French Research in Computer Virology and Operational Cryptology

Eric Filiol
efiliol@esat.terre.defense.gouv.fr

ESAT Rennes - Virology and Cryptology Lab.

Canada - France Meeting on Security
Vancouver - December 6-8th, 2007

Plan

Introduction

- Software protection against malware is less and less efficient (UK DTI report 2004).
- The level of **detected** attacks is still rather low :
  - "Without efforts" attacks.
  - Conceptual weaknesses on the defense side.
- Defense against malware evolves far slower than threats.
- Failure of the software world : security vulnerabilities, strongly limited efficiency of AV...
- What about of (far) sophisticated, targeted attacks ?

Introduction (2)

- The vision of the attacker(s) is never considered from a proactive point of view.
  - Hard to manage legal constraints (France - LCEN 2004).
  - Hard to teach computer virology (Calgary - 2003).
  - Difficulty to publish reproducible results.
- How to defend and protect without the attacker's vision ?
- Malware protection must consider both technological watch and proactive research.

Introduction (3)

Operational cryptology and steganography : the situation is quite the same !

- Applied cryptanalysis.
- Efficient cryptanalysis.
- Legal, police and military aspects *versus* academic/industrial interests.
- How to prove that a cryptosystem is efficiently breakable without releasing any reproducible cryptanalytic clue ?

Strong links between computer virology and operational cryptology/steganography !

Summary of the talk

Plan

Computer virology

- Theoretical and formalisation aspects of computer virology.
  - Exploration of computability and complexity issues of detection.
  - Identification of new viral and antiviral schemes and technologies.
  - Computability theory, complexity theory, formal languages theory, discrete mathematics.
- Experimental validation of theoretical results.

Computer virology (2)

A strong need for experimental and operational validation.

- What are the operational conditions for a theoretical attack to be efficient ?
- Strong need to prove that attacks represent a real risk.
- Programming & reverse engineering techniques, operating system & network science, statistics.
- Simulation capabilities (worm propagation).
- Experiments are done on dedicated confinement networks.

Computer virology (3) : teaching

About 2500 students teached per year.

- Both military (90 %) and civilian (10 %).
- From basic teaching (around 15 hours) to high level expertise degree course (150 hours).
- For the expertise level (5 %) :
  - Operational ability to react, analyze, manage and clean in a context of an undetected, targeted malware attack.
  - Teaching through technical challenges.
- For the graduate level (10 %) : ability to prepare a Ph D or to work as engineer.

Operational cryptology and steganography

Theoretical and practical research in both fields with partial applications in computer virology.

- Cryptanalysis of symmetric systems mostly based on the combinatorial view.
- Steganalysis.
- Applied cryptanalysis.

Our main research goal :

- Zero-knowledge proof of cryptanalysis (E0 - 2007).

Operational cryptology and steganography (2)

About 900 students teached per year.

- Both military (95 %) and civilian (5 %).
- From basic teaching (around 8 hours) to high level expertise degree course (80 hours).
- For the expertise level (3 %) :
  - Operational ability to perform analysis of encrypted data by known cryptanalytic techniques and/or forensics techniques.
  - Teaching through technical challenges.
- For the graduate level (2 %) : ability to prepare a Ph D or to work as engineer.

Computer virology and cryptology

Apply techniques from one field to the other one and conversely.

- Use of viral techniques to break cryptosystem (viral applied cryptanalysis) in an operational context.
- Use of cryptographic techniques in malware algorithmics (obfuscation, poly- & metamorphism, bypassing detection...).
- Use of cryptanalytic techniques to analyse malware codes.

Our "clients"

For academic purposes :

