

New directions in security by obscurity

Dusko Pavlovic

Royal Holloway

October 2011

Security by
obscurity

Dusko Pavlovic

Introduction
Obscurity
Attackers
Directions
Summary



Outline

Introduction

Background: Security and obscurity

Idea: Attack models

Approach: Directions

Summary

Security by
obscurity

Dusko Pavlovic

Introduction
Obscurity
Attackers
Directions
Summary



Outline

Introduction

What is a resource?

Complexities as resources

Background: Security and obscurity

Idea: Attack models

Approach: Directions

Summary

Security by
obscurity

Dusko Pavlovic

Introduction
Resources
Complexities
Obscurity
Attackers
Directions
Summary



Resource



Security by
obscurity

Dusko Pavlovic

Introduction
Resources
Complexities
Obscurity
Attackers
Directions
Summary



Utility



Security by
obscurity

Dusko Pavlovic

Introduction

Resources

Complexities

Obscurity

Attackers

Directions

Summary

Residue



Security by
obscurity

Dusko Pavlovic

Introduction

Resources

Complexities

Obscurity

Attackers

Directions

Summary

Exploitation is easy



Security by
obscurity

Dusko Pavlovic

Introduction

Resources

Complexities

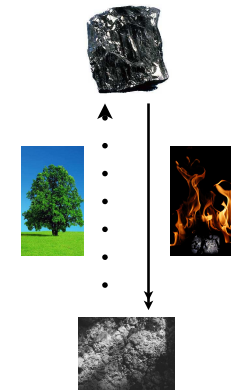
Obscurity

Attackers

Directions

Summary

Regeneration is hard



Security by
obscurity

Dusko Pavlovic

Introduction

Resources

Complexities

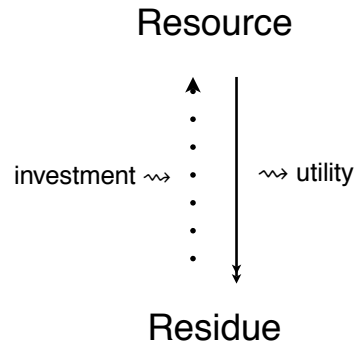
Obscurity

Attackers

Directions

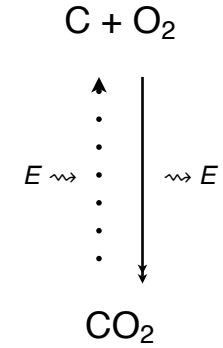
Summary

Resources yield one-way functions



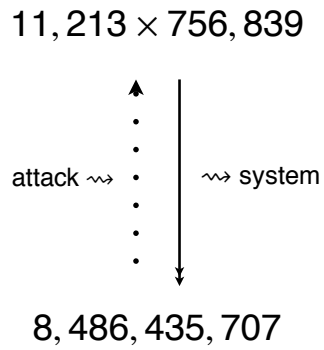
- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources**
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Resources yield one-way functions



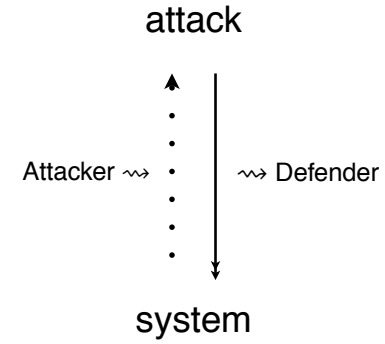
- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources**
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Computational resources for security



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources**
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Wanted: "Logical resources for security"



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources**
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Question

Do logical resources for security exist?

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Notation



ATTACK

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Idea

Suppose that you are given a system C such that



$$\Downarrow$$
$$P = NP$$

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Idea

Suppose that you are given a system C such that



$$\Downarrow$$
$$P = NP$$

Would you consider it secure?

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Resources
- Complexities
- Obscurity
- Attackers
- Directions
- Summary

Idea

Suppose that you are given a system \mathcal{L} such that



\mathcal{L}



$P \neq NP$

Would you consider it secure?



Security by
obscurity

Dusko Pavlovic

Introduction

Resources

Complexities

Obscurity

Attackers

Directions

Summary

Idea

Theorem

System \mathcal{L} is secure enough to protect an account with \$1,000,000

Proof.

