OSY.SSI[2019][2]

ACCESS DENIED

Insert video here.

All definitions in one little playlet

All definitions in one little playlet

- Computer: What is your name?

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?
  - "To seek the Holy Grail"

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?
  - "To seek the Holy Grail"
- Computer: Let me check if you can do that...

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?
  - "To seek the Holy Grail"
- Computer: Let me check if you can do that...
  - This is **authorization**.

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?
  - "To seek the Holy Grail"
- Computer: Let me check if you can do that...
  - This is **authorization**.
- Computer: Sorry mate, you can't do this. Access denied.

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?
  - "To seek the Holy Grail"
- Computer: Let me check if you can do that...
  - This is **authorization**.
- Computer: Sorry mate, you can't do this. Access denied.
  - This is **access control**.

All definitions in one little playlet

- Computer: What is your name?
  - This is **identification**.
- Computer: Prove it.
  - This is **authentication**.
- Computer: What is your quest?
  - "To seek the Holy Grail"
- Computer: Let me check if you can do that...
  - This is **authorization**.
- Computer: Sorry mate, you can't do this. Access denied.
  - This is **access control**.

What could go wrong?

Table of Contents

Access control

The goal of access control is to provide

- Confidentiality
- Integrity

It is implemented by a low level *reference monitor*.

Access control

The goal of access control is to provide

- Confidentiality
- Integrity

It is implemented by a low level *reference monitor*.

Access control implementations must be **NEAT**.

- Non-bypassable
- Evaluable
- Always invoked
- Tamper-proof

(insert personal anecdote)


ENTER
ENTER
DO NOT
ENTER

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)
- Access is granted or denied based on:

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)
- Access is granted or denied based on:
  - Identity (who can...)

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)
- Access is granted or denied based on:
  - Identity (who can...)
  - Action (...do what...)

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)
- Access is granted or denied based on:
  - Identity (who can...)
  - Action (...do what...)
  - Resource (...on what...)

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)
- Access is granted or denied based on:
  - Identity (who can...)
  - Action (...do what...)
  - Resource (...on what...)
  - Context (... and when.)

Access control

AC assumes a form of identifiable causality.

- AC tells what can be done to a resource (data, a system, etc.)
- Access is granted or denied based on:
  - Identity (who can...)
  - Action (...do what...)
  - Resource (...on what...)
  - Context (... and when.)

Example : `chmod`

So far so good

Question: How are *access rights* and *security properties* related?

So far so good

Question: How are *access rights* and *security properties* related?

Not obvious... More on that in a minute!

AC in practice? CBAC vs ACL

- **Capability-based (CBAC):** You are given a token that provides access (think key).
- **Access control lists (ACL):** Access is granted by your presence on a list (think VIP Party!)
- **Discretionary vs. Mandatory** (DAC/MAC): who decides rights?

Also RBAC, LBAC, GBAC, RSBAC, OrBAC...

Whichever flavour you fancy most, they both rely on:

- a notion of identity
- a form of authority in control

Table of Contents

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...
- Maybe not the way to get something done...

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...
- Maybe not the way to get something done...
- What about an imperfect approach?

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...
- Maybe not the way to get something done...
- What about an imperfect approach?

Weak version: what enables to tell someone from a given group for some time?

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...
- Maybe not the way to get something done...
- What about an imperfect approach?

Weak version: what enables to tell someone from a given group for some time?

- It suffices for this someone to own (temporarily) something the others don't.

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...
- Maybe not the way to get something done...
- What about an imperfect approach?

Weak version: what enables to tell someone from a given group for some time?

- It suffices for this someone to own (temporarily) something the others don't.
- We shall call this something the « Secret ».

What is identity?

When Metaphysics meets Science

Strong version: what characterises an individual?

- Hard (if fascinating) philosophical problem (self/identity/haecceity/ipseity)...
- Maybe not the way to get something done...
- What about an imperfect approach?

Weak version: what enables to tell someone from a given group for some time?

- It suffices for this someone to own (temporarily) something the others don't.
- We shall call this something the « Secret ».

Henceforth,

$$\text{Identity} \Leftrightarrow \text{Having the Secret}$$

What's a good secret?

A good secret has the following properties:

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**: the secret cannot be copied by anyone else.

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**: the secret cannot be copied by anyone else.
- **Revokability**

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**: the secret cannot be copied by anyone else.
- **Revokability**: the secret can be destroyed if needed.

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**: the secret cannot be copied by anyone else.
- **Revokability**: the secret can be destroyed if needed.

Examples ?

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**: the secret cannot be copied by anyone else.
- **Revokability**: the secret can be destroyed if needed.

Examples ? **Realistic examples**?

What's a good secret?

A good secret has the following properties:

- **Immarcescibility**: it doesn't change over time
- **Unicity**: no one else has the same secret
- **Incessibility**: the secret cannot be given to anyone else
- **Inimitability**: the secret cannot be copied by anyone else.
- **Revokability**: the secret can be destroyed if needed.

