Security and Trust I: 4. Flow Security

Dusko Pavlovic

UHM ICS 355
Fall 2014

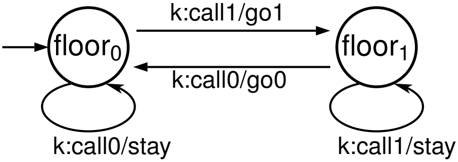
Outline

Outline

The elevator example again

Elevator model

- Q = {floor0, floor1}
- I_k = {k:call0, k:call1}, $k \in \mathbb{L}$ = {Alice, Bob}
- O = {go0, go1, stay}
- θ :



The elevator example again

Elevator interference

The histories

$$(\text{A:call0} \;\; \text{B:call1}) \quad \text{and} \quad (\text{A:call1} \;\; \text{B:call1})$$

are for Bob

- indistinguishable by the inputs, since he only sees Bob:call1 in both of them, yet they are
- distinguishable by the outputs, since Bob's channel outputs are
  - $(\text{A:call0} \;\; \text{B:call1}) \longmapsto \text{go1}$
  - $(\text{A:call1} \;\; \text{B:call1}) \longmapsto \text{stay}$

The elevator example again

Question

How does Bob really use the interference?

The elevator example again

Answer

He derives *another* channel

$$\frac{\{\text{A:call0}, \text{A:call1}, \text{B:call0}, \text{B:call1}\}^+ \rightharpoondown \{\text{stay}, \text{go}\}}{\{\text{B:call0}, \text{B:call1}\}^+ \rightharpoondown \{\text{A\_home}, \text{A\_out}\}}$$

The elevator example again

Answer

He derives *another* channel

$$\frac{\{\text{A:call0, A:call1, B:call0, B:call1}\}^+ \rightharpoondown \{\text{stay, go}\}}{\{\text{B:call0, B:call1}\}^+ \rightharpoondown \{\text{A\_home, A\_out}\}}$$

This is a *covert channel*.

The elevator example again

Different flows

- $\{$A:call0, A:call1, B:call0, B:call1$\}^+ \to \{$stay, go$\}$ makes Alice and Bob flow through the elevator
- $\{$B:call0, B:call1$\}^+ \to \{$A_home, A_out$\}$ makes the information about Alice flow to Bob

What is *flow*?

Intuition

The *flow* of a channel is the observed traffic that flows through it

- (water flow, information flow, traffic flow. . .)

What is *flow*?

Flow vs channel

- A deterministic unshared channel implements a single flow. There are two usages
  - either the channel $I^+ \xrightarrow{f} O$ induces the flow $I^* \xrightarrow{\vec{f}} O^*$
  - or the history $\vec{x}$ induces the flow $\vec{f}(\vec{x})$ along the channel $I^+ \xrightarrow{f} O$

What is *flow*?

Flow vs channel

- A deterministic unshared channel implements a single flow. There are two usages
  - either the channel $I^+ \xrightarrow{f} O$ induces the flow $I^* \xrightarrow{\vec{f}} O^*$
  - or the history $\vec{x}$ induces the flow $\vec{f}(\vec{x})$ along the channel $I^+ \xrightarrow{f} O$
- A deterministic *shared* channel $I^+ \xrightarrow{\vec{f}} O$ contains the flows $I_k^* \xrightarrow{\vec{f}_k} O^*$.
  - The mapping $I^* \xrightarrow{\vec{f}} O^*$ is a flow only if there is a global observer.

What is *flow*?

Flow vs channel

- A deterministic unshared channel implements a single flow. There are two usages
  - either the channel $I^+ \xrightarrow{f} O$ induces the flow $I^* \xrightarrow{\vec{f}} O^*$
  - or the history $\vec{x}$ induces the flow $\vec{f}(\vec{x})$ along the channel $I^+ \xrightarrow{f} O$
- A deterministic *shared* channel $I^+ \xrightarrow{\vec{f}} O$ contains the flows $I_k^* \xrightarrow{\vec{f}_k} O^*$.
  - The mapping $I^* \xrightarrow{\vec{f}} O^*$ is a flow only if there is a global observer.
- A possibilistic channel $I^+ \xrightarrow{f} \wp O$ contains multiple deterministic channels which induce the possible flows

Channeling interference

In general, any user k who seeks the interferences in a shared channel $\vec{f}$ builds a derived *interference channel* $\widehat{f_k}$

$$\frac{I^* \xrightarrow{\vec{f}} O^*}{\begin{array}{ccc} I_k^* & \xrightarrow{\widehat{f_k}} & \wp O \\ \vec{x}_k & \longmapsto & \left\{ \vec{f}_k\left(\vec{y}\right) \mid \vec{y}\restriction_k = \vec{x}_k \right\} \end{array}}$$

Channeling interference

In general, any user k who seeks the interferences in a shared channel $\vec{f}$ builds a derived *interference channel* $\widehat{f_k}$

$$\frac{I^* \xrightarrow{\vec{f}} O^*}{\begin{array}{ccc} I^*_k & \xrightarrow{\widehat{f_k}} & \wp O \\ \vec{x}_k & \longmapsto & \left\{\vec{f}_k\left(\vec{y}\right) \mid \vec{y}\restriction_k = \vec{x}_k\right\} \end{array}}$$

On the input $\vec{x}_k$ the interference channel $\widehat{f_k}$ outputs a *possible* output $\vec{f}_k(\vec{y})$, where $\vec{y}\restriction_k = \vec{x}_k$, i.e. $\vec{y}$ is a *possible world* for $\vec{x}_k$.

Channeling interference

Remark

- $\widehat{f_k}$ is not a deterministic channel.
- Nondeterministic channels may be
  - *possibilistic* $I^+ \to \wp_* O \subset \{0,1\}^O$
  - *probabilistic* $I^+ \to \Upsilon O \subset [0,1]^O$
  - *quantum* $I_+ \to \Theta O \subset \{z \in \mathbb{C} \mid |z| \leq 1\}^O$

Channeling interference

Remark

- $\widehat{f_k}$ is not a deterministic channel.
- Nondeterministic channels may be
  - *possibilistic* $I^+ \to \wp_* O \subset \{0,1\}^O$
  - *probabilistic* $I^+ \to \Upsilon O \subset [0,1]^O$
  - *quantum* $I_+ \to \mathbf{\Theta} O \subset \{z \in \mathbb{C} \mid |z| \leq 1\}^O$

(We define the possibilistic and the probabilistic versions later, and do not study the quantum channels here.)