Proving $P \neq NP$ yields \$1,000,000 from Clay Institute. \square



Security by
obscurity

Dusko Pavlovic

Introduction

Resources

Complexities

Obscurity

Attackers

Directions

Summary

Alarm

If $P \neq NP$, then this is **security by obscurity**:

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



Outline

Introduction

Background: Security and obscurity

Idea: Attack models

Approach: Directions

Summary



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

Summary

What is security by obscurity?

Kerckhoffs' Principle

"The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

Jean Guillaume Auguste Victor François Hubert Kerckhoffs

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- Summary

What is security by obscurity?

Shannon's Maxim

"The enemy knows the system."

Claude Shannon

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- Summary

Secure key vs obscure system



Lock can only be opened using the correct key

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- Summary

Secure key vs obscure system



... and **not** by breaking the system

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- Summary

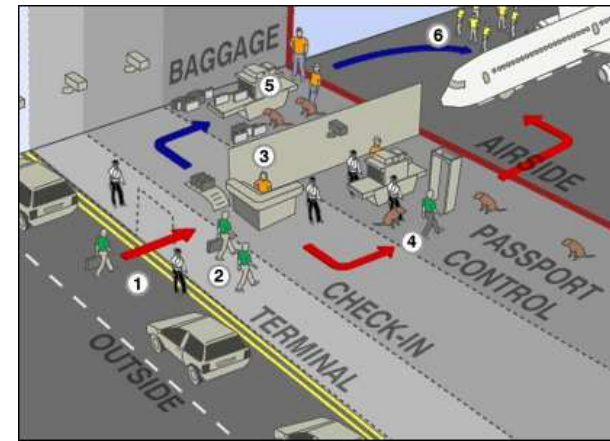
Outside cryptography



there are systems with no key

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity**
- Attackers
- Directions
- Summary

Outside cryptography

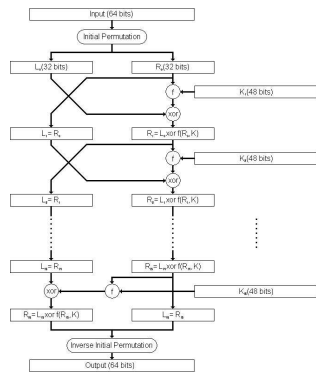


there is not much more to hide except the system

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity**
- Attackers
- Directions
- Summary

In cryptography

- ▶ keys = data
- ▶ system = program

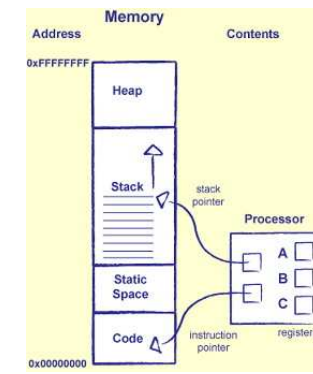


- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity**
- Attackers
- Directions
- Summary

In computation

(Gödel, Von Neumann, Kleene)

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

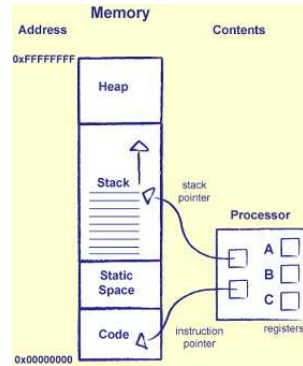


- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity**
- Attackers
- Directions
- Summary

In computation

(Gödel, Von Neumann, Kleene)

- ▶ keys = data = program
 - ▶ data \rightsquigarrow encrypted
- ▶ system = program = data
 - ▶ programs \rightsquigarrow obfuscated



Security by obscurity

Dusko Pavlovic

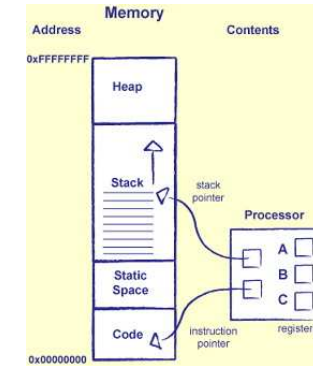
- Introduction
- Obscurity
- Attackers
- Directions
- Summary

In computation

(Gödel, Von Neumann, Kleene)

- ▶ keys = data = program
 - ▶ data \rightsquigarrow encrypted
- ▶ system = program = data
 - ▶ programs \rightsquigarrow obfuscated

Theorem [Barak et al]
Obfuscators do not exist.



