Computing the Leakage of Information-Hiding Systems

Miguel E. Andrés
Radboud University, The Netherlands

Catuscia Palamidessi
INRIA and LIX, France

Peter Van Rossum
Radboud Univeristy, The Netherlands

Geoffrey Smith
SCIS, USA

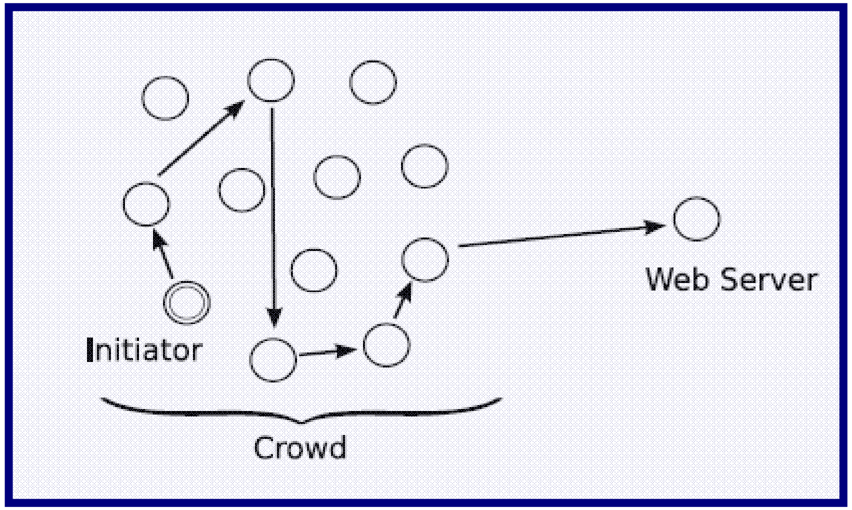
Motivation

- Information Hiding

  The problem of constructing protocols or programs that protect sensitive information from being deduced by some adversary

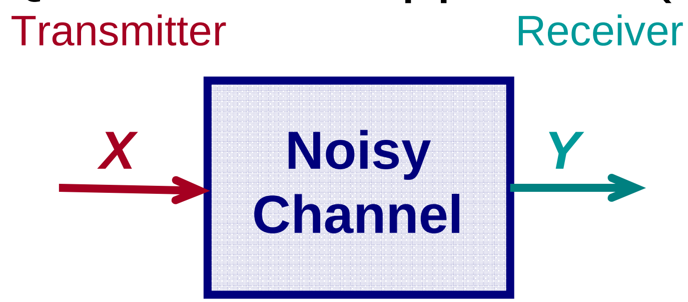
  - **Anonymity**: Design mechanisms to prevent an observer of network traffic from deducing who is comunicating
  - **Secure Information Flow**: Prevent programs from leaking their secret input to an observer of their public output

- Example: Crowds



Motivation

- Quantitative Approach (Information Theory)

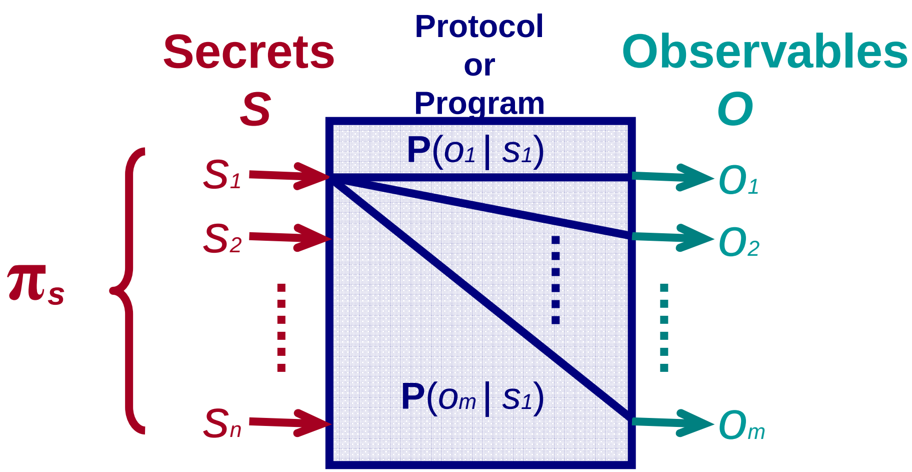


P(y | x) inherent fixed property of the communication channel

	y_1	...	y_n
x_1	$P(y_1 \vert x_1)$	...	$P(y_n \vert x_1)$
⋮	⋮		
x_m	$P(y_1 \vert x_m)$		$P(y_n \vert x_m)$

Channel Matrix

- IHS's as noisy channels



Noisy Channel

	o_1	...	o_n
s_1	$P(o_1 \vert s_1)$	...	$P(o_n \vert s_1)$
⋮	⋮		
s_m	$P(o_1 \vert s_m)$		$P(o_n \vert s_m)$

