SOS

Software safety and security

Simon Castellan & Thomas Jensen

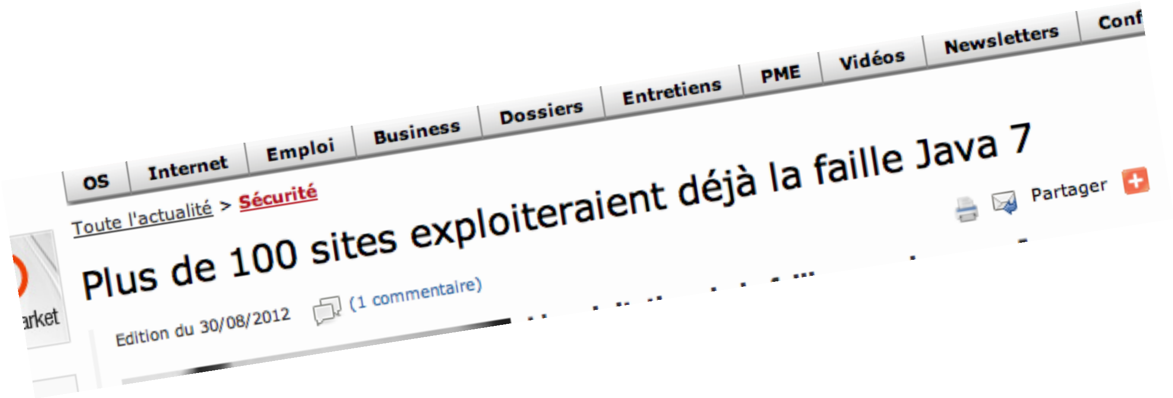
Master 2 "Sciences Informatiques"

Software safety and security

A first distinction:

- **Safety**: a program does not make errors (is functionally correct)
- **Security**: does not leak my secrets

Software safety and security



Toute l'actualité > Sécurité

Plus de 100 sites exploiteraient déjà la faille Java 7

Edition du 30/08/2012 (1 commentaire)

A first distinction:

- **Safety**: a program does not make errors (is functionally correct)
- **Security**: does not leak my secrets

Software security

Software must guarantee the

- **confidentiality**,
- **integrity** and
- **availability**

of critical data.

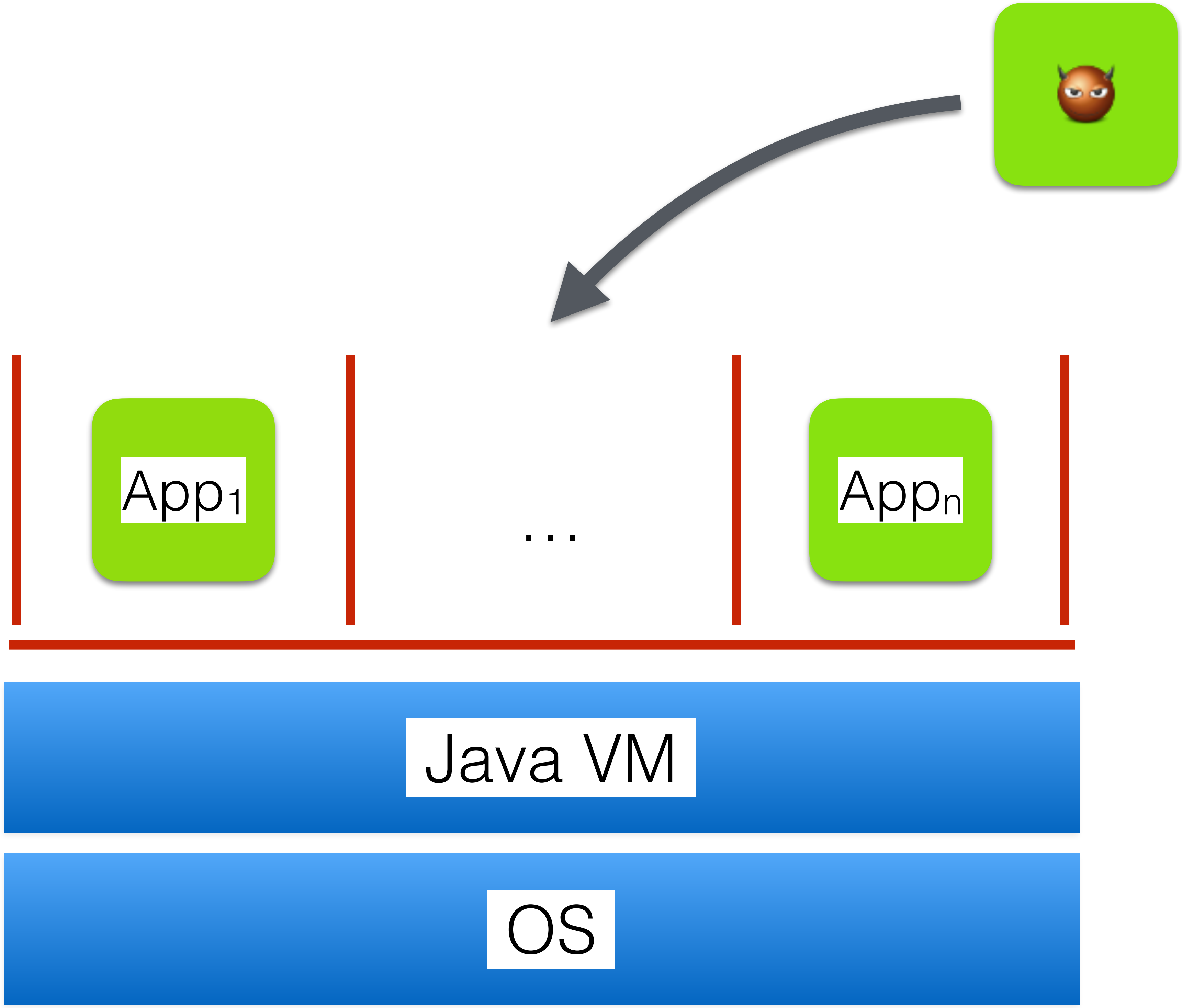
But how?