Security by obscurity

Dusko Pavlovic

- Introduction
- Obscurity
- Attackers
- Directions
- Summary

In poker

- ▶ keys = hands of cards
- ▶ system = tactics



Security by obscurity

Dusko Pavlovic

- Introduction
- Obscurity
- Attackers
- Directions
- Summary

In games

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

- ▶ keys = players' states
- ▶ system = players' types



Security by obscurity

Dusko Pavlovic

- Introduction
- Obscurity
- Attackers
- Directions
- Summary

In games

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

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



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

Summary

In games

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

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



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

Summary

Kerckhoffs' Principle
Security is a game of
imperfect information.

In security games

(Kerckhoffs, Shannon)

- ▶ keys \leftrightarrow cryptanalysis
 - ▶ **hard**
- ▶ system \leftrightarrow decompilation
 - ▶ **easy**



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

Summary

Claim

Security is a game of **incomplete** information

Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

Summary



Kerckhoffs' Principle
Security is a game of
imperfect information.

Claim

There is security by obscurity even in cryptography

- ▶ **not** through obfuscated code
- ▶ **but** through **logically complex** algorithms

Security by obscurity
Dusko Pavlovic

- Introduction
- Obscurity**
- Attackers
- Directions
- Summary

Outline

Introduction

Background: Security and obscurity

Idea: Attack models

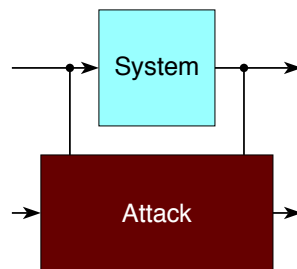
Approach: Directions

Summary

Security by obscurity
Dusko Pavlovic

- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

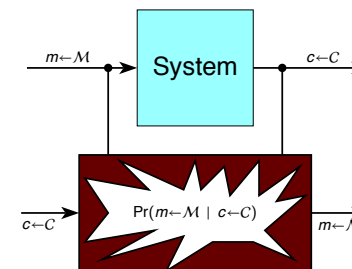
Security as a game



Security by obscurity
Dusko Pavlovic

- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Shannon's attacker: computationally unbounded (omnipotent computer)

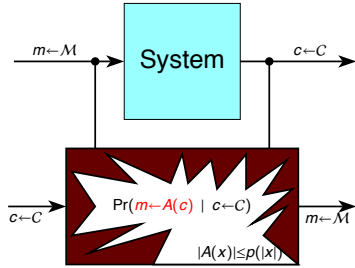


If a source conveys some information, the attack will extract that information.

Security by obscurity
Dusko Pavlovic

- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

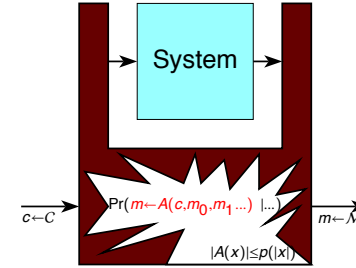
Diffie-Hellman's attacker: computationally bounded
(real computer)



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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

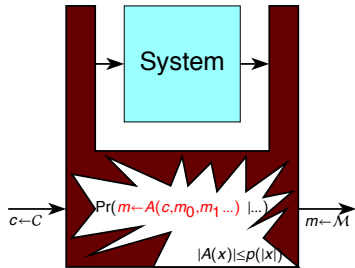
Adaptive attacker: queries the system
(still a real computer)



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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

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?

