Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations
Blackbox Security

Mobile Cryptography

Aspects of Model Program

Representation
Attacks and
Environment

Summary

Different Concepts for Program Obfuscation

Yury Lifshits

Mathematics & Mechanics Faculty Saint Petersburg State University

Spring 2005 - SETLab

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating

Transformations
Blackbox Security

Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

1 Applications

- Classical Cryptography
- Software Protection
- Mobile Agents Technology
- Other

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating

Transformations
Blackbox Security

Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

1 Applications

- Classical Cryptography
- Software Protection
- Mobile Agents Technology
- Other

2 Main Approaches

- Obfuscating Transformations
- Blackbox Security
- Mobile Cryptography

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches

Obfuscating Transformations Blackbox Security

Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

1 Applications

- Classical Cryptography
- Software Protection
- Mobile Agents Technology
- Other

2 Main Approaches

- Obfuscating Transformations
- Blackbox Security
- Mobile Cryptography

3 Aspects of Model

- Program Representation
- Attacks and Environment

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating

Transformations
Blackbox Security

Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

Applications for Obfuscation

Today: only short overview of applications

In details: Lecture 4 - "Applications for Obfuscation"

```
al(*seek\040p
                                  0;*);foreach(1,.3)
          A-99A (I
      {<DATA> ; } my
                                @camellhump:mv#camel:
  my#Canel (while)
                               contable (*%-6
9s*, $ ):myedromedary
                               1=split(//):if(defined(#
                             p=split(//);)while(edromed)
=<para>)) (ecamel1hum
 rv1) (mv#camel1hump=0
                           :mv#CAMEL=3:if(defined(# =shif
       t (edromedary)
                        1)44/\S/) {$camel1hump+=1<<$CAMEL:}
      $CAMEL--: if (d efined ($ =shift (edromedary1)) 44/\s/) (
     #camellhump+=1 <<#cameL:)#cameL--:if(defined(# =shift)
     @camelihump))s4/\S/)(#camelihump+=1<<#CAMEL:)#CAMEL::if(</pre>
     defined(#_sshift(@camellhump))&&/\5/)(#camellhump+=1<<#CAME
    L::)#camel.=(split(//.*\040..m^(/J\047\134)L*7rx*)) [#camel1h
      umpl:)#camel.=*\n*:}@camellhump=split(/\n/.#camel):foreach(@
      camellhump) (chomp; #Camel=#_;y/LJF7\173\175 \047/\061\062\063\
      064\065\066\067\070/:v/12345678/JL7F\175\173\047'/:# =reverse:
      print*# \040#Camel\n*: | foreach (@camel1hump) (chomp:#Camel=# :v
       /LJF7\173\175'\047/12345678/:v/12345678/JL7F\175\173\0 47'/:
        # =reverse:print*\040# #Camel\n*:)*::s/\s*//g::eval:
           (*geek\040DATA.0.0:*):undef#/:# =<DATA>:g/\g*//g:(
            ; A.*_;; map{eval*print\*$_\**;}/.(4)/q;
                  50\145\040\165\163\145\040\157\1 46\040\1 41\0
                    40\143\141 \155\145\1 54\040\1
                                                     51\155\
                    \147\145\0 40\151\156 \040\141
                     157\143\
                                151\141\16 4\151\1
                     \040\167
                               \151\164\1
                                           50\040
                                                         120\1
                     45\162\
                               154\040\15
                     1\040\1
                              64\162\1
                                            41\144
                                                          \145\
                     155\14
                               1\162\
                                                          0\15
                                040\11
                                          7\047\
                                 1\154\1 54\171
                                                          1040
                                   012\101\16
                                                          3\16
                                     7\143\15
                                     4\145\163
                                                          1054
                                    \111\156\14
                                                         3\056
                                  125\163\145\14
                                                         410401
                                51\164\1 50\0
                                                        40\160\
                                                       \155\151
                \163\163
              57\156\056
```

)	r	ıc	:6	P	ot	S	5	C	þ
0	f	u	s	C	a	t	i	o	r

C

Applications

Classical

Cryptography Software Protection

Mobile Agents Technology

Other Main

Approaches Obfuscating

Transformations **Blackbox Security**

Mobile Cryptography

Aspects of Model Program

Representation Attacks and Environment

Summary

Classical Cryptography

What applications in cryptography can we imagine?

