Automata and Formal Languages (10)

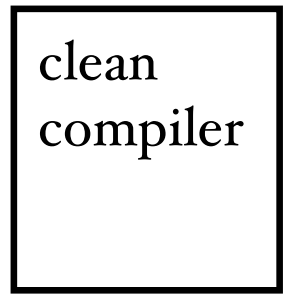
Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)

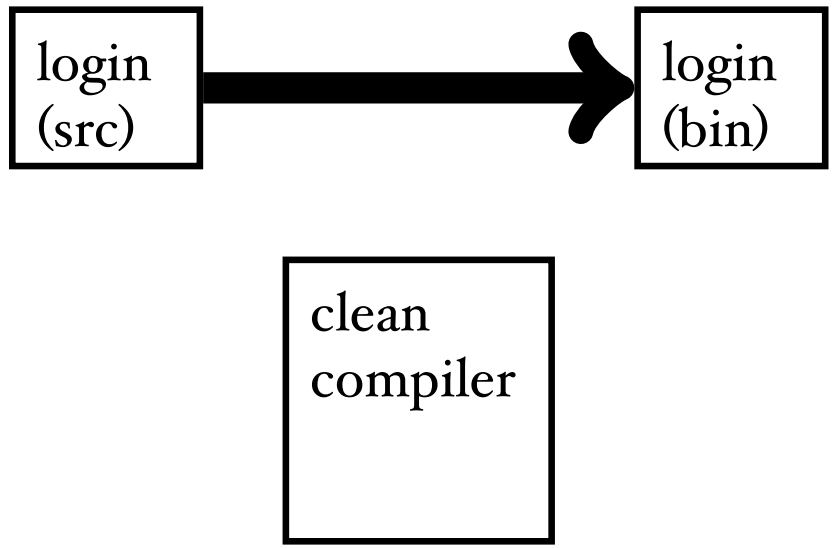
Slides: KEATS (also home work is there)

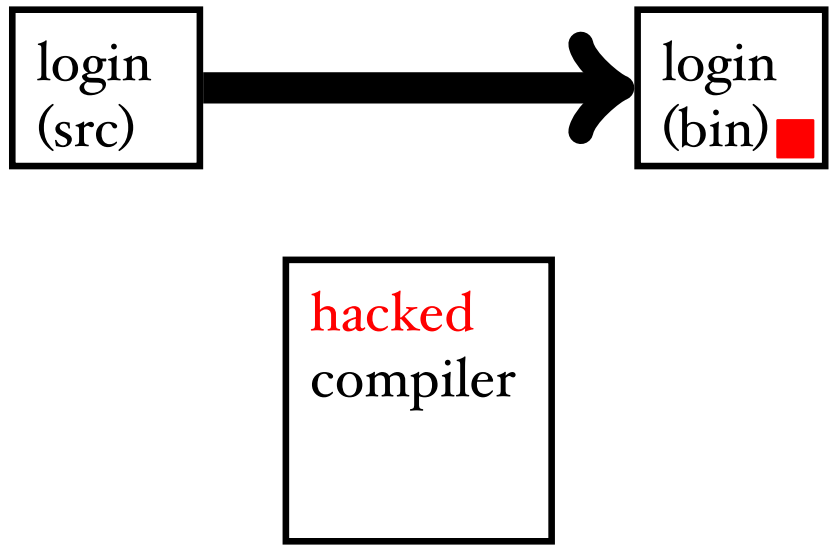
Using a compiler,
how can you mount the
perfect attack against a system?

What is a perfect attack?