Channeling interference

Lemma

A channel $I^* \xrightarrow{\vec{f}} O^*$ satisfies the noninterference requirement for k if and only if the induced interference channel $I_k^+ \xrightarrow{\widehat{f_k}} \wp O$ is deterministic, i.e. emits at most one output for every input.

$$\begin{array}{ccc} I_k^* & \xrightarrow{\qquad \widehat{f_k} \qquad} & \wp O \\ \uparrow & & \uparrow \\ I_k^+ & \xrightarrow{\qquad\qquad} & O \end{array}$$

Covert channel

Definition

Given a shared channel f, a *covert channel* $\widehat{f}$ is derived from f by one or more subjects in order to implement different flows from those specified for f.

Covert channel

Remarks

- The covert channels in the literature usually extract the *information* about the interference.
- If channels model any resource use in general, then covert channels model any covert resource use, or abuse.
- Many familiar information flow attack patterns apply to other resources besides information.
- Modeling the information flows in a broader context of resource flows seems beneficial both for information security and for resource security.

Example 1

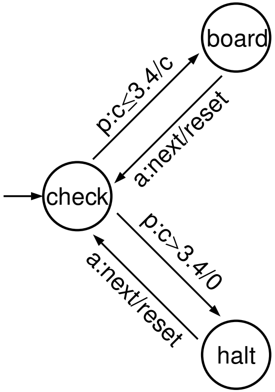
TSA liquid requirement

No more than 3.4oz of liquid carried by passengers.

Example 1

TSA checkpoint process

- Q = {check, board, halt}
- $\mathbb{L} = \{\mathbf{p}\text{assenger} < \mathbf{a}\text{gent}\}$
- I_p = {p:c≤3.4, p:c>3.4}
- I_a = {a:next}
- O = {c, 0, reset}
- θ :



Example 1

TSA checkpoint breach

A group of passengers can form a covert channel by adding

- a new security level for **b**ombers
- a new state **bomb** and
- a new transition where the bombers pool their resources

Example 1

TSA checkpoint breach

A group of passengers can form a covert channel by adding

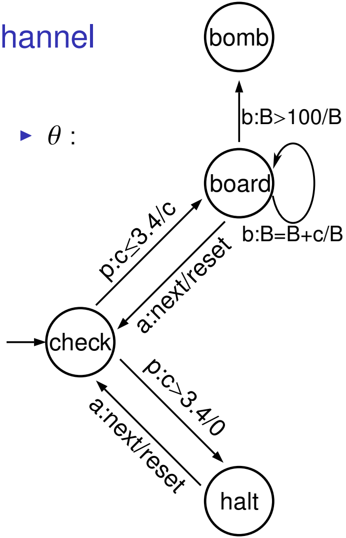
- a new security level for **b**ombers
- a new state **bomb** and
- a new transition where the bombers pool their resources

Attack: n subjects with a clearance **b** join their liquids together into a container **B** to get up to $n \times 3.4$ oz of liquid.

Example 1

TSA checkpoint with covert channel

- Q = {check, board, halt, bomb}
- $\mathbb{L} = \{\textbf{p}\text{assenger} < \textbf{a}\text{gent}, \textbf{p}\text{assenger} < \textbf{b}\text{omber}\}$
- I_p = {p:c≤3.4, p:c>3.4}
- I_a = {a:next}
- I_b = {b:B=B+c}
- O = {c, B, 0, reset}
- θ :



Example 2

Fortress gate

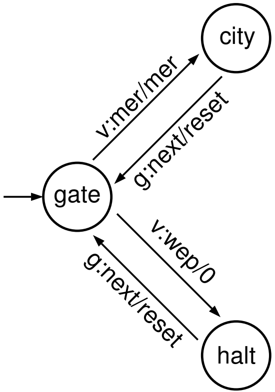
- The fortress wall prevents entry into the city.
- The fortress gate is an entry channel which
  - stops soldiers with **weap**ons
  - lets merchants with **mer**chandise

Example 2

Fortress gate process

- Q = {gate, city, jail}
- $\mathbb{L} = \{\mathbf{visitor} < \mathbf{guard}\}$
- I_v = {v:mer, v:wep}
- I_g = {g:next}
- O = {mer, wep, 0, reset}

- θ :



Example 2

Fortress gate breach

The attackers form a covert channel by adding

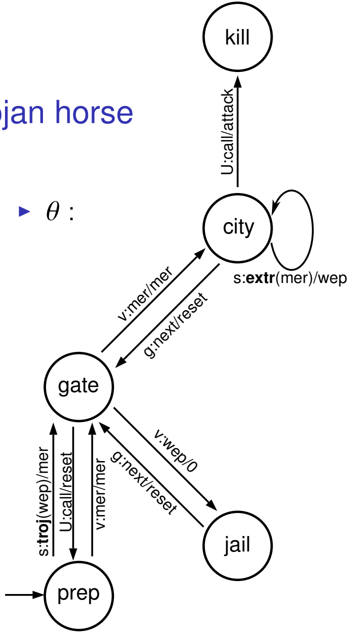
- new security classes **s**oldier and **U**lysses
- new actions
  - **troj**(wep): hide a weapon into a merchandise
  - **extr**(mer): extract a hidden weapon
  - call: call soldiers to kill
- new states to
  - **prep**are for the attack
  - **kill** the inhabitants
- new transitions
  - **prep→gate**
  - **gate→prep**
  - **city→kill**

Example 2

Fortress gate breach with Trojan horse

- Q = {gate, city, jail, prep, kill}
- $\mathbb{L}$ = {**v**isitor < **g**uard, **v**isitor < **s**oldier < **U**lysses}
- I_v = {v:mer, v:wep}
- I_g = {g:next}
- I_s = {s:mer, s:**extr**(mer), s:wep, s:**troj**(wep)}
- I_U = {U:call}
- O = {mer, wep, 0, reset,

- θ :

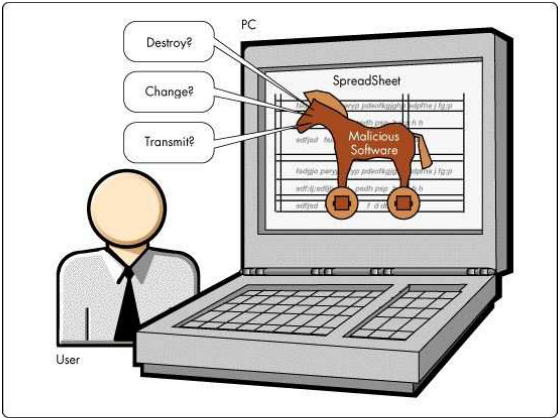


Trojan horse

A covert channel tunneled
through a functional and authenticated channel

Trojan horse

The same attack pattern applies for most channel types



The authentication is often realized through *social engineering*.