- use secure programming languages
- follow secure programming guidelines
- static program analysis for spotting vulnerabilities
- monitor executions (dynamic analysis)

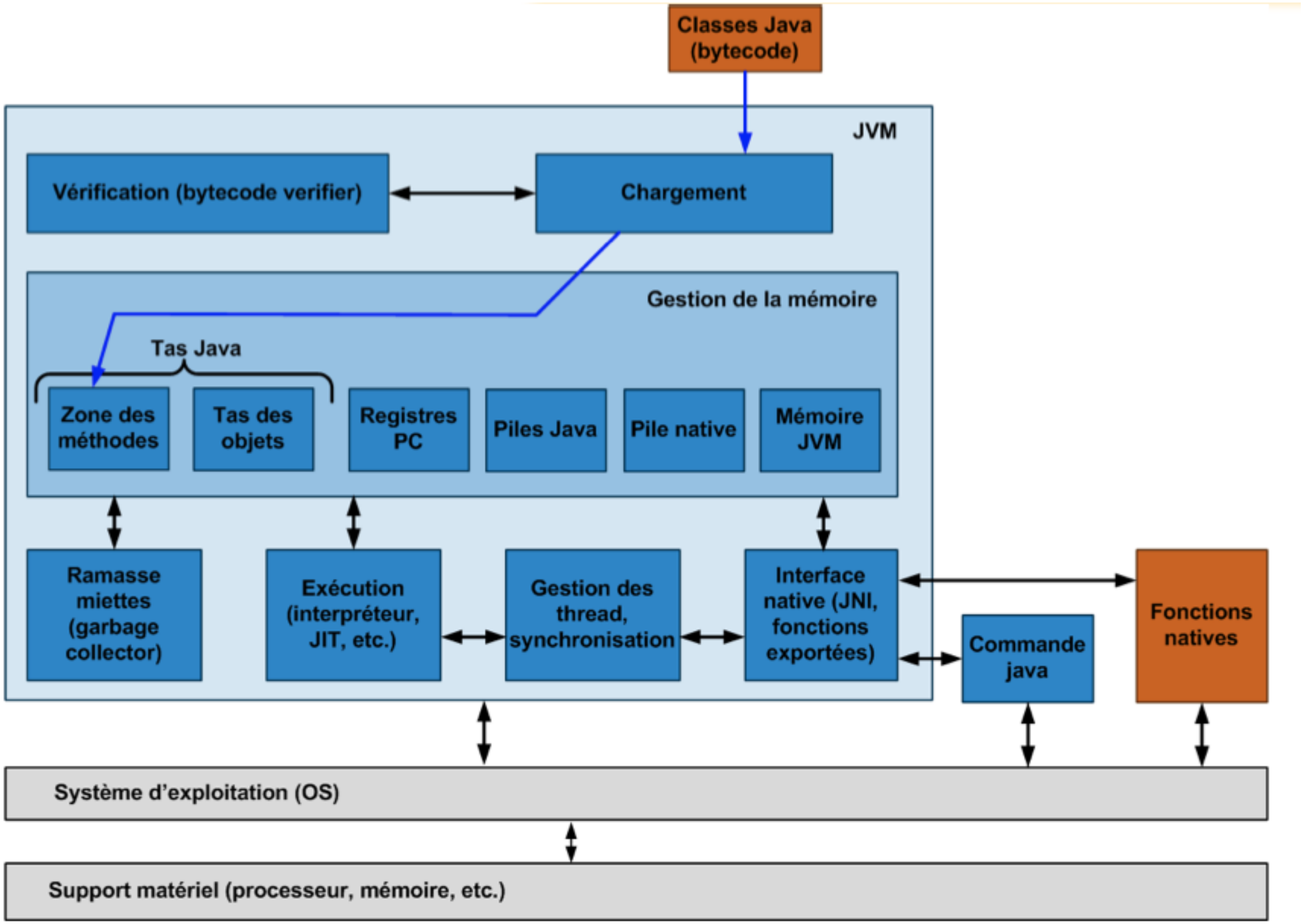
Many aspects of software security

- Viruses, worms, ransomware
- Secure cryptographic protocols
- Operating systems security
    - Isolation of processes, secure crypto,
- Web browser security
- Application security
    - trusting/validating foreign code (eg on an app store)

Ex: The Java virtual machine



The interior of the Java virtual machine


Classes Java (bytecode)
JVM
Vérification (bytecode verifier)
Chargement
Gestion de la mémoire
Tas Java
Zone des méthodes
Tas des objets
Registres PC
Piles Java
Pile native
Mémoire JVM
Ramasse miettes (garbage collector)
Exécution (interpréteur, JIT, etc.)
Gestion des thread, synchronisation
Interface native (JNI, fonctions exportées)
Commande java
Fonctions natives
Système d'exploitation (OS)
Support matériel (processeur, mémoire, etc.)

Program semantics

A formal description of the **meaning** of a program

- avoid ambiguities
- write correct interpreters and compilers
- reason about programs

Comes in different flavours:

- operational
- logic/axiomatic
- denotational/mathematical

Static program analysis

Analyzing the behaviour of a program

- without executing it
- giving correct predictions.

Techniques

- types, program logics,
- data flow analysis.

Information flow analysis

"Is there any point to which you would wish to draw my attention?"

"To the curious incident of the dog in the night-time."

"The dog did nothing in the night-time."

"That was the curious incident," remarked Sherlock Holmes.

A.Conan Doyle: Silver Blaze (1892)

