Automata and Formal Languages (9)

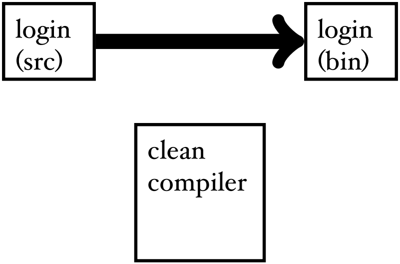
Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS (also home work is there)

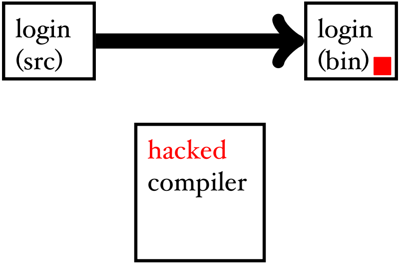
**Using a compiler,
how can you mount the
perfect attack against a system?**

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

$\boxed{\text{clean compiler}}$


login
(src)
login
(bin)
clean
compiler


login
(src)
login
(bin)
hacked
compiler

my compiler (src)

V0.01

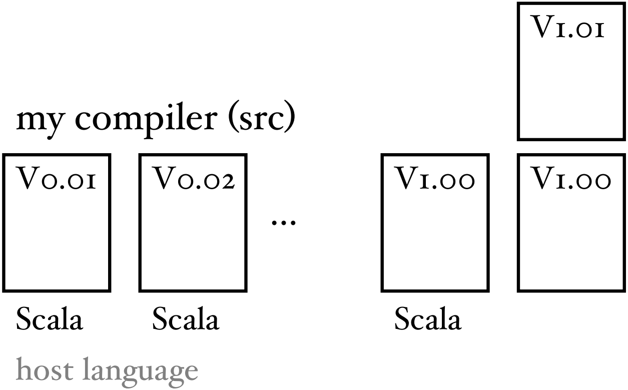
Scala

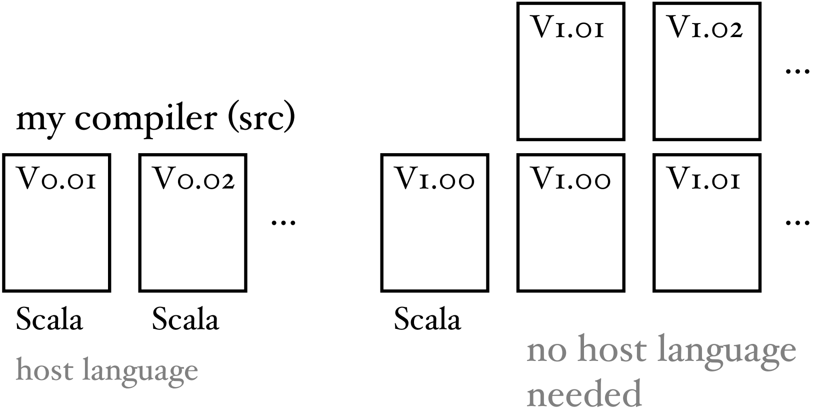
host language

my compiler (src)

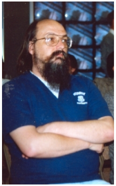
V0.01	V0.02	...	V1.00
Scala	Scala		Scala

host language


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


my compiler (src)
V0.01
V0.02
...
V1.00
V1.00
V1.01
...
V1.01
V1.02
...
Scala
Scala
host language
Scala
no host language needed

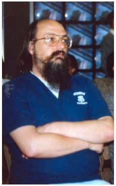
Hacking Compilers



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.

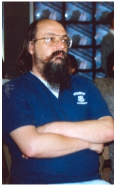
Hacking Compilers



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)*

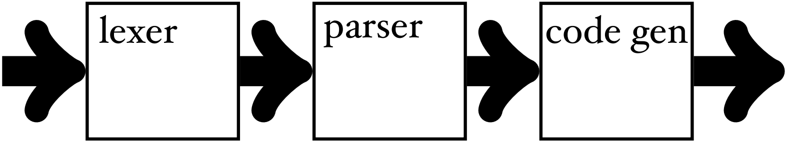
Hacking Compilers



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.

Our Compiler



lexer input: string

lexer output: sequence of tokens
(white space and comments filtered out)

parser output: abstract syntax tree

code gen output: assembler byte code /
assembler machine code

For-Loops

$\texttt{for}\ \mathit{Id}\ \texttt{:=}\ \mathit{AExp}\ \texttt{upto}\ \mathit{AExp}\ \texttt{do}\ \mathit{Block}$

```
for i := 2 upto 4 do {
  write i
}
```

While-Language

$$
\begin{array}{lcl}
\mathit{Stmt} & \rightarrow & \text{skip} \\
 & | & \mathit{Id} := \mathit{AExp} \\
 & | & \text{if } \mathit{BExp} \text{ then } \mathit{Block} \text{ else } \mathit{Block} \\
 & | & \text{while } \mathit{BExp} \text{ do } \mathit{Block} \\
 & | & \text{write } \mathit{Id} \\
 & | & \text{read } \mathit{Id} \\
\mathit{Stmts} & \rightarrow & \mathit{Stmt} \;;\; \mathit{Stmts} \\
 & | & \mathit{Stmt} \\
\mathit{Block} & \rightarrow & \{\mathit{Stmts}\} \\
 & | & \mathit{Stmt} \\
\mathit{AExp} & \rightarrow & \ldots \\
\mathit{BExp} & \rightarrow & \ldots
\end{array}
$$