Resource security beyond policies

- Norms and policies are established to assure the behaviors of the *specified* subjects participating in a *specified* process
  - Access control limits the interactions through *specified* channels.
  - Noninterference also limits the interactions through *unspecified* channels.

Resource security beyond policies

- But sometimes (in networks) you don't know
  - who you are sharing a resource with, or
  - what exactly is the process of sharing

Resource security beyond policies

- But sometimes (in networks) you don't know
  - who you are sharing a resource with, or
  - what exactly is the process of sharing
- The external influences of *unspecified subjects* in *unknown roles* can only be observed as *nondeterminism*:
  - possibilistic, or
  - probabilistic

Outline

Recall interference channel

- Shared deterministic flows induce posibilistic channels

$$\frac{I^* \xrightarrow{\vec{f}} O^*}{\begin{array}{ccc} I_k^* & \xrightarrow{\widehat{f_k}} & \wp O \\ \vec{x}_k & \longmapsto & \left\{\vec{f}_k\left(\vec{y}\right) \mid \vec{y}\restriction_k = \vec{x}_k\right\} \end{array}}$$

Recall interference channel

- Shared deterministic flows induce posibilistic channels

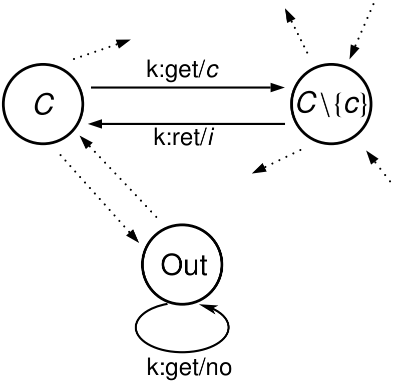
$$\frac{I^* \xrightarrow{\vec{f}} O^*}{\begin{array}{ccc} I_k^* & \xrightarrow{\widehat{f_k}} & \wp O \\ \vec{x}_k & \longmapsto & \left\{\vec{f}_k\left(\vec{y}\right) \mid \vec{y}\restriction_k = \vec{x}_k\right\} \end{array}}$$

- The interferences at the level k of the deterministic channel Q are observed as the possibility of multiple different outputs on the same local input.
  - A deterministic channel f satisfies the noninterference requirement at the level k if and only if the interference channel $\widehat{f_k}$ is deterministic.

Possibilistic channels

Example: Car rental process

- Q$= \wp$(Cars)
- I_k = {k:get,k:ret}, $k \in \mathbb{L}$ = Customers
- O = Cars ∪ Invoices ∪ {Out}
- θ :



Possibilistic channels

Example: Car rental channel

When a subject *k* requests a car, the cars that she may *possibly* get depend on the other subjects' requests:

$$\begin{array}{rcl} \{\text{k:get}, \text{k:ret} \mid k \in \mathbb{L}\}^{+} & \to & \wp(\text{Cars}) \\ \vec{x} \,@\, \text{k:get} & \longmapsto & Y_{\vec{x}} \subseteq \text{Cars} \end{array}$$

where $Y_{\vec{x}} = \text{Cars} \setminus \big(\text{gotten out in } \vec{x} \setminus \text{returned back in } \vec{x}\big)$

Possibilistic channels

Example: Car rental channel

When a subject k requests a car, the cars that she may *possibly* get depend on the other subjects' requests:

$$\begin{array}{rcl} \{\text{k:get}, \text{k:ret} \mid k \in \mathbb{L}\}^{+} & \to & \wp(\text{Cars}) \\ \vec{x} @ \text{k:get} & \longmapsto & Y_{\vec{x}} \subseteq \text{Cars} \end{array}$$

where $Y_{\vec{x}} = \text{Cars} \setminus \left(\text{gotten out in } \vec{x} \setminus \text{returned back in } \vec{x}\right)$

The interference is unavoidable.

What is a possibilistic channel?

Definition

A *possibilistic channel* with

- the *inputs* (or *actions*) from A
- the *outputs* (or *observations*) from B

is a relation

$$f \quad : \quad A^{+} \to \wp B$$

which is prefix closed, in the sense that

$$f(\vec{x} @ a) \neq \emptyset \quad \Longrightarrow \quad f(\vec{x}) \neq \emptyset$$

holds for all $\vec{x} \in A^{+}$ and $a \in A$.

What is a possibilistic channel?

Notation

For a possibilistic channel $I^+ \xrightarrow{f} \wp O$, we write

$$\vec{x} \underset{f}{\vdash} y \quad \text{when} \quad y \in f(\vec{x})$$

What is a possibilistic channel?

Notation

For a possibilistic channel $I^+ \xrightarrow{f} \wp O$, we write

$$\vec{x} \vdash_f y \quad \text{when} \quad y \in f(\vec{x})$$

When there is just one channel, or f is clear from the context, we elide the subscript and write

$$\vec{x} \vdash y \quad \text{when} \quad y \in f(\vec{x})$$

What is a possibilistic channel?

Definition

A *possibilistic channel* with

- the *inputs* (or *actions*) from A
- the *outputs* (or *observations*) from B

is a relation

$$\vdash \quad \subseteq \quad A^{+} \times B$$

which is prefix closed, in the sense that

$$\exists z.\ \vec{x}@a \vdash z \quad \Longrightarrow \quad \exists y.\ \vec{x} \vdash y$$

holds for all $\vec{x} \in A^{+}$ and $a \in A$.