Information flow analysis

"Is there any point to which you would wish to draw my attention?"

"To the curious incident of the dog in the night-time."

"The dog did nothing in the night-time."

"That was the curious incident," remarked Sherlock Holmes.

A.Conan Doyle: Silver Blaze (1892)

Detect different ways of leaking secret information

- x:= my_secret; my_wall := x
- **if** secret = 0 **then** print(0) **else** print (1)
- **if** one_secret = 0 **then**
    another_secret := exp(x,p) mod n;
else skip;

SOS

- Courses on "fundamental techniques"
  - operational semantics,
  - types,
  - data flow analysis.
- Courses of "specialization"
  - static and dynamic information flow control,
  - abstract interpretation,
  - side channels.
- Presentation of research articles.

Organization

- Planning on
  - http://www.irisa.fr/celtique/teaching/SOS/
- Quiz:
  - Tuesday12 October (two hours exercise solving)
- Student presentations of articles:
  - Last week of October.

Planning, lecture notes

Lecture	Date	Topic	Teacher	Handout
1	14/09/2021	Operational semantics (While)	SC	
2	15/09/2021	Operational semantics (References)	SC	
3	21/09/2021	Lambda-calculus and type systems	SC	
4	22/09/2021	Information flow analysis	TJ	
5	28/09/2021	Information flow analysis	TJ	
6	29/09/2021	Dataflow analysis	TJ	
	05/10/2021	Interval analysis and abstract interpretation		
7	06/10/2021	Alias analysis	TJ	
8	12/10/2021	QUIZ	TJ	
9	13/10/2021	Side channel analysis	TJ	
10	19/10/2021	(preparation of presentations)		
11	20/10/2021	(preparation of presentations)		
12	26/10/2021	Student presentations		
13	27/10/2021	Student presentations		
14	02/11/2021	Fall break	SC,TJ	
15	03/11/2021	Fall break	SC,TJ	