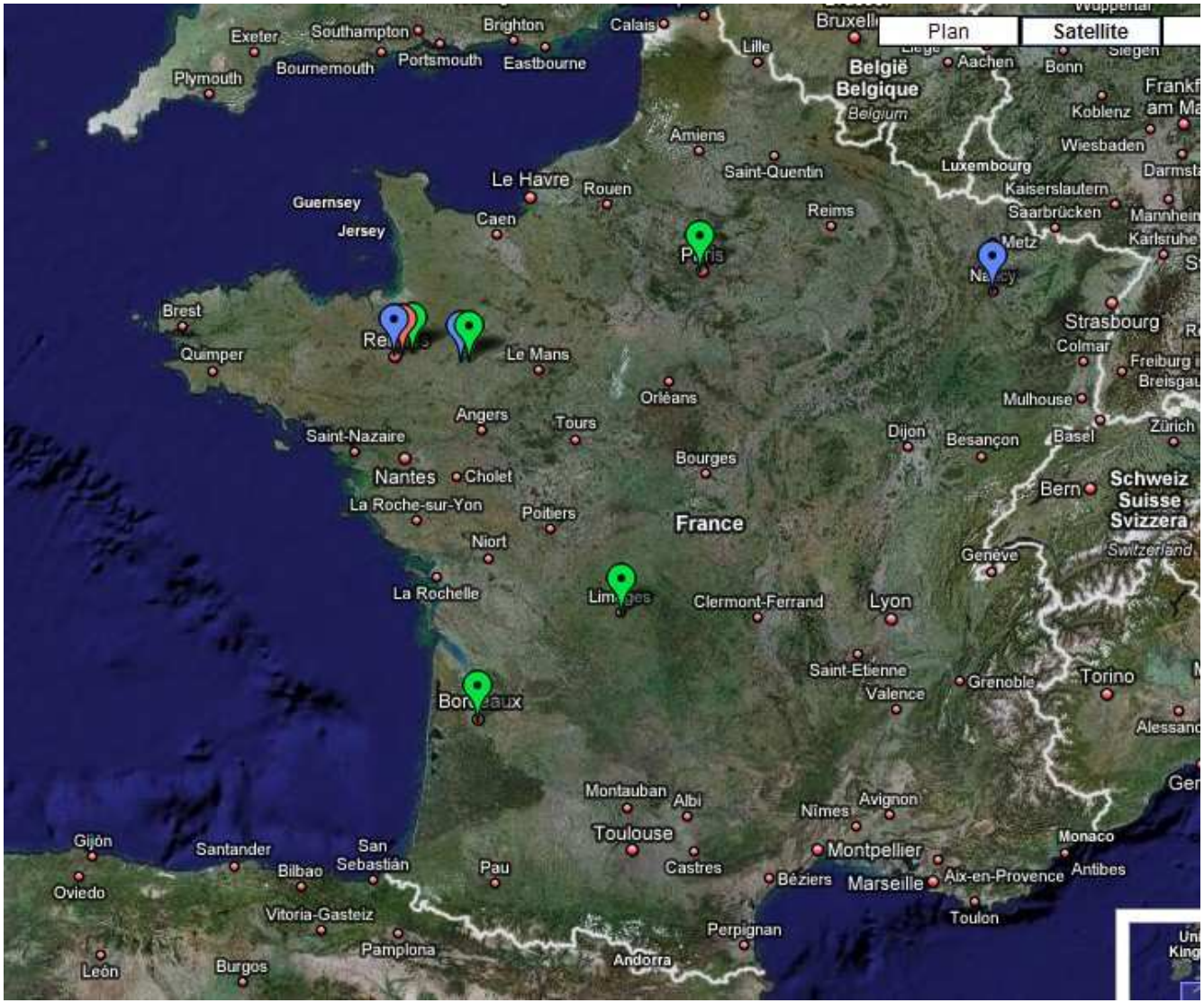
- Universities (graduate level) and engineer schools.
- Dept. of justice.
- Industry.

For consulting and technical expertise :

- Dept. of Defense, Interior and Justice.
- Industry.

Plan

Geographic summary



Research in Computer Virology

Only two research lab in France.

- ESAT/ESIEA in Rennes/Laval (since 2001).
- LORIA/Carte in Nancy (since 2005).

Some other lab have research activities in computer security close to computer virology : Supelec (SSIR) in Rennes.

ESAT/ESIEA zone

Virology and Cryptology lab. located in two areas :

- French Army Signals Academy in Rennes (military part).
- ESIEA in Laval (civilian part).
- Sixteen researchers (12 permanent members/4 Ph D).
- Welcome civilian/foreign researchers/students.

ESAT/ESIEA zone (2)

- High security platforms for malware experimentation.
- Computing center (48-nodes cluster).
- Worm propagation simulation environment.
- Theoretical and operational aspects in computer virology, cryptology and steganography.
- Editorial management of the Journal in Computer Virology.
- Scientific direction of the EICAR conference.
- Is about to become national expertise lab in AV certification.

ESAT/ESIEA zone (3)

- Aside academic research, strong expertise activities for the Dept. of Justice and Interior.
  - Forensics and legal expertise in sensitive cases.
  - Consulting activities.
- Applications of research to :
  - Dept. of Defense (computer warfare analysis expertise).
  - Industry for testing activities.
- These activities enrich both research and teaching activities.

LORIA/Carte Lab

Carte project located in Nancy. Headed by Prof. Marion. Close co-operation with the ESAT zone.

- Six members (3 permanent members/3 Ph D).
- Theoretical research on viral and antiviral models.
- Hosts the TCV Conference since 2006.
- Drives the ARA Virus project in close co-operation with the ESAT zone.

Plan

What we offer

- To welcome Canadian students for Ph D thesis.
  - Profile : pure and applied mathematics with good programming skills.
  - Aim : to open to the north-american zone.
- To welcome Canadian students for graduate courses in computer security.
- Co-operation and exchanges with Canadian labs :
  - Joint research works.
  - Sharing case analysis experience in European malware activity.
  - Developing industrial co-operation in AV technologies.

What we look for

- Sending French or European Ph D students (from a few weeks to one year or more).
  - We cannot welcome all students : we have more demands than positions.
- Initiating research projects.
  - A lot of theoretical/applied research topics have been identified.
  - Impossible for us to cover them all.
- Sharing case analysis experience in north-american malware activity.

Canadian potential partners

Aside France, Canada is the only country having an academic research activity in computer virology.

- University of Calgary (Prof. John Aycock).
- Ecole polytechnique de Montréal (Prof. José Fernandez).
  - Support of an industrial partner (ESET).
  - Informal contacts already exist.

Thanks for your attention