Examples ? **Realistic examples**?

In short, secrets seem to require... access control themselves.

Aside: Keep secrets secret!

Authentication

An *authentication protocol* checks that you indeed know the secret.

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**: if you have the secret, all goes well.

$$\Pr\left[\mathrm{Auth}_{X,Y}(X) \mid s \in X\right] = 1 - \mathrm{negl}$$

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**: if you have the secret, all goes well.

$$\Pr\left[\mathrm{Auth}_{X,Y}(X) \mid s \in X\right] = 1 - \mathrm{negl}$$

- **Signifiance**

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**: if you have the secret, all goes well.

$$\Pr\left[\mathrm{Auth}_{X,Y}(X) \mid s \in X\right] = 1 - \mathrm{negl}$$

- **Signifiance**: if all goes well, it means you had the the secret.

$$\Pr\left[s \in X \mid \mathrm{Auth}_{X,Y}(X)\right] = 1 - \mathrm{negl}$$

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**: if you have the secret, all goes well.

$$\Pr\left[\mathrm{Auth}_{X,Y}(X) \mid s \in X\right] = 1 - \mathrm{negl}$$

- **Signifiance**: if all goes well, it means you had the the secret.

$$\Pr\left[s \in X \mid \mathrm{Auth}_{X,Y}(X)\right] = 1 - \mathrm{negl}$$

- **Non-transferability**

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**: if you have the secret, all goes well.

$$\Pr\left[\mathrm{Auth}_{X,Y}(X) \mid s \in X\right] = 1 - \mathrm{negl}$$

- **Signifiance**: if all goes well, it means you had the the secret.

$$\Pr\left[s \in X \mid \mathrm{Auth}_{X,Y}(X)\right] = 1 - \mathrm{negl}$$

- **Non-transferability**: the transcript cannot be used to authenticate to a third party.

$$\Pr\left[\mathrm{Auth}_{X,Z}(Y) \mid \mathrm{Auth}_{X,Y}(X)\right] = \mathrm{negl}$$

Authentication

An *authentication protocol* checks that you indeed know the secret.

Such a protocol should have the following properties:

- **Correctness**: if you have the secret, all goes well.

$$\Pr\left[\mathrm{Auth}_{X,Y}(X) \mid s \in X\right] = 1 - \mathrm{negl}$$

- **Signifiance**: if all goes well, it means you had the the secret.

$$\Pr\left[s \in X \mid \mathrm{Auth}_{X,Y}(X)\right] = 1 - \mathrm{negl}$$

- **Non-transferability**: the transcript cannot be used to authenticate to a third party.

$$\Pr\left[\mathrm{Auth}_{X,Z}(Y) \mid \mathrm{Auth}_{X,Y}(X)\right] = \mathrm{negl}$$

Examples ?

Intermezzo: granting access

Software and the chair-keyboard interface

Intermezzo: granting access

Software and the chair-keyboard interface

We spend our time *delegating* rights and *granting* access.

Intermezzo: granting access

Software and the chair-keyboard interface

We spend our time *delegating* rights and *granting* access.

- Launching programs (they access files, sockets etc.)

Intermezzo: granting access

Software and the chair-keyboard interface

We spend our time *delegating* rights and *granting* access.

- Launching programs (they access files, sockets etc.)
- Spyware running with the user's rights

Intermezzo: granting access

Software and the chair-keyboard interface

We spend our time *delegating* rights and *granting* access.

- Launching programs (they access files, sockets etc.)
- Spyware running with the user's rights
- Phishing...

Intermezzo: granting access

Software and the chair-keyboard interface

We spend our time *delegating* rights and *granting* access.

- Launching programs (they access files, sockets etc.)
- Spyware running with the user's rights
- Phishing...Tabnapping!

Good practice: **Principe of least priviledge** (PLP).

How to achieve non-transferability?

Any idea?

Zero-knowledge proofs

Exercise: can you prove you know where's Wally without revealing his position?

Fact:

Zero-knowledge proofs

Exercise: can you prove you know where's Wally without revealing his position?

Fact: Zero-knowledge proofs exist.

Zero-knowledge proofs

Exercise: can you prove you know where's Wally without revealing his position?

Fact: Zero-knowledge proofs exist. For many things (all of **NP**).

ZKP: A Math Example

Proving knowledge of a discrete log

P claims to know x such that $y = g^x$.

- **Commitment:** P chooses random r and sends $t = g^r$
- **Challenge:** V chooses random c and sends it to P.
- **Response:** P sends $s = r + xc$.
- **Verfication:** V checks whether $g^s = ty^c$.

ZKP: A Math Example

Proving knowledge of a discrete log

P claims to know x such that $y = g^x$.

- **Commitment:** P chooses random r and sends $t = g^r$
- **Challenge:** V chooses random c and sends it to P.
- **Response:** P sends $s = r + xc$.
- **Verfication:** V checks whether $g^s = ty^c$.

Exercise: Understand why it is ZK and non-transferable!

Important distinctions

So we have:

- A secret (which is secret)
- An authentication mechanism (which is public)
- An access control policy (which may be public or not)

These three things are different and (in principle) independent.

REMEMBER THIS: Separation between policy and mechanism

Table of Contents

Formal models

The goal of a formal model is to prove security properties. Why proofs?

This becomes necessary as soon as the system becomes large.

Bell and LaPadula designed the first provable AC model.

The Bell-LaPadula Model

The archetypical Access Control

The Bell-LaPadula Model

The archetypical Access Control

- L (MLS lattice) e.g.:

$$\text{unclassified} < \text{classified} < \text{secret} < \text{top secret}$$

The Bell-LaPadula Model

The archetypical Access Control

- L (MLS lattice) e.g.:

  $$\text{unclassified} < \text{classified} < \text{secret} < \text{top secret}$$

- O (objects with classification $\in L$)
- S (subjects with clearance $\in L$)
- A (operations: r, w)

The Bell-LaPadula Model

The archetypical Access Control

- L (MLS lattice) e.g.:

  $$\text{unclassified} < \text{classified} < \text{secret} < \text{top secret}$$

- O (objects with classification $\in L$)
- S (subjects with clearance $\in L$)
- A (operations: r, w)
- **Key idea:** "Good" state + "valid" operation $\Rightarrow$ "Good" state.

The Bell-LaPadula Model

Valid operations

The Bell-LaPadula Model

Valid operations

- *no read-up*: a subject can only read *lower*-level objects ;

The Bell-LaPadula Model

Valid operations

- *no read-up*: a subject can only read *lower*-level objects ;
- *no write down*: a subject can only write objects to *higher* levels

The Bell-LaPadula Model

Valid operations

- *no read-up*: a subject can only read *lower*-level objects ;
- *no write down*: a subject can only write objects to *higher* levels

Bell, LaPadula, Schell for the U.S. Department of Defense (DoD).

The Bell-LaPadula Model

Valid operations

- *no read-up*: a subject can only read *lower*-level objects ;
- *no write down*: a subject can only write objects to *higher* levels

Bell, LaPadula, Schell for the U.S. Department of Defense (DoD).

The Bell-LaPadula Model

Valid operations

- *no read-up*: a subject can only read *lower*-level objects ;
- *no write down*: a subject can only write objects to *higher* levels

Bell, LaPadula, Schell for the U.S. Department of Defense (DoD).

Everything can be formulated as a formal automaton and checked.

It's elegant it's fast it's simple it's used all over.

The Bell-LaPadula Model

Valid operations

- *no read-up*: a subject can only read *lower*-level objects ;
- *no write down*: a subject can only write objects to *higher* levels

Bell, LaPadula, Schell for the U.S. Department of Defense (DoD).

Everything can be formulated as a formal automaton and checked.

It's elegant it's fast it's simple it's used all over.

Does the job?

The Bell-LaPadula Model

Some limitations...

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account
- Assumes security clearance and classification do not change

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account
- Assumes security clearance and classification do not change
- No clear separation between mechanism and policy

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account
- Assumes security clearance and classification do not change
- No clear separation between mechanism and policy
- Assumes that a state with no confidentiality is a “good” state

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account
- Assumes security clearance and classification do not change
- No clear separation between mechanism and policy
- Assumes that a state with no confidentiality is a “good” state
- Top-secret attractor, unless exceptions introduced

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account
- Assumes security clearance and classification do not change
- No clear separation between mechanism and policy
- Assumes that a state with no confidentiality is a “good” state
- Top-secret attractor, unless exceptions introduced
- Worst of all: doesn’t even do the job about confidentiality...

The Bell-LaPadula Model

Some limitations...

- Integrity, availability... not taken into account
- Assumes security clearance and classification do not change
- No clear separation between mechanism and policy
- Assumes that a state with no confidentiality is a “good” state
- Top-secret attractor, unless exceptions introduced
- Worst of all: doesn’t even do the job about confidentiality...

Do you see why?

Hidden channel!

There is a *hidden* channel in the BLP model.

Hidden channel!

There is a *hidden* channel in the BLP model.
Worse: there is no *provable* way around it in general (Shannon, Turing).

Hidden channel!

There is a *hidden* channel in the BLP model.
Worse: there is no *provable* way around it in general (Shannon, Turing).
Dilemma: *expressive* AC *vs. correct* AC.

Hidden channel!

There is a *hidden* channel in the BLP model.
Worse: there is no *provable* way around it in general (Shannon, Turing).
Dilemma: *expressive* AC *vs. correct* AC.

BLP crime: confusing policy and mechanism

Information flow?

Question: can *information flow* be blocked?

Information flow?

Question: can *information flow* be blocked? Can it be blocked selectively ?

Information flow?

Question: can *information flow* be blocked? Can it be blocked selectively ?

More about that in the next lecture!

Now applaud and rush for your lunch like your lives depend on it

And don't forget to brush your teeth