New directions in security by obscurity

Dusko Pavlovic

Royal Holloway

September 2011

Outline

Introduction

Background: Security and obscurity

Idea: Attack models

Approach: Directions

Summary

Resource

Introduction

What is a resource?

Complexities as resources

Background: Security and obscurity

Idea: Attack models

Approach: Directions

Summary

Utility

Residue

Outline

Introduction

Background: Security and obscurity

Idea: Attack models

Approach: Directions

Summary
Exploitation is easy

Resources yield one-way functions

Computational resources for security

Regeneration is hard

Resources yield one-way functions

Wanted: "Logical resources for security"
Question

Do logical resources for security exist?

Notation

\[ \text{ATTACK} \]

\[ C \xrightarrow{} P = NP \]

\[ L \xrightarrow{} P \neq NP \]

Idea

Suppose that you are given a system \( C \) such that \( C \xrightarrow{} P = NP \). Would you consider it secure?

Idea

Suppose that you are given a system \( L \) such that \( L \xrightarrow{} P \neq NP \). Would you consider it secure?

Idea

Theorem

System \( L \) is secure enough to protect an account with $1,000,000.

Proof.

Proving \( P \neq NP \) yields $1,000,000 from Clay Institute.
If $P \neq NP$, then this is security by obscurity:

- security of the system $\mathcal{L}$ is based on
- obscurity of the proofs of $P \neq NP$
Security by obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

Summary

Outside cryptography

there are systems with no key

there is not much more to hide except the system

In cryptography

(Gödel, Von Neumann, Kleene)

- keys = data
- system = program

In computation

(Gödel, Von Neumann, Kleene)

- keys = data = program
- system = program = data

Theorem [Barak et al]

Obfuscators do not exist.
In poker

- keys = hands of cards
- system = tactics

In games (Von Neumann-Morgenstern, Harsanyi, Aumann...)

- keys = players' states
  - (im)perfect information
- system = players' types
  - (in)complete information

Kerckhoffs’ Principle
Security is a game of imperfect information.

In security games (Kerckhoffs, Shannon)

- keys ↔ cryptanalysis
  - hard
- system ↔ decompilation
  - easy

Kerckhoffs’ Principle
Security is a game of imperfect information.

Claim
Security is a game of incomplete information
**Claim**

There is security by obscurity even in cryptography

- not through obfuscated code
- but through logically complex algorithms

**Outline**

**Introduction**

Background: Security and obscurity

**Idea: Attack models**

Approach: Directions

**Summary**

**Security as a game**

Shannon's attacker: computationally unbounded
(omnipotent computer)

If a source conveys some information, the attack will extract that information.

**Diffie-Hellman's attacker: computationally bounded**
(real computer)

Public key determines the corresponding private key, but the attacker cannot compute one from the other.

**Adaptive attacker: queries the system**
(still a real computer)

If there is a vulnerability, an attack algorithm will make use of it.
Adaptive attacker: queries the system
(still a real computer)

If there is a vulnerability,
an attack algorithm will make use of it.
But where do the attack algorithms come from?

Kerckhoffs’ attacker: logically unbounded
(omnipotent programmer)

If there is an attack,
the attacker will find it.

Security by obscurity
Dusko Pavlovic
Introduction
Obscurity
Attackers
Directions
Summary

Kerckhoffs’ attacker: logically unbounded
(omnipotent programmer)

If an attack exists,
the attacker will find it.

System

Attacker

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

 Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

 Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.

System algorithm

Attack algorithm

If an attack exists,
the attacker will find it.
Real attacker: logically bounded
(someone’s student)

<table>
<thead>
<tr>
<th>power</th>
<th>unbounded</th>
<th>bounded</th>
</tr>
</thead>
<tbody>
<tr>
<td>computational</td>
<td>Shannon</td>
<td>Diffie-Hellman</td>
</tr>
<tr>
<td>rationality</td>
<td>Cournot</td>
<td>Simon</td>
</tr>
</tbody>
</table>
| logical | Kerckhoffs | ????

