Researches on Computer Security in France
A never complete summary
2003–2007

Claude Kirchner

INRIA
Bordeaux—Nancy

December 2007

Computer security

Security and trust are pervasive and durable problematics

They set often difficult scientific and technological questions, for instance in informatics, mathematics, control, electronics, physics, law, geo-strategy, ...

Computer security is a fundamental topics

- National sovereignty
- Individual liberties and democracy
- Economy
- Health

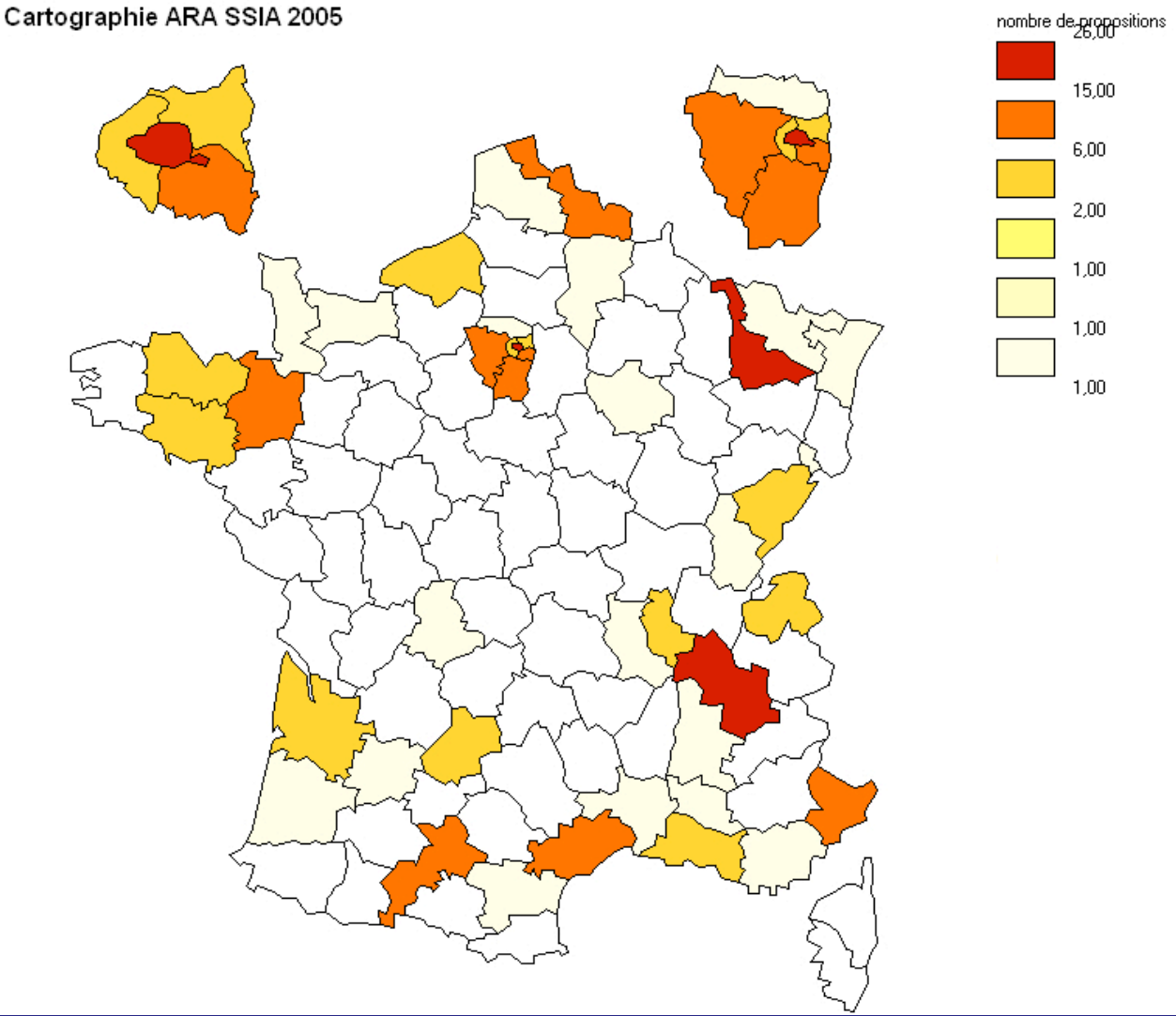
A somehow abstract and hidden topics that is often "invisible"

- how to test, decide, assert, prove security ?