Applications

Classical

Cryptography Software Protection Mobile Agents

Technology Other

Main **Approaches**

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

Classical Cryptography

What applications in cryptography can we imagine?

→ Private key cryptosystem → Public key cryptosystem It was mentioned even in famous Diffie-Hellman paper.

Classical Cryptography

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main **Approaches** Obfuscating

Other

Transformations **Blackbox Security** Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

What applications in cryptography can we imagine?

- → Private key cryptosystem → Public key cryptosystem It was mentioned even in famous Diffie-Hellman paper.
- Homomorphic encoding

Main **Approaches** Obfuscating

Other

Transformations **Blackbox Security** Mobile Cryptography

Aspects of Model Program Representation

Attacks and Environment Summary Classical Cryptography

What applications in cryptography can we imagine?

- → Private key cryptosystem → Public key cryptosystem It was mentioned even in famous Diffie-Hellman paper.
- Homomorphic encoding
- Random oracles removing

Software Protection

Yury Lifshits

Applications Classical Cryptography

Software Protection

Mobile Agents
Technology
Other

Main

Approaches

Obfuscating Transformations Blackbox Security Mobile

Cryptography
Aspects of
Model

Program Representation Attacks and Environment

Summary

Situation: we distribute (sell) software products.

Applications Classical Cryptography

Software Protection
Mobile Agents
Technology
Other

Main Approaches

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

Situation: we distribute (sell) software products.

Question: Threats and applications you see?

Competitors threat (reusing your code)

Applications Classical Cryptography

Software Protection Mobile Agents Technology

Main Approaches

Approaches
Obfuscating
Transformations

Blackbox Security
Mobile

Cryptography
Aspects of

Model

Program
Representation
Attacks and
Environment

Summary

Situation: we distribute (sell) software products.

- Competitors threat (reusing your code)
- ⇒ Intelligent tampering (changing parameters)

Software Protection

Yury Lifshits

Applications
Classical
Cryptography

Software Protection Mobile Agents Technology

Main Approache

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile
Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

Situation: we distribute (sell) software products.

- Competitors threat (reusing your code)
- ⇒ Intelligent tampering (changing parameters)
- Threat of functionality changes (protection demo-versions)

Applications Classical Cryptography

Software Protection
Mobile Agents
Technology
Other

Main

Approaches
Obfuscating
Transformations

Blackbox Security
Mobile
Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

Situation: we distribute (sell) software products.

- Competitors threat (reusing your code)
- ⇒ Intelligent tampering (changing parameters)
- Threat of functionality changes (protection demo-versions)
- ⇒ Watermarks protection

Yury Lifshits

Applications Classical

Classical Cryptography Software Protection Mobile Agents Technology

Main Approaches

Approache: Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography Aspects of

Model
Program
Representation
Attacks and

Environment Summary

Mobile Agents Technology

Situation: we distribute programs for our needs.

Applications

Classical Cryptography Software Protection

Mobile Agents Technology Other

Main Approaches

Approaches
Obfuscating
Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

Mobile Agents Technology

Situation: we distribute programs for our needs.

Question: Threats and applications you see?

⇒ Privacy: e.g. internet-distributed computation

Main

Other

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile
Cryptography

Cryptography
Aspects of

Model

Program
Representation
Attacks and
Environment

Summary

Mobile Agents Technology

Situation: we distribute programs for our needs.

- ⇒ Privacy: e.g. internet-distributed computation
- ⇒ Keys protection: buying agents.

Applications Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

Situation: we distribute programs for our needs.

- ⇒ Privacy: e.g. internet-distributed computation
- > Keys protection: buying agents.
- Intelligent tampering

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Other

Approaches
Obfuscating
Transformations
Blackbox Security
Mobile
Cryptography

Aspects of Model Program

Program Representation Attacks and Environment

Summary

Other applications

Question: More applications?

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations

Blackbox Security
Mobile
Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

Other applications

Question: More applications?

Yes!