(Possibilistic state machines and processes)

Definition

A *possibilistic state machine* is a map

$$Q \times I \xrightarrow{Nx} \wp(Q \times O)$$

where Q, I, O are finite sets.

(Possibilistic state machines and processes)

Definition

A *possibilistic state machine* is a map

$$Q \times I \xrightarrow{Nx} \wp(Q \times O)$$

where Q, I, O are finite sets.

A *possibilistic process* is a possibilistic state machine with a chosen initial state.

(Possibilistic state machines and processes)

Remark

Possibilistic processes do not in general induce possibilistic channels.

Possibilisitc output machines and processes

Definition

A *possibilistic output machine* is a map

$$Q \times I \xrightarrow{\theta} Q \times \wp O$$

where Q, I, O are finite sets.

A *possibilistic output process* is a possibilistic output machine with a chosen initial state.

Possibilistic output machines and processes)

Remark

Possibilistic output processes induce possibilistic channels.

Trace representation

$$\frac{\dfrac{q \in Q \qquad\qquad Q \times I \xrightarrow{\theta} Q \times \wp O}{I^* \to \wp O}}{I^* \times I \xrightarrow{\theta^*} I^* \times \wp O}$$

Memory

- A possibilistic channel *with no memory* is a binary relation $A \to \wp B$.

Flows through a possibilistic channel

Definition

The *flow* through a channel $f : A^* \to \wp B$ is a partial function

$$\vec{f}_\bullet \quad : \quad A^* \rightharpoonup B^*$$

such that

$$\begin{aligned} \vec{f}_\bullet() &= () \text{ and} \\ \vec{f}_\bullet(\vec{x})\downarrow \;\wedge\; \exists b.\ \vec{x}@a \underset{f}{\vdash} b \quad \Longleftrightarrow \quad & \vec{f}_\bullet(\vec{x}@a) = \vec{f}_\bullet(\vec{x})@b \end{aligned}$$

holds for all $\vec{x} \in A^*$ and $a \in A$.

Possibilistic channels and flows

Remark

- Specifying a deterministic channel was equivalent to specifying a deterministic flow.
- Every possibilistic channel induces many flows.

Possibilistic channels in computation

- Bob and Charlie using the same network at the same clearance level may enter the same inputs in parallel, and observe several outputs at once.
- The possible multiple outputs may be observed by entering the same inputs
  - *sequentially* or
  - *in parallel*.
- The actual computations are abstracted away from the channels.

Possibilistic channels in computation

- Bob enters his inputs into the channel, and observes the interferences with Alice's inputs as the multiple possible outputs.
  - He observes the interference as the different results of the same local actions.

Possibilistic channels in computation

- Bob enters his inputs into the channel, and observes the interferences with Alice's inputs as the multiple possible outputs.
  - He observes the interference as the different results of the same local actions.
- In network computation, the subjects usually don't even know each other.
  - The different possibilities are viewed as the *external choices* made by the unobservable environment.

Security consequence

- A user of a deterministic channel could recognize interference by observing different outputs on the same input:

$$\frac{I^+ \xrightarrow{\vec{f}} O}{I_k^* \xrightarrow{\widehat{f_k}} \wp O}$$

Security consequence

- A user of a deterministic channel could recognize interference by observing different outputs on the same input:

$$\frac{I^+ \xrightarrow{\vec{f}} O}{I_k^* \xrightarrow{\widehat{f_k}} \wp O}$$

- A user of a possibilistic channel can always expect different outputs of the same input:

$$\frac{I^+ \xrightarrow{\vec{f}} \wp O}{I_k^* \xrightarrow{\widehat{f_k}} \wp O}$$

Security consequence

- A user of a deterministic channel could recognize interference by observing different outputs on the same input:

$$\frac{I^+ \xrightarrow{\vec{f}} O}{I_k^* \xrightarrow{\widehat{f_k}} \wp O}$$

- A user of a possibilistic channel can always expect different outputs of the same input:

$$\frac{I^+ \xrightarrow{\vec{f}} \wp O}{I_k^* \xrightarrow{\widehat{f_k}} \wp O}$$

  - The user does not even know who she interferes with
  - The environment makes the *"external choices"*

Security consequence

- Possibilistic channels arise in nature
- Possibilistic models are too crude for security.

Outline

Probabilistic channels

Example: Car rental channel

When a subject k requests to rent a car, the cars that she will *probably* get depend on the other subjects' requests, *and* on the habits of the channel

$$\begin{array}{ccc} \{\text{k:get}, \text{k:ret} \mid k \in \mathbb{L}\}^+ & \to & \Upsilon(\text{Cars}) \\ \vec{x} @ \text{k:get} & \longmapsto & Y_{\vec{x}} \end{array}$$

where $Y_{\vec{x}}$ is a random selection from

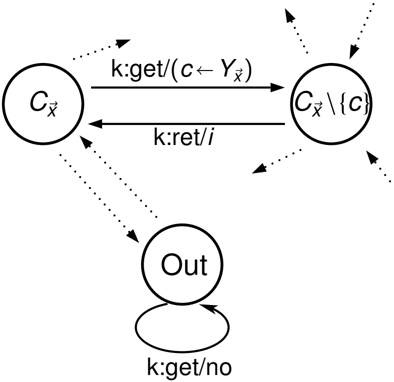
$$\text{Cars} \setminus \left(\text{Taken in } \vec{x} \setminus \text{Returned in } \vec{x}\right)$$

.

Probabilistic channels

Example: Car rental process

- Q$= \wp$(Cars)
- I_k = {k:get,k:ret}, $k \in \mathbb{L}$ = Customers
- O = Cars ∪ Invoices ∪ {Out}
- θ :



What is a probabilistic channel?

Definitions we'll need

A *partial random element* X over a countable set A is given by a subprobability distribution υ_X over A, i.e. a function

$$\upsilon_X \; : \; A \; \rightarrow \; [0,1]$$

such that $\sum_{x \in A} \upsilon(x) \leq 1$.

What is a probabilistic channel?

Definitions we'll need

A *partial random element* X over a countable set A is given by a subprobability distribution υ_X over A, i.e. a function

$$\upsilon_X \; : \; A \; \to \; [0,1]$$

such that $\sum_{x \in A} \upsilon(x) \leq 1$.