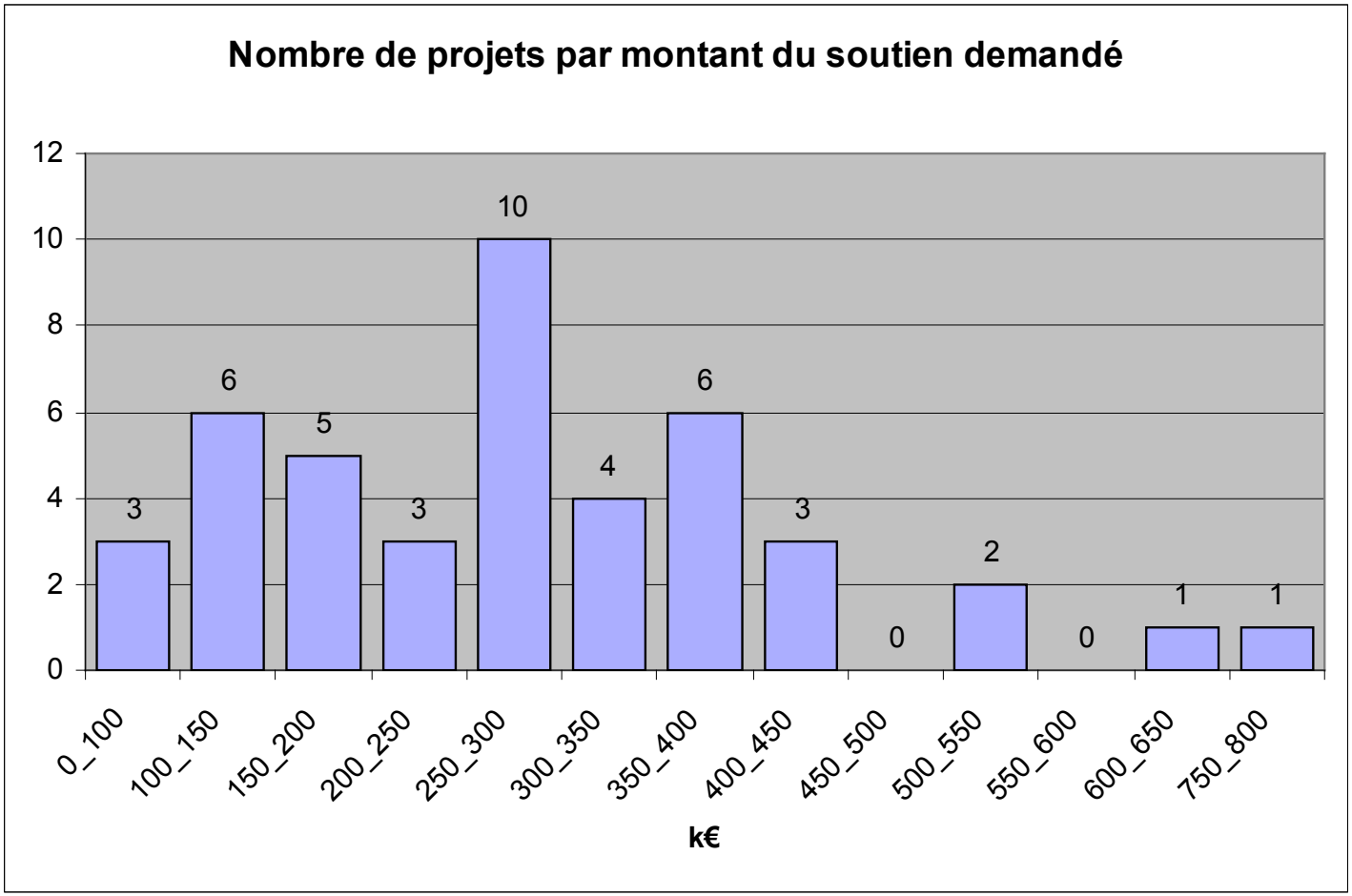
Summary of the computer security programs : 2003–07

