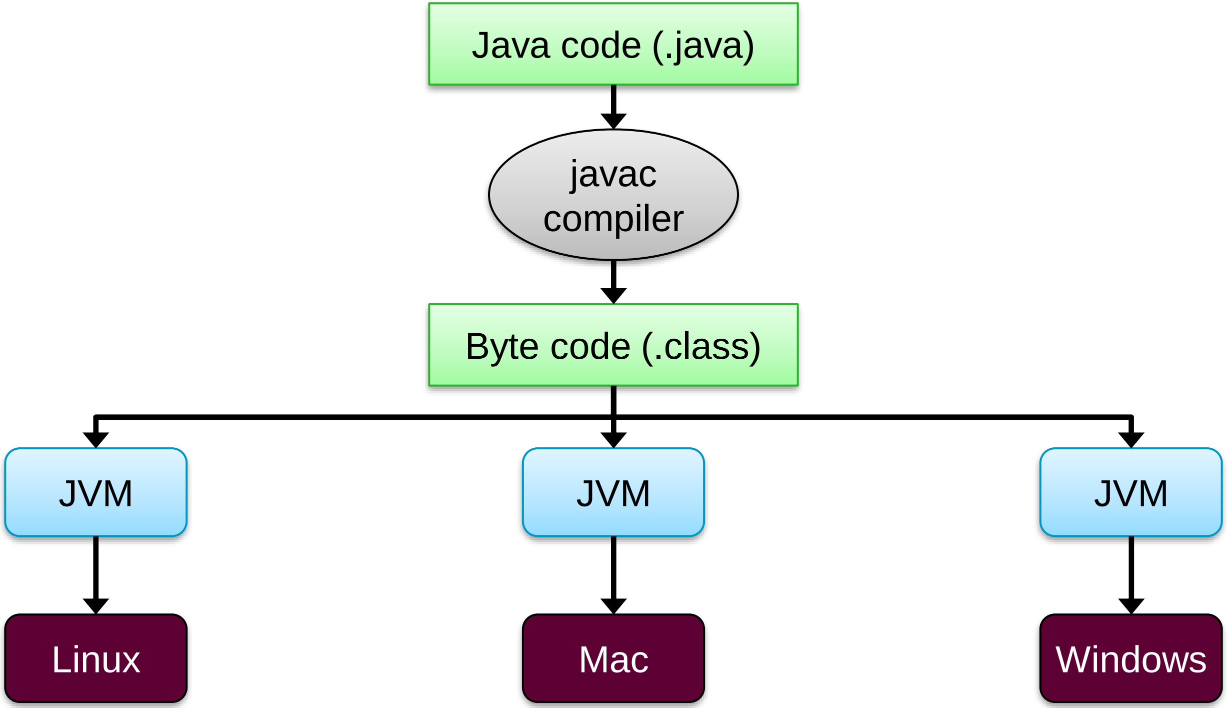
UNIVERSITY OF TWENTE.

Java & security

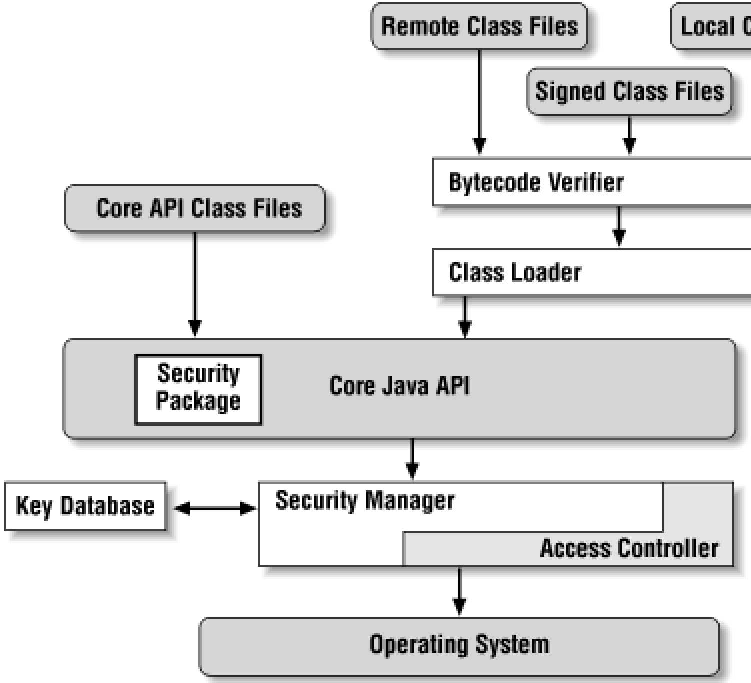
Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

SIMPLIFIED JAVA OVERVIEW



JVM SECURITY OVERVIEW



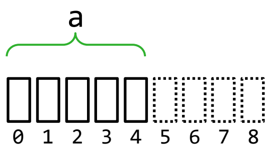
- Manages what resources (network, files, etc.) code can access.
- Allows for the creation of sandboxes.
- Has a bad track-record! (e.g., security of browser applets).