We usually write

$$\upsilon_X(x) \quad = \quad \upsilon(X = x)$$

What is a probabilistic channel?

Definitions we'll need

The set of all partial random elements over the set X is

$$\Upsilon A = \left\{ \upsilon(X = -) : A \to [0,1] \mid \sum_{x \in A} \upsilon(X = x) \le 1 \right\}$$

What is a probabilistic channel?

Definitions we'll need

A *partial random function* is a function $f : A \to \Upsilon B$.

What is a probabilistic channel?

Definition

A *probabilistic channel* with

- the *inputs* (or *actions*) from A
- the *outputs* (or *observations*) from B

is partial random function

$$f \quad : \quad A^+ \to \Upsilon B$$

which is prefix closed, in the sense that

$$\sum_{z \in B} \upsilon\big(f(\vec{x}@a) = z\big) \quad \leq \quad \sum_{y \in B} \upsilon\big(f(\vec{x}) = y\big)$$

for all $\vec{x} \in A^+$ and $a \in A$.

What is a probabilistic channel?

Notation

For a probabilistic channel $I^+ \xrightarrow{f} \Upsilon O$, we write

$$\left[\vec{x} \underset{f}{\vdash} y\right] \quad = \quad \upsilon\Big(f(\vec{x}) = y\Big)$$

What is a probabilistic channel?

Notation

For a probabilistic channel $I^+ \xrightarrow{f} \Upsilon O$, we write

$$\left[\vec{x} \underset{f}{\vdash} y\right] \quad = \quad \upsilon\Big(f(\vec{x}) = y\Big)$$

When there is just one channel, or f is clear from the context, we elide the subscript and write

$$\left[\vec{x} \vdash y\right] \quad = \quad \upsilon\Big(f(\vec{x}) = y\Big)$$

What is a probabilistic channel?

Notation

For a probabilistic channel $I^+ \xrightarrow{f} \Upsilon O$, we write $\left[\vec{x} \vdash Y\right]$ and view Y as the source where

$$\upsilon(Y = y) \quad = \quad \upsilon(f(\vec{x}) = y)$$

for the given history $\vec{x} \in I^+$

What is a probabilistic channel?

Definition

A *probabilistic channel* with

- the *inputs* (or *actions*) from A
- the *outputs* (or *observations*) from B

is a partial random element

$$\left[- \vdash -\right] \quad \in \quad \Upsilon(A^{+} \times B)$$

which is prefix closed, in the sense that

$$\sum_{z \in B} \left[\vec{x}@a \vdash z\right] \quad \leq \quad \sum_{y \in B} \left[\vec{x} \vdash y\right]$$

holds for all $\vec{x} \in A^{+}$ and $a \in A$.

Memory

- A probabilistic channel *with no memory* is a partial random function $A \to \Upsilon B$.

Information theoretic channel

Any probabilistic channel can be extended

$$\frac{I^+ \xrightarrow{f} \Upsilon O}{\begin{array}{ccc} \Upsilon\left(I^+\right) & \xrightarrow{\overline{f}} & \Upsilon O \\ \vec{X} & \longmapsto & Y \end{array}}$$

where

$$\upsilon\big(Y = y\big) \quad = \quad \sum_{\vec{x} \in I^+} \upsilon\big(\vec{X} = \vec{x}\big) \cdot \upsilon\big(f(\vec{x}) = y\big)$$

Information theoretic channel

Notation

The extensions align with the usual information theoretic channel notation

$$\left[X_1, X_2, \ldots, X_n \vdash Y\right] \quad = \quad \upsilon\left(\overline{f}(X_1, X_2, \ldots X_n) = Y\right)$$

Probabilistic interference channel

Shared channels induce interference channels

$$\frac{I^{+} \xrightarrow{[\vdash]} \Upsilon O}{I_k^{+} \xrightarrow{[\vdash]_k} \Upsilon O}$$

where

$$\left[\vec{x}_k \vdash y\right]_k = \sum_{\vec{x} \in I^{+}} \upsilon(\vec{x}_k = \vec{x}\restriction_k) \cdot \left[\vec{x} \vdash y\right]$$

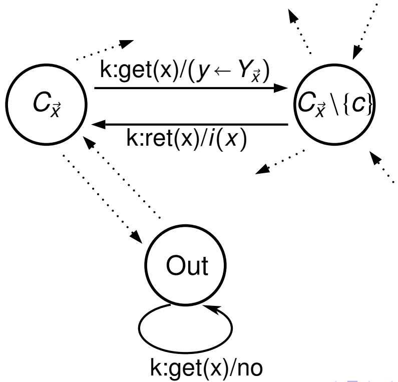
Probabilistic interference channel

Probabilistic interference is exploited through Bayesian inference.

Has Alice rented a car?

Example: Car rental process

- Q= $\wp$(Cars), Cars = {9 toyotas, 1 porsche}
- I_k = {k:get(x),k:ret(x)}, $k \in$ {Alice, Bob}$\cup$ Others, $x \in$ Cars
- O = Cars $\cup$ Invoices $\cup$ {Out}
- θ :



Has Alice rented a car?

Covert channel

- Bob wonders whether Alice is in town.
  - She always rents a car.
- Bob knows that Alice likes to rent the porsche.
  - She does not get it one in 5 times.
- Bob requests a rental and gets the porsche.
  - How likely is it that Alice is in town?

Has Alice rented a car?

Bob considers the following events

a: Alice has rented a car

- Alice:get(car) occurs in $\vec{x}$

m: The porsche is available

- Bob:get(porsche) results in porsche $\leftarrow Y_{\vec{x}}$

Has Alice rented a car?

Bob's beliefs

- $\upsilon(m \mid a) = \frac{1}{5}$
  - If Alice is in town, then the chance that the porsche is available is $\frac{1}{5}$.
- $\upsilon(m \mid \neg a) = \frac{9}{10}$
  - If Alice is not in town, then the chance that the porsche is available is $\frac{9}{10}$.
- $\upsilon(a) = \frac{1}{2}$
  - A priori, the chance that Alice is in town is 50-50.

Has Alice rented a car?

Bob's reasoning

- $\upsilon(a \mid m) = \frac{\upsilon(a,m)}{\upsilon(m)}$

Has Alice rented a car?

