FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

11ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

LA GENDARMERIE & LES OFFICIERS DE LA RÉSERVE CITOYENNE

FRC 2018
11ème édition

WWW.FRC.ALSACE
@CYBERMENACES

FRC 2018 : ANIMATION

M. Gilbert GOZLAN

Directeur de la Sûreté - La Poste Nord & Est
Président de l'association AD Honores Réseau Alsace
Colonel (RC) de la gendarmerie nationale

FRC 2018 : DISCOURS D'OUVERTURE

Colonel Marc CLERC

Commandant Adjoint de la région de gendarmerie Grand Est,
Commandant le groupement de gendarmerie départementale du Bas-Rhin

FRC 2018 : DISCOURS D'OUVERTURE

M. Jean-Michel HAGET

Dirigeant de Just My Home
Président de la commission Intelligence économique
à la CCI Alsace Eurométropole

FRC 2018 : PROGRAMME

AGIR POUR LA CONFIANCE NUMERIQUE

13h00 — ACCUEIL DES PARTICIPANTS

13h30 — DISCOURS D'OUVERTURE

Colonel Marc CLERC
Commandant adjoint de la région de gendarmerie Grand Est.
Commandant le groupement de gendarmerie départementale du Bas-Rhin.

Monsieur Jean-Luc HEIMBURGER
Président de la CCI Alsace Eurométropole.

Monsieur Jean-Luc MARX
Préfet du Bas-Rhin.
Préfet de la région Grand Est.

Animation
Monsieur Gilbert GOZLAN
Directeur de la Sûreté - la Poste Nord & Est.
Président de l'association AD HONORES Réseau Alsace.
Lieutenant-Colonel (RC) de la gendarmerie nationale.

14h00 — CONFERENCE PLENIÈRE

LA CRYPTOGRAPHIE : DU SECRET A LA CONFIANCE

Monsieur Jacques STERN
Professeur émérite à l'École normale supérieure.
Médaille d'or du CNRS en 2006, RSA Award for Excellence en 2007, prix Science et Défense 2008
Auteur de "La Science du secret".

14h30 — TABLE RONDE #1

LA CONFIDENTIALITE DES DONNEES

La confidentialité des données dans le cloud... : utopie ou réalité ?
Monsieur Ludovic HAYE
Maire de Rixheim, Dirigeant de CyberDiag.
Chef d'escadron (RC) de la gendarmerie nationale.

Le RGPD pour les entreprises : syndrome de Bruxelles ou incitation structurante ?
Monsieur Fouad GADACHA
Responsable des processus et des opérations et DPO de NXO-Telecom.

PME / TPE : besoin de sécurité et critère de confidentialité
Monsieur Michel ROCHELET
Référent ANSSI Région Grand-Est.

15h30

DÉMONSTRATION OPÉRATIONNELLE : LES MOTS DE PASSE

Messieurs Gabin MICHALET, Mohamed BABACAR SARR, Nicolas GREINER et Thibaud GASSER
Etudiants de l'Ecole Nationale Supérieur d'Ingénieurs Sud Alsace (ENSISA), Université de Haute Alsace.

15h45 — PAUSE

16h20 — TABLE RONDE #2

LES CONTRÔLES D'ACCES

La gestion des accès : comment ou pourquoi ?
Monsieur Thomas VIERLING
Directeur et Consultant Senior de LPB Conseil.

Authentification pour l'accès au réseau d'une université.
Monsieur Alexandre HECK
Responsable infrastructures et systèmes à l'Université de Haute Alsace.

OpenID / FranceConnect et WebAuthentification.
Monsieur Clément OUDOT
Identity Solutions Manager de Worteks.

17h20 — CONFERENCE DE CLÔTURE

Cybersécurité, cybercriminalité, quelles évolutions législatives ?
Madame Myriam QUEMENER
Magistrat, docteur en droit, avocat général près la Cour d'appel de Paris, service économique, financier et numérique.
Auteur de : "Le droit face à la disruption numérique".

18h00 — CONCLUSION DE LA JOURNÉE

Colonel Marc CLERC et Monsieur Gilbert GOZLAN

18h30 — COCKTAIL

Salle de conférence de l'ENA

FRC 2018 11ème édition

FRC 2018 : NOS PARTENAIRES

FRC 2018 : NOS PARTENAIRES

CCI ALSACE EUROMÉTROPOLE

FRC 2018 : NOS PARTENAIRES

FRC 2018 : NOS PARTENAIRES

CLUSIR EST

FRC 2018 : NOS PARTENAIRES

FRC 2018 : NOS SPONSORS

FRC 2018 : NOS SPONSORS

BANQUE POPULAIRE
ALSACE LORRAINE CHAMPAGNE

ADDITIONNER LES FORCES, **MULTIPLIER LES CHANCES**

FRC 2018 : NOS SPONSORS

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
COLMAR

Partenaire de la marque Alsace

FRC 2018 : NOS SPONSORS

FRC 2018 : NOS SPONSORS

SOCIETE GENERALE

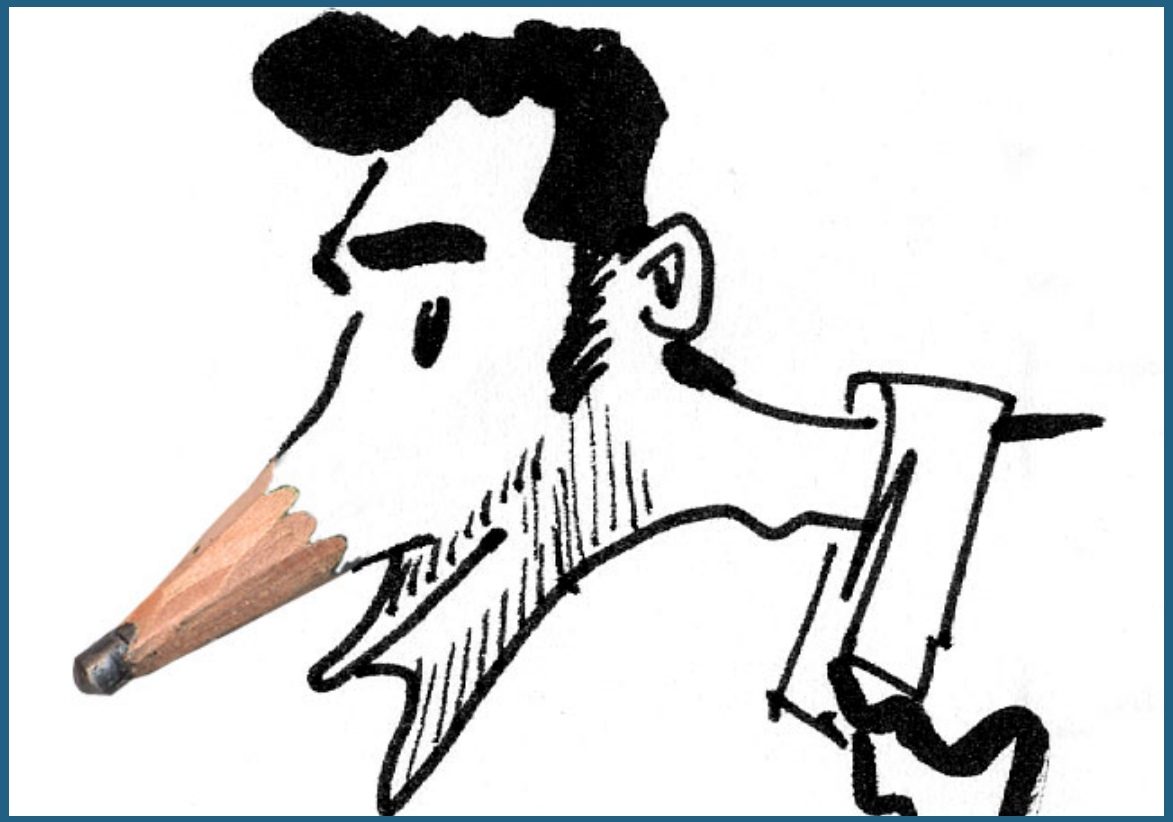
La Gendarmerie, la RC et AD Honores

FRC 2018 : NOTRE OBJECTIF

Connaître et partager les enjeux

Adopter et faire adopter les bons comportements et les bonnes actions à mettre en œuvre

FRC 2018 : Le dessinateur



M. Laurent SALLES

Code wifi :

Identifiant	cyber
Mot de passe	wGw98G6t
Nom	cyber
Profil	EVENEMENT

N’hésitez pas à consulter notre site :

www.frc.alsace

Et nous rejoindre sur Twitter :

@cybermenaces

FRC 2018 : CONFÉRENCE PLÉNIÈRE

La cryptographie : du secret à la confiance

M. Jacques STERN

Professeur émérite à l'Ecole normale supérieur
Médaille d'or du CNRS en 2006
RSA Award for Excellence en 2007
Prix Sciences et Défense en 2008
Auteur de « La Science du secret »

Résumé

- Brève histoire de la cryptologie
- Les 40 dernières années
  - RSA et sa sécurité
  - Utilisation des courbes elliptiques
  - Sécurisation des communications
  - Sécurisations des transactions
  - Dématérialisation et signature électronique
- Quelques défis récents et futurs
  - Protection de la vie privée
  - La menace quantique

Qu'est ce que la cryptologie ?

- La science des messages secrets
- La trilogie fondamentale :
  - Intégrité
  - Authenticité
  - Confidentialité
- Combine conception & analyse: cryptographie et cryptanalyse

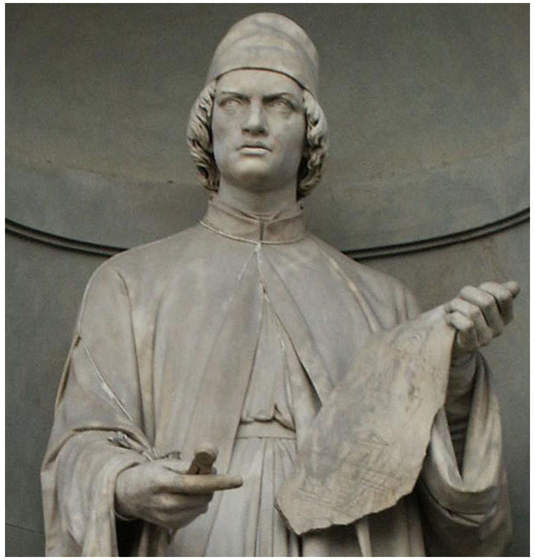
Antiquité

Scytale ca. 440 AC

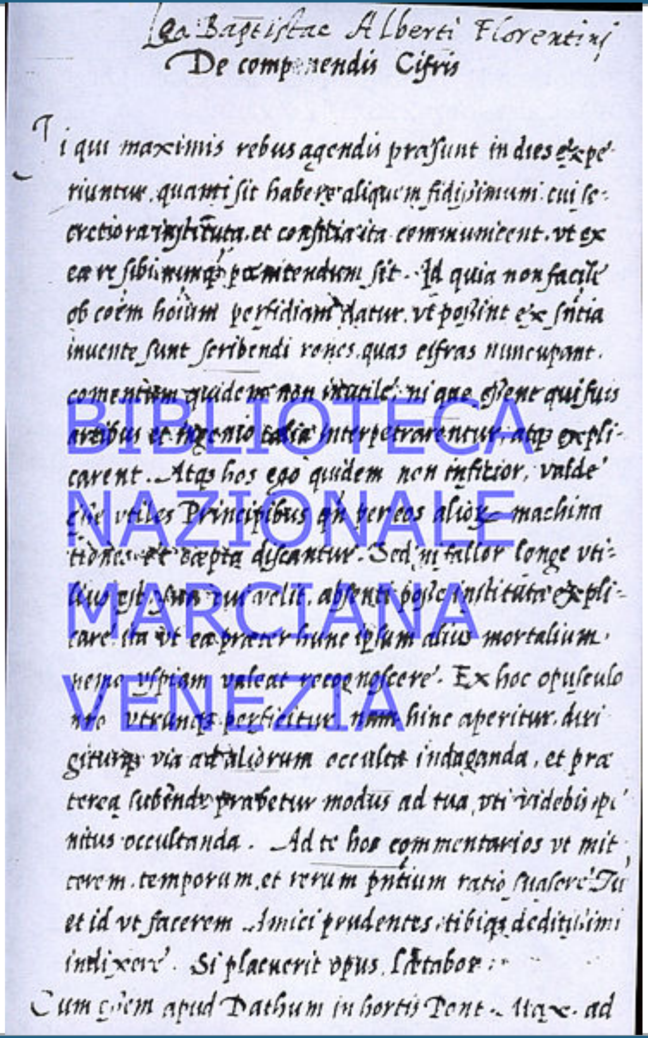
Al-Kindi

Première page du traité de Al Kindi ca. 850 (Document 4832 Bibliothèque al-sulaymaniyya, Turquie)

Alberti

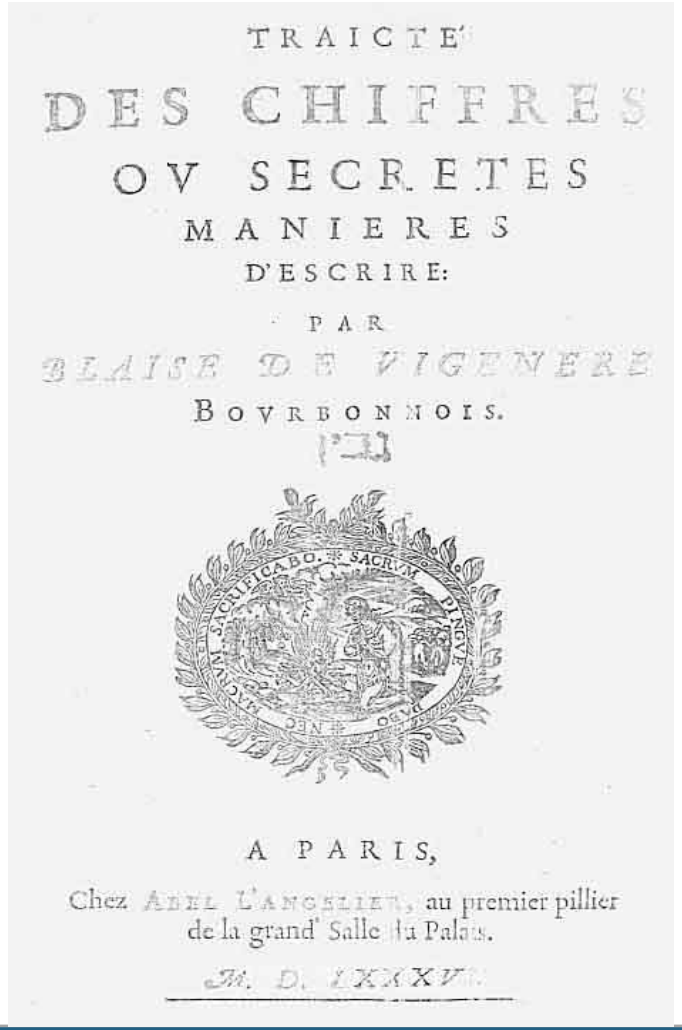


De Componendis cifris ca. 1466


Leo Bap. Alberti Florentini
De componendis Cifris

Vigenère

Traîté des chiffres 1585



TRAICTE'

DES CHIFFRES

OV SECRETES

MANIERES

D'ESCRIRE:

PAR

BLAISE DE VIGENERE

BOVRBONNOIS.

A PARIS,

Chez ABEL L'ANGELIER, au premier pillier
de la grand' Salle du Palais.

M. D. LXXXVI.

Kerckhoffs

II.

DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE.

Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégra-

La Cryptographie Militaire 1883

Shannon

To use the system a key is first selected and sent to the receiving point. The choice of a key determines a particular transformation in the set forming the system. Then a message is selected and the particular transformation corresponding to the selected key applied to this message to produce a cryptogram. This cryptogram is transmitted to the receiving point by a channel and may be intercepted by the "enemy*." At the receiving end the inverse of the particular transformation is applied to the cryptogram to recover the original message.

If the enemy intercepts the cryptogram he can calculate from it the *a posteriori* probabilities of the various possible messages and keys which might have produced this cryptogram. This set of *a posteriori* probabilities constitutes his knowledge of the key and message after the interception. "Knowledge" is thus identified with a set of propositions having associated probabilities. The calculation of the *a posteriori* probabilities is the generalized problem of cryptanalysis.

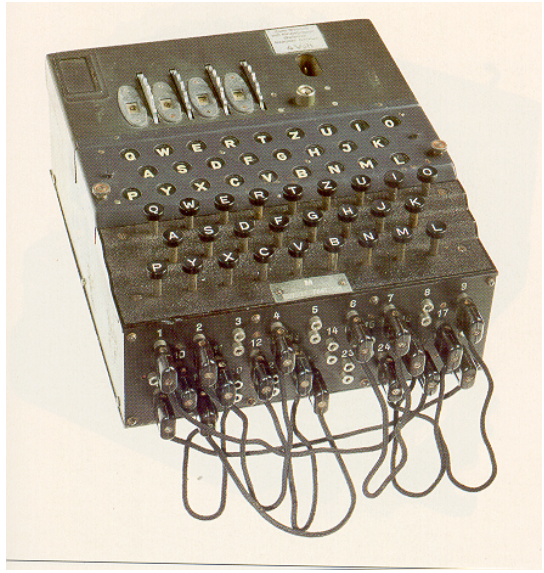
As an example of these notions, in a simple substitution cipher with random key there are 26! transformations, corresponding to the 26! ways we can substitute for 26 different letters. These are all equally likely and each therefore has an *a priori* probability $\frac{1}{26!}$. If this is applied to "normal English"

* The word "enemy," stemming from military applications, is commonly used in cryptographic work to denote anyone who may intercept a cryptogram.

