Policy and Models in Information Security (Part I)

Ioanna Maratsi - HT21

Lecture Content

- Challenges and goals
- The complexity of problems and the solutions
- Addressing computer & system security
- Policies, Models
- Formal models solutions for
  - Confidentiality
  - Integrity
  - More general

Principles that we would like to abide by

Security

- Liberating via inclusion, understanding, not limitations and confinements
- Enabler for openness and transparency
- Creation and adoption of digital services

Privacy

- it is not what you know, but how you use it
  - Responsibility
  - Accountability
  - Anonymization
  - De-anonymization

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Challenges and goals

TRUST

- Interoperability
- Measuring the state of democracy
- Availability and equity of access
- Responsibility and accountability
- Stewardship of big and open data
- Sustainability of human networking

- Security
- Surveillance
- Omnipresence
- Access
- Right to be forgotten
- Right to be wrong
- Identity
- Availability
- Privacy

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

The complexity

- *Not feasible to have a system which is not subject to errors (hardware or software) introducing security vulnerabilities*

How do we address these problems?

- *If not completely, then at least pragmatically*

Goal:

Make them acceptable in a real-world context

Formal systems

We need to produce a system that can be validated and verified with respect to security

- ***Validated*** *– we are building the right system*
- ***Verified*** *– we are building the system in the right way*

How?

Formal language – Mathematics/Logic

System security

- *In general, security aims to preserve the (digital) system the way it is functional and operational by observing and following a defined policy (or policies)*

- *In 1976 Harrison, Ruzzo & Ullman proved that computer systems security is* ***undecidable***

System security /2

The basic question of Computer Security:

"Given a computer system, how can we determine whether it is secure?"

In other words:

"Under what conditions can we/an algorithm determine whether a system is secure?"

Models, policies, machines

- We are in a world of digital (discrete) systems
- We do not need to check continuously (with respect to time) the state of the system
- A selection of important discrete points will be sufficient, whenever the state of the system changes
- We need to understand what is going with the system - represent and capture the main states

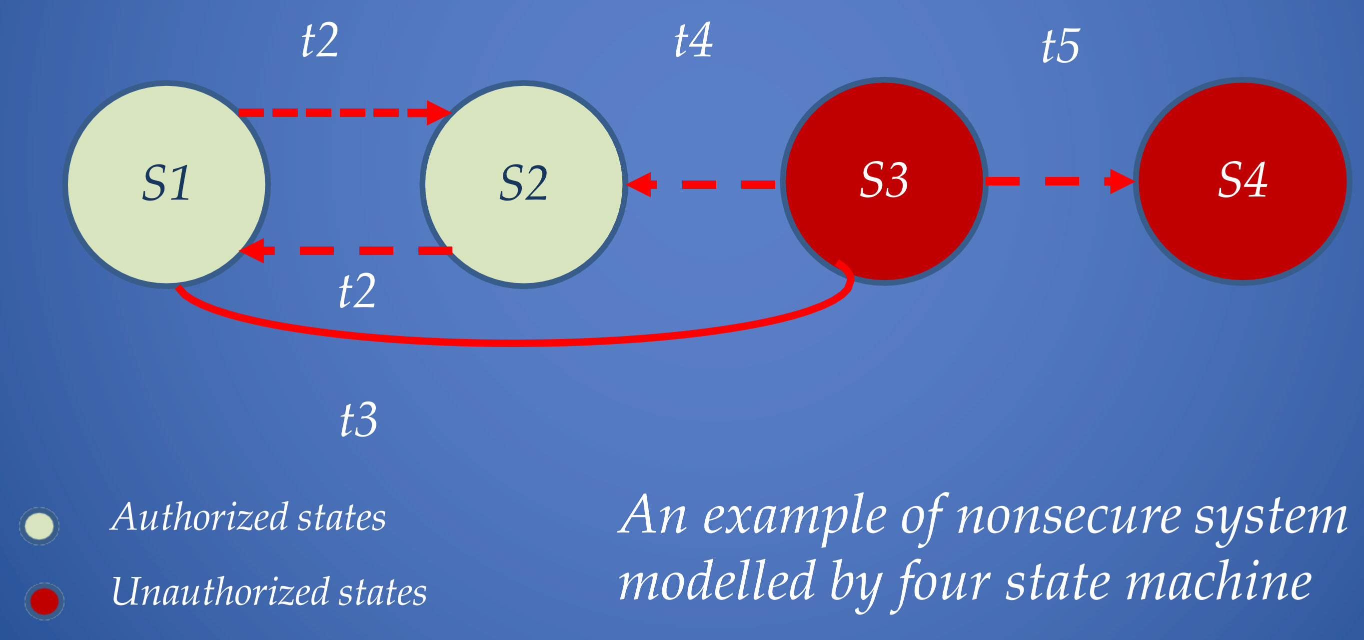
Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Models, policies, finite automata

- *A range of state machines from the simplest - finite deterministic machine - to the universal ones - Turing machines*
- *However, no progress with respect to decidability.*
- *Let us assume that our CS is a finite state machine or automation with a set of transition functions.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Simple finite state machine



An example of nonsecure system modelled by four state machine

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Ideally

- *Pick up a model based on a finite state machine*
- *Identify all states that make the model secure*
- *Check that the start or initial state is secure*
- *Make sure that each time you move, you start with a secure state you also end up in a secure state*
- *The system stays secure, namely the model preserves "security"*
- *Security theorem*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Models and policies

- *Security policy is just a statement of what is and what is not allowed.*
- *If one wants to enforce a policy, there is a need a mechanism (s) or a procedure (s) for doing so.*
- *As indicated, we would like to preserve the security of the system where we have*
  - *Safe or secure states*
  - *Unsafe or nonsecure states*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Models and policies /2

- *Both policies and models can be used for*
  - *Evaluation (including auditing and risk assessment) of*
  - *To prove or disprove the security of a system*

A model can consist of one or more policies

Security policy

- Security policy is a statement that partitions or divides the set of states into two sub-sets of (1) authorized or secure states, and (2) unauthorized or nonsecure states.
- A secure system is the one that starts in a authorized state (the initial state) and cannot enter an unauthorized state.
- If the system transits in an unauthorized state we can have a breach of security.

Security policy /2

We can express a policy as an access control matrix, where we can have the rights that certain subjects have on certain objects.

*The **policy** defines the authorized set of states A and let R be the set of rights of the system:*

Security policy /3

Definition 1:

When a generic right r is added to an element of the access control matrix ***not*** *already containing r, that right is said to be leaked.*

Definition 2:

If a system can never leak the right r, the system (including the initial state s0) is called safe with respect to the right r.

Security policy /4

So,

A secure system corresponds to a model safe with respect to all access rights BUT a model safe with respect to all rights does not ensure a secure system.

Secure system => model safe with respect to all rights

Not necessarily vice versa!

Computer security

- CIA triad
  - Confidentiality
  - Integrity
  - Availability
  - (Authenticity)

- Countermeasures
  - Preventive
  - Mitigating
  - Transferring
  - Recovery

Formalizing the CIA triad

Confidentiality:

Let X be a set of entities and I information. Then I has the property of confidentiality relative to X if no member of X can have information from I.

Formalizing the CIA triad /2

Integrity:

Let X be a set of entities and I information or a resource. Then I has the property of integrity relative to X if all members of X trust I.

Formalizing the CIA triad /3

Availability:

Let X be a set of entities and I information or a resource. Then I has the property of availability relative to X if all members of X can access I.

Types of Security Policies

- ***Military Security Policy (Governmental Security Policy)***
- *Developed primarily to provide confidentiality*

- ***Commercial Security Policy***
- *Developed primarily to provide integrity*

Trading between Confidentiality & Integrity

- *A confidentiality policy is dealing only with confidentiality*
- *An integrity policy is dealing only with integrity*

Note: *Both confidentiality and military policies deal with confidentiality, however, a confidentiality policy does not deal with integrity at all, whereas a military policy may!*
The same applies for integrity and commercial policies.

Types of Access Control

A security policy can use two types of access control, alone or in combination.

In one, access control is left to the discretion of the owner (discretionary access control - DAC)

In the other, the operating system controls access and the owner cannot overwrite the controls (mandatory access control - MAC)

Returning to Confidentiality Policies

A confidentiality policy (also known as "information flow policy"), prevents the unauthorized disclosure of information.

We present one such policy, the Bell-La Padula Model

The primary model

- Bell-LaPadula (BLP) – proposed in 1970’s as a model for access control
- Not surprisingly – the provenance in a military or a defence context
- Two types of entities – objects and subjects
- Each entity is assigned a security class
- Security classes adhere to a strict hierarchical structure described by security levels

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Reality check - U.S. military classification scene

- *Top secret >secret >confidential >restricted >unclassified*
- *It is possible to increase the granularity of the model by introducing a set of categories or compartments for each security level*

Why?

- *So we can address the issue of combining different classifications*
- *A subject is assigned a security level and a category to access an object*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Discussion

- *Information can be organized into*
  - *Gross levels and categories*
- *Users granted*
  - *Clearances to access certain categories of data*
- *Example – corporation or organization*
  - *Four levels on the scheme*
    - *Strategic (planning documents and data)*
    - *Sensitive (financial and personnel data)*
  - *Strategic > sensitive > confidential > public*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Clearances and classifications

- *A subject – has a security clearance of a certain level*
- *An object – has a security classification of a certain level*
- *Security classes – regulate or control the manner by which a subject may access an object.*
- *Four access modes (not necessarily limited)*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Modes of operation

- *Four modes*
  - *Read (only)*
  - *Append (only write)*
  - *Write (both read and write)*
  - *Execute (no read, no write) – invoke an object for an execution*
- *Multilevel security – defined multiple categories and levels of data*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

A multilevel security system

- *A multilevel secure system for confidentiality:*
  - *No read up: A subject can only read an object of less or equal security level – <u>simple security property</u> – ss-property.*
  - *No write down: A subject can only write into an object of greater or equal security level or the <u>star property</u> *-property.*
  - *ss-property + *-property – confidentiality as a form of mandatory access control (MAC).*
  - *ds – property - discretionary access control (DAC). An individual may grant another individual access based on the MAC rules.*
  - *To access = one needs a necessary authorization and to satisfy the MAC rules.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Formal description of BLP

- *Based on the current state of the system, where each state is described by a 4-tupple (b, M, f, H)*
- *Current access set b: made from triplets (subject, object, access-mode) or*
- *(s, o, a) translates to – a subject s has access to an object o in (an access) mode a.*
- *The triple also defines that the access mode is currently being exercised.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Formal description of BLP/2

- *Access matrix M: The matrix element Mij indicates the access modes in which a subject Si is permitted to access an object Oj.*

Objects

Subjects *Files* *Processes* *Drives*

Objects

	S_1	S_2	F_1	F_2	P_2	P_2	D_1
S_1	*control*	*owner*	*read**	*read owner*	*wakeup*	*wakeup*	*seek*
S_2		*control*	*write**	*execute*			*owner*
S_3				*write*	*stop*		

Extended access control matrix

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Formal description of BLP/3

- *Let us formalise the properties:*
  - *ss-property: every triple of the form (Si, Oj, read) in the current access set b has the property fc(Si) >=fi(Oj)*
  - **-property: every triple of the form (Si, Oj, append) in the current access set b has the property fc(Si) =<fi(Oj), while every triple of the form (Si, Oj, write) in the current access set b has the property fc(Si) =fo(Oj).*
  - *ds-property: If (Si, Oj, Ax) is a current access (is in b) then the access mode As is recorded in (Si, Oj) element of M. That is (Si, Oj, Ax) implies that Ax is an element of M [Si, Oj].*
- *The three properties define a confidentiality secure system, which can be formally proven.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Formal description of BLP/4

- *When is a system secure ?*
  1. *The current security state of the system (b, M,f, H) is secure iff every element of b satisfies the three properties.*
  2. *The security state of the system is changed by any operation that changes any of the four components of the system (b, M, f, H).*
  3. *A secure system remains secure as long as any state change does not violate the three properties.*
- *Basically, we can prove that the system will preserve the security of the system by proving that (1), (2), and (3) are true.*
- *Each property is a theorem whose validity can be proved.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Formal description of BLP/5

- *Set of rules and abstract operations that change the state of the system.*
  1. *Get access / add a triple (subject, object, access-mode)*
  2. *Release access / remove a triple (subject, object, access-mode)*
  3. *Change object level / change the value of Fo(Oj)*
  4. *Change current level / change the value of Fc(Si)*
  5. *Give access permission / add an access mode*
  6. *Rescind access permission / delete an access mode*
  7. *Create an object / attach an object to the current tree structure H as a leaf*
  8. *Delete a group of objects / detach an object and all other objects beneath it in the hierarchy*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Reflections on BLP limitations and problems

- *Almost a universal model for secure computing, but do not get your hopes too high, since*
- *A single system cannot address both confidentiality and integrity*
  - *One cannot deal with powers and secrets under the same roof*
  - *May exclude present and future technologies benefiting both*
- *Cooperating conspirator issue*
  - *In the presence of covert channels – especially if we have shared resources: *- property might not be enforceable*
  - *The model breaks down – a high clearance (trusted) subject may execute a low classified (untrusted) executable data*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Reflections on BLP limitations and problems/2

- *Assumption of tranquillity - there are no changes in the access control data.*
- *Covert channels – communication pipes which allow transfer of data that violate a security policy of a system.*
- *We have channels*
  - *Storage (such as OS messages, file names)*
  - *Timing (such as monitoring system performance)*
- *BLP model is not able to detect covert pipes.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Reflections on BLP limitations and problems/3

- *The problems actually are congenital to all MLS models*
  - *You can have only one focus – confidentiality (powers) or integrity (secrets)*
  - *They are incompatible; namely, it is not possible to treat them simultaneously with the same model in a specific system*
  - *The exception is the Chinese Wall model*
  - *Now, we can focus on integrity or secrets*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.