Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?

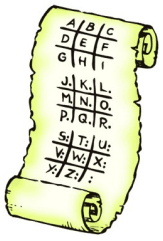




- Prove that there is no attack under some assumptions.

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?

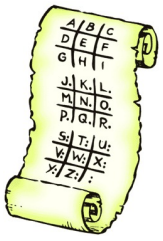




- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?



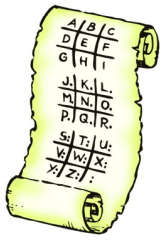


- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

How can we be convinced that a proof is correct?

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?



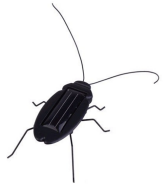


- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

How can we be convinced that a proof is correct?

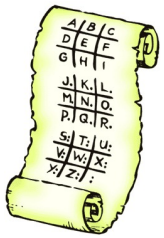






Security of Cryptographic Protocols

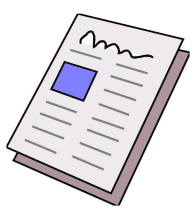
How can we be convinced that a protocols is secure?





- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

How can we be convinced that a proof is correct?





My Reasearch Topics

- Automatic security proof of cryptosystems
- Cryptographic accumulators
- e-services : e-voting, e-auction, e-reputation, e-cash, e-exam
- Anonymous storage
- Witness of honesty
- WSN : SR3, 5 topologies, IDS

Outline:

Outline:

Outline:

Outline:

Outline

Traditional security properties

- Common security properties are:
  - Confidentiality or Secrecy: No improper disclosure of information
  - Authentification: To be sure to talk with the right person. disclosure of information
  - Integrity: No improper modification of information
  - Availability: No improper impairment of functionality/service

Authentication

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

Mechanisms for Authentication

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 (PFS) is s a property of key-agreement protocols that ensures that a session key derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future.
- Non-repudiation (also called accountability) is where one can establish responsibility for actions.
- Fairness is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- Privacy

  Anonymity: secrecy of principal identities or communication relationships.

  Pseudonymity: anonymity plus link-ability.

  Data protection: personal data is only used in certain ways.

e-services :

- e-voting
- e-auction
- e-examen
- e-reputation
- e-cash
- e-passport
- ...

Users except more properties and security with electronic services!

Outline

Example

Needham Schroeder Key Echange 1976

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

- Use cryptography
- Small programs
- Distributed

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to B : \{N_B\}_{Pub(B)}$$

Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to I : \{N_A, N_B\}_{Pub(A)} \qquad I \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to B : \{N_B\}_{Pub(B)}$$

Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to I : \{N_A, N_B\}_{Pub(A)} \qquad I \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Computer-Aided Security

Outline

Summary

5 points to bring home

- Security is everywhere (IoT)
- Security design is a global process
- Security = Cryptography + Properties + Adversaries
- Users have to be educated
- Computer-Aided Security

Thank you for your attention.

Questions ?

Success Story of Formal Verification

Tools based on different theories for several properties

- 1995 Casper/FRD [Lowe]
- 2001 Proverif [Blanchet]
- 2003 Proof of certified email protocol with Proverif [AB]
  OFMC [BMV]
  Hermes [BLP]
  Flaw in Kerberos 5.0 with MSR 3.0 [BCJS]
- 2004 TA4SP [BHKO]
- 2005 SATMC [AC]
- 2006 CL-ATSE [Turuani]
- 2008 Scyther [Cremers]
  Flaw of Single Sign-On for Google Apps with SAT-MC [ACCCT]
  Proof of TLS using Proverif [BFCZ]
- 2010 TOOKAN [DDS] using SAT-MC for API
- 2012 Tamarin [BCM]