657

Communication Theory of Secrecy Systems 1949

Turing



230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

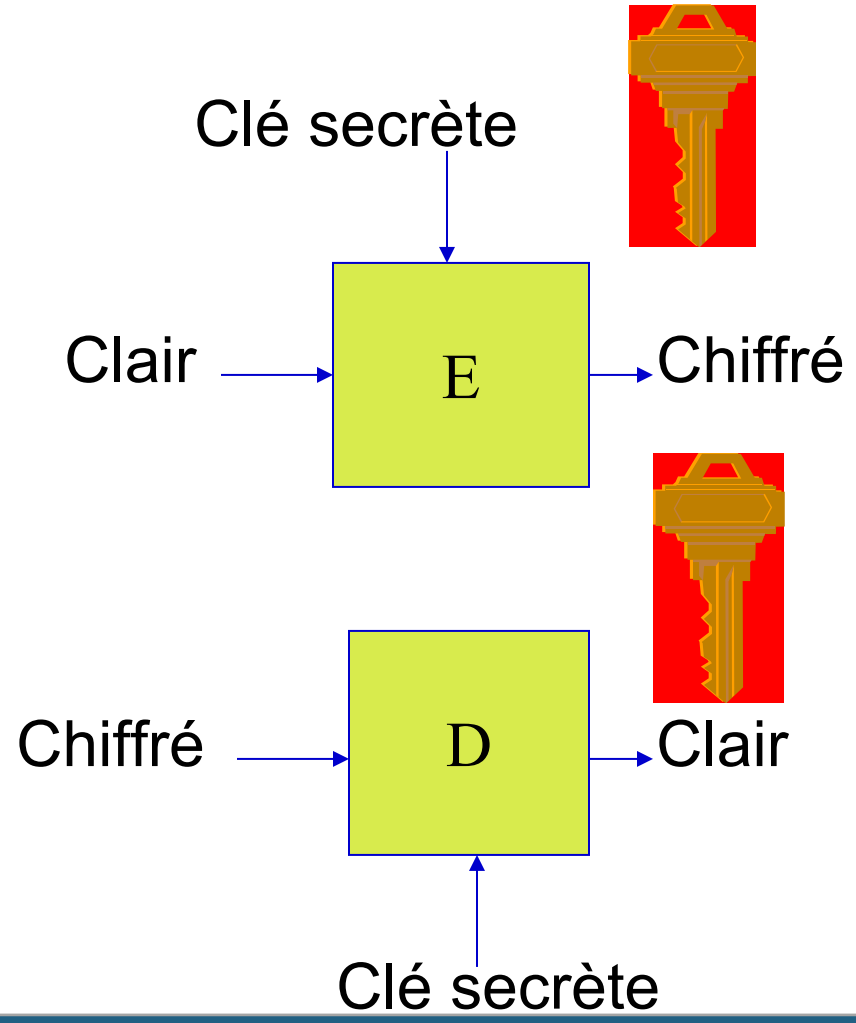
Although the class of computable numbers is so great, and in many ways similar to the class of real numbers, it is nevertheless enumerable. In § 8 I examine certain arguments which would seem to prove the contrary. By the correct application of one of these arguments, conclusions are reached which are superficially similar to those of Gödel†. These results

† Gödel, "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I", *Monatshefte Math. Phys.*, 38 (1931), 173–198.

On computable numbers 1936

Le chiffrement symétrique

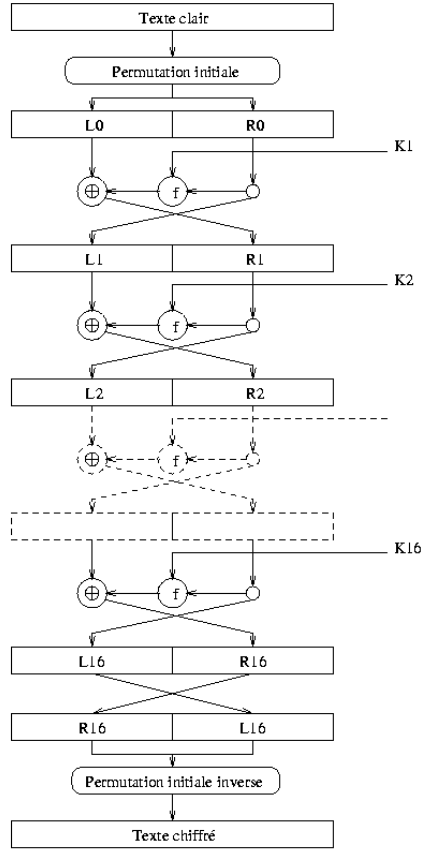
- **La même clé préalablement échangée entre tous les utilisateurs sert au chiffrement et au déchiffrement**



DES (1975) -> AES (2000)

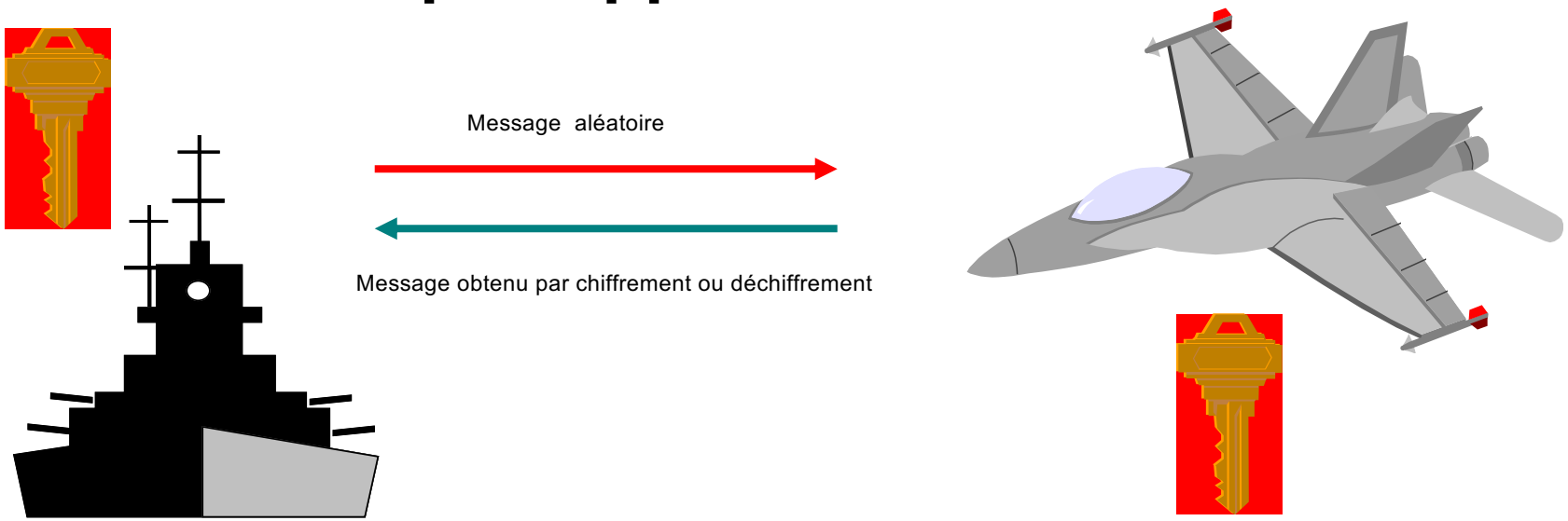
- Chiffre avec des clefs de 56 bits
- Cryptanalyses théoriques (différentielle et linéaire 1993)
- Cryptanalyse par recherche exhaustive en 1998
- Remplacé par Triple DES et AES

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16



Authenticité

- La capacité de chiffrer et/ou déchiffrer garantit l'authenticité
- Une fonction à clé non réversible calculant un « condensat » suffit
- L'authenticité n'est pas opposable aux tiers



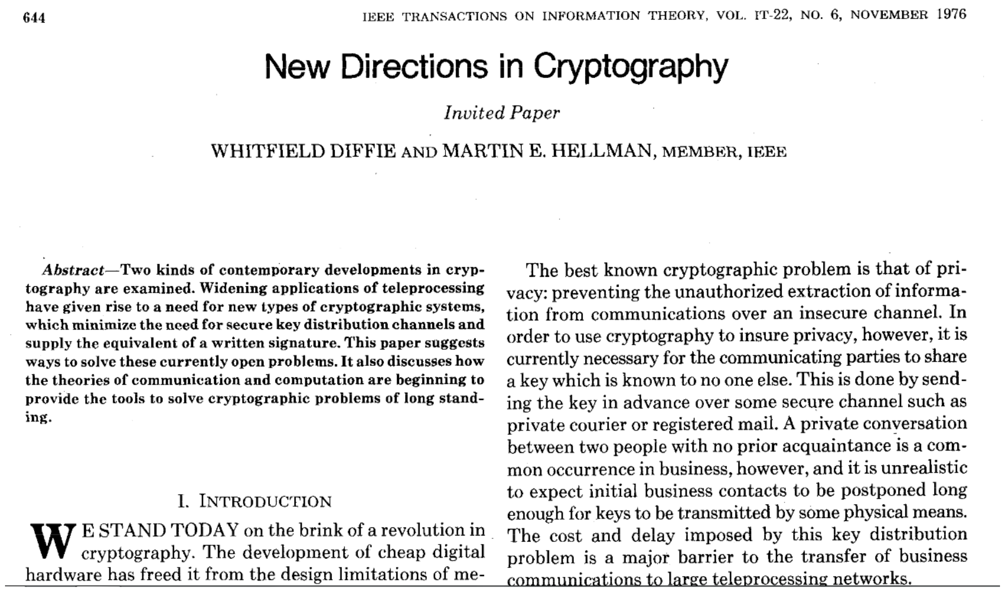
Intégrité : de SHA1 à SHA3

- **Assurée par une fonction crypto sans clé *f* résistante aux collisions: c-à-d tq qu'il soit « pratiquement » impossible de construire deux messages m et m' distincts tq *(m)=f(m')***

- **23/02/2017: première collision sur la norme SHA1 de 1995**

- **Nouvelles normes SHA2 et SHA3 (2002, 2008, 2012)**

Le chiffrement à clé publique : 1976 - 1978



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

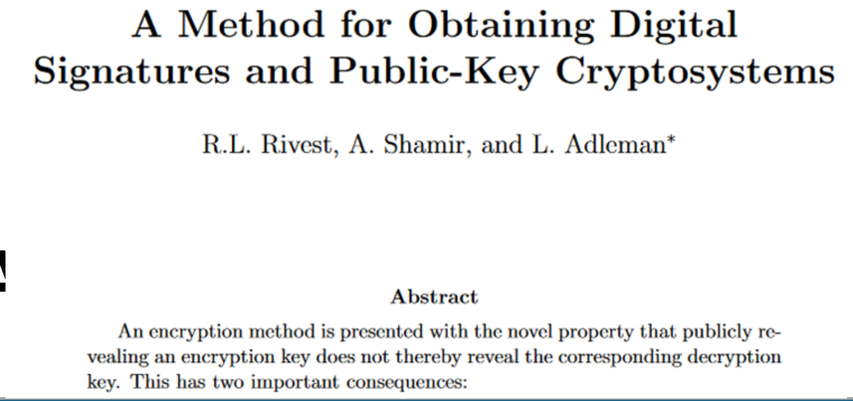
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of me-

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.



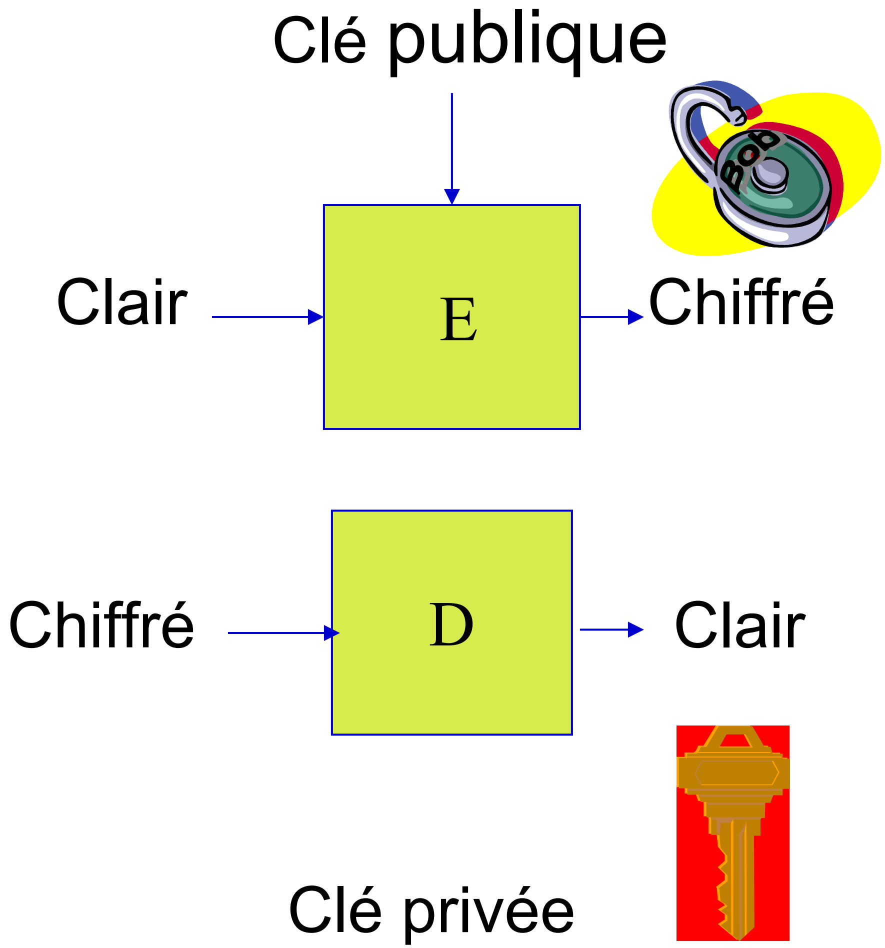
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

- **1976 DH**
- **1978: RSA**



RSA : 1763 - 1978

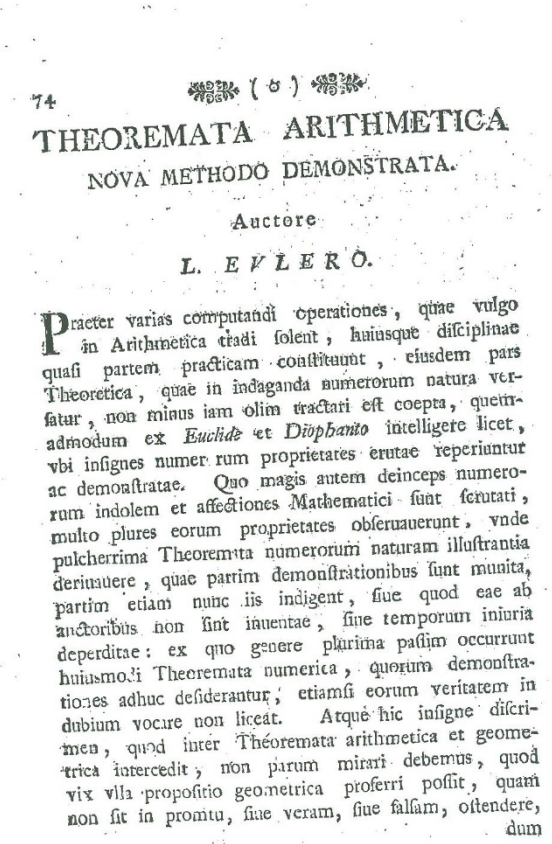
- $n=pq$ **public**
- e **public**
- $d=e^{-1} \bmod \varphi(n)$ **privé**

Leonard Euler 1707-1783

(-/dé)chiffrement

$\mathbf{E}(m) = m^e \bmod n$

$\mathbf{D}(c) = c^d \bmod n$



74 (6)

THEOREMATA ARITHMETICA
NOVA METHODO DEMONSTRATA.

Auctore
L. EVLERO.

Praeter varias computandi operationes, quae vulgo in Arithmetica tradi solent, huiusque disciplinae quasi partem practicam constituunt, eiusdem pars Theoretica, quae in indaganda numerorum natura versatur, non minus iam olim tractari est coepta, quemadmodum ex *Euclide* et *Diophanto* intelligere licet, vbi insignes numerorum proprietates erutae reperiuntur ac demonstratae. Quo magis autem deinceps numerorum indolem et affectiones Mathematici sunt scrutati, multo plures eorum proprietates obseruauerunt, vnde pulcherrima Theoremata numerorum naturam illustrantia deriuauere, quae partim demonstrationibus sunt munita, partim etiam nunc iis indigent, siue quod eae ab auctoribus non sint inuentae, siue temporum iniuria deperditae: ex quo genere plurima passim occurrunt huiusmodi Theoremata numerica, quorum demonstrationes adhuc desiderantur, etiamsi eorum veritatem in dubium vocare non liceat. Atque hic insigne discrimen, quod inter Theoremata arithmetica et geometrica intercedit, non parum mirari debemus, quod vix vlla propositio geometrica proferri possit, quam non sit in promtu, siue veram, siue falsam, ostendere, dum

Novi Commentarii Academiae Scientarum Petropolitanae 8, 1763, 74-104

RSA avant RSA !

Coroll. 2.

49. Contra autem iam supra vidimus productum ex duobus pluribusue residuis in classe residuorum reperiri. Vnde sequitur ex vno non-residuo et quotcunque residuis in classe non-residuorum occurrere debere.

Scholion.