	2003 ACI	2004 ACI	2005 SSIA	2006 SETIN	2007 SESUR
# proposals	64	41	44	39	40
# teams involved in a proposal	129	112	172	142	149
# people involved in a proposal	794	429	569	479	615
by proposal	12.8	13.2	12	12	15.4
# accepted proposals	28	19	20	18	13
# teams involved in accep. prop.	75	58	50	64	50
# people involved in accep. prop.	326	256	244	235	181
by proposal	11,6	13,4	12,2	13	13.9
Total funding (Meuros)	5.121	4.5	4.8	6.47	6.95 *
additional PhD fundings (#)	9	7			

Geography of proposals



Typical fundings



Themes of accepted proposals

- Secured data bases
  CASC (03)
- Biométrie
  BIO_MUL (03)
  FAR3D (07) Face Analysis and Recognition using 3D
  ASFIP (07) Attack Standardization for FIngerPrint system certification

Formal system development

Corss (03) Desirs (03) Dispo (03) Geccoo (03) Modulogic (03)
alidecs (04) fiacre (04)

AdvanceCheck (05)	Model checking infini
ARROWS (05)	Structures de données avec pointeurs
CompCert (05)	Certification de compilateur
MoDyFiable (05)	Modularité Dynamique Fiable
Safecode (05)	Composants sûrs de fonctionnement
Averiss (06)	Vérification automatisée de systèmes logiciels
Check-Bound (06)	Model Checking Stochastique
DOTS (06)	Systèmes distribués, ouverts et temporisés
TACOS (06)	Assemblage de composants digne de confiance

Cryptography

CESAM (03) ; CHRONOS (03) ; OCAM (03) ; ROSSIGNOL (03) ; UNIHAVEGE (03) acsion (04)
formacrypt (05) CrySCoE (05) Nuget (05)

EDHASH (06) Evaluation et conception de fonctions de hachage cryptographiques
MAC (06) Methodes Algebriques pour la Cryptographie
RAPIDE (06) Conception et analyse de chiffrements à flot efficaces pour les environnements contraints

SCALP (07) Security of Cryptographic Algorithms with Probabilities
SEQURE (07) Symmetric Encryption with QUantum key REnewal
PAMPA (07) Password Authentication and Methods for Privacy and Anonymity

- Fiabilité des systèmes répartis
  Fragile (04) Mosaic (04)
  Safe_necs (05) Conception coordonnée des systèmes tolérants
- Intrusion
  Cadho (04) Daddi (04)
  PLACID (06) Modèles graphiques probabilistes et logiques de descriptions pour la corrélation d'alertes en détection d'intrusions

- Informatique pour la sûreté et la sécurité
  Constructif (03) ; Edemoi (03)
  Behavior (04)
- Matériel et sécurité
  Mars (04) Venus (04)
  RFIDAP (07) RFID Authentication and Privacy
  FME3 (07) Enhancing the Evaluation of Error consequences using Formal Methods

- Watermarking
  Tadorne (04)
  Tsar (05) Transfert sécurisé d'images d'art haute résolution
- Mobile objects
  CRISS (03) SPOPS (03)
  Kaa (04)
- Security policies
  Potestat (04)
  Cops (05) Composition de politiques et de services
  Polux (06) Expression pour l'unification des politiques de sécurité
  FLUOR (07) Convergence du contrôle de FLux et d'Usage dans les Organisations