Idea

<table>
<thead>
<tr>
<th>computational complexity</th>
<th>secrecy</th>
<th>logical complexity</th>
<th>obscurity</th>
</tr>
</thead>
</table>

Two directions

- hinder adaptation of attack to system
- improve adaptation of system to attack

Two directions

- hinder adaptation of attack to system
  - use algorithmic information theory in security
- improve adaptation of system to attack
  - use epistemic game theory in security

Question

What is logical complexity?

- Which proofs / algorithms are hard to construct?
Question
What is logical complexity?

- Which proofs / algorithms are hard to construct?
- Which attack algorithms are hard to derive from which system algorithms?

Question
Is there "one-way programming"?

\[
\begin{align*}
&\text{attack} \\
&\Rightarrow \\
&\text{Defender} \\
&\Rightarrow \\
&\text{system}
\end{align*}
\]

Predictability and probability

- Predictable events are improbable

"We arrange in our thought all possible events in various classes; and we regard as extraordinary those classes which include a very small number. In the game of heads and tails, if heads comes up a hundred times in a row then this appears to us extraordinary, because the almost infinite number of combinations that can arise in a hundred throws are divided in regular sequences, or those in which we observe a rule that is easy to grasp, and in irregular sequences, that are incomparably more numerous."

Pierre-Simon Laplace

- Probability is not about predictability

"In everyday language we call random those phenomena where we cannot find a regularity allowing us to predict precisely their results. Generally speaking, there is no ground to believe that random phenomena should possess any definite probability. Therefore, we should distinguish between randomness proper (as absence of any regularity) and stochastic randomness (which is the subject of probability theory). There emerges the problem of finding reasons for the applicability of the mathematical theory of probability to the real world."

Andrei N. Kolmogorov
Probability is not about events

- Probability only describes ensembles of events
- Information theory only speaks of global properties.
- "Which local function is entropy the integral of?"
Predictable = programmable

Ray Solomonoff (1960): Science as programming
- \( \Pr(1 \mid 01010101010101010101010101010101) = 0 \)
- \( \Pr(1 \mid 01001100110000111110110000111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101100001111101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
Algorithmic information is a measure of unpredictability.

Is algorithmic information a good concept of logical complexity?

Charles Bennett: Logical depth
- of an organism: the time it takes to evolve
  - virus: computationally simple, logically deep
- of an algorithm: the time complexity of its derivation
  - PRIMES: computationally simple, logically deep
- logical depth measures complexity
  - evolutionary processes
  - as computational processes

**Definition**

Logical complexity of \( a \in \mathbb{N} \) is the time complexity of the simplest program that outputs \( a \)

\[
D(a) = \bigwedge_{\|p\| = a} \|p\| \quad \text{for all } C(p) = a
\]
Logical distance

Definition

Logical distance of \(a, b \in \mathbb{N}\) is the complexity of the simplest program that inputs \(a\) and outputs \(b\)

\[
D(a, b) = \bigwedge_{|p(a)| = |b|} \frac{1}{|p|} |\{p\}|
\]

Idea of logical security

\[\downarrow\]

\[L \ni P \neq NP\]

\[D(L, \neg L) \geq D(L, \neg P \neq NP)\]

Task

Implement this idea.

Approach

Epistemic game theory of security.
Adaptive attacker: queries the system (still a real computer)

If there is a vulnerability, an attack algorithm will make use of it.

Game of attack vectors

Fortification

System must defend all vectors, Attacker just needs one

Game of attack vectors

Honeypot

System passively observes Attacker

Game of attack vectors

Sampling

System actively queries Attacker

Game of attack vectors

Adaptation

Attacker must defend all markers, System just needs one

Game of attack vectors

From fortification to adaptation
Adaptive defender: queries the users
(another computer)

If the attacker queries the system
then the system should query the attacker

It is good to keep the invaders out...

...but it is better to bring them in

One-way-programming: adaptive immune response

Arms race for algorithms

Socratic method: Answer questions by questions
Outline

Introduction
Background: Security and obscurity
Idea: Attack models
Approach: Directions
Summary

Summary

Obstacles

- complexity of strategies with incomplete information
- incompleteness of theories of logical distance

New directions in security by obscurity

- improve adaptation of system to attack
  - use epistemic game theory in security
  - turn compromise into advantage
    - from fortification to adaptation
  - hinder adaptation of attack to system
    - use algorithmic information theory in security
    - leverage emergent behaviors
      - emergency as logical complexity