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Kerckhoffs' attacker: **logically** unbounded
(omnipotent programmer)

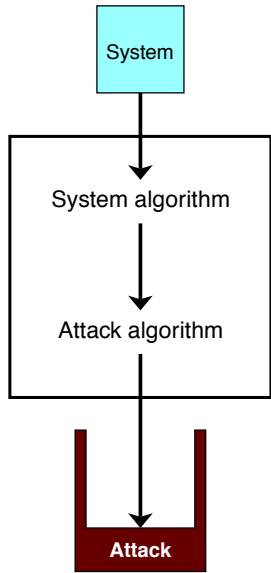


If there is an attack, the attacker will find it.

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Kerckhoffs' attacker: logically unbounded

(omnipotent programmer)

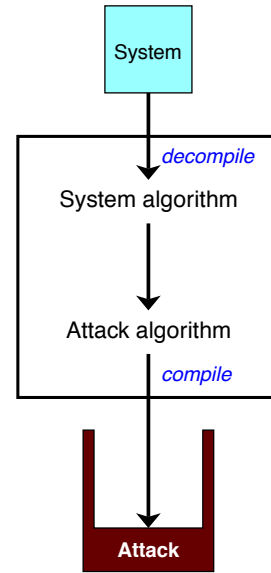


If an attack exists, the attacker will find it

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Kerckhoffs' attacker: logically unbounded

(omnipotent programmer)

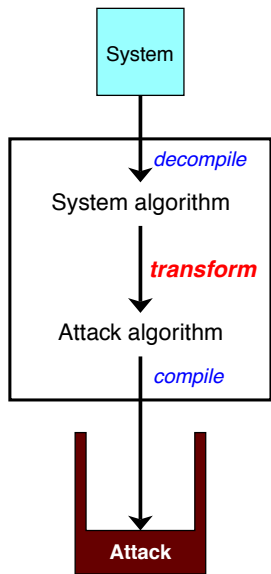


If an attack exists, the attacker will find it.

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Kerckhoffs' attacker: logically unbounded

(omnipotent programmer)

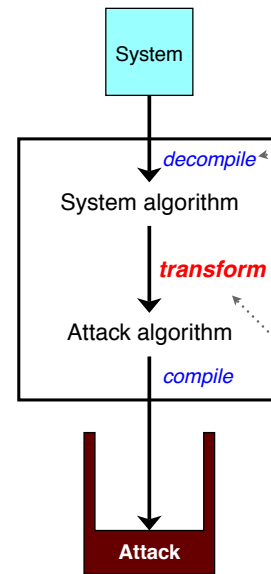


If an attack exists, the attacker will find it

- 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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Real attacker: logically bounded

(someone's student)

<i>power</i>	<i>unbounded</i>	<i>bounded</i>
computational	Shannon	Diffie-Hellman
rationality	Cournot	Simon
logical	Kerckhoffs	?????

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Idea

$$\frac{\text{computational complexity}}{\text{secrecy}} = \frac{\text{logical complexity}}{\text{obscurity}}$$

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Two directions

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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers**
- Directions
- Summary

Outline

Introduction

Background: Security and obscurity

Idea: Attack models

Approach: Directions

x-direction: Algorithmic information theory

y-direction: Epistemic game theory

Summary

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Question

What is logical complexity?

- ▶ Which proofs / algorithms are hard to construct?

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Question

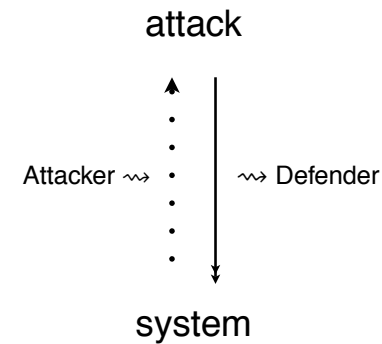
What is logical complexity?

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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Question

Is there "one-way programming"?



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Probability is not about events

- ▶ Probability only describes ensembles of events

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

Probability is not about events

- ▶ Probability only describes ensembles of events
- ▶ Information theory only speaks of global properties.

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

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?"

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

How do we predict events?