50. Vis huius demonstrationis isto nititur fundamento, quod si inter residua occurrant partes 1, a, b, c, d, etc. ad diuisorem primae, atque α fuerit etiam pars ad diuisorem prima in his residuis non contenta, tum producta omnia αa, αb, αc, αd, etc. non solum in residuis non occurrere, quod quidem perfecte est demonstratum, sed etiam ea esse partes ad diuisorem N primas, omnesque inter se diuersas; seu si ea per N, actu diuidantur, relinqui residua diuersa. Illud quidem per se est perspicuum; cum enim tam α, quam a, b, c, d, etc. sint numeri ad N primi, etiam eorum producta ad N prima sint necesse est. Quod autem producta αa, αb, αc, αc, etc. sint omnia ad N relata inter se diuersa, intelligitur, quod si verbi gratia duo αa et αb per N diuisa paria darent residua, eorum differentia $\alpha b - \alpha a = \alpha(b-a)$ per N esset diuisibilis, ideoque et $b-a$; id quod hypothesi, quod a, et b sint diversae partes ad N primae, repugnat.

Theorema 10.

51. Exponens minimae potestatis x^ν, quae per numerum N ad x primum diuisa vnitatem relinquit,

 vel

vel est aequalis numero partium ad N primarum, vel huius numeri semissis, aliaue eius pars aliquota.

Demonstratio.

Sit n numerus partium ad N primarum, quarum cum ν constituant residua, erit numerus non-residuorum $= n-\nu$. Vidimus autem hunc numerum esse vel $= 0$, vel $= \nu$, vel $= 2\nu$, vel alii cuipiam multiplo exponentis ν. Sit ergo $n-\nu = (m-1)\nu$, ita vt m denotet vel vnitatem, vel alium quemuis numerum integrum, atque hinc obtinebimus $n = m\nu$ et $\nu = \frac{n}{m}$: vnde patet exponentem minimae potestatis ipsius x, quae per N diuisa vnitatem relinquit, esse vel $= n$, si $m = 1$, vel $= \frac{n}{2}$, si $m = 2$, vel in genere esse partem quampiam aliquotam numeri n, qui exprimit multitudinem partium ad diuisorem N primarum. Q. E. D.

Coroll. 1.

52. Si x^ν fuerit minima potestas, quae per numerum N ad x primum diuisa vnitatem relinquit, sequentes potestates idem residuum relinquentes sunt $x^{2\nu}$, $x^{3\nu}$, $x^{4\nu}$, $x^{5\nu}$, etc. neque praetera vllae aliae dantur, quae per N diuisae vnitatem relinquant.

Coroll. 2.

53. Exponens ergo huius potestatis minimae semper cum numero partium ad diuisorem N primarum ita connectitur, vt sit vel illi ipsi, vel cuipiam eius parti aliquotae, aequalis.

Scholion.

Sécurité algorithmique

- **Liée à la difficulté d'un problème de calcul : trouver deux nombres premiers *p* et *q* à partir de leur produit *n***
- **Le record**

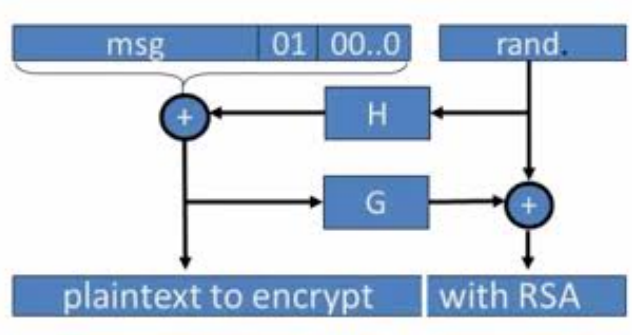
We are pleased to announce the factorization of RSA768, from RSA's challenge list. On December 12, 2009, we found the factors :

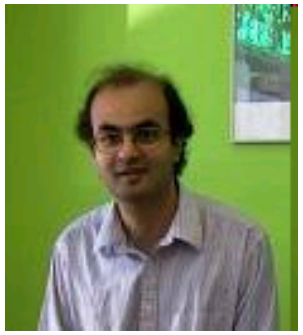
33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489
*
36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

The factors have 384 bits/116 digits.

K.Aoki, J.Franke, A.K. Lenstra, E.Thomé, J. W. Bos, P.Gaudry, A.Kruppa, P. L. Montgomery, D. Arne Osvik, H.te Riele, P.Zimmermann A.Timofeev

Format RSA - OAEP





- **Proposé par Bellare and Rogaway 1994**
- **« Prouvé sûr » par Fujisaki, Okamoto, Pointcheval et Stern 01**

Preuves formelles de sécurité

- Verifier les preuves de sécurité formellement
- Une voie de recherché active
- Des succès utilisant des assistants de preuve

Beyond Provable Security
Verifiable IND-CCA Security of OAEP

Gilles Barthe[1], Benjamin Grégoire[2],
Yassine Lakhnech[3], and Santiago Zanella Béguelin[1]

[1] IMDEA Software
[2] INRIA Sophia Antipolis-Méditerranée
[3] Université Grenoble 1, CNRS, Verimag

Abstract. OAEP is a widely used public-key encryption scheme based on trapdoor permutations. Its security proof has been scrutinized and amended repeatedly. Fifteen years after the introduction of OAEP, we present a machine-checked proof of its security against adaptive chosen-ciphertext attacks under the assumption that the underlying permutation is partial-domain one-way. The proof can be independently verified by running a small and trustworthy proof checker and fixes minor glitches that have subsisted in published proofs. We provide an overview of the proof, highlight the differences with earlier works, and explain in some detail a crucial step in the reduction: the elimination of indirect queries made by the adversary to random oracles via the decryption oracle. We also provide—within the limits of a conference paper—a broader perspective on independently verifiable security proofs.

1985 : Courbes elliptiques

- **Dimensionnement plus faible dû à l'efficacité moindre des attaques**
- **Miller**
- **Koblitz**

MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 203–209

Elliptic Curve Cryptosystems

By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday

Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over GF(2^n). We discuss the question of primitive points on an elliptic curve modulo p, and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.

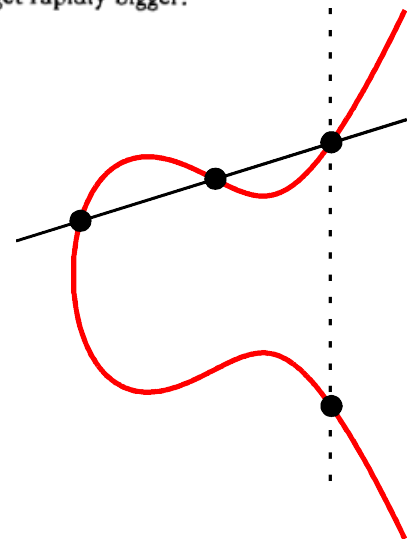
Use of Elliptic Curves in Cryptography

Victor S. Miller

Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over GF(p). As computational power grows, this disparity should get rapidly bigger.



Sécurité des communications (1)

- La « puce » contenue dans la carte « SIM » pilote

  - l'authentification de l'usager
  - le chiffrement sur la voie aérienne
  - en utilisant un chiffrement symétrique

Sécurité des communications (2)

- Le protocole de communication « SSL » permet l'établissement simple d'une connexion sécurisée

- Sa mise en œuvre passe par l'utilisation par les serveurs de couples clé publique / clé privée

Transactions par cartes

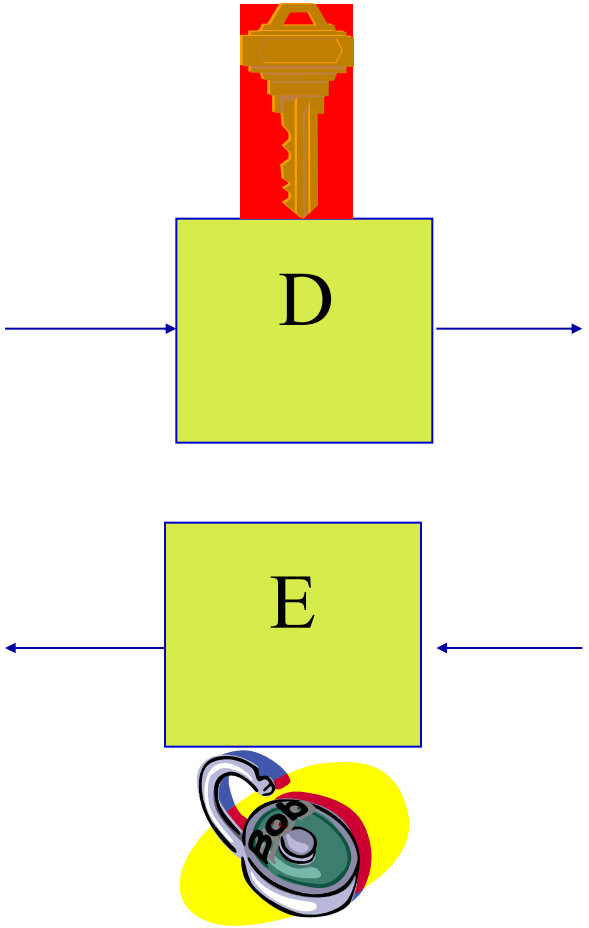
- **La « puce » contenue dans la carte, pilote l'authentification du porteur, de la carte et de la transaction**

Couple
clé publique / clé privée

Clé secrète symétrique

Le RSA permet la signature

- Un authentifiant opposable aux tiers
- Obtenu en appliquant D au message à signer
- Vérifiable à l'aide de la seule clé publique
- D'autres méthodes pour signer ont été proposées



Dématérialisation et signature électronique

En plein développement

universign

Quels seront les prochains secteurs à adopter la signature électronique ?

0 commentaires

Partager :

DocuSign®

Le chiffrement homomorphe

Un problème posé dès 1978

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos

Massachusetts Institute of Technology
Cambridge, Massachusetts

I. INTRODUCTION

Encryption is a well-known technique for preserving the privacy of sensitive information. One of the basic, apparently inherent, limitations of this technique is that an information system working with encrypted data can at most store or retrieve the data for the user; any more complicated operations seem to require that the data be decrypted before being operated on.

A FULLY HOMOMORPHIC ENCRYPTION SCHEME

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Craig Gentry
September 2009

Protection de la vie privée

- **Autorise le calcul sur les données chiffrées (Crypto-computing)**

- **S'applique pour la protection de la vie privée**

2010 – 11 : Variantes / implantations

Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes

Nigel P. Smart[1] and Frederik Vercauteren[2]

[1] Dept. Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB,
United Kingdom
nigel@cs.bris.ac.uk
[2] COSIC - Electrical Engineering,
Katholieke Universiteit Leuven,
Kasteelpark Arenberg 10,
B-3001 Heverlee,
Belgium
fvercaut@esat.kuleuven.ac.be

Abstract. We present a fully homomorphic encryption scheme which has both relatively small key and ciphertext size. Our construction fol-

PKC09 EC 11

EC10

Fully Homomorphic Encryption over the Integers

Marten van Dijk[1], Craig Gentry[2], Shai Halevi[2], and Vinod Vaikuntanathan[2]

[1] MIT CSAIL
[2] IBM Research

Abstract. We construct a simple fully homomorphic encryption scheme, using only elementary modular arithmetic. We use Gentry's technique to construct a fully homomorphic scheme from a "bootstrappable" somewhat homomorphic scheme. However, instead of using ideal lattices over a polynomial ring, our bootstrappable encryption scheme merely uses addition and multiplication over the integers. The main appeal of our scheme is the conceptual simplicity.

Implementing Gentry's Fully-Homomorphic Encryption Scheme

Craig Gentry* and Shai Halevi*

IBM Research

Abstract. We describe a working implementation of a variant of Gentry's fully homomorphic encryption scheme (STOC 2009), similar to the variant used in an earlier implementation effort by Smart and Vercauteren (PKC 2010). Smart and Vercauteren implemented the underlying "somewhat homomorphic" scheme, but were not able to implement the bootstrapping functionality that is needed to get the complete scheme to work. We show a number of optimizations that allow us to implement all aspects of the scheme, including the bootstrapping functionality.

La menace quantique

- **Proceedings of the 35th FOCS, Santa Fe, NM, Nov. 20--22, 1994**
- **SIAM J.Sci.Statist.Comput. 26 (1997)**

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Factorisation quantique

- La menace est prise au sérieux
- En réponse: normalisation de la cryptographie « post-quantique »

Table 5: *Quantum factorization records*

Number	# of factors	# of qubits needed	Algorithm	Year implemented	Implemented without prior knowledge of solution
15	2	8	Shor	2001 [2]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2009 [5]	×
	2	8	Shor	2012 [6]	×
21	2	10	Shor	2012 [7]	×
143	2	4	minimization	2012 [1]	✓
56153	2	4	minimization	2012 [1]	✓
291311	2	6	minimization	not yet	✓
175	3	3	minimization	not yet	✓

High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311

Zhaokai Li, Nikesh S. Dattani, Xi Chen, Xiaomei Liu, Hengyan Wang, Richard Tanburn, Hongwei Chen, Xinhua Peng, Jiangfeng Du

(Submitted on 25 Jun 2017)

In previous implementations of adiabatic quantum algorithms using spin systems, the average Hamiltonian method with Trotter's formula was conventionally adopted to generate an effective instantaneous Hamiltonian that simulates an adiabatic passage. However, this approach had issues with the precision of the effective Hamiltonian and with the adiabaticity of the evolution. In order to address these, we here propose and experimentally demonstrate a novel scheme for adiabatic quantum computation by using the intrinsic Hamiltonian of a realistic spin system to represent the problem Hamiltonian while adiabatically driving the system by an extrinsic Hamiltonian directly induced by electromagnetic pulses. In comparison to the conventional method, we observed two advantages of our approach: improved ease of implementation and higher fidelity. As a showcase example of our approach, we experimentally factor 291311, which is larger than any other quantum factorization known.

Subjects: **Quantum Physics (quant-ph)**
Cite as: **arXiv:1706.08061 [quant-ph]**
(or **arXiv:1706.08061v1 [quant-ph]** for this version)

Submission history

From: Jiangfeng Du [view email]
[v1] Sun, 25 Jun 2017 08:53:02 GMT (1276kb,D)

Conclusion : la Crypto en 2018

- La sécurité des crypto-algorithmes est comprise et discutée
- Les méthodes asymétriques devraient résister dans un avenir prévisible
- Mais la recherche d' alternatives post – quantiques devrait se poursuivre
- Et l'attention devrait aussi se porter sur la sécurité des développements et des environnements

FRC 2018 : TABLE RONDE #1

LA CONFIDENTIALITÉ DES DONNÉES

FRC 2018
11ème édition

FRC 2018 : LA CONFIDENTIALITÉ DES DONNÉES

M. Ludovic HAYE
Maire de Rixheim, Dirigeant de CyberDiag,
Lieutenant-Colonel (RC) de la gendarmerie nationale

M. Fouad GADACHA
Responsable des processus et des opérations et DPO de NXO-Telecom

M. Michel ROCHELET
Référent ANSSI Région Grand-Est

LA CONFIDENTIALITÉ DES DONNÉES

M. Ludovic HAYE

La confidentialité des données dans le cloud : utopie ou réalité ?

La réalité est que la confidentialité reste le 1er frein à l'adoption

Plus généralement: le manque de sécurité est de loin l'objection que l'on entend le plus souvent dans la bataille que se livrent opposants et défenseurs du cloud computing.

(*véritable crainte ou excuse pour ne pas y aller ?)*

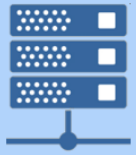
Le cloud « 100% secure »
reste en effet une utopie…

Paradigme du Cloud

« Comment tirer profit des avantages du Cloud tout en conservant mes données commerciales de façon sûre et confidentielle ? »

2 solutions :

- l'architecture de l'application est hébergée en **Pure Cloud**.
- Soit en **Hybrid Cloud** ce qui signifie que l'utilisateur peut conserver les données ayant le plus de valeur (Clients, Contrats, Données financières, etc.) sur son réseau et utiliser du Cloud uniquement des données non marquées, anonymes.