Bob's reasoning

- $\upsilon(a \mid m) = \frac{\upsilon(a,m)}{\upsilon(m)}$
  - $\upsilon(a,m) = \upsilon(m|a) \cdot \upsilon(a) = \frac{1}{5} \cdot \frac{1}{2} = \frac{1}{10}$
  - $\upsilon(m) = \upsilon(a,m) + \upsilon(\neg a, m)$

Has Alice rented a car?

Bob's reasoning

- $\upsilon(a \mid m) = \frac{\upsilon(a,m)}{\upsilon(m)}$
  - $\upsilon(a,m) = \upsilon(m|a) \cdot \upsilon(a) = \frac{1}{5} \cdot \frac{1}{2} = \frac{1}{10}$
  - $\upsilon(m) = \upsilon(a,m) + \upsilon(\neg a, m)$
    - $\upsilon(m, \neg a) = \upsilon(m|\neg a) \cdot \upsilon(\neg a) = \frac{9}{10} \cdot \frac{1}{2} = \frac{9}{20}$

Has Alice rented a car?

Bob's reasoning

- $\upsilon(a \mid m) = \frac{\upsilon(a,m)}{\upsilon(m)}$
  - $\upsilon(a, m) = \upsilon(m|a) \cdot \upsilon(a) = \frac{1}{5} \cdot \frac{1}{2} = \frac{1}{10}$
  - $\upsilon(m) = \upsilon(a, m) + \upsilon(\neg a, m)$
    - $\upsilon(m, \neg a) = \upsilon(m|\neg a) \cdot \upsilon(\neg a) = \frac{9}{10} \cdot \frac{1}{2} = \frac{9}{20}$
  - $\upsilon(m) = \frac{1}{10} + \frac{9}{20} = \frac{11}{20}$

Has Alice rented a car?

Bob's reasoning

- $\upsilon(a \mid m) = \frac{\upsilon(a,m)}{\upsilon(m)}$
  - $\upsilon(a,m) = \upsilon(m|a) \cdot \upsilon(a) = \frac{1}{5} \cdot \frac{1}{2} = \frac{1}{10}$
  - $\upsilon(m) = \upsilon(a,m) + \upsilon(\neg a, m)$
    - $\upsilon(m, \neg a) = \upsilon(m|\neg a) \cdot \upsilon(\neg a) = \frac{9}{10} \cdot \frac{1}{2} = \frac{9}{20}$
  - $\upsilon(m) = \frac{1}{10} + \frac{9}{20} = \frac{11}{20}$
- $\upsilon(a \mid m) = \frac{\frac{1}{10}}{\frac{11}{20}} = \frac{2}{11}$

Has Alice rented a car?

Bob's reasoning

- $\upsilon(a \mid m) = \frac{\upsilon(a,m)}{\upsilon(m)}$
  - $\upsilon(a, m) = \upsilon(m|a) \cdot \upsilon(a) = \frac{1}{5} \cdot \frac{1}{2} = \frac{1}{10}$
  - $\upsilon(m) = \upsilon(a, m) + \upsilon(\neg a, m)$
    - $\upsilon(m, \neg a) = \upsilon(m|\neg a) \cdot \upsilon(\neg a) = \frac{9}{10} \cdot \frac{1}{2} = \frac{9}{20}$
  - $\upsilon(m) = \frac{1}{10} + \frac{9}{20} = \frac{11}{20}$
- $\upsilon(a \mid m) = \frac{\frac{1}{10}}{\frac{11}{20}} = \frac{2}{11}$

If the porsche is available, then the chance that Alice is in town is 2 in 11.

Has Alice rented a car?

Bob's learning

- Bob's *input information* (or *prior belief*) before renting the car was that the chance that Alice was in town was $\frac{1}{2}$.
- Bob's *channel information* (or *posterior belief*) after renting the car was that the chance that Alice was in town was $\frac{2}{11}$.

Has Alice rented a car?

Quantifying noninterference

- A channel satisfies the *k*-noninterference requirement if *k* learns nothing from using it:

$$\text{channel information} \quad = \quad \text{input information}$$

Has Alice rented a car?

Quantifying noninterference

- A channel satisfies the *k*-noninterference requirement if *k* learns nothing from using it:

$$\text{posterior belief} \quad = \quad \text{prior belief}$$

Has Alice rented a car?

Quantifying noninterference

- A channel satisfies the k-noninterference requirement if k learns nothing from using it:

$$\text{posterior belief} \quad = \quad \text{prior belief}$$

- The degree of the channel noninterference is

$$\frac{\text{posterior belief}}{\text{prior belief}} \leq 1 \quad \text{or} \quad \frac{\text{prior belief}}{\text{posterior belief}} \leq 1$$

Has Alice rented a car?

Quantifying noninterference

- A channel satisfies the k-noninterference requirement if k learns nothing from using it:

$$\text{posterior belief} \quad = \quad \text{prior belief}$$

- The degree of the channel noninterference is

$$\text{for the rental channel:} \qquad \frac{\frac{2}{11}}{\frac{1}{2}} = \frac{4}{11}$$

Outline

Recall noninterference

Definition

A shared deterministic channel $I^+ \xrightarrow{f} O$ satisfies the *noninterference* requirement at the level k if for all states of the world $\vec{x}, \vec{y} \in I^*$ holds

$$\vec{x} \lfloor k \rfloor \vec{y} \quad \Longrightarrow \quad \vec{x} \lceil f_k \rceil \vec{y}$$

where

$$\vec{x} \lfloor k \rfloor \vec{y} \quad \Longleftrightarrow \quad \vec{x}\upharpoonright_k = \vec{y}\upharpoonright_k$$
$$\vec{x} \lceil f_k \rceil \vec{y} \quad \Longleftrightarrow \quad f_k(\vec{x}) = f_k(\vec{y})$$

Recall noninterference

Definition

A shared deterministic channel $I^+ \xrightarrow{f} O$ satisfies the *noninterference* requirement at the level k if for all states of the world $\vec{x}, \vec{y} \in I^*$ holds

$$\vec{x} \lfloor k \rfloor \vec{y} \implies \vec{x} \lceil f_k \rceil \vec{y}$$

where

$$\vec{x} \lfloor k \rfloor \vec{y} \iff \vec{x}\restriction_k = \vec{y}\restriction_k \qquad \leftsquigarrow \text{input view}$$

$$\vec{x} \lceil f_k \rceil \vec{y} \iff f_k(\vec{x}) = f_k(\vec{y}) \qquad \leftsquigarrow \text{channel view}$$