- ▶ $01010101010101010101010101010101 \dots 01$ can be written as
 - ▶ $(01)^{50}$

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

Predictable = programmable

Ray Solomonoff (1960): Science as programming

- ▶ $\Pr(1 \mid 0101010101010101010101010101 \dots 01) = 0$
- ▶ $\Pr(1 \mid 010011000111000011110 \dots 11) = 1$
- ▶ $\Pr(1 \mid 110100010011010100101 \dots 00) = \frac{1}{2}$

Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

x-direction

y-direction

Summary

Algorithmic information

Definition (Solomonoff 1960, Komogorov 1965)

Algorithmic information contained in data a is the length of the shortest program that outputs a

$$C(a) = \bigwedge_{\{p \mid ()=a\}} |p|$$

Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

x-direction

y-direction

Summary

Algorithmic information

Theorem (Schack 1997)

Algorithmic information is the local function that yields entropy as its global average

$$H(q) \approx \int_{i \in I} C(q_i)$$

Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

x-direction

y-direction

Summary

Algorithmic distance

Definition

Algorithmic distance between $a, b \in \mathbb{N}$ is the length of the shortest program that inputs a and outputs b

$$C(a, b) = \bigwedge_{\{p \mid (a)=b\}} |p|$$

Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

x-direction

y-direction

Summary

Idea

- ▶ Algorithmic information is a measure of unpredictability.

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

Idea

- ▶ Algorithmic information is a measure of unpredictability.
- ▶ Is algorithmic information a good concept of logical complexity?

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

Idea

Charles Bennett: Logical depth

- ▶ of an organism: the time it takes to evolve
 - ▶ virus: computationally simple, logically deep

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

Idea

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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction**
- y-direction
- Summary

Idea of logical security



\mathcal{L}



$P \neq NP$

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

Idea of logical security

$$D(\mathcal{L}, \text{rocket} \mathcal{L}) \geq D(\mathcal{L}, \neg P \neq NP)$$

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

Task

Implement this idea.

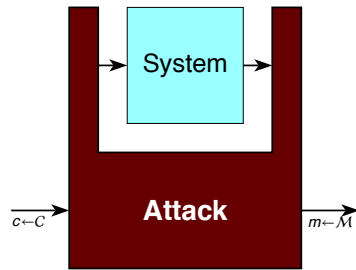
- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

Approach

Epistemic game theory of security.

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

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



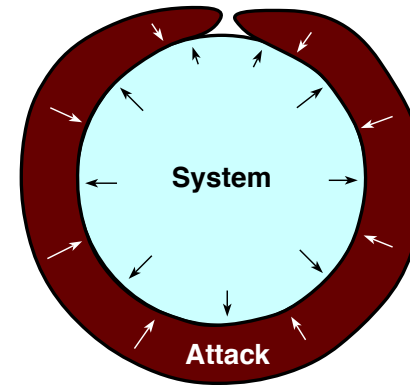
If there is a vulnerability,
an attack algorithm will make use of it.



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Game of attack vectors

Fortification



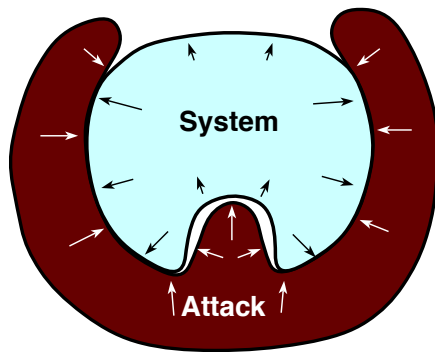
System must defend all vectors, Attacker just needs one



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Game of attack vectors

Honeypot



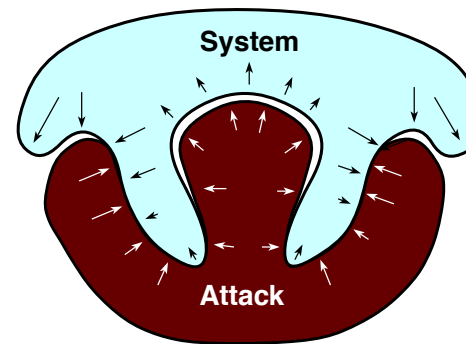
System passively observes Attacker



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Game of attack vectors

Sampling



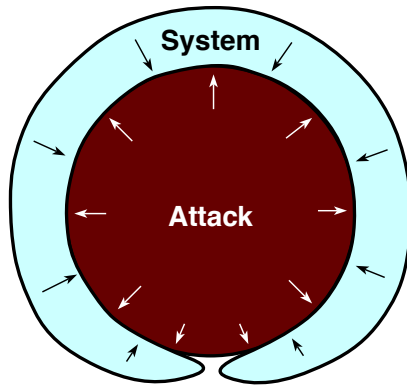
System actively queries Attacker



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
- x-direction
- y-direction
- Summary