Interpreter

$$
\begin{array}{lcl}
\text{eval}(\boldsymbol{n}, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \boldsymbol{n} \\
\text{eval}(\boldsymbol{x}, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \boldsymbol{E}(\boldsymbol{x}) \quad \text{lookup } \boldsymbol{x} \text{ in } \boldsymbol{E} \\
\text{eval}(\boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \text{eval}(\boldsymbol{a}_1, \boldsymbol{E}) + \text{eval}(\boldsymbol{a}_2, \boldsymbol{E}) \\
\text{eval}(\boldsymbol{a}_1 - \boldsymbol{a}_2, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \text{eval}(\boldsymbol{a}_1, \boldsymbol{E}) - \text{eval}(\boldsymbol{a}_2, \boldsymbol{E}) \\
\text{eval}(\boldsymbol{a}_1 * \boldsymbol{a}_2, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \text{eval}(\boldsymbol{a}_1, \boldsymbol{E}) * \text{eval}(\boldsymbol{a}_2, \boldsymbol{E}) \\
\\
\text{eval}(\boldsymbol{a}_1 = \boldsymbol{a}_2, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \text{eval}(\boldsymbol{a}_1, \boldsymbol{E}) = \text{eval}(\boldsymbol{a}_2, \boldsymbol{E}) \\
\text{eval}(\boldsymbol{a}_1 \mathrel{!=} \boldsymbol{a}_2, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \neg(\text{eval}(\boldsymbol{a}_1, \boldsymbol{E}) = \text{eval}(\boldsymbol{a}_2, \boldsymbol{E})) \\
\text{eval}(\boldsymbol{a}_1 < \boldsymbol{a}_2, \boldsymbol{E}) & \stackrel{\text{def}}{=} & \text{eval}(\boldsymbol{a}_1, \boldsymbol{E}) < \text{eval}(\boldsymbol{a}_2, \boldsymbol{E})
\end{array}
$$

Interpreter (2)

$$
\begin{array}{lcl}
\mathrm{eval}(\mathrm{skip}, \boldsymbol{E}) & \stackrel{\mathrm{def}}{=} & \boldsymbol{E} \\
\mathrm{eval}(\boldsymbol{x} := \boldsymbol{a}, \boldsymbol{E}) & \stackrel{\mathrm{def}}{=} & \boldsymbol{E}(\boldsymbol{x} \mapsto \mathrm{eval}(\boldsymbol{a}, \boldsymbol{E})) \\
\multicolumn{3}{l}{\mathrm{eval}(\mathrm{if}\ \boldsymbol{b}\ \mathrm{then}\ \boldsymbol{cs}_1\ \mathrm{else}\ \boldsymbol{cs}_2, \boldsymbol{E}) \stackrel{\mathrm{def}}{=}} \\
\multicolumn{3}{l}{\qquad\qquad \mathrm{if}\ \mathrm{eval}(\boldsymbol{b}, \boldsymbol{E})\ \mathrm{then}\ \mathrm{eval}(\boldsymbol{cs}_1, \boldsymbol{E})} \\
\multicolumn{3}{l}{\qquad\qquad\qquad\qquad\qquad\quad \mathrm{else}\ \mathrm{eval}(\boldsymbol{cs}_2, \boldsymbol{E})} \\
\multicolumn{3}{l}{\mathrm{eval}(\mathrm{while}\ \boldsymbol{b}\ \mathrm{do}\ \boldsymbol{cs}, \boldsymbol{E}) \stackrel{\mathrm{def}}{=}} \\
\multicolumn{3}{l}{\qquad\qquad \mathrm{if}\ \mathrm{eval}(\boldsymbol{b}, \boldsymbol{E})} \\
\multicolumn{3}{l}{\qquad\qquad \mathrm{then}\ \mathrm{eval}(\mathrm{while}\ \boldsymbol{b}\ \mathrm{do}\ \boldsymbol{cs}, \mathrm{eval}(\boldsymbol{cs}, \boldsymbol{E}))} \\
\multicolumn{3}{l}{\qquad\qquad \mathrm{else}\ \boldsymbol{E}} \\
\mathrm{eval}(\mathrm{write}\ \boldsymbol{x}, \boldsymbol{E}) & \stackrel{\mathrm{def}}{=} & \{\ \mathrm{println}(\boldsymbol{E}(\boldsymbol{x}))\ ;\ \boldsymbol{E}\ \}
\end{array}
$$

Compiling Writes

write x

```
.method public static write(I)V        (library function)
   .limit locals 5
   .limit stack 5
   iload 0
   getstatic java/lang/System/out Ljava/io/PrintStream;
   swap
   invokevirtual java/io/PrintStream/println(I)V
   return
.end method
```

iload $E(x)$
invokestatic write(I)V

```
.class public XXX.XXX
.super java/lang/Object

.method public <init>()V
  aload_0
  invokenonvirtual java/lang/Object/<init>()V
  return
.end method

.method public static main([Ljava/lang/String;)V
  .limit locals 200
  .limit stack 200
```

(here comes the compiled code)

```
  return
.end method
```