Quantified noninterference

Definition

A shared probabilistic channel $I^+ \stackrel{f}{\to} \Upsilon O$ satisfies the *noninterference* requirement at the level k if for all states of the world $\vec{x}, \vec{y} \in I^*$ holds

$$\vec{x}\lfloor k \rfloor \vec{y} \quad \leq \quad \vec{x}\lceil f_k \rceil \vec{y}$$

where

$$\vec{x}\lfloor k \rfloor \vec{y} \quad = \quad \bigwedge_{\vec{x}_k \in I_k^+} \left| \frac{\upsilon\left(\vec{x}\restriction_k = \vec{x}_k\right)}{\upsilon\left(\vec{y}\restriction_k = \vec{x}_k\right)} \right|$$

$$\vec{x}\lceil f_k \rceil \vec{y} \quad = \quad \bigwedge_{z \in O} \left| \frac{\upsilon\left(f_k(\vec{x}) = z\right)}{\upsilon\left(f_k(\vec{y}) = z\right)} \right|$$

Quantified interference

Definition

The amount of interference that a user at the level k of the shared probabilistic channel $I^+ \xrightarrow{f} \Upsilon O$ can extract to distinguish the histories $\vec{x}, \vec{y} \in I^+$ is

$$\begin{aligned} \iota(\vec{x},\vec{y}) &= -\log \left| \frac{\vec{x}\lfloor k \rfloor \vec{y}}{\vec{x}\lceil f_k \rceil \vec{y}} \right| \\ &= \left| \log\left(\vec{x}\lfloor k \rfloor \vec{y}\right) - \log\left(\vec{x}\lceil f_k \rceil \vec{y}\right) \right| \end{aligned}$$

where…

Notation

- The *normalized ratio* is defined

$$\left|\frac{x}{y}\right| = \begin{cases} \frac{x}{y} & \text{if } x \le y \\ \frac{y}{x} & \text{if } x > y \end{cases}$$

Notation

- The *normalized ratio* is defined

$$\left|\frac{x}{y}\right| = \begin{cases} \frac{x}{y} & \text{if } x \leq y \\ \frac{y}{x} & \text{if } x > y \end{cases}$$

- It is the multiplicative version of the more familiar *absolute difference*

$$|x - y| = \begin{cases} y - x & \text{if } x \leq y \\ x - y & \text{if } x > y \end{cases}$$

Connection

- from absolute value to normalized ratio

$$\vdash\!\frac{x}{y}\!\dashv \quad = \quad 2^{|\log x - \log y|}$$

- from normalized ratio to absolute value

$$|x - y| \quad = \quad \log \vdash\!\frac{2^x}{2^y}\!\dashv$$

Question

- But why is this the right way to quantify noninterference?

Question

- But why is this the right way to quantify noninterference?
- In which sense do the numbers $\vec{x}\lfloor k \rfloor \vec{y}$ and $\vec{x}\lceil f_k \rceil \vec{y}$ quantify and generalize the relations $\vec{x}\lfloor k \rfloor \vec{y}$ and $\vec{x}\lceil f_k \rceil \vec{y}$

Quantified equivalences

Recall partial equivalence relations

An equivalence relation over a set A is a function

$$A \times A \xrightarrow{R} \{0, 1\}$$

such that

$$xRy = yRx \qquad\qquad xRy \wedge yRz \leq xRz$$

Quantified equivalences

Equivalence kernel

An *equivalence kernel* over a set A is a function

$$A \times A \xrightarrow{R} [0,1]$$

such that

$$xRy = yRx \qquad\qquad xRy \cdot yRz \leq xRz$$

Quantified equivalences

Equivalence kernel over ΥA

Recall the set of partial random elements over A

$$\Upsilon A = \left\{ \upsilon(X = -) : A \to [0,1] \mid \sum_{x \in A} \upsilon(X = x) \leq 1 \right\}$$

Quantified equivalences

Equivalence kernel over ΥA

Recall the set of partial random elements over A

$$\Upsilon A \quad = \quad \left\{ \upsilon(X = -) : A \to [0,1] \mid \sum_{x \in A} \upsilon(X = x) \leq 1 \right\}$$

It comes equipped with the canonical equivalence kernel, defined

$$[X \sim Y] \quad = \quad \bigwedge_{a \in A} \left| \frac{\upsilon(X = a)}{\upsilon(Y = a)} \right|$$

Quantified equivalences

Exercise

Show that $[X \sim Y]$ is an equivalence kernel, i.e. that it satisfies the quantified symmetry and transitivity, as defined 3 slides ago.

Quantified equivalences

Input view is an equivalence kernel

k's prior belief tells how likely is each $\vec{x}_k \in I_k^+$ to be the local view of any $\vec{y} \in I^+$, which is given by a partial random element

$$\upsilon(\vec{x}_k = \vec{x}\restriction_k) : \; I^+ \quad \rightharpoonup \quad [0,1]$$

Quantified equivalences

Input view is an equivalence kernel

k's prior belief tells how likely is each $\vec{x}_k \in I_k^+$ to be the local view of any $\vec{y} \in I^+$, which is given by a partial random element

$$\upsilon(\vec{x}_k = \vec{x}\restriction_k) : \; I^+ \quad \rightharpoonup \quad [0,1]$$

Rearranging k's beliefs into partial random elements over I_k^+

$$\upsilon(\vec{x}\restriction_k = \vec{x}_k) : \; I_k^+ \quad \rightharpoonup \quad [0,1]$$

we define the input view

$$\vec{x}\lfloor k \rfloor \vec{y} \quad = \quad \bigwedge_{\vec{x}_k \in I_k^+} \left| \frac{\upsilon\left(\vec{x}\restriction_k = \vec{x}_k\right)}{\upsilon\left(\vec{y}\restriction_k = \vec{x}_k\right)} \right|$$

Quantified equivalences

Remark

Note that for every $\vec{x}_k \in I^+$ and every $\vec{y} \in I^+$ holds

$$\vec{x}_k \lfloor k \rfloor \vec{y} \quad = \quad \upsilon\left(\vec{x}_k = \vec{y}\upharpoonright_k\right)$$