- Proof, verification
  Cortos (03) ; Dynamo (03) ; Persee (03) ; Sure Paths (03) ;
  Vera (03) ; Versydis (03) ; V3F (03)
  Apron (04) Satin (04)
  Controvert (05) Vérification de systèmes de contrôle

  RAVAJ (06) Réécriture et Approximation pour la Vérification d'Applications Java
  RIMEL (06) Raffinement Incrémental de Modèles événementiels
  SSURF (06) Sureté et Sécurité avec Focal

  CAVERN (07) Constraints and Abstractions for program VERificatioN
  VERAP (07) Vérification Approchée Probabiliste

- Networks
  PRESTO (03) Réseaux Quantiques (03) SPLASH (03)
  TRANSCHAOS (03)
  Metrosec (04) Serac (04) sr2i (04)
  Cladis (05) Conception multicouches pour réseaux ad-hoc
  Sarah (05) Services distribués pour réseaux ad hoc

  SFINCS (07) Securing Flow of INformation for Computing pervasive Systems

- Security and law
  Fabriano (03)
  Asphales (04)
  Nebbiano (06) Sécurité et fiabilité des techniques de tatouages

  LISE (07) Liability Issues in Software Engineering

- Systèmes embarqués
  Amaes (05) Méthodes Avancées pour les Systèmes Autonomes et Embarqués

  Reve (05) Réutilisation sûre de composants embarqués

  FoToVP (06) Outils formels pour le prototypage virtuel des systèmes embarqués
  VAL-AMS (06) Validation avec haute fiabilité pour les circuits analogiques et mixtes

- Grille et sécurité
  BGPR (05) Calcul ambient sûr
  PARSEC (06) Parallélisme et sécurité
- SOC
  OverSoc (05) Reconfigurable systems on chip
  Safe (05) Fpga sécurisé asynchrone pour les systèmes embarqués
- Intelligence ambiante
  SOGEA (05) Sécurité des jeux. Equilibres et Algo répartis

- Virus
  Virus (05) Théorie des virus
- Multiagents
  FACOMA (06) Fiabilisation d'Applications COopératives
  Multi-Agents
- Confidence
  ForTrust (06) Analyse et formalisation de la confiance sociale
  AVOTE (07) Analyse formelle de protocoles de vote électronique

Today ?

Strong pushes of many national and international reports (Lasbordes)
e.g.

- DCSSI report
- INRIA Strategic plan

missing program at ANR, but some Challenges may be funded, and other ANR programs will be funding security
Some cooperations with other countries (e.g. Japan)

INRIA is involved in research on many aspects of security

- Strategic plan, one of the main objectives : "guarantee the reliability and security of software intensive systems"
- Today, on the 160 INRIA teams, 25% are concerned by security in the large
- Historically, a strong involvement in :
  - cryptology
  - language design, logic and proofs
  - vision
- Since less than 5 years, strong increasing implication in all the INRIA themes

Examples of topics

Wire and wireless network security, integrity, supervision

Hypercom@Rocq, Madyne@loria, Mascotte@Sophia, Planete@RA

Vision

Orion@Sophia, Ariana@Sophia, Vista@Irisa, Imedia@Rocq, Prima@RA

Cryptology

Tanc@Futur.lix, Code@Rocq, Cacao@Nancy, cascade@Paris.ens

Security evaluation and certification

Cassis@loria, Secsi@Futur.lsv, {Comete Parsifal}@Futur.lix, Lande@Irisa, Vasy@RA

iPPE

Logical@Futur Protheo@Loria Cristal@Rocq

Examples of topics

Smart Card

Lande@Irisa, Everest@Sophia, ProVal@Futur.lsv

Safe operating systems

Sardes@RA, Pops@Futur.lifl

Static analysis

Cristal@Rocq Compose@Bordeaux Lande@Irisa

Bio-identification

Metiss@Irisa

DRM

Texmex@irisa, Temics@irisa

Virus

Code@Rocq.rennes, Calligramme@Loria

Privacy

Planete@RA

Start-ups related to security

- Trusted logic (Security and formal proofs)
- CAPS Entreprise (Static analysis)
- Esterel Technology (Software dependability)
- PolySpace Technologies (Test and Validation)
- Time-AT (Video supervision)
- Blue Eye Video (Video security)
- IRIS (Video supervision)

INRIA–Industry Security day

120 industrial people, large success
First hit **google{inria securite}**

Which futur ?