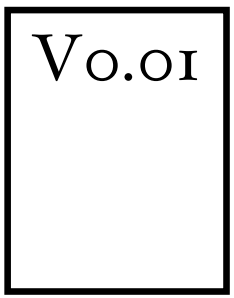
1. you can potentially completely take over a target system
2. your attack is (nearly) undetectable
3. the victim has (almost) no chance to recover


clean
compiler


login
(src)
login
(bin)
clean
compiler


login
(src)
login
(bin)
hacked
compiler

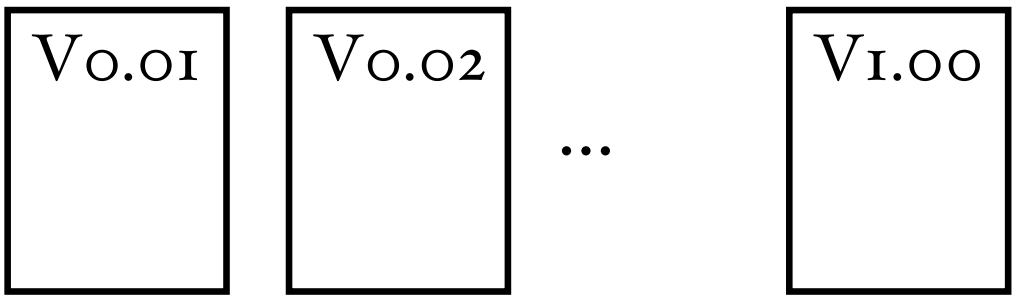
my compiler (src)