Applications Classical Cryptography

Cryptography
Software Protection
Mobile Agents
Technology
Other

Main Approaches

Obfuscating Transformations Blackbox Security Mobile Cryptography

Aspects of Model Program

Program Representation Attacks and Environment

Summary

Question: More applications?

Yes!

⇒ Virus development

Applications Classical Cryptography Software Protection Mobile Agents

Technology Other

Approaches
Obfuscating
Transformations

Blackbox Security
Mobile
Cryptography
Aspects of

Question: More applications?

Yes!

- ⇒ Virus development
- ⇒ Watermark attacks

Attacks and Environment Summary

Model Program Representation

An Obfuscator

Yury Lifshits

Applications

Classical Cryptography

Software Protection Mobile Agents

Technology Other

Main

Approaches

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program Representation Attacks and

Environment Summary In details: Lecture 2 - "Obfuscating transformations"



Applications

Classical

Cryptography Software Protection Mobile Agents

Technology Other

Main

Approaches

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Aspects of

Model

Program Representation Attacks and Environment

Summary

In details: Lecture 2 - "Obfuscating transformations"



- Functionality preserving
- Increase of code size, time & space requirements are restricted (usually by constant factor)
- Obfuscated program is not readable (not understandable)

Yury Lifshits

Classification of obfuscating transformations

Applications
Classical
Cryptography
Software Protection
Mobile Agents
Technology

Other Main

Approaches

Obfuscating

Transformations

Blackbox Security Mobile

Cryptography
Aspects of
Model

Program
Representation
Attacks and
Environment

Summary

Yury Lifshits

Classification of obfuscating transformations

Applications Classical Cryptography

Software Protection Mobile Agents Technology Other

Main

Approaches

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

What can we obfuscate in the program?

Layout transformations Change formatting information

Yury Lifshits

Classification of obfuscating transformations

Applications Classical Cryptography Software Protection Mobile Agents Technology

Other

Approaches

Obfuscating

Transformations

Blackbox Security
Mobile
Cryptography

Aspects of Model

Program Representation Attacks and

Environment Summary

- Layout transformations Change formatting information
- Control flow transformations
 Alter control program and computation

Yury Lifshits

Classification of obfuscating transformations

Applications Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches

Obfuscating Transformations

Blackbox Security

Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

- Layout transformations
 Change formatting information
- Control flow transformations Alter control program and computation
- Aggregation transformation
 Refactor program using aggregation methods

Yury Lifshits

Classification of obfuscating transformations

Applications Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches

Obfuscating Transformations

Blackbox Security
Mobile
Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

- Layout transformations
 Change formatting information
- □ Control flow transformations
 □ Alter control program and computation
- Aggregation transformation Refactor program using aggregation methods
- Data transformations Use information encoding

Yury Lifshits

Applications

Classical Cryptography

Software Protection Mobile Agents

Technology
Other

Main

Approaches

Obfuscating

Transformations

Blackbox Security Mobile

Mobile Cryptography

Aspects of Model Program

Representation Attacks and Environment

Summary

Quality of Obfuscation

How good our obfuscation is?

Applications Classical Cryptography

Software Protection Mobile Agents Technology

Main Approaches

Obfuscating

Obfuscating Transformations

Blackbox Security
Mobile
Cryptography

Cryptography
Aspects of

Model Program

Representation Attacks and Environment

Summary

How good our obfuscation is?

Strength can be measured by:

⇒ Potency

$$\frac{E(P')}{E(P)} - 1$$

- Resilience
 Trivial, weak, strong, full, one-way
- Cost Free, cheap, costly, expensive
- Stealthy

Applications

Classical Cryptography

Software Protection Mobile Agents

Mobile Agent Technology Other

Main

Approaches
Obfuscating

Obfuscating Transformations

Blackbox Security

Mobile Cryptography

Aspects of

Model

Program
Representation
Attacks and
Environment

Summary

What do we want to get?



Applications Classical

Cryptography
Software Protection
Mobile Agents
Technology
Other

Main

Approaches
Obfuscating

Transformations

Blackbox Security
Mobile
Cryptography

Aspects of

Model Program Representation

Attacks and Environment

Summary

What do we want to get?

```
mysterious.c

int mysterious(imt x, in

{
   int z;
   z=x+y;
   returnz z;
}
```

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches

Obfuscating Transformations

Blackbox Security

Mobile Cryptography

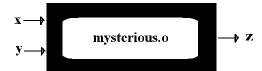
Aspects of

Model Program

Representation Attacks and Environment

Summary

What do we want to get?