We are in an international situation where mastering security means mastering information

Nations sovereignty

"Information dominance" has no equivoque :

"The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage".

This *executive order 12333* of December 4, 1981 is not new, what is new indeed is its generalisation to all levels of sovereignty, economy, social life, medias, . . . , and the fact that it concerns nations as well as compagnies, associations and individuals.

Privacy : more that 4,000,000 CCTV cameras in the UK

The exact number of CCTV cameras in the UK is not known but a 2002 working paper by Michael McCahill and Clive Norris of UrbanEye, based on a small sample in Putney High Street, estimated the number of surveillance cameras in private premises in London around 500,000 and the total number of cameras in the UK around 4,200,000.

In 2002, the UK had one camera for every 14 people.

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks
- OS and security, TCG : provable confidence

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks
- OS and security, TCG : provable confidence
- Network management and security : protocols, RFID

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks
- OS and security, TCG : provable confidence
- Network management and security : protocols, RFID
- Crisis management, cert : 24/24, 7/7

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks
- OS and security, TCG : provable confidence
- Network management and security : protocols, RFID
- Crisis management, cert : 24/24, 7/7
- E-vote : shall we allow it ?

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks
- OS and security, TCG : provable confidence
- Network management and security : protocols, RFID
- Crisis management, cert : 24/24, 7/7
- E-vote : shall we allow it ?
- Medical files : multidisciplinary questions and research : from DB to medicine

Some investigated directions

- No security without appropriate laws : see the results of the Asphales project
- Virus : See Eric's talk
- Defense and attack : High level security labs
- Safety and security : buffer overflow
- Smart cards : physical attacks
- OS and security, TCG : provable confidence
- Network management and security : protocols, RFID
- Crisis management, cert : 24/24, 7/7
- E-vote : shall we allow it ?
- Medical files : multidisciplinary questions and research : from DB to medicine
- RFID : Internet of objects

Some exciting research topics

- provable confidence

Some exciting research topics

- provable confidence
- formal security policies

Some exciting research topics

- provable confidence
- formal security policies
- initial versus final semantics

Some exciting research topics

- provable confidence
- formal security policies
- initial versus final semantics
- provable cryptology

Some exciting research topics

- provable confidence
- formal security policies
- initial versus final semantics
- provable cryptology
- towards provable security :

Some exciting research topics

- provable confidence
- formal security policies
- initial versus final semantics
- provable cryptology
- towards provable security :
  - what does it mean ? how to do it ?

Some exciting research topics

- provable confidence
- formal security policies
- initial versus final semantics
- provable cryptology
- towards provable security :
  - what does it mean ? how to do it ?
  - use of statistical methods, towards intelligent learning methods.

Do not forget . . .

- Computer security is *not* apparent, unsecurity is . . . but too late

Do not forget . . .

- Computer security is *not* apparent, unsecurity is . . . but too late
- High-level managers must first be convinced and should act

Do not forget . . .

- Computer security is *not* apparent, unsecurity is . . . but too late
- High-level managers must first be convinced and should act
- Education should be improved

Do not forget . . .

- Computer security is *not* apparent, unsecurity is . . . but too late
- High-level managers must first be convinced and should act
- Education should be improved
- Explore the six dumbest ideas in computer security : `http://www.ranum.com/security/computer_security/editorials/dumb`

Conclusion

Computer security is at the cross of fundamental needs of the societies as well as of the individuals.

It is durable and pervasive : questions and research will not starve tomorrow.

Attackers are intelligents, inventive and have considerable financial, technical and sometime political power with then.

High level theoretical to applied researches are needed to understand and solve the difficult and often interesting questions raised.

Questions ?