Support de stockage	Sécurité	Accès	Coût	Remarque d'utilisation
 Ordinateur professionnel	★★☆☆ Sujet au piratage informatique, aux détériorations et pannes	★☆☆☆ Pas adapté au partage, nécessite l'utilisation d'un support externe ou d'Internet (mail, cloud…)	★★★★ Pas de coût supplémentaire ou coût peu important	- Pour un stockage temporaire - Nécessité de crypter les données confidentielles et sensibles
 Support externe	★☆☆☆ - Sujet au vol, à la perte du support - Durée de vie limitée (dégradation du matériel)	★★★☆ Facilement transportable, il permet de transférer les données vers un autre ordinateur	★★★★ Pas de coût supplémentaire ou coût peu important	- Pour un stockage temporaire - Nécessité de crypter ou de sécuriser physiquement les données confidentielles et sensibles
 Serveur institutionnel	★★★★ Stockage fiable, durable et sécurisé (contre le vol, le piratage, les incendies…)	★★☆☆ La connexion au serveur institutionnel ne facilite pas le travail avec des personnes extérieures	★★☆☆ Coût assez important mais pas forcément répercuté sur l'usager	- Pour un stockage plus pérenne - Adapté pour le stockage de données sensibles et des versions « stables » de vos données - Toutes les institutions ne proposent pas ce service
 Serveur Cloud	★★☆☆ On ne sait pas vraiment où sont stockées les données, ni ce qu'elles deviennent	★★★★ Permet un travail synchronisé avec toutes les personnes ayant été autorisées au partage	★★☆☆ Payant à partir d'une certaine limite de stockage	- Pour un partage avec des personnes externes à l'institution - Ne pas y mettre de données sensibles ou confidentielles - Pas de contrôle sur la procédure de sauvegarde des données

Bref historique de l'évolution des mentalités

- 8-9 ans on ne parlait pas encore de cloud ss (stockage propriétaire)
- 4-5 ans certains y sont allés frileusement (pas tjs avec les bonnes données)
- Enfin depuis 3 ans, la question n'est plus de l'utiliser ou non, mais comment y aller (pure cloud ou hybrid)

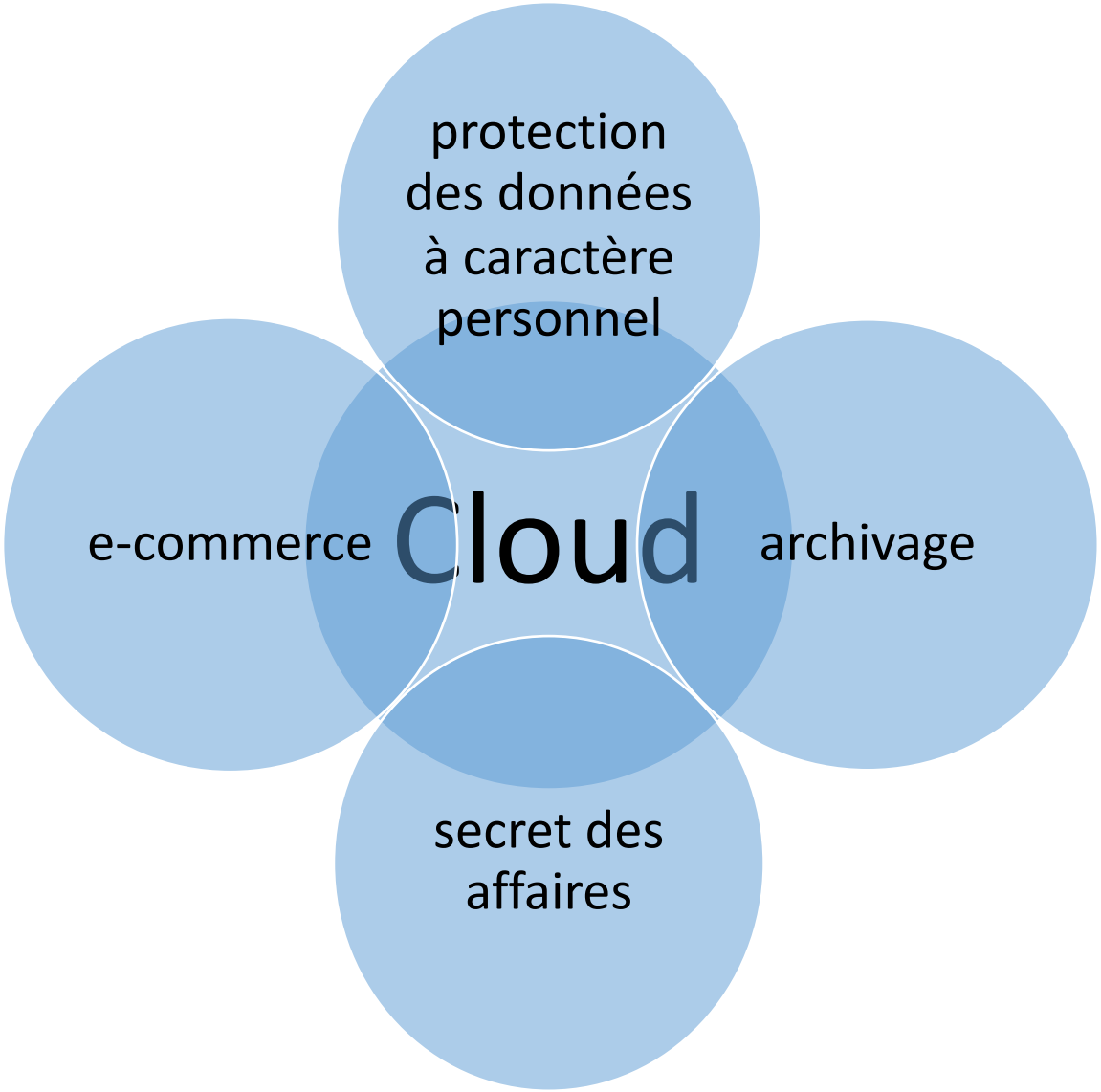
Le cloud lui-même a évolué :

- la baisse des prix du stockage
- l'amélioration de la bande passante
- Le développement des services proposés (infra diminue en interne / on demand)

De toute évidence, l'adoption des services cloud dépend avant tout des **exigences réglementaires,** des **questions de confidentialité** et de **sécurité**. Plus la réglementation va se développer et gagner en maturité, plus les entreprises profiteront pleinement des bénéfices du cloud computing.

La sécurité/confidentialité (angle juridique et législatif)

En Europe, tout particulièrement, les règles régissant la confidentialité sont on ne peut plus strictes et de nombreux gouvernements interdisent aux entreprises d'exporter les données au-delà des frontières (Longbottom 2008).


protection des données à caractère personnel
e-commerce
Cloud
archivage
secret des affaires

La sécurité/confidentialité (les questions à se poser)

- Quelles sont les technologies de sécurité particulières mises en place par le fournisseur ?
- Comment les sauvegardes de données sont-elles gérées et où les données sont-elles stockées ? (jeux de réplication)
- Comment le chiffrement est-il utilisé ?
- Où sont situés les datacenters ?

La sécurité/confidentialité (angle technique)

- TRANSMISSION DES DONNÉES (ligne chiffrée SSL ou data)

- STOCKAGE DES DONNÉES

✓ honnêteté du fournisseur …

✓ si chiffrement il y a, quid de la gestion des clés ?

- ACCÈS AUX DONNÉES (mécanismes d'authentification sont adéquats)

  Identification classique (Ident. Mdp, Mdp SMS)

  Authentification forte (Ident., Mdp, Mdp Token)

- DESTRUCTION DES DONNÉES (en fin de contrat)

La sécurité/confidentialité (angle technique):

Le chiffrement homomorphe très prometteur…

La sécurité/confidentialité (angle géographique)

- Cloud du GAFAM (sociétés américaines soumises au Patriot Act) (Cas SpideRoak (zero knowledge)

- Cloud Européen (Mozy (iso27001), OVH, Wimi, Wuala…)

Ce qu'il faut retenir

- Bien étudier les contrats en amont
- Le choix du fournisseur et surtout des sous-traitants
- Partir sur un « Cloud hybrid »
- Rester sur le territoire Européen
- Chiffrer ses données durant les transfert et dans le cloud
- S'assurer des conditions de stockage

LA CONFIDENTIALITÉ DES DONNÉES

M. Fouad GADACHA

Le RGPD pour les entreprises : syndrome de Bruxelles ou incitation structurante ?

Qu'est-ce qu'une donnée personnelle ?

Données personnelles

Informations associées à un nom

Nom, prénom

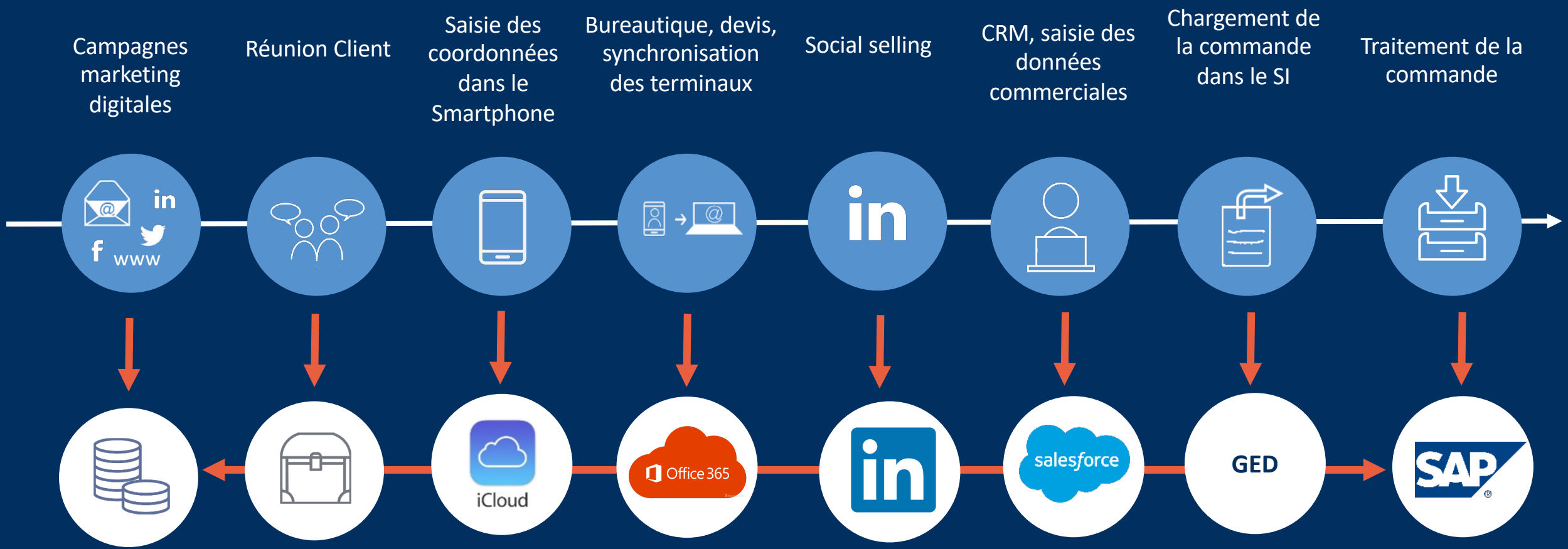
Informations qui permettent d'identifier une personne

Photo, numéro de sécu, numéro de téléphone,…

Informations anonymes dont le recoupement permet l'identification

Empreinte digitale, ADN, adresse IP,…

Des données personnelles client partout !



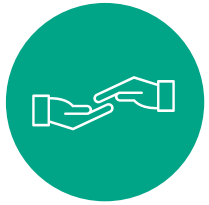
Passer des contraintes aux bénéfices

Contraintes

Obligations du RGPD :

- Garantir les nouveaux droits à la personne
- Etablir un registre de traitement des données
- Désigner un DPO
- Mener une étude d'impact
- Notifier les failles de sécurité
- …

Mise en œuvre par NXO



Bénéfices

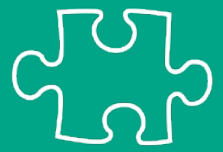
- Plus de confiance et de fidélité
- Meilleure gestion des données
- Responsabiliser les acteurs

Déclinaison par NXO du RGPD

Juridique

Technique

Organisationnelle



Assurer la confidentialité des données

Nouvelles relations contractuelles

Nouveaux salariés	Adaptation du contrat de travail
Clients	Avenant sur contrats existants et adaptation des CGV
Fournisseurs	Audit et Adaptation des CGA

Principes et outils

Renforcer	La sécurité périmétrique L'authentification Le chiffrement La prévention des fuites de données
Limiter maitriser	L'accès aux données Les droits des comptes à privilèges
Contrôler détecter	Sonde de détection Sonde d'analyse de réseau Outil d'analyse comportemental

Catalogue NXO fournitures de solutions de Sécurité

Organisation et communication

- Formation et sensibilisation des collaborateurs
- Nomination d’un DPO
- Cartographie des données
- Adaptation du Manuel de Gestion des Données

Conclusion

RGPD = Constat pertinent

Pour NXO = Prise de conscience et Accélérateur de bonnes pratiques

LA CONFIDENTIALITÉ DES DONNÉES

M. Michel ROCHELET

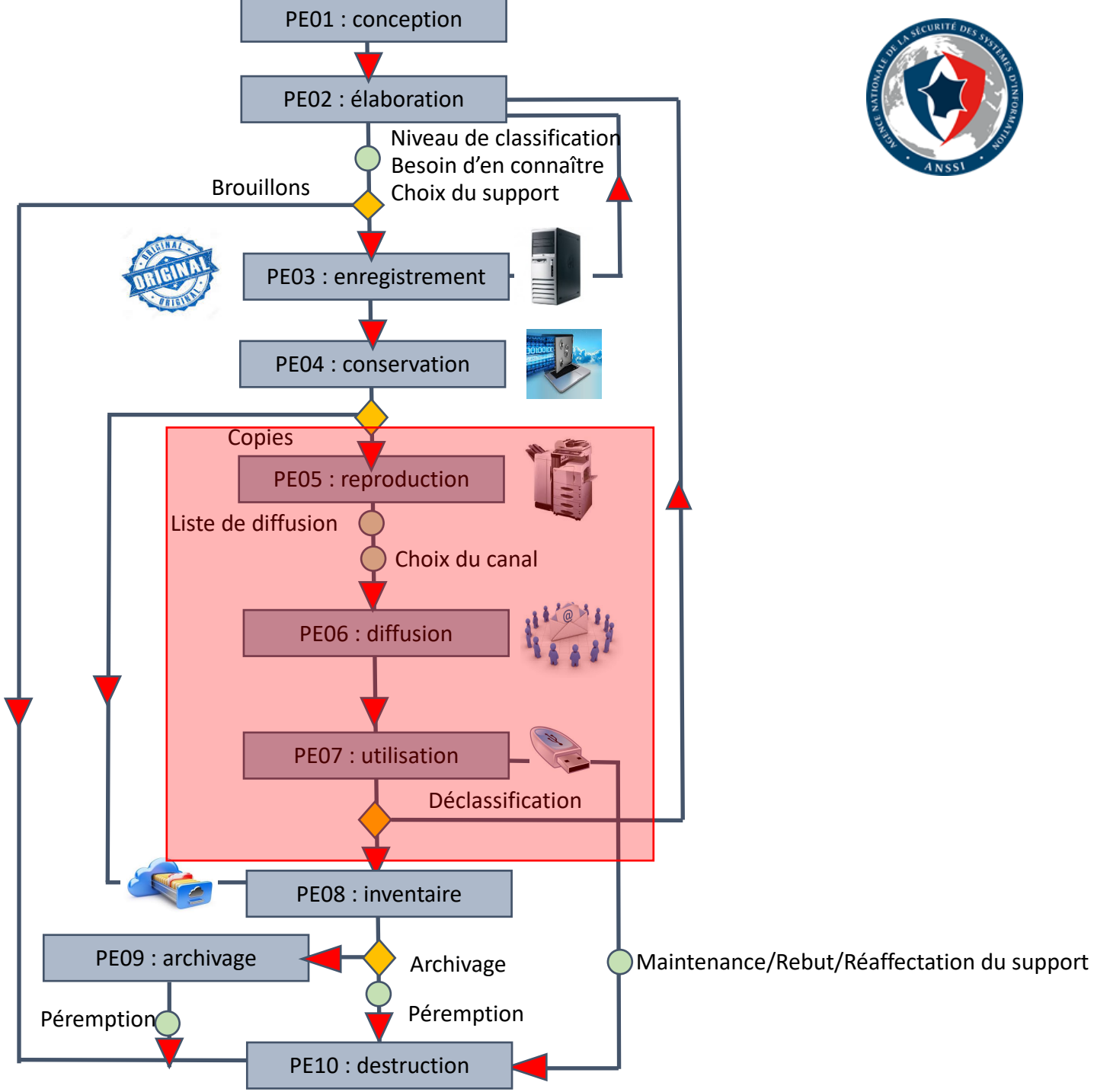
PME / TPE : besoin de sécurité et critère de confidentialité

- CYBERSÉCURITÉ -

Besoin de sécurité et confidentialité

- **Cartographie**
  des actifs informationnels
- **Analyse de risque**
  Besoin de sécurité (D.I.C)
- **Mesures de protection de la confidentialité**

Cycle de vie de l'information confidentielle (exemple)



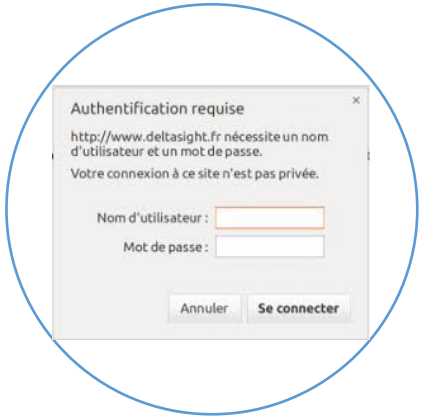
PRÉSERVER LA CONFIDENTIALITÉ
- Les fondamentaux -

Analyser
le risque

Séparer
les usages

Cloisonner
les réseaux

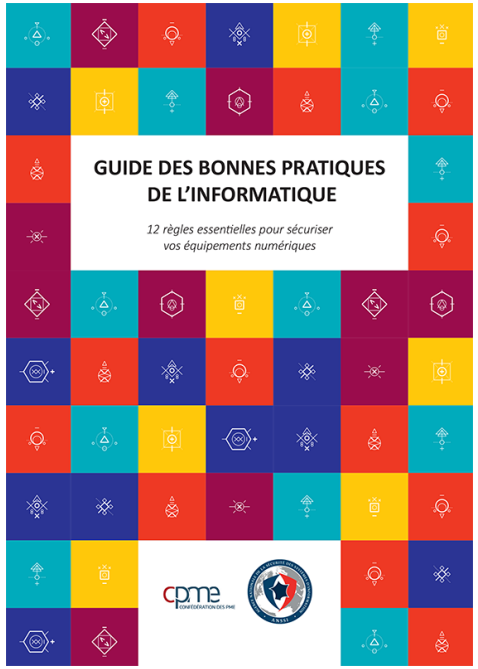
Contrôler
les accès



Sécuriser
les supports amovibles

Chiffrer
les informations sensibles

LA CYBERSÉCURITÉ
- Pour aller plus loin -



https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/

https://www.ssi.gouv.fr/guide/guide-dhygiene- informatique/

LA CYBERSÉCURITÉ
- L'autoformation à la SSI -

➢ **MOOC de l'ANSSI : SecNum Académie**

https://secnumacademie.gouv.fr/

SecNum académie
ANSSI

QUESTIONS ?
RÉPONSES

DÉMONSTRATION OPÉRATIONNELLE : LES MOTS DE PASSE

M. Gabin MICHALET
M. Mohamed BABACAR SARR
M. Nicolas GREINER
M. Thibaud GASSER

ensisa
École nationale supérieure d'ingénieurs sud Alsace

Les 10 mots de passe les plus utilisés

En 2017 :

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou

Principe de l'algorithme utilisé

L'algorithme a divers fonctionnement possibles :

- Force brute : Essais de toutes les combinaisons de caractères.
- Attaque par « dictionnaire » : utilisation des mots de passe communs ainsi que des mots ou des noms revenant souvent.
- Indices : Attaque par dictionnaire et utilisation des données accessibles autour des mots de passe afin de trouver des indices pour résoudre le mot de passe. En cas de multiples mots de passe, les mots de passe cassés sont ajoutés au dictionnaire.