Quotients

Recall that every partial function $A \stackrel{f}{\rightharpoondown} B$ induces the partial equivalence relation on A

$$x(f)y \iff f(x) = f(y)$$

Quotients

Recall that every partial function $A \xrightarrow{f} B$ induces the partial equivalence relation on A

$$x(f)y \iff f(x) = f(y)$$

Analogously, every partial stochastic function $A \xrightarrow{f} \Upsilon B$ induces the equivalence kernel

$$x(f)y = \bigwedge_{b \in B} \left| \frac{\upsilon(f(x) = b)}{\upsilon(f(y) = b)} \right|$$

Channel view

Hence

$$\vec{x} \lceil f_k \rceil \vec{y} \quad = \quad \bigwedge_{z \in O} \left| \frac{\upsilon\left(f_k(\vec{x}) = z\right)}{\upsilon\left(f_k(\vec{y}) = z\right)} \right|$$

. . . and hence noninterference

Definition

A shared probabilistic channel $I^+ \xrightarrow{f} \Upsilon O$ satisfies the *noninterference* requirement at the level k if for all states of the world $\vec{x}, \vec{y} \in I^*$ holds

$$\vec{x} \lfloor k \rfloor \vec{y} \quad \leq \quad \vec{x} \lceil f_k \rceil \vec{y}$$

where

$$\vec{x} \lfloor k \rfloor \vec{y} \quad = \quad \bigwedge_{\vec{x}_k \in I_k^+} \left| \frac{\upsilon\left(\vec{x}\restriction_k = \vec{x}_k\right)}{\upsilon\left(\vec{y}\restriction_k = \vec{x}_k\right)} \right|$$

$$\vec{x} \lceil f_k \rceil \vec{y} \quad = \quad \bigwedge_{z \in O} \left| \frac{\upsilon\left(f_k(\vec{x}) = z\right)}{\upsilon\left(f_k(\vec{y}) = z\right)} \right|$$

. . . and quantified interference

Definition

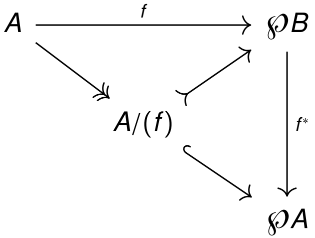
The amount of interference that a user at the level k of the shared probabilistic channel $I^+ \xrightarrow{f} \Upsilon O$ can extract to distinguish the histories $\vec{x}, \vec{y} \in I^+$ is

$$\begin{aligned} \iota(\vec{x}, \vec{y}) &= -\log \left| \frac{\vec{x} \lfloor k \rfloor \vec{y}}{\vec{x} \lceil f_k \rceil \vec{y}} \right| \\ &= \left| \log \left(\vec{x} \lfloor k \rfloor \vec{y} \right) - \log \left(\vec{x} \lceil f_k \rceil \vec{y} \right) \right| \end{aligned}$$

(An aside about the partitions)

The partition induced by the kernel of any function $A \stackrel{f}{\to} B$ or relation $A \stackrel{f}{\to} \wp B$ are obtained as the image of the composite with its inverse image

$$\begin{array}{ccc} \wp B & \xrightarrow{f^*} & \wp A \\ V & \longmapsto & \bigcup \{U \subseteq A \mid f(U) \subseteq V\} \end{array}$$



(An aside about the partitions)

The same construction lifts to *stochastic* functions, which are the partial random functions $A \xrightarrow{f} \Upsilon B$ such that for every $b \in B$ holds

$$f_\bullet(b) \quad = \quad \sum_{a \in A} f_a(b) \quad < \quad \infty$$

(An aside about the partitions)

The same construction lifts to *stochastic* functions, which are the partial random functions $A \stackrel{f}{\to} \Upsilon B$ such that for every $b \in B$ holds

$$f_\bullet(b) \quad = \quad \sum_{a \in A} f_a(b) \quad < \quad \infty$$

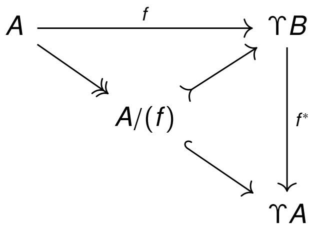
Hence

$$\frac{A \stackrel{f}{\to} \Upsilon B}{\begin{array}{ccc} B & \stackrel{\widetilde{f}}{\to} & \Upsilon A \\ b & \longmapsto & \frac{1}{f_\bullet(b)} \cdot \lambda a.\, f_a(b) \end{array}}$$

(An aside about the partitions)

The partition induced by the kernel of any stochastic function $A \xrightarrow{f} \Upsilon B$ are obtained as the image of the composite with its inverse image

$$\begin{array}{ccc} \Upsilon B & \xrightarrow{f^*} & \Upsilon A \\ \beta & \longmapsto & \sum_{b \in B} \beta(b) \cdot \widetilde{f_b} \end{array}$$



Outline

What did we learn?

- Interference is exploited through a special family of *covert channels*.

- Other failures of channel security are realized through other types of covert channels.

- The external interferences[1] on the functioning of a channel manifest themselves though *many possible* outputs on the same input.
  - Hence *possibilistic processes*.

- Gathering information about the external interferences requires *quantifying* the *probabilities* of the various possible inputs.
  - *Possibilistic processes* allow quantifying interference.

[1] by the environment, or by unobservable subject

Statistical disclosure is a probabilistic channel

- Statistical disclosure outputs data from a family of databases randomized as to preserve privacy and anonymity.

Statistical disclosure is a probabilistic channel

- Statistical disclosure outputs data from a family of databases randomized as to preserve privacy and anonymity.
- A randomization method of statistical disclosure can be viewed as a shared probabilistic channel.

Differential privacy is a bound on interference

- Security of statistical disclosure is a difficult problem, recently solved in terms of *differential privacy*.

Differential privacy is a bound on interference

- Security of statistical disclosure is a difficult problem, recently solved in terms of *differential privacy*.
- Differential privacy turns out to be a method for **limiting the amount of interference**, as defined above.

Huh?

- But what is differential privacy?

Huh?

- But what is differential privacy?
- We first need to define privacy, don't we?