Very limited information:

- input-output behavior
- running time

Applications

Classical Cryptography Software Protection

Software Protect
Mobile Agents
Technology
Other

Main Approaches

Obfuscating

Transformations

Blackbox Security

Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

We are interested in 2 types of polynomial-time analyzers:

Ana is a source-code analyzer that can read the program.

BAna is a black-box analyzer that only queries the program as an oracle.

$$BAna^{P}(time(P))$$

Program
Representation
Attacks and
Environment

Summary

We are interested in 2 types of polynomial-time analyzers:

Ana is a source-code analyzer that can read the program.

BAna is a black-box analyzer that only queries the program as an oracle.

$$BAna^{P}(time(P))$$

Black-Box security

Ana can't get more information than BAna could

Yury Lifshits

Applications

Classical

Cryptography Software Protection

Mobile Agents

Technology Other

Main

Approaches

Obfuscating

Transformations

Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

How to formalize property hiding?

Classical Cryptography

Software Protection Mobile Agents Technology

Other

Approaches

Obfuscating Transformations

Blackbox Security
Mobile

Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

How to formalize property hiding?

Instance: two families of programs Π_1 and Π_2

Adversary task: given a program $P \in \Pi_1 \cup \Pi_2$ to decide whether $P \in \Pi_1$ or $P \in \Pi_2$.

Classical Cryptography Software Protection

Mobile Agents Technology

Main

Approaches

Obfuscating Transformations

Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

How to formalize property hiding?

Instance: two families of programs Π_1 and Π_2

Adversary task: given a program $P \in \Pi_1 \cup \Pi_2$ to decide whether $P \in \Pi_1$ or $P \in \Pi_2$.

<u>Desirable protection</u>: make adversary task as difficult as well-known computationally hard problem is.

Classical

Cryptography
Software Protection

Mobile Agents Technology Other

Main

Approaches

Obfuscating Transformations

Blackbox Security

Mobile Cryptography

Aspects of Model Program

Representation Attacks and Environment

Summary

How to formalize constant hiding?

Classical

Cryptography Software Protection Mobile Agents

Technology Other

Main

Approaches Obfuscating

Transformations

Blackbox Security Mobile

Cryptography

Aspects of

Model

Program Representation Attacks and Environment

Summary

How to formalize constant hiding?

Instance: family of programs

$$\Pi = \{P | P \text{ computes } f(s, x); \ s \in S\}$$

Adversary task: given a program $P \in \Pi$ to compute parameter s.

Classical

Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches

Obfuscating Transformations

Blackbox Security

Mobile

Cryptography

Aspects of Model

Program Representation Attacks and

Environment Summary

How to formalize constant hiding?

Instance: family of programs

$$\Pi = \{P | P \text{ computes } f(s, x); \ s \in S\}$$

Adversary task: given a program $P \in \Pi$ to compute parameter s.

Desirable protection: make adversary task as difficult as well-known computationally hard problem is.

Other

Approaches

Obfuscating Transformations

Blackbox Security
Mobile

Cryptography

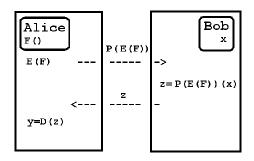
Aspects of Model

Program Representation Attacks and Environment

Summary

More details: Lecture 5 - "Basic Complexity Results"

What is encrypted computation?



Basic task: keep F unknown to Bob.

Main

Approaches Obfuscating

Transformations **Blackbox Security**

Mobile Cryptography

Aspects of Model Program Representation Attacks and

Environment Summary

Extendings of Encrypted Computation

Additional tasks of encrypted computation model:

- Move difficult computations to Bob D is easier than F
- Reduce communication complexity In the case $sizeof((F(x)) \ll sizeof(x)$. Example: x is database
- Keep x secret from Alice

Concepts of Obfuscation

Yury Lifshits

Applications

Classical Cryptography

Software Protection Mobile Agents Technology

Other

Main Approaches

Obfuscating Transformations

Blackbox Security Mobile

Cryptography

Aspects of Model

Program Representation Attacks and

Environment Summary

Currently studied representations

Obfuscating techniques development depends on used program representation

Concepts of Obfuscation

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents

Technology Other

Main Approaches

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Cryptography
Aspects of

Model Program

Representation Attacks and Environment

Summary

Currently studied representations

Obfuscating techniques development depends on used program representation

So what sort of programs are we going to protect?