From: http://www.onjava.com/pub/a/onjava/excerpt/java_security_ch1/index.html?page=4

JAVA'S SECURITY ADVANTAGES (COMPARED TO C)

Runtime constraints & bounds checking

```java
int a[] = new int[5];
a[8]= 3;
```

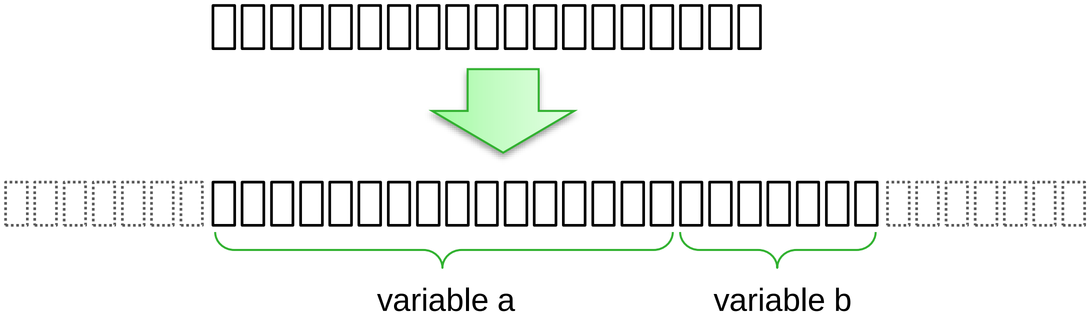


```
Exception in thread "main" java.lang.ArrayIndexOutOfBoundsException: 8
             at module2.security.example.Main.main(Main.java:7)
             …
```

JAVA’S SECURITY ADVANTAGES (COMPARED TO C)

- Less susceptible to buffer overflows

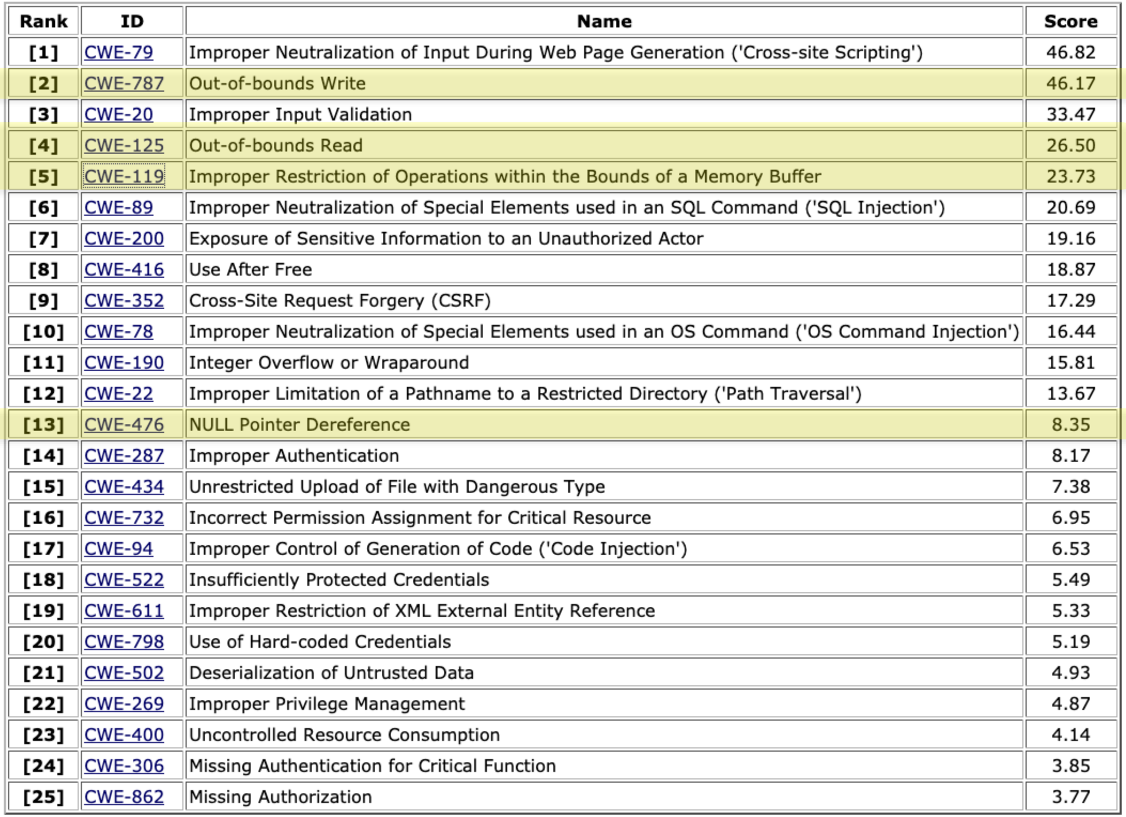
  This could happen in C:



- No pointer arithmetic in Java

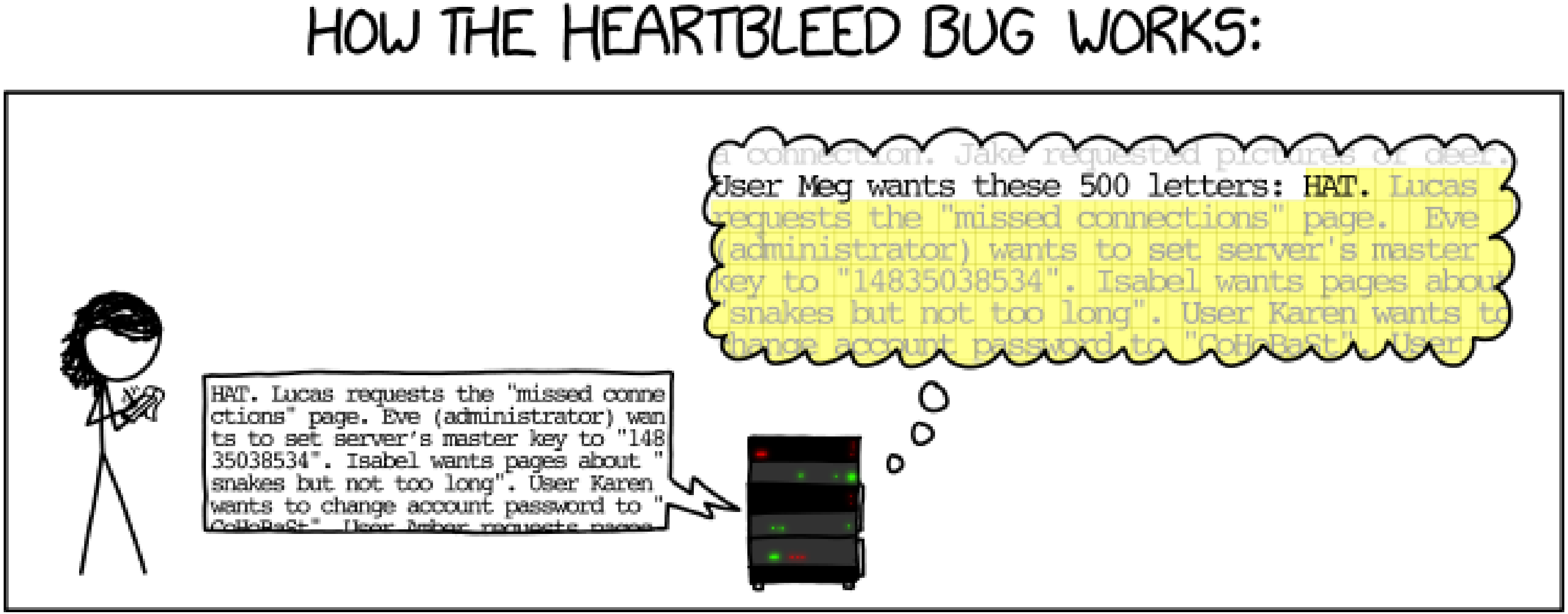
TOP 25 MOST DANGEROUS SOFTWARE WEAKNESSES

http://cwe.mitre.org/top25/



Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
[11]	CWE-190	Integer Overflow or Wraparound	15.81
[12]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67
[13]	CWE-476	NULL Pointer Dereference	8.35
[14]	CWE-287	Improper Authentication	8.17
[15]	CWE-434	Unrestricted Upload of File with Dangerous Type	7.38
[16]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.95
[17]	CWE-94	Improper Control of Generation of Code ('Code Injection')	6.53
[18]	CWE-522	Insufficiently Protected Credentials	5.49
[19]	CWE-611	Improper Restriction of XML External Entity Reference	5.33
[20]	CWE-798	Use of Hard-coded Credentials	5.19
[21]	CWE-502	Deserialization of Untrusted Data	4.93
[22]	CWE-269	Improper Privilege Management	4.87
[23]	CWE-400	Uncontrolled Resource Consumption	4.14
[24]	CWE-306	Missing Authentication for Critical Function	3.85
[25]	CWE-862	Missing Authorization	3.77

EXAMPLE OF ADVANTAGES OF BOUNDS CHECKING


HOW THE HEARTBLEED BUG WORKS:
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed conne ctions" page. Eve (administrator) wan ts to set server's master key to "148 35038534". Isabel wants pages about " snakes but not too long". User Karen wants to change account password to " CoHoBaSt". User Amber requests pages

From: http://xkcd.com/1354/

UNIVERSITY OF TWENTE.

Java & security

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts