

Introduction to Security Models

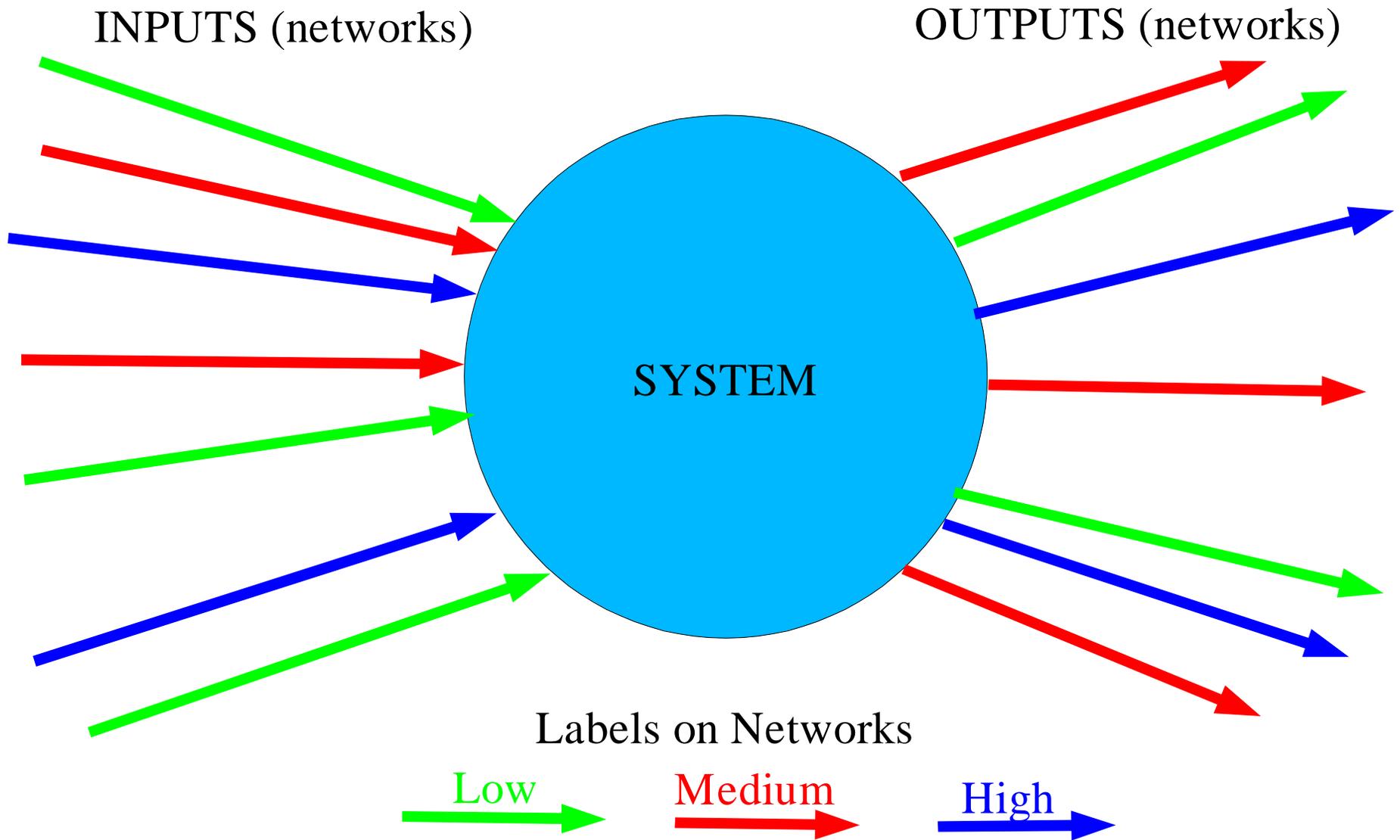
Lecture 1

CS4605

George W. Dinolt

Naval Postgraduate School

Simple System



The Trivial Exact Match Policy

- There are *wires* or directed networks
- There are *pieces of information*
- There are *security labels*
- It is possible to associate a *security label* with each *piece of information* – represents the actual sensitivity of the *information*
- *System* doesn't change the sensitivity of information
- All the information carried on a wire is at the same *security* level (has the same *label*)

Trivial Policy

- System is a “router”
- Policy is “Exact Match”
 - Input from **Low** network can only be output on **Low** network
 - Input from **Medium** network can only be output on **Medium** network
 - Input from **High** network can only be output on **High** network

Policy “Properties”

- Assumptions
 - The bits from the **Low** input networks represent **low** information
 - The bits from the **Medium** input networks represent **medium** information
 - The bits from the **High** input networks represent **High** information

Policy Properties (Cont.)

- Assertions
 - System
 - Does not modify bits
 - Only sends bit out that have been received
 - The bits output to **Low** networks represents **low** information
 - Etc..

The Model (in Mathematics)

- Sets (Terms)
 - Information Unit (IU)
 - Security Labels (SL)
- Definitions
 - $Stream = \langle iu : iu \in IU \rangle$ (sequence of iu 's)
 - $Networks = \{ (st, sl) : st \in Stream, sl \in SL \}$
 - $InputNetworks = OutputNetworks = Networks$
 - $System \subseteq InputNetworks \times OutputNetworks$

The Model

- *System is Secure* if and only if
 - For all $outnet = (outStream, outLabel) : OutputNetworks$ of *System*
 - For all $iu : iu \in outStream$,
 - There exists $inet = (inStream, inLabel)$ in *InputNetworks* of *System*
 - such that
 - $inLabel = outLabel$ (exact match policy)
 - $iu \in inStream$ (same data was input at the level)

Problems with the Model

- This isn't very formal yet
- It is not clear what the “boundary” is (yet)
- We haven't modeled the system actions (this is a static model or a model of a snapshot)
- No guarantee that the output won't happen before the input (a prescient system)
- The *iu*'s could be misrouted (but not a security violation?)

What is the Model?

- The model really defines a collection of pairs of sets of the form (X, Y) where
 - $X \subseteq \text{InputNetworks}$
 - $Y \subseteq \text{OutputNetworks}$
 - Elements of X and Y have a specified relationships
- $M = \{ (X, Y) : X \subseteq \text{InputNetworks}, Y \subseteq \text{OutputNetworks}, \forall (sty, sly) \in Y, \forall iu \in sty, \exists (stx, slx) \in X \ni iu \in stx \ \& \ sly = slx \}$
- Don't worry about being able to read this now.

A Write-Up Policy

- There are wires or networks
- There is information carried on the wires
- There is an **(ordered)** set of security labels
- Each piece of information has a sensitivity which is represented by one of the **(ordered)** set of security labels
- There are **(ordered)** security labels associated with each wire that map to the sensitivity of the information it carries.
- The sensitivity of any information carried on a wire should be **no more than** the sensitivity associated with that wire by the wire's security label

Write Up Policy

- System is a “router”
- Policy is “Write Up”
 - Input from **Low** network can be output on **Low**, **Medium** and **High** networks
 - Input from **Medium** network can be output on **Medium** and **High** networks
 - Input from **High** network can only be output on **High** network

Write-up Policy Properties

- Assumptions
 - The bits from the **Low** input networks represent **low** information
 - The bits from the **Medium** input networks represent at most **medium** information
 - The bits from the **High** input networks represent at most **High** information

Write Up Policy (Continued)

- Assertions
 - System
 - Does not modify bits
 - Only sends bit out that have been received
 - The bits output to **Low** networks represents **low** information
 - Etc..

Write Up – Definitions

- Sets (Terms)
 - Information Unit (IU)
 - Security Labels (SL) (ordered by “ \leq ”)
- Definitions
 - $Stream = \langle iu : iu \in IU \rangle$ (sequence of iu's)
 - $Networks = \{ (st, sl) : st \in Stream, sl \in SL \}$
 - $InputNetworks = OutputNetworks = Networks$
 - $System \subseteq InputNetworks \times OutputNetworks$

Modified Model – Write Up

- *System is Secure* if and only if
 - For all $outNet = (outStream, outLabel) : OutputNetwork$
 - For all $iu : iu \in outStream$
 - There exists $inNet = (inStream, inLabel) : InputNetwork$ such that
 - $inLabel \leq outLabel$ (**write up policy**)
 - $iu \in inStream$ (same data was input at the level)

Simple Exercises

- Suppose you have an ordered security label set.
- Suppose you have a set of components
- Suppose one were to interconnect the components (outputs of one becoming the inputs of others, etc.) to form new systems.
 - What policy would this “composition” satisfy if each component satisfied an “exact match” security property?
 - Same if each component satisfied “Write-up”?
 - Suppose you combined “exact match” components and “write-up” components, what would the result be.
 - What is the relationship between systems that satisfy “exact match” and systems that satisfy “write-up”?