Turing Machines / Circuits (function computing)

Applications Classical Cryptography Software Protection Mobile Agents

Technology Main

Other

Approaches Obfuscating Transformations

Blackbox Security Mobile

Cryptography Aspects of

Model Program

Representation Attacks and Environment

Summary

Obfuscating techniques development depends on used program representation

- Turing Machines / Circuits (function computing)
- ⇒ C++/Java code.

Currently studied representations

Applications
Classical
Cryptography
Software Protection
Mobile Agents
Technology
Other

Main Approaches

Approaches
Obfuscating
Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program Representation

Attacks and Environment

Summary

Obfuscating techniques development depends on used program representation

- Turing Machines / Circuits (function computing)
- ⇒ C++/Java code
- ⇒ Assembler code

Main

Approaches
Obfuscating
Transformations

Blackbox Security
Mobile
Cryptography

Aspects of

Model Program

Representation Attacks and Environment

Summary

Currently studied representations

Obfuscating techniques development depends on used program representation

- ☐ Turing Machines / Circuits (function computing)
- ⇒ C++/Java code
- ⇒ Assembler code
- Rational function / Matrix representation

Concepts of Obfuscation

Yury Lifshits

Applications

Classical Cryptography Software Protection

Mobile Agents Technology Other

Main

Approaches
Obfuscating

Transformations
Blackbox Security

Mobile Cryptography

Aspects of Model

Program Representation

Attacks and Environment

Summary

Search for other representations

Is it enough?

Concepts of Obfuscation

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main Approache

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model

Program Representation

Attacks and Environment

Summary

Search for other representations

Is it enough?

Classical Cryptography Software Protection Mobile Agents Technology

Main Approache

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography Aspects of

Model

Program Representation

Attacks and Environment

Summary

Search for other representations

Is it enough?

Not! New models should contain:

Current state of the program.

Classical Cryptography

Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating

Transformations
Blackbox Security

Mobile Cryptography Aspects of

Model

Program Representation

Attacks and Environment

Summary

Search for other representations

Is it enough?

- Current state of the program.
- Self-modifiable code

Classical Cryptography Software Protection Mobile Agents Technology Other

Main

Approaches Obfuscating

Transformations **Blackbox Security** Mobile

Cryptography

Aspects of Model

Program Representation Attacks and

Environment Summary

Is it enough?

- Current state of the program.
- Self-modifiable code
- Notion of computation trace.

Approaches

Obfuscating

Transformations **Blackbox Security**

Mobile Cryptography

Aspects of Model

Program

Representation Attacks and Environment

Summary

Search for other representations

Is it enough?

- Current state of the program.
- Self-modifiable code
- Notion of computation trace.
- Other formalizations for functionality preserving.

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches

Obfuscating Transformations

Blackbox Security
Mobile
Cryptography

Aspects of Model Program Representation

Attacks and Environment

Summary

Classical Cryptography Software Protection Mobile Agents Technology

Main Approache

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography Aspects of

Model
Program
Representation
Attacks and

Environment Summary

What should we specify about adversary?

⇒ Adversary knowledge about protected program

Classical Cryptography Software Protection Mobile Agents Technology Other

Main Approaches

Obfuscating Transformations

Blackbox Security
Mobile
Cryptography

Aspects of Model Program Representation

Attacks and Environment

Summary

- ⇒ Adversary knowledge about protected program
 - Member of family

Classical Cryptography Software Protection Mobile Agents Technology

Main

Other

Approaches Obfuscating

Transformations **Blackbox Security**

Mobile Cryptography

Aspects of Model Program

Representation Attacks and Environment

Summary

- Adversary knowledge about protected program
 - Member of family
 - Known function unknown parameters (data) and state.