Game of attack vectors

Adaptation

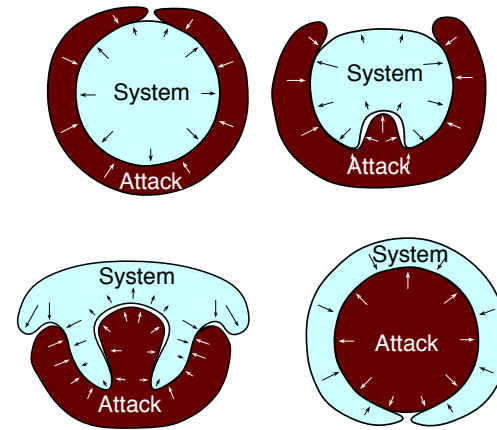


Attacker must defend all markers, System just needs one

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

Game of attack vectors

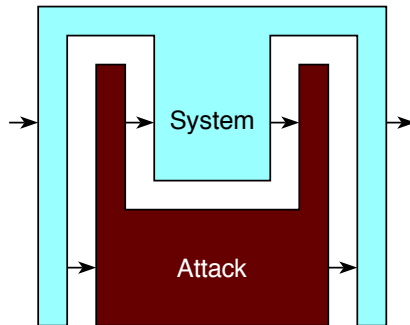
From fortification to adaptation



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

Adaptive defender: queries the users

(another computer)



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

- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

It is good to keep the invaders out . . .



- Security by obscurity
- Dusko Pavlovic
- Introduction
- Obscurity
- Attackers
- Directions
 - x-direction
 - y-direction
- Summary

... but it is better to bring them in



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

x-direction

y-direction

Summary

... but it is better to bring them in



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

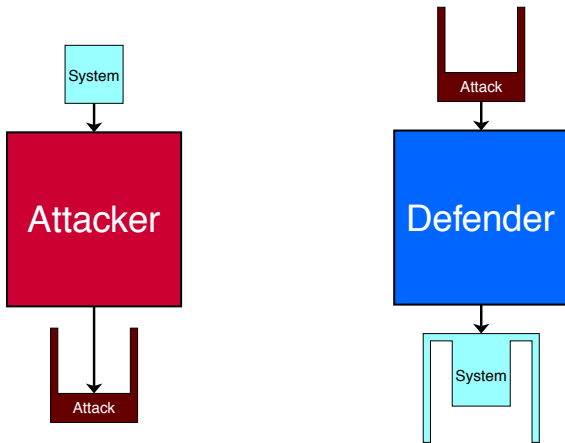
x-direction

y-direction

Summary

One-way-programming: adaptive immune response

Arms race for algorithms



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

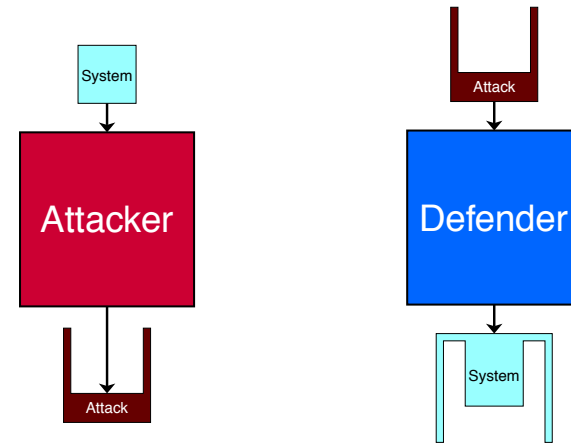
Directions

x-direction

y-direction

Summary

Arms race for algorithms



Security by
obscurity

Dusko Pavlovic

Introduction

Obscurity

Attackers

Directions

x-direction

y-direction

Summary

Socratic method: Answer questions by questions