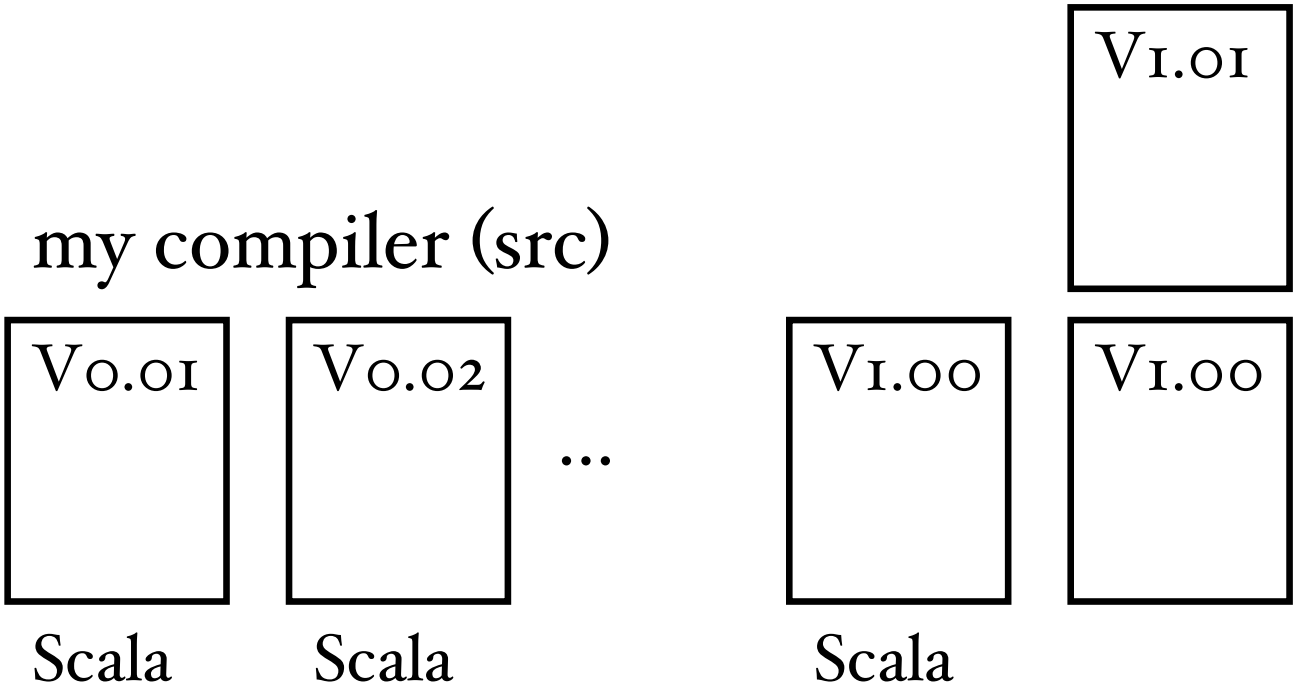
Scala

host language

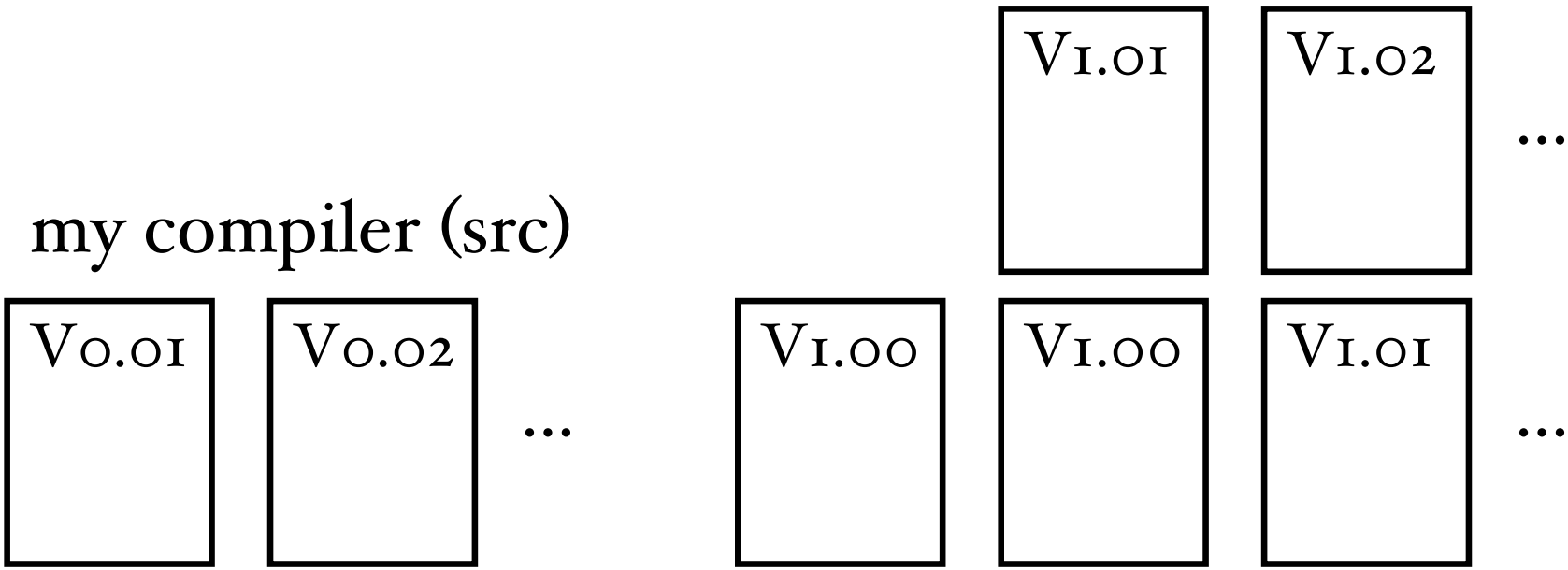
my compiler (src)



host language


V1.01
my compiler (src)
V0.01
V0.02
...
V1.00
V1.00
Scala
Scala
Scala
host language

my compiler (src)



Hacking Compilers

Ken Thompson
Turing Award, 1983

Ken Thompson showed how to hide a Trojan Horse in a compiler without leaving any traces in the source code.

No amount of source level verification will protect you from such Thompson-hacks.

Therefore in safety-critical systems it is important to rely on only a very small TCB.

Hacking Compilers

Ken Thompson
Turing Award, 198

1) *Assume you ship the compiler as binary and also with sources.*
2) *Make the compiler aware when it compiles itself.*
3) *Add the Trojan horse.*
4) *Compile.*
5) *Delete Trojan horse from the sources of the compiler.*
6) *Go on holiday for the rest of your life. ;o)*

Hacking Compilers

Ken Thompson
Turing Award, 1983

Ken Thompson showed how to hide a Trojan Horse in a compiler without leaving any traces in the source code.

No amount of source level verification will protect you from such Thompson-hacks.

Therefore in safety-critical systems it is important to rely on only a very small TCB.