Applications Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model Program

Representation Attacks and Environment

Summary

- ⇒ Adversary knowledge about protected program
 - Member of family
 - Known function unknown parameters (data) and state.
- ⇒ Adversary task (attack)

Classical Cryptography Software Protection Mobile Agents Technology Other

Main

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model Program

Representation
Attacks and
Environment

Summary

- ⇒ Adversary knowledge about protected program
 - Member of family
 - Known function unknown parameters (data) and state.
- ⇒ Adversary task (attack)
 - Classification follows in Lecture 4.

Potential for Obfuscation

Yury Lifshits

Applications

Classical Cryptography Software Protection

Mobile Agents Technology

Main

Approaches
Obfuscating

Obfuscating Transformations

Blackbox Security
Mobile

Mobile Cryptography Aspects of

Model Program

Representation Attacks and Environment

Summary

Is it possible to protect every program?

Yury Lifshits

Applications Classical

Cryptography
Software Protection
Mobile Agents
Technology
Other

Main

Approaches
Obfuscating

Transformations
Blackbox Security
Mobile

Mobile Cryptography

Aspects of Model Program

Representation
Attacks and
Environment

Summary

Is it possible to protect every program?

- ⇒ How to measure potential of obfuscation?
 - Learnability: black-box learnable functions are impossible to obfuscate.
- What couldn't be protected?
 - Input-Outbut behaviour
 - Traces

Network model

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Other Main

Approaches
Obfuscating
Transformations
Blackbox Security

Mobile Cryptography Aspects of

Model
Program
Representation
Attacks and

Environment Summary What are interesting network extentions of the model?

Network model

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology Other

Main Approaches

Obfuscating Transformations

Blackbox Security Mobile Cryptography

Aspects of Model Program

Representation
Attacks and
Environment

Summary

What are interesting network extentions of the model?

- Many programs cooperate
- Programs are migrating
- Programs can be recharged
- ⇒ Different sources for inputs (outside connections)

Concepts of Obfuscation

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations

Blackbox Security Mobile Cryptography

Aspects of Model Program Representation Attacks and

Summary

Summary

Rough idea of applications: cryptosystem design, mobile agents technology, software protection.

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations

Blackbox Security Mobile Cryptography

Aspects of Model Program Representation

Attacks and Environment

- Rough idea of applications: cryptosystem design, mobile agents technology, software protection.
- Basic approaches: obfuscating transformations, black-box security, encrypted computation.

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

- Rough idea of applications: cryptosystem design, mobile agents technology, software protection.
- ➡ Basic approaches: obfuscating transformations, black-box security, encrypted computation.
- Further aspects of the model: program representation, state protection, adversary description, functionality preserving.

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations

Blackbox Security Mobile Cryptography

Aspects of Model

Program
Representation
Attacks and
Environment

Summary

- Rough idea of applications: cryptosystem design, mobile agents technology, software protection.
- ➡ Basic approaches: obfuscating transformations, black-box security, encrypted computation.
- Further aspects of the model: program representation, state protection, adversary description, functionality preserving.

Yury Lifshits

Applications

Classical Cryptography Software Protection Mobile Agents Technology

Main

Approaches
Obfuscating
Transformations
Blackbox Security

Mobile Cryptography

Aspects of Model

Program Representation Attacks and Environment

Summary

- Rough idea of applications: cryptosystem design, mobile agents technology, software protection.
- ➡ Basic approaches: obfuscating transformations, black-box security, encrypted computation.
- ⇒ Further aspects of the model: program representation, state protection, adversary description, functionality preserving.

Question Time!

Not covered by the talk

Gray & white security Approximate obfuscators Operations on obfuscated code Adversary success Nondeterministic nature Modifying algorithm vs. modifying code Complexity of deobfuscation: NP, NP-hard, undecidable, one-way... Obfuscation on specification level Wroblewsky model

Concepts of Obfuscation

Yury Lifshits

Back Up Slides

Not covered by the talk
References



Yury Lifshits

Program Obfuscation. A Survey [in Russian]

http://logic.pdmi.ras.ru/~yura/of/survey1.pdf



Luis F.G. Sarmenta

Protecting Programs from Hostile Environments

For Further Reading

http://bayanihancomputing.net/papers/ae/ae.ps