Comment récupérer le fichier de mots de passe ?

Récupérer le fichier de mots de passe est relativement simple à partir du moment où la personne a un accès physique à la machine.

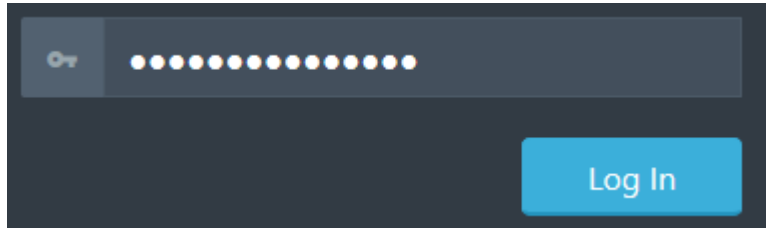
Si une personne réussit à s'infiltrer à distance et à récupérer des accès administrateurs, elle peut alors récupérer le fichier.

Solution : Mot de passe plus compliqué

Les mots de passe qui sont craqués le plus facilement sont les plus simples.

Un mot de passe contenant au moins 8 caractères dont des chiffres / majuscules / minuscules / caractères spéciaux sera très long à casser.

Par exemple Xf?UKCg3\R`6 nécessitera plus de temps que azerty



Mais cela pose un problème : **Comment les retenir ?**

Mauvais moyens pour retenir un mot de passe

L'écrire sur un papier rangé dans un tiroir / posé à côté / sous le clavier de l'ordinateur.

L'écrire dans un bloc-notes sur votre machine (MotDePasse.txt…). Si pour n'importe quelle raison quelqu'un vient à trouver ce fichier tous vos mots de passe seront compromis.

Mes Mots de Passe.txt - Bloc-notes

Fichier Edition Format Affichage ?

```
Compte machin.com = 12345678
Compte truc.fr = password
Compte chose.fr = azerty
```

Moyens mnémotechniques

Une méthode assez simple pour se souvenir d'un mot de passe compliqué est de partir d'une phrase simple (ex: Le soleil, c'est chaud) et d'en garder seulement une partie (ex: Lsl,c'ecd).

Bien entendu, l'utilisateur peut utiliser des phrases ou des suites de mots plus longues ou plus compliquées.

Moyens externes : les gestionnaires de mot de passe

Utilisation d'un mot de passe maître (fort de préférence) pour accéder à un fichier crypté de ses mots de passe.

Le logiciel, une fois déverrouillé, remplit les champs des mots de passe automatiquement.

Liste non-exhaustive de gestionnaires de mots de passe

- LastPass
- KeePass
- LogMeOnce
- RoboForm
- Sticky Password
- Et beaucoup d’autres …

LastPass

KeePass

LogmeOnce

RoboForm

StickyPassword
securing your personal data

Conclusion

Avoir des mots de passe forts permet d'accroître la sécurité.

Cependant, il faut tout de même s'en souvenir ou bien le stocker.

Il faut donc faire attention à l'endroit où on le stocke car cela peut rendre caduque l'efficacité d'un mot de passe fort.


Pause !

FRC 2018 : TABLE RONDE #2

LES CONTRÔLES D'ACCÈS

FRC 2018 : LES CONTRÔLES D'ACCÈS

M. Thomas VIERLING
Directeur et Consultant Senior de LPB Conseil

M. Alexandre HECK
Responsable infrastructures et systèmes à l'Université de Haute Alsace

M. Clément OUDOT
Identity Solutions Manager de Worteks

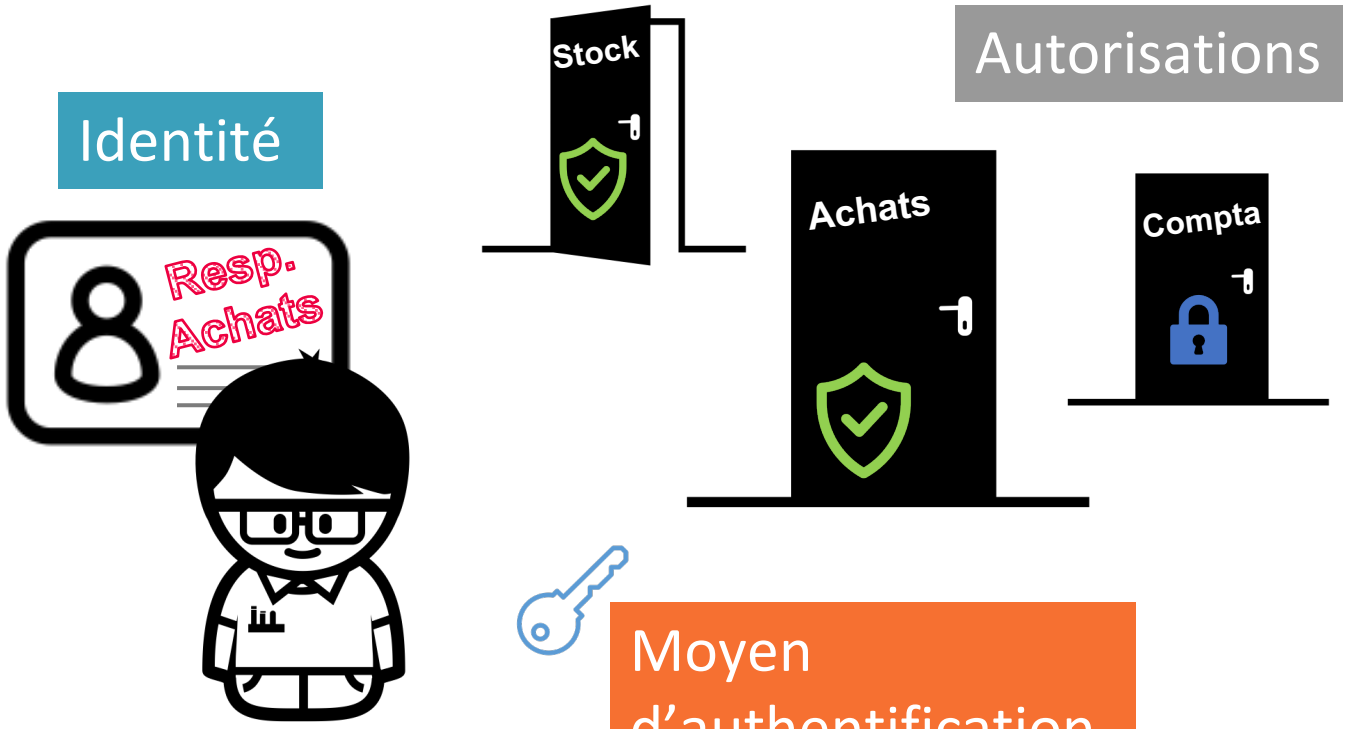
LES CONTRÔLES D'ACCÈS

M. Thomas VIERLING

La gestion des accès : comment et pourquoi ?

1. La gestion des accès

Maîtrise des accès



2. Absence de gestion : quels sont les risques?

Perte de maîtrise du SI

Perte de traçabilité

Perte de confidentialité

Fuite de données
Par erreur humaine ou par malveillance

Manque de segmentation
Propagation de ransomware, data miner

3. Comment maîtriser les accès ?

Comprendre **l'organisation de l'entreprise**
Pour se projeter dans la segmentation des accès

Impliquer les responsables **métiers**
Pour concevoir l'organisation des droits de leurs profils métiers

Connaître son **SI**
Pour faire le lien entre les applications et métiers

Définir **des processus**
Afin d'automatiser l'attribution et révocation de droits

4. Le mot de passe

Responsabiliser les utilisateurs

Le mot de passe est **confidentiel et personnel**

Aussi précieux que le code de votre carte bancaire !

Fournir un moyen de **sécurisation** du mot de passe

Définir des **règles d'utilisation**

Ne jamais le **divulguer ni le réutiliser**

Utiliser un **coffre fort sécurisé** ou **fédérer l'identité : OpenID**

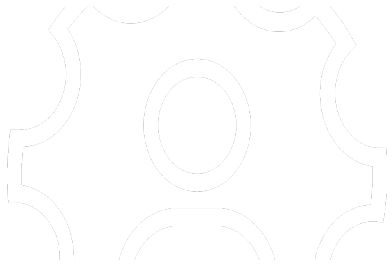
Chaque utilisateur pourra stocker des mots de passe de façon sécurisée et en partager en interne et externe, ou se connecter à l'aide d'un compte unique !

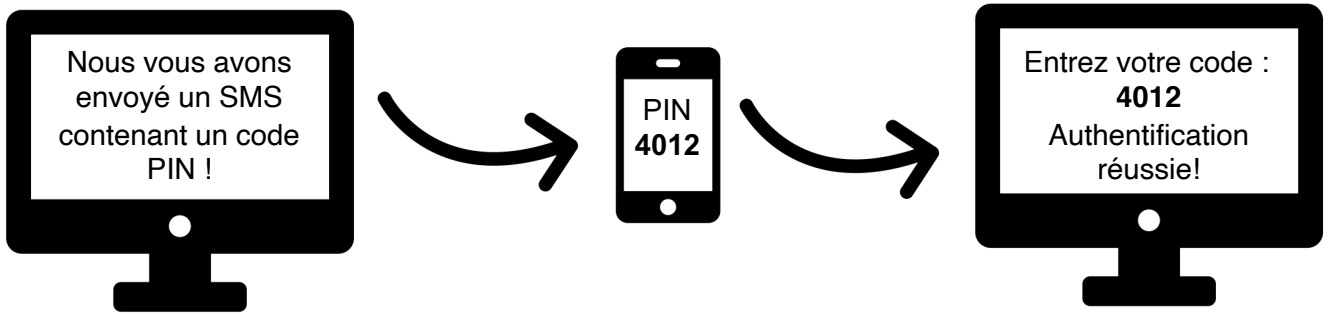
5. Les nouveaux moyens d'accès

Authentification multi-facteurs

Biométrie

Radio / Electronique





Conclusion

Niveau de **confidentialité**

Qu'est ce qui est réellement confidentiel ?

Contrôle et **sécurisation** des accès machines

Réseau d'entreprise 802.1X

IoT

Analyser le **risque** et connaître **ses obligations**

Classifier les données

RGPD

Données sensibles

LES CONTRÔLES D'ACCÈS

M. Alexandre HECK

Authentification pour l'accès au réseau d'une université

L'université de Haute Alsace

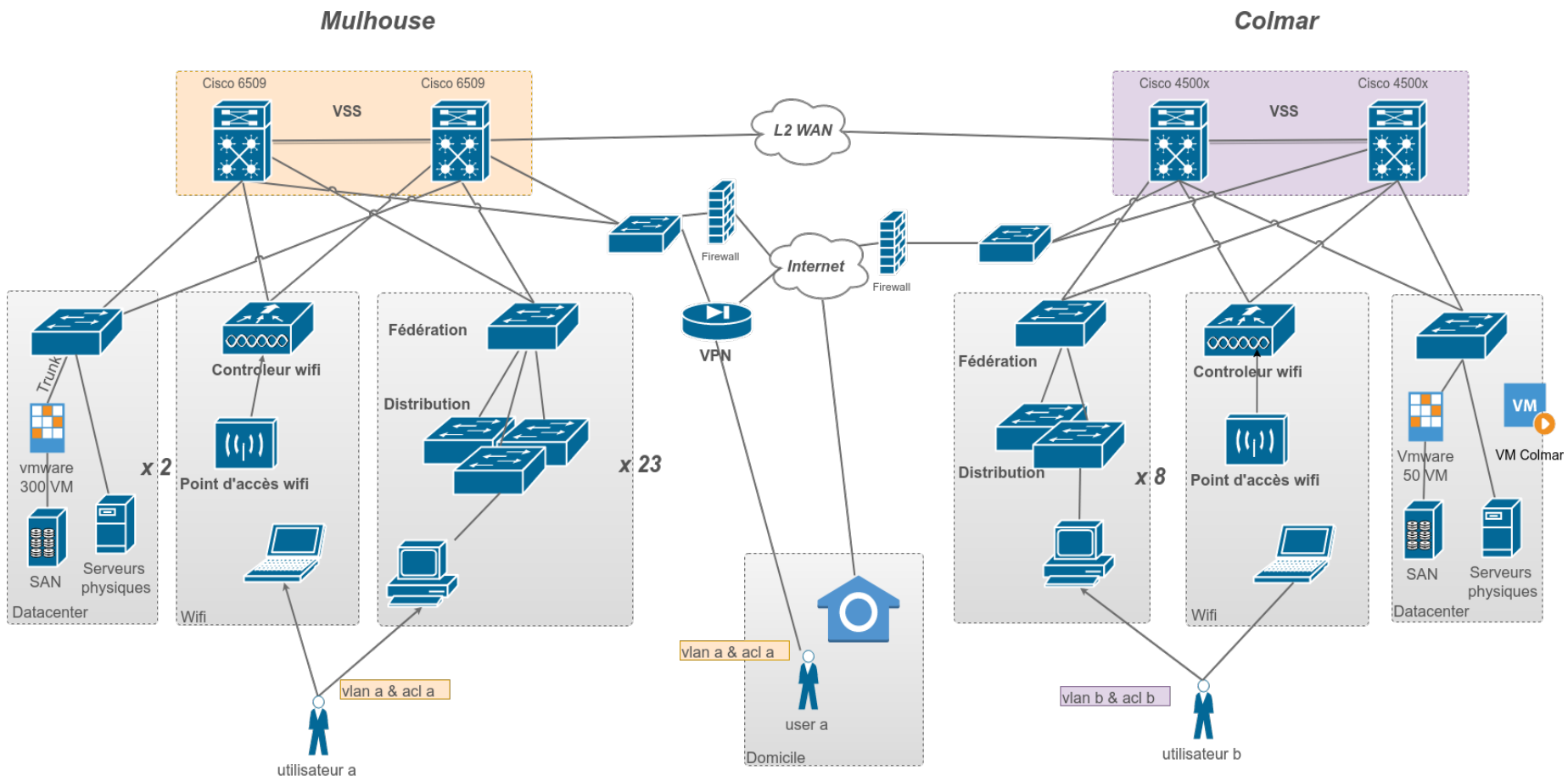
- Quelques chiffres
  - 11000 usagers, 10000 étudiants, 1000 personnels
  - 8 composantes, 15 laboratoires
  - 3000 postes de travail
  - De plus en plus d'objets connectés
  - Une université sur 2 villes Mulhouse et Colmar et 5 sites.

Pourquoi vouloir authentifier pour permettre l'accès au réseau

- Nécessité d'assurer sécurité et traçabilité des accès tout en augmentant la mobilité numérique des usagers (Axe stratégique).

- Répondre aux obligations de la PSSIe.
  - Objectif 13/34 action RES-CLOIS : *Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.*

Le réseau de l'UHA

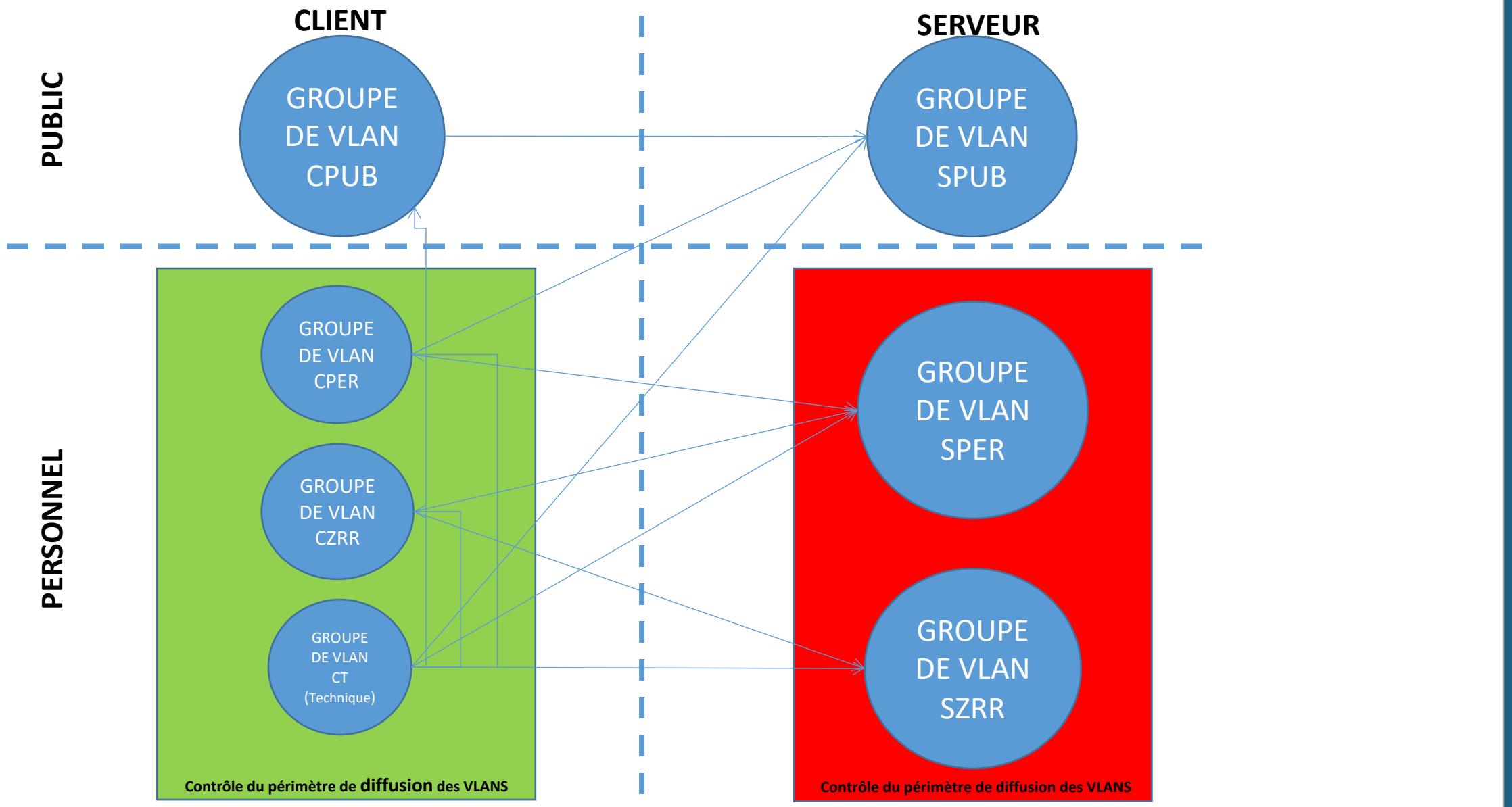


- 300 commutateurs de distributions, 250 bornes WIFI, 100 vlan, 3000 lignes d'ACL
- Organisation logique proche des bâtiments.
- Des usagers de plus en plus mobiles.

L'organisation logique la clé

- Mécanisme tels que SGT (Secure Group Tagging) non implémentable dans l'état
  - Réseau trop hétérogène
  - Modifications matérielles trop conséquentes.
- Une solution pragmatique
  - Authentification via 802.1x -> radius (FreeRadius) -> ldap
- Un concept
  - « vlan à la demande »
  - Transmettre le vlan id lors du message d'autorisation
- Repenser l'organisation des réseaux logiques

Organisation générale des groupes de réseau logiques



Les outils

- Pouvoir implémenter cette réorganisation
  - Disposer d'outils et les valider
    - POC ISE : Identity Secure Engine (CISCO).
    - Possibilité d'évolution vers SGT demain.
  - Entre deux plaques métropolitaines (vxLAN).

Authentifier pour permettre l'accès au réseau : état

- VLAN à la demande WIFI en production.
- VLAN à la demande/VPN en production.
- VLAN à la demande/réseau en POC.
  - Pour des usagers « testeurs ».
  - Pour les objets connectés (MAB).
- Pilotage logiciel : gagner en expérience : former les équipes.
- Le vrai temps (long) du projet est dans la conduite du changement et non dans la technique !

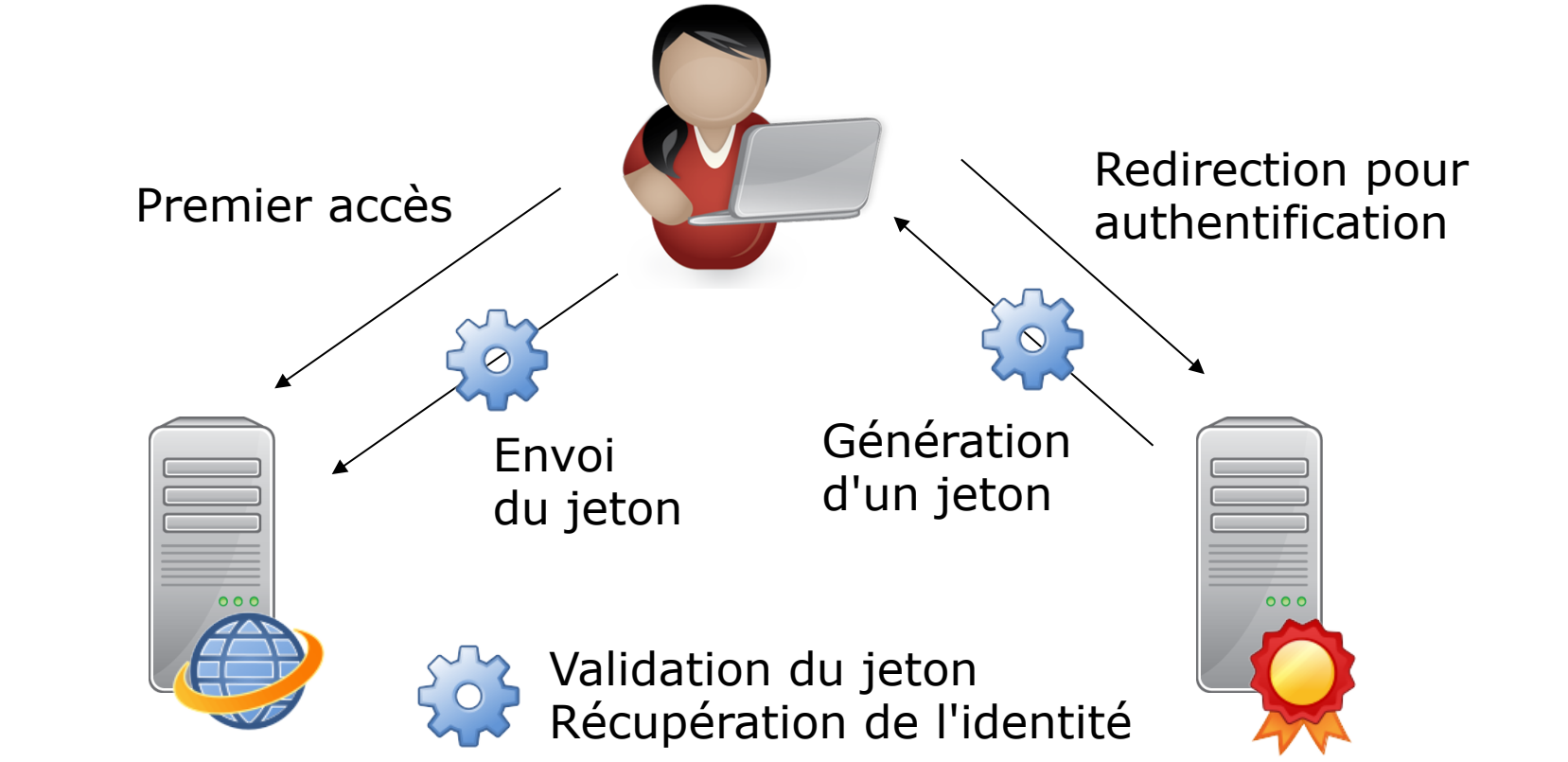
LES CONTRÔLES D'ACCÈS

M. Clément OUDOT

Open ID / FranceConnect et WebAuthentification

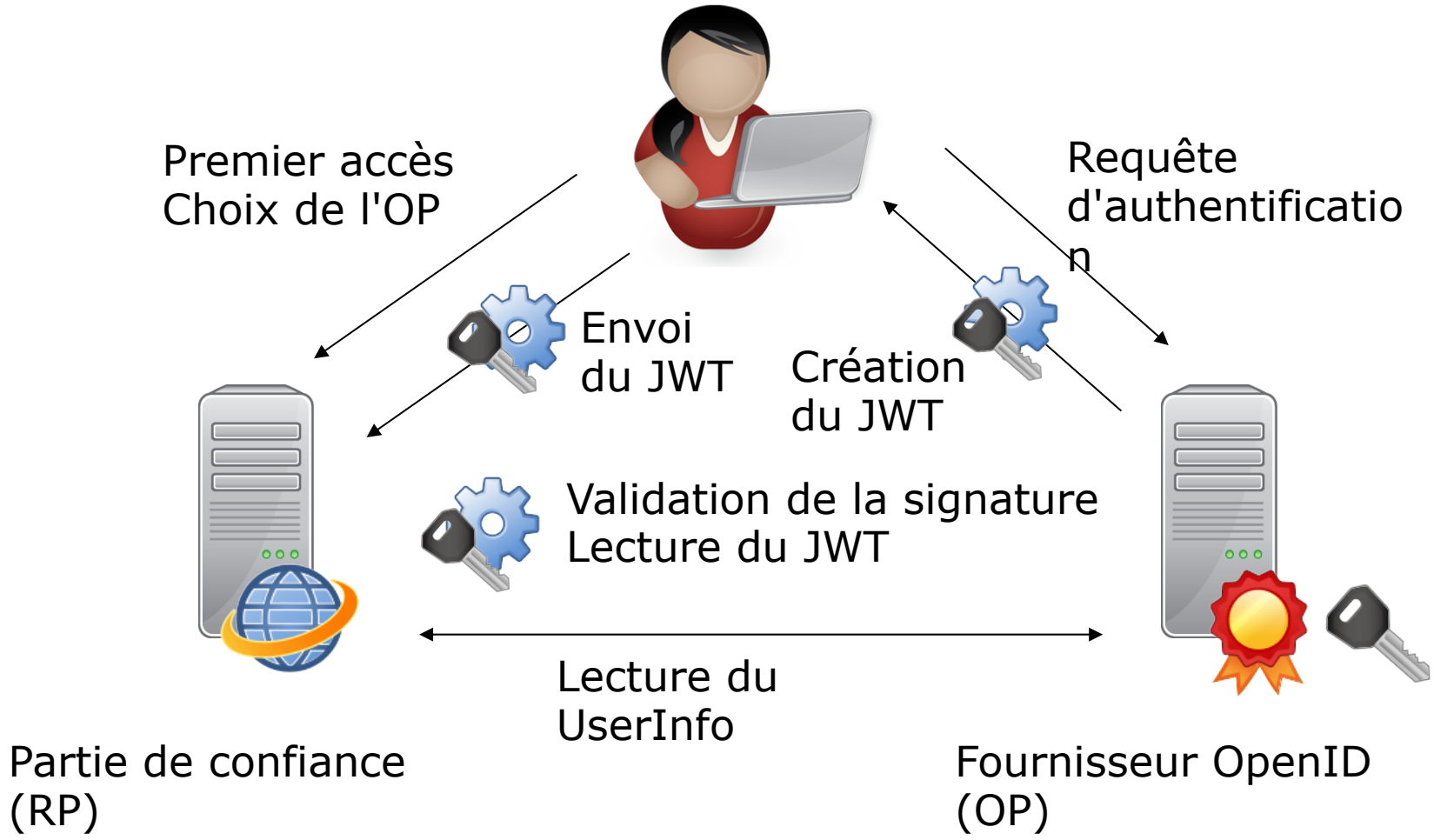
Fonctionnement basique de l'authentification unique Web (WebSSO)

1. L'utilisateur accède sans être authentifié à une application intégrée au WebSSO
2. Il est redirigé sur un service d'authentification qui valide son identité et fournit un jeton
3. Le jeton est transmis à l'application qui obtient l'identité de l'utilisateur en validant/résolvant ce jeton
4. L'utilisateur accède aux autres applications sur le même principe, sans se réauthentifier


Premier accès
Redirection pour
authentification
Envoi
du jeton
Génération
d'un jeton
Validation du jeton
Récupération de l'identité
Application Web
Portail d'authentification

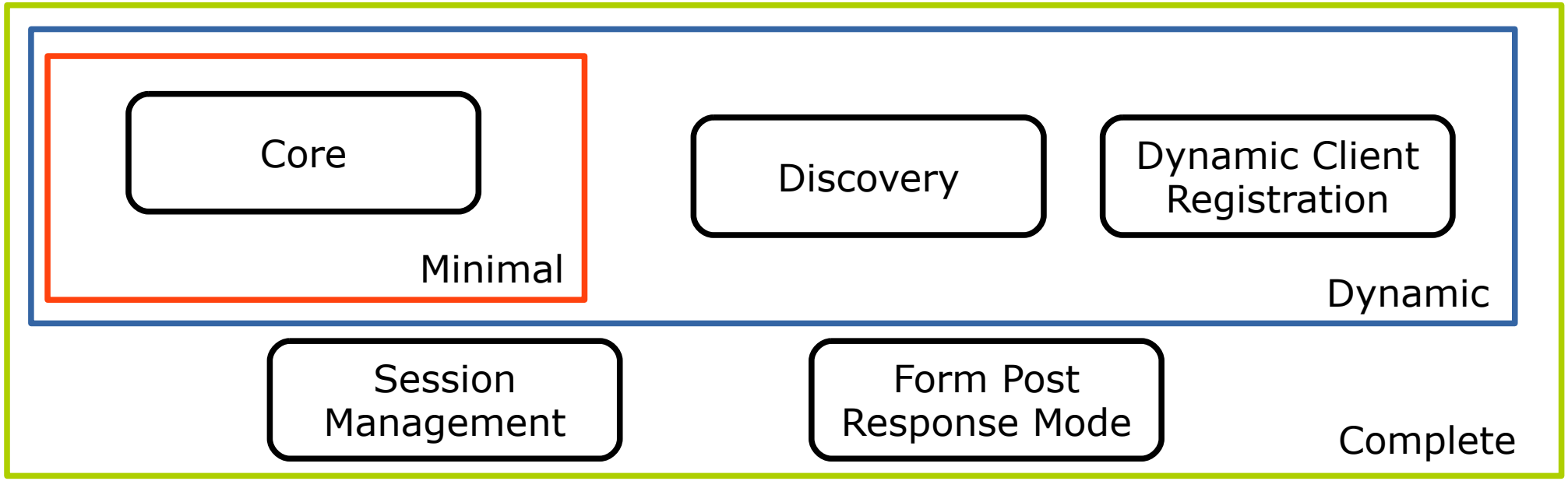
Le protocole OpenID Connect

- Basé sur OAuth2, REST, JSON, JWT, JOSE
- Adapté aux navigateurs Web et aux applications mobiles natives
- Publication des informations de configuration au format JSON
- Consentement de l'utilisateur requis sur le partage d'attributs

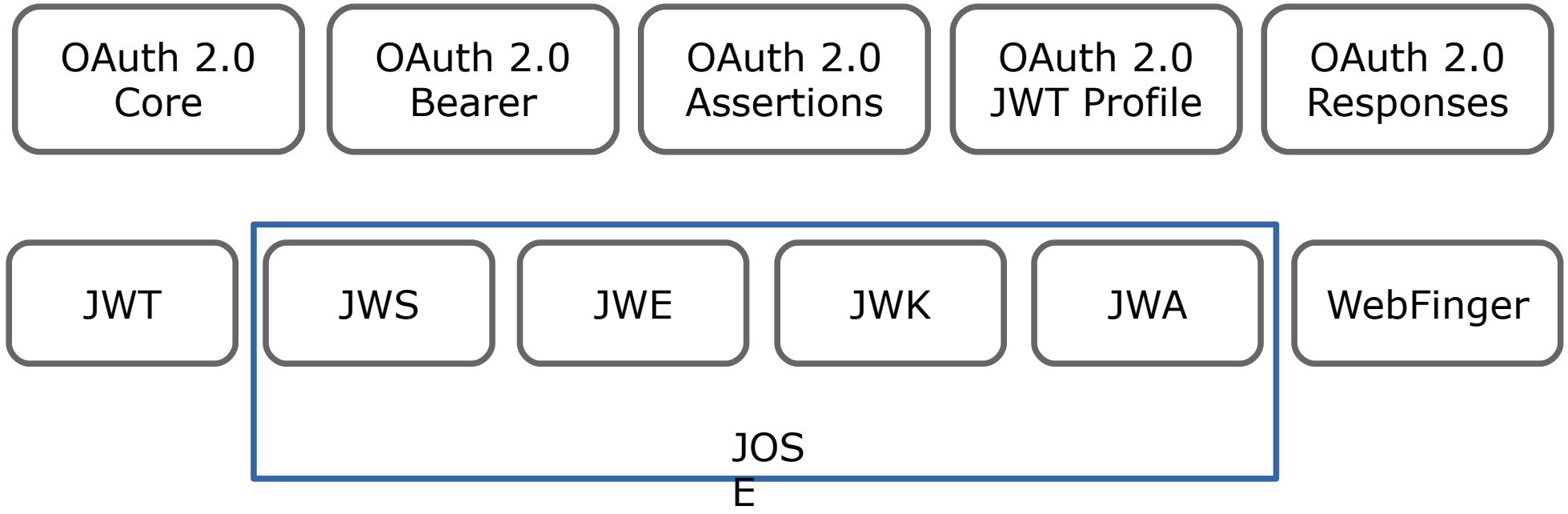

Premier accès
Choix de l'OP
Envoi
du JWT
Requête
d'authentificatio
n
Création
du JWT
Validation de la signature
Lecture du JWT
Lecture du
UserInfo
Partie de confiance
(RP)
Fournisseur OpenID
(OP)

Spécification du protocole

- Publiées sur le site de la [fondation OpenID]



Autres standards impliqués




```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

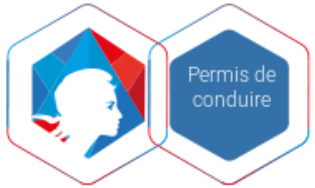
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
) secret base64 encoded
```

http://jwt.io/

France Connect

Un service d'authentification

- FranceConnect ne fournit pas directement l'authentification, mais s'appuie sur des fournisseurs d'identités agréés, comme le service des impôts
- Après authentification, une « identité pivot » est transmise au service final (site d'une mairie, service public, etc.)
- Les échanges sont réalisés à l'aide du protocole OpenID Connect



Connectez-vous simplement avec **FranceConnect**,
Choisissez parmi l'un des organismes ci dessous

Consulter les points de son permis

Site service-public.fr

IDENTITÉ

Nom de naissance :	OUDOT	Date de naissance :	20/08/1980
Nom d'usage :	OUDOT	Commune de naissance :	Reims
Prénom :	Clément Pierre	Département de naissance :	Marne
Sexe :	Homme	Pays de naissance :	FRANCE

Identité vérifiée grâce à

France Connect

Identité pivot (particulier)

Champs	Type	Description
given_name	string	prénoms séparés par des espaces (standard OpenIDConnect)
family_name	string	le nom de famille de naissance (standard OpenIDConnect)
birthdate	string	la date de naissance au format YYYY-MM-DD (standard OpenIDConnect)
gender	string	male pour les hommes, female pour les femmes (standard OpenIDConnect)
birthplace	string	le code INSEE du lieu de naissance (ou une chaîne vide si la personne est née à l'étranger)
birthcountry	string	le code INSEE du pays de naissance

Identité pivot (entreprise)

Champs	Type	Description
given_name	string	prénoms séparés par des espaces (standard OpenIDConnect)
family_name	string	le nom de famille (standard OpenIDConnect)
email	string	l'adresse mail de la personne
siret	string	le numéro SIRET ou SIREN de l'entreprise (non standard)

QUESTIONS ?
RÉPONSES

FRC 2018
11ème édition

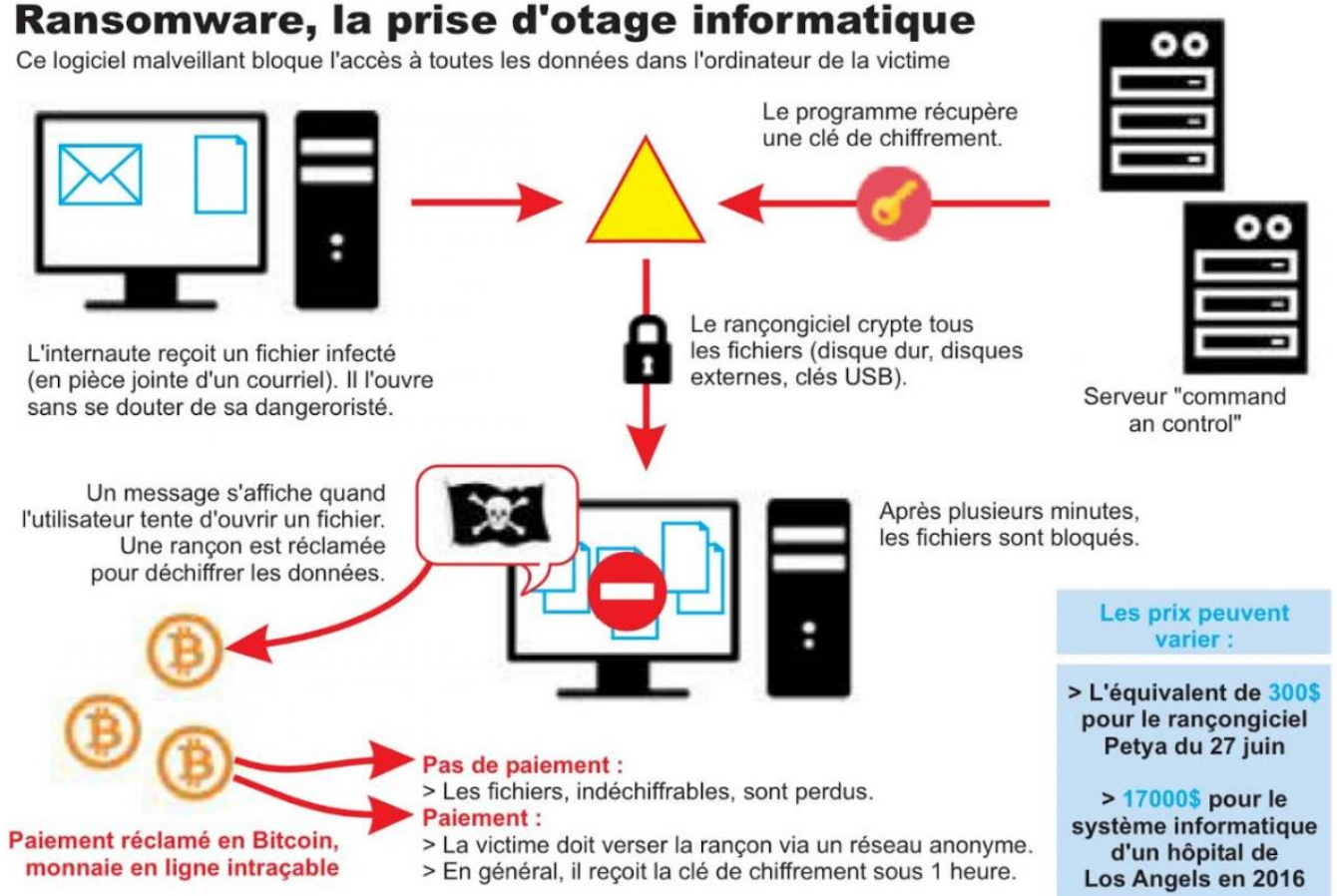
FRC 2018 : CONFÉRENCE DE CLÔTURE
Cybersécurité, cybercriminalité, quelles évolutions législatives?

Mme. Myriam QUEMENER

Magistrat, docteur en droit,
Avocat général près la Cour d'appel de Paris,
Service économique, financier et numérique,
Auteur de : "Le droit face à la disruption numérique"

Ransomware, la prise d'otage informatique

Ce logiciel malveillant bloque l'accès à toutes les données dans l'ordinateur de la victime



Les prix peuvent varier :

> L'équivalent de 300$ pour le rançongiciel Petya du 27 juin

> 17000$ pour le système informatique d'un hôpital de Los Angels en 2016

Cybertendances

- Cybercriminalité organisée et fraudes
- Une posture plus agressive des délinquants, avec des modes d'action relevant de plus en plus souvent de l'extorsion: *sextorsion*, rançongiciels chiffrants
- La croissance du nombre et de l'ampleur des **détournements de données,**
- Les logiciels malveillants sont une menace croissante, avec une évolution dans le domaine des botnets bancaires
- Les FOVI qui touchent de nombreux pays occidentaux avec des formes de plus en plus sophistiquées d'accès aux informations permettant l'ingénierie sociale ;
- Les **attaques en déni de service** (DDoS) sont un mode opératoire en croissance,
- Les **cryptoactifs (**le ***bitcoin)*** sont devenues le moyen transactionnel de choix pour les échanges financiers entre cybercriminels

Les modes opératoires

Phishing

Carding

Sim Swapping

Jackpotting &blackbox

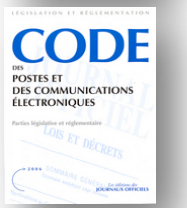
Malware bancaire

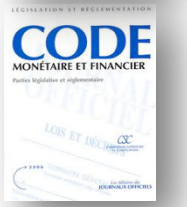
APT

Botnet

Cibles: systèmes bancaires & de paiement

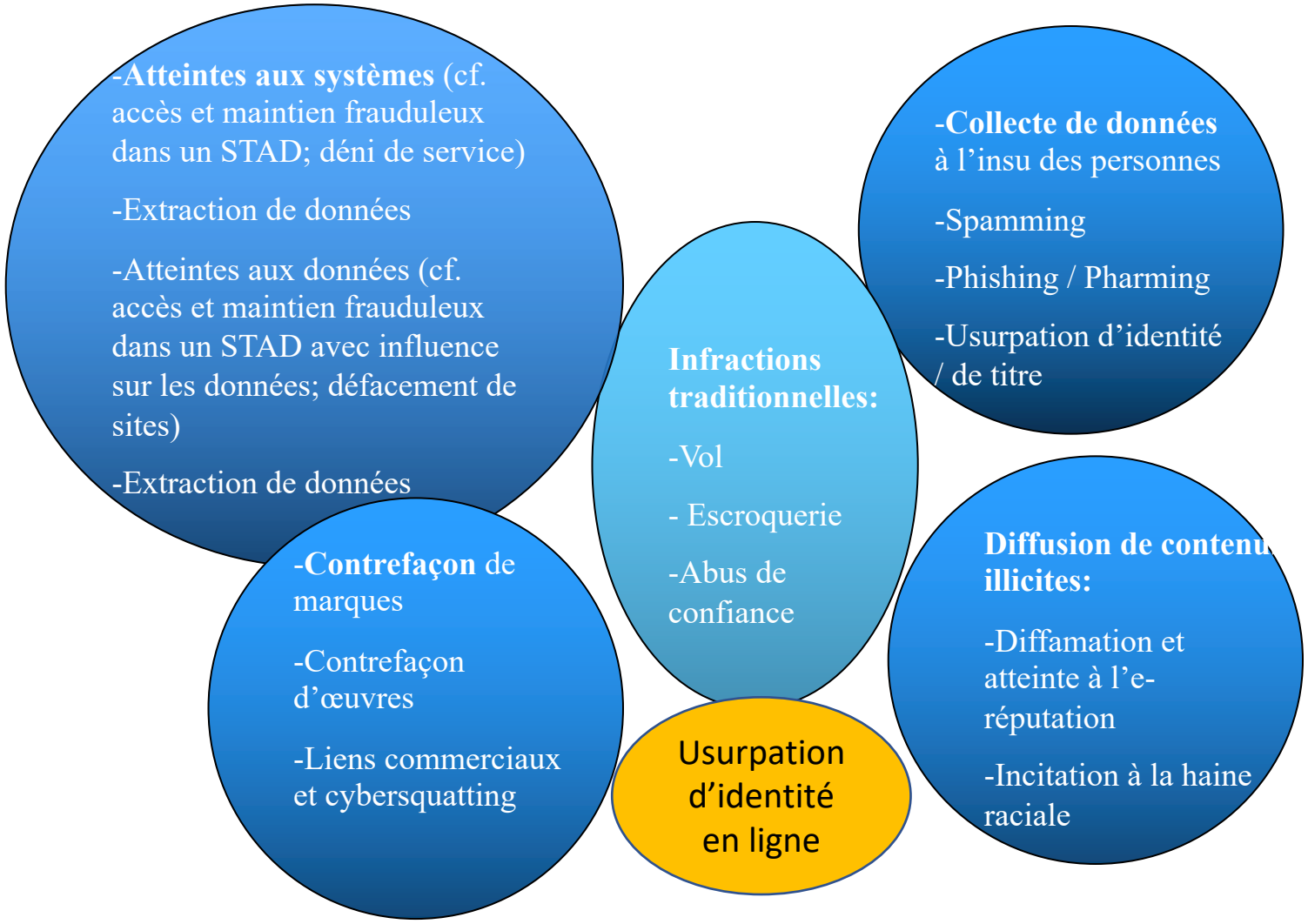
Les codes





- **Le Code Pénal** : définition des infractions précisant les peines encourues : contraventions, crimes et délits
- **Le Code de la Propriété Intellectuelle** définit les droits d'auteurs et artistiques et la protection des inventions et connaissances techniques. (CPI)
- **Le Code de Procédure Pénale** désigne sous le nom d'enquêtes, les missions et actes de police judiciaire qui consistent à **constater** les infractions, à en **rassembler** les preuves et à en **rechercher** les auteurs (CPP)
- **Le Code des Postes et des Communications Electroniques**, regroupe, des dispositions législatives et réglementaires relatives au service postal et aux communications électroniques. (CPCE)
- **Le Code Monétaire et Financier**, regroupe, des dispositions législatives et réglementaires relatives aux paiements et transactions financières (CMF)

Les infractions pouvant réprimer le piratage informatique et ses conséquences



Les procédures à l'ère numérique

- Adaptation à la recherche de la preuve numérique
- Spécificité de cette preuve
- Volatilité
- Extranéité

La loi du 13 novembre 2014

- En matière pénale, afin de prendre en compte les évolutions technologiques, la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a incriminé le « vol » de données et a créé l'infraction d'atteinte à un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État commise en bande organisée.

- La loi du 24 juillet 2015 relative au renseignement a par ailleurs rehaussé les peines pour les différentes atteintes à un système de traitement automatisé de données.

La loi du 13 novembre 2014

- Les techniques d'enquête pouvant être mises en œuvre ont été renforcées. Ainsi, la loi du 13 novembre 2014 a créé un régime procédural spécifique applicable aux enquêtes et poursuites portant sur des atteintes à un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État commises en bande organisée, avec notamment la possibilité de réaliser des surveillances, infiltrations et enquêtes sous pseudonyme.

L’évolution numérique en matière d’enquête

- Le code de procédure pénale permet l'utilisation de plusieurs procédés nouveaux en matière de criminalité organisée, mis en œuvre par l'« agence nationale des techniques d'enquêtes numériques judiciaires » et coordonnés par le « comité d'orientation des techniques d'enquêtes numériques judiciaires », créés par le décret n° 2017-614 du 24 avril 2017.

- La notion de « technique d'enquête numérique » est une notion qui donne une dynamique résolument moderne aux enquêtes judiciaires. Pourtant, la réalité est beaucoup moins satisfaisante.

Evolution en matière de compétence territoriale

- La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale a créé un nouvel article 113-2-1 dans le Code pénal qui dispose : « Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République ».

- Le législateur privilégie le domicile de la victime personne physique ou le siège social de la personne morale pour retenir la compétence.

La loi du 3 juin 2016

- Adaptation des règles de compétence territoriale en prévoyant que tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique commis au préjudice d’une personne résidant en France est réputé commis sur le territoire national, et en octroyant une compétence nationale aux parquet et juridictions de Paris (pôle de l'instruction, tribunal correctionnel et cour d'assises) pour l’ensemble des atteintes à un système de traitement automatisé de données.

La loi n° 2016-731 du 3 juin 2016, renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale

- Appréhension à distance de données, indépendamment de la détention matérielle du système ou du support. Ces techniques d'investigations sont donc largement dématérialisées, qui s'apparent à un piratage informatique élaboré.

- Pareil développement des investigations numériques interroge cependant, car leur nature juridique devrait être davantage discutée.

L'émergence d'un droit de la cybersécurité

- Le 27 avril 2016 (règlement général sur la protection des données) ;applicable le 25 mai 2018

- Le 8 juin 2016 (directive UE 2016/943 sur le secret des affaires et les renseignements stratégiques) ; loi du 30 juillet 2018

- Le 6 juillet 2016 (directive UE 2016/1148 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des SI dans l'UE). le 27 avril 2016 (règlement général sur la protection des données) ; loi du 26 février 2018

Accès aux correspondances stockées (art.706-95-1 à 706-95-3 du CPP)

- Redoutant que la personne puisse supprimer toutes les correspondances numériques avant la réalisation de la perquisition, le législateur instaure un nouveau cadre légal permettant la **saisie de correspondances stockées par la voie des communications électroniques**, **à l'insu** de la personne concernée, de manière indépendante de la perquisition.
- Ce dispositif vise un champ d'application plus large que celui de l'interception judiciaire.
- En effet, il autorise la saisie, **à distance**, d'**éléments stockés** sur une adresse électronique, y compris si celle-ci n'est plus active. La saisie peut également concerner une **adresse mail** ou un **identifiant informatique**, notamment lorsqu'il s'agit de cibler les échanges sécurisés qui interviennent via certaines applications telles que Whatsapp ou Skype.

Mise en œuvre des dispositifs techniques IMSI catcher

Dans le cadre de la criminalité et de la délinquance organisées (articles 706-73 et 706-73-1 du CPP), le recours au dispositif dit « IMSI catcher » est désormais possible. Les immunités prévues à l'art. 100-7 du CPP sont toujours applicables, à savoir **dans le véhicule, le bureau ou le domicile d'un** :

- député,
- sénateur,
- avocat,
- magistrat.

Avec ces nouveaux articles du CPP, l'« IMSI catcher » ne peut être mis en œuvre pour une finalité autre que celle de la recherche et de la constatation des infractions pour lesquelles il a été autorisé. Le fait que ces opérations révèlent des infractions autres que celles visées dans la décision du magistrat ne constitue cependant pas une cause de nullité des procédures incidentes.

LPM, art 22 : responsabilités et obligations des OIV en termes de protection de leurs installations

- Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, sont tenus de coopérer à leurs frais, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste.

Directive NIS

- Cette directive est destinée à assurer un *« niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne »*.

- Les *« opérateurs de services essentiels »* et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

En France la LPM a déjà intégré ces dispositions

- En France , les arrêtés encadrant la sécurité des OIV (Opérateurs d'importance vitale).
- Ces mesures qui découlent de l'article 22 de la Loi de programmation militaire votée fin 2013, incluent la notification des incidents de sécurité à l'Anssi (Agence nationale de sécurité des systèmes d'information).
- Chaque État membre devra désigner un ou des centres de réponse aux incidents de sécurité informatique (CSIRT), ou un centre de réponse aux urgences informatiques (CERT), pour alerter, suivre et analyser les incidents à l'échelon national. La création d'un réseau européen de CSIRT nationaux est prévue, ainsi que la mise en place d'un *« groupe de coopération »* stratégique de cybersécurité. Il sera composé de représentants des États membres, de la Commission européenne et de l'Agence européenne de la sécurité des réseaux et de l'information (ENISA).
- La directive NIS entrera en vigueur vingt jours après sa publication prochaine au Journal officiel de l'Union européenne. Les États membres de l'UE auront ensuite 21 mois, soit jusqu'au début de l'année 2018, pour transposer la directive dans leur législation nationale.

Directive NIS

- Le renforcement par chaque Etat de la cybersécurité d'« opérateurs de services essentiels » au fonctionnement de l'économie et de la société via
  - La définition au niveau national de règles de cybersécurité auxquels ces derniers devront se conformer ;
  - L'obligation pour les opérateurs de notifier les incidents ayant un impact sur la continuité de leurs services essentiels.

- L'instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines de l'informatique en nuage, des moteurs de recherche et places de marché en ligne.

Le RGPD / Rappel des grandes lignes

- *Le RGPD s'appliquera dès lors qu'un responsable du traitement ou un sous-traitant est établi sur le territoire de l'UE ou qu'un résident européen est directement visé par un traitement de données.*
- Désignation d'un délégué à la protection des données
- Violation de données personnelles (obligation de notification à la CNIL)
- Réalisation d'analyses d'impact relatives à la protection des données
- Droit à l'oubli consacré
- Droit à la portabilité des données personnelles
- Transferts de données hors Union européenne
- Amendes administratives et sanctions (*La violation des dispositions du RGPD fait l'objet d'amendes administratives pouvant s'élever jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent*)

Et le paquet Cyber

- La Commission a proposé de renforcer la résilience et la capacité de réaction de l'UE aux cyberattaques en renforçant l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), en créant un cadre de certification de cybersécurité à l'échelle de l'UE, un plan d'action relatif aux modalités de réaction aux crises et incidents de grande ampleur en matière de cybersécurité, ainsi qu'un Centre européen de recherche et de compétences en matière de cybersécurité.
- Transformation de l'ENISA en agence européenne de cybersécurité
- Création d'un label européen pour les entreprises
- Enfin, dans l'objectif de dissuader les cybercriminels, la Commission souhaite que l'Union européenne renforce son arsenal répressif par le droit pénal, par une **nouvelle directive sur la fraude ou la contrefaçon des moyens de paiement en ligne notamment les monnaies virtuelles.**

Le cadre juridique des objets connectés

- C'est la loi informatique et liberté du 6 janvier 1978, depuis régulièrement complétée, qui donne un cadre juridique à la protection des données personnelles en France.
- Au niveau européen, le règlement européen sur la protection des données du 14 avril 2016 entrera en vigueur pour tous les États membres le 25 mai 2018
- La loi pose un **principe de loyauté** dans la collecte des données via des objets connectés : cette collecte doit être proportionnée et pertinente par rapport à l'objectif poursuivi. Seules les données nécessaires à l'usage requis peuvent être exigées. Cela signifie notamment qu'il est interdit de collecter des données à l'insu du consommateur, et de les utiliser à d'autres fins que celles annoncées.
- Ce principe de loyauté entraîne une obligation d'information de l'utilisateur sur l'identité du collecteur, la finalité de la collecte de données, son caractère obligatoire ou facultatif, les conséquences d'un défaut de communication, les destinataires de ces données, le droit d'opposition, d'accès, de modification et de suppression.

L'extension de la procédure du coût d'achat par la loi du 3 juin 2016

- Comme en matière de trafic de stupéfiants, la loi n° 2016-731 du 3 juin 2016 autorise le recours à la technique d'enquête dite du « coup d'achat » qui permet notamment aux forces de l'ordre (C. pr. pén., art. 706-106) et aux agents des douanes (C. douanes, art. 67 *bis*-1) d'acquérir des armes pour constater les infractions mentionnées au 12° de l'article 706-73 du même code.

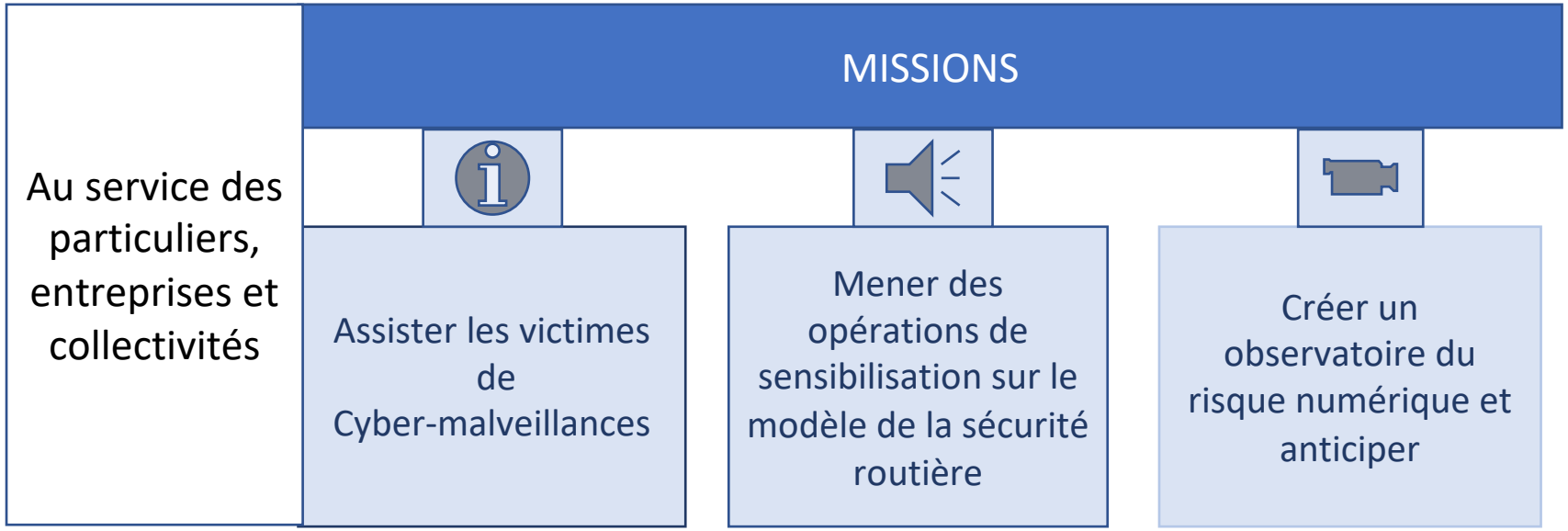
- En outre, les agents des douanes peuvent recourir à la technique de l'infiltration pour caractériser les infractions en matière d'armes (C. douanes, art. 67 *bis*).

La loi du 30 novembre 2017

- Les dispositifs (surveillances, interceptions, infiltration, sonorisation, IMSI catcher, captation de données informatiques) mis en œuvre dans le cadre d'une enquête de flagrance ou préliminaire devaient être clos à la clôture de l'enquête pour être éventuellement repris sur autorisation d'un juge d'instruction dans le cadre de la poursuite des investigations sur commission rogatoire.

- En matière terroriste (depuis la loi du 3 juin 2016 et son article 706-24-2 du CPP), ces dispositifs peuvent être maintenus pendant un délai de quarante-huit heures après changement du cadre d'enquête , la géolocalisation avait été omise par la loi précédente

Dispositif national d'assistance aux victimes d'actes de cybermalveillance



Issu de la stratégie nationale pour la sécurité du numérique

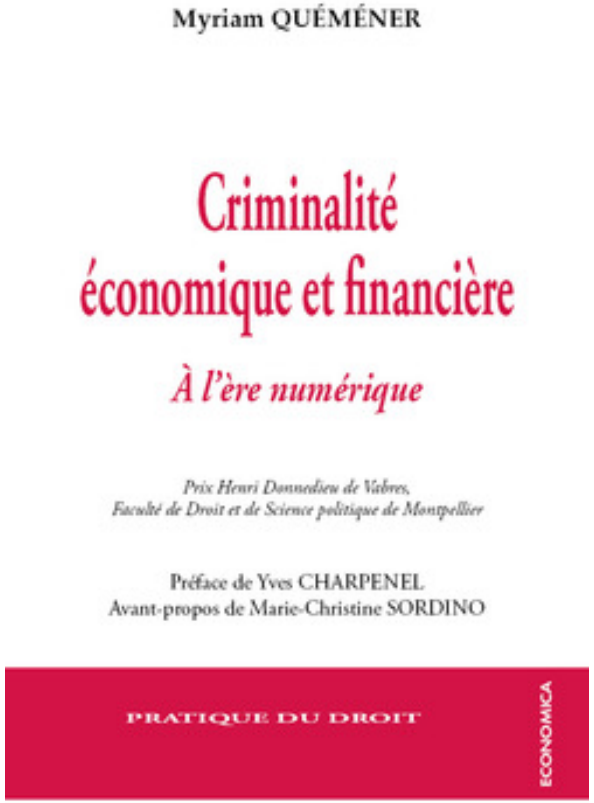
Quelques jurisprudences

- Dans un arrêt du 25 octobre 2017, la Chambre commerciale de la Cour de Cassation invoque la nécessaire recherche de la négligence du consommateur pour trancher les contestations de remboursement en cas de phishing. Le simple fait pour la juridiction de proximité de ne pas avoir recherché si la personne victime d'un phishing aurait pu avoir conscience que le courriel qu'elle avait reçu était frauduleux contrevient en effet aux dispositions de l'article L.133-16 du Code Monétaire et Financier.
- Les banques sont satisfaites de cette décision importante qui permet aux banques de durcir leur politique en matière de remboursement des cas de fraudes.
- Cette contre-attaque du domaine bancaire mérite quelques approfondissements.
- En l'espèce, un consommateur titulaire d'un compte auprès d'une grande banque française s'est estimé victime d'une fraude et a sollicité le remboursement de plusieurs achats qu'il n'avait pas réalisés.
- Par une méthode dite de phishing, des fraudeurs se faisant passer pour un opérateur de téléphonie et d'internet ont adressé au consommateur un courriel l'invitant à communiquer son nom, son numéro de carte bancaire, la date d'expiration de celle-ci et le cryptogramme figurant au verso.

Caractérisation d'une atteinte à un STAD par utilisation d'un keylogger

- Par un arrêt du **16 janvier 2018**, la Cour de cassation a confirmé la condamnation prononcée par la Cour d'appel d'Aix-en-Provence à l'encontre d'un individu sur le fondement notamment de l'article 323-1 du Code pénal, qui incrimine l'introduction et le maintien frauduleux dans un système de traitement automatisé de données (STAD).
- La Cour a considéré que les juges du fond avaient bien caractérisé le délit en relevant que "*la détention d'un keylogger, sans motif légitime par* [le prévenu]*, que celui-ci ne contest*[ait] *pas avoir installé (…) pour intercepter (…) par l'espionnage de la frappe du clavier les codes d'accès et accéder aux courriels échangés (…) caractéris*[ai]*ent suffisamment sa mauvaise foi et le*[s] *délit*[s] *tant dans* [son] *élément matériel qu'intentionnel*".

- Merci de votre attention
- Des questions?



La Gendarmerie, la RC et AD Honores

FRC 2018 : REMERCIEMENTS

L'équipe d'organisation

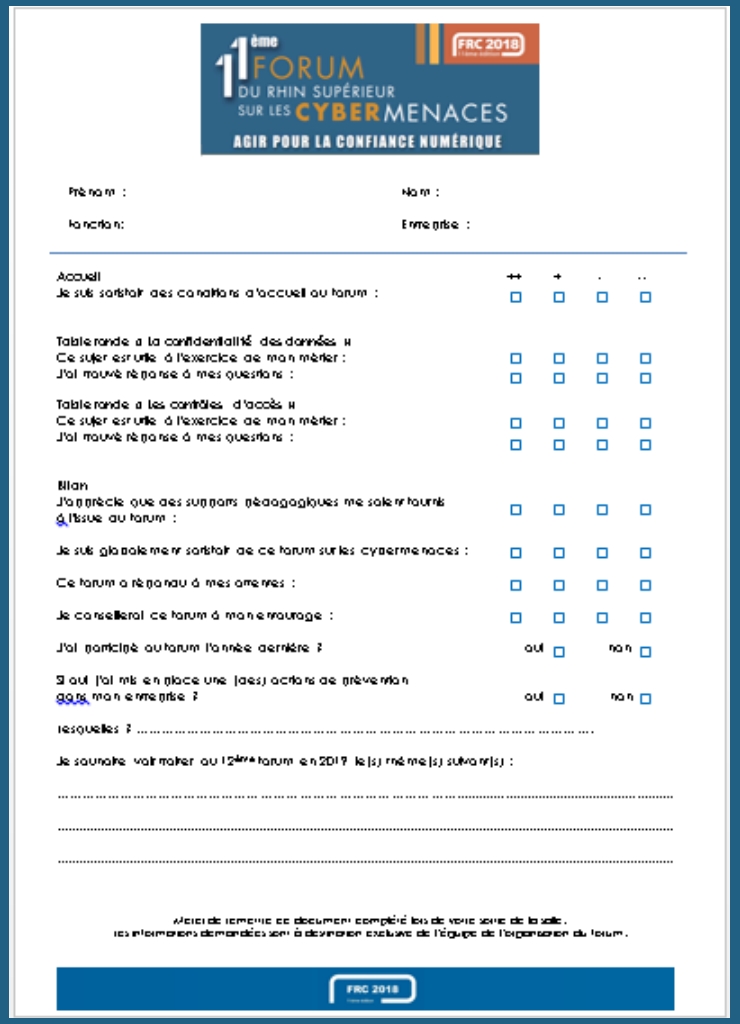
Daniel GUINIER
Emmanuelle HAASER
Ludovic HAYE
Isabelle HUCK
Cl. Didier LIMET
Adj. Pierre MEYER
Johan MOREAU
Camille MUNGRA
Adj. Barbara PAJNO
LCL. Jean-Michel ROBINET
Didier SCHERRER
Manuel SPRAUL
Véronique WADEL
Jonathan WEBER

FRC 2018 : REMERCIEMENTS

Dessinateur
M. Laurent SALLES

Equipe technique de l'ENA

FRC 2018 : FICHE D'ÉVALUATION



11ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

AGIR POUR LA CONFIANCE NUMÉRIQUE

FRC 2018

Prénom :

Nom :

Fonction :

Entreprise :

	++	+	-	--
Accueil				
Je suis satisfait des conditions d'accueil au forum :	☐	☐	☐	☐
Table ronde « La confidentialité des données »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « Les contrôles d'accès »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Bilan				
J'apprécie que des supports pédagogiques me soient fournis à l'issue du forum :	☐	☐	☐	☐
Je suis globalement satisfait de ce forum sur les cybermenaces :	☐	☐	☐	☐
Ce forum a répondu à mes attentes :	☐	☐	☐	☐
Je conseillerai ce forum à mon entourage :	☐	☐	☐	☐

J'ai participé au forum l'année dernière ? oui ☐ non ☐

Si oui, j'ai mis en place une (des) actions de prévention dans mon entreprise ? oui ☐ non ☐

Lesquelles ? .....

Je souhaite voir traiter au 12ème forum en 2019 le(s) même(s) sujet(s) :

.....

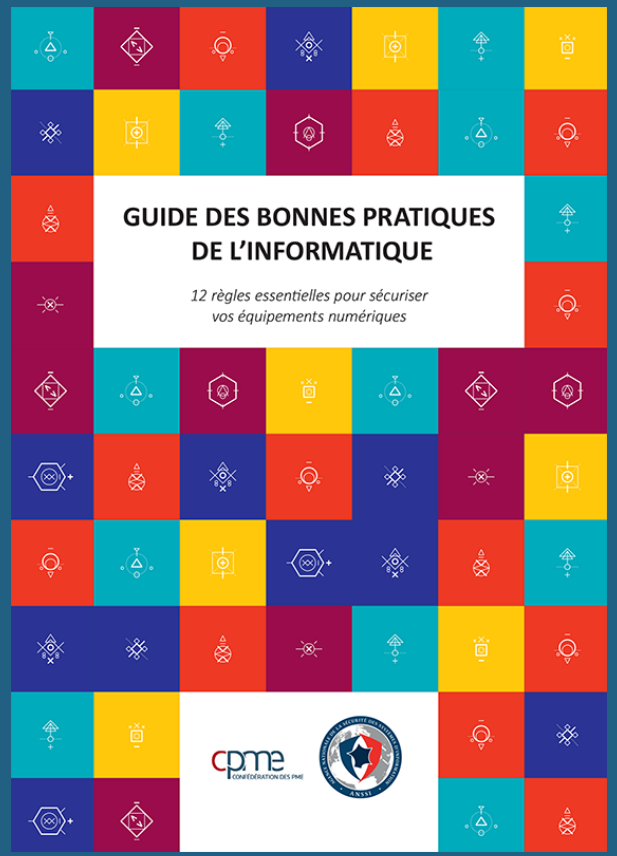
.....

.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.

FRC 2018

FRC 2018 : DOCUMENTS À VOTRE DISPOSITON



FRC

Notre site : www.frc.alsace

Notre Twitter : @cybermenaces

NOS PROCHAINS RENDEZ-VOUS

Forum International de la Cybersecurité

SECURITY AND PRIVACY BY DESIGN

Europe kicks off !

FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ
| 22 ET 23 JANVIER 2019 | LILLE GRAND PALAIS

NOS PROCHAINS RENDEZ-VOUS

FER 2019

Forum Emploi Reconversion

Le 21 mars 2019

NOS PROCHAINS RENDEZ-VOUS

Au printemps 2019

NOS PROCHAINS RENDEZ-VOUS

Le 5 novembre 2019