Channel Matrix C

Motivation

- Information Leakage
  - Vulnerability (in one try)
    - A priori vulnerability

$$V(S)=\max_{s} \pi(s)$$

    - A posteriori vulnerability

$$V(S|O) = \sum_{o} \max_{s} \mathbf{P}(s|o)\times\mathbf{P}(o) = \sum_{o} \max_{s} \mathbf{C}(o|s)\times\pi(s)$$

  - Multipilicative Leakage

$$L_{\times}(C,\pi) = V(S|O) \,/\, V(S)$$

  - Additive Leakage

$$L_{+}(C,\pi) = V(S|O) - V(S)$$

  - Maximum Leakage

$$ML_{\times}(C) = \max_{\pi\in D(S)} L_{\times}(C,\pi) \quad \text{and} \quad ML_{+}(C) = \max_{\pi\in D(S)} L_{+}(C,\pi)$$

*Leakage is defined in terms of the channel matrix **C**!*

Motivation

- What we do (contributions)
  - Model IHS's using automata
  - We present two techniques to compute the channel matrix and leakage of an IHS
    - Reachability Analysis
    - Quantitative Counterexample Generation
      - Also providing approximation
      - Also providing feedback for debugging
  - Show how to use our techniques to compute and approximate leakage of different different form of IHS's
  - Show that for interactiving IHS's the definition of associated channel proposed in literature is not sound.
    - However, we note that it is still possible to define its leakage in a consistent way and show that our methods extend smoothly to this case.

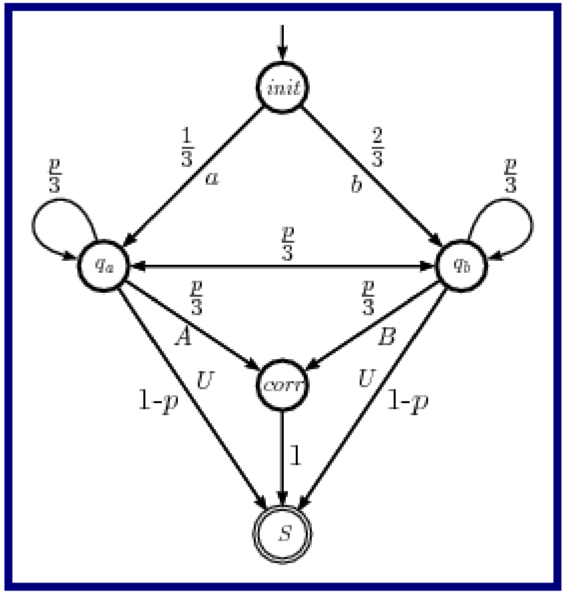
Overview

- Motivation
- Information-hiding systems as automata
- Reachability analysis approach
- Iterative approach
  - Regular expressions techniques
  - SCC analysis technique
  - Identifying high-leakage sources
- Information-hiding systems with variable a priori
- Interactive information-hiding systems
- Future work

Information-hiding systems as automata

- Probabilistic automata

$\mathcal{M} = (Q, A, \delta)$ where
- Q is a finite set of ***states***
- A a finite set of ***actions***
- $\delta : Q \to D(A \times Q)$ is the ***transition function***



Paths represent possible *evolutions* of the automaton, each *path* has an associated *probability*

$$init \xrightarrow{a} q_a \xrightarrow{A} corr \xrightarrow{\tau} S$$

$$\mathbf{P}(init \xrightarrow{a} q_a \xrightarrow{A} corr \xrightarrow{\tau} S) = \tfrac{1}{3} \cdot \tfrac{p}{3} \cdot 1$$

- Information-hiding systems

- $\mathcal{I} = (\mathcal{M}, A_S, A_O, A_T)$ where
  - $\mathcal{M} = (Q, A, \delta)$ is a probabilistic automaton
  - A_S, A_O, and A_T are disjoint sets of *secret*, *observable*, and ***internal*** actions
  - δ *satisfies:*
    - *Secret actions* can occur only at the *beginning*
    - Only *internal actions* can occur in *cycles*
- Assume a *known* a priori distribution π

Overview

- Motivation
- Information-hiding systems as automata
- **Reachability analysis approach**
- Iterative approach
  - Regular expressions techniques
  - SCC analysis technique
  - Identifying high-leakage sources
- Information-hiding systems with variable a priori
- Interactive information-hiding systems
- Future work

Reachability analysis approach

- Goal: compute channel matrix *C*

	o_1	...	o_n
s_1	P(o_1|s_1)	...	P(o_n|s_1)
⋮	⋮		
s_m	P(o_1|s_m)		P(o_n|s_m)

Channel Matrix

P(o_i|s_j)=P(o_i□s_j)/π(s_j)

	o_1	...	o_n
s_1	P(o_1□s_1)	...	P(o_n□s_1)
⋮	⋮		
s_m	P(o_1□s_m)		P(o_n□s_m)

Matrix of joint Probabilities

- Solution: system of linear equations

Note P(o|s)=P(o□s)/π(s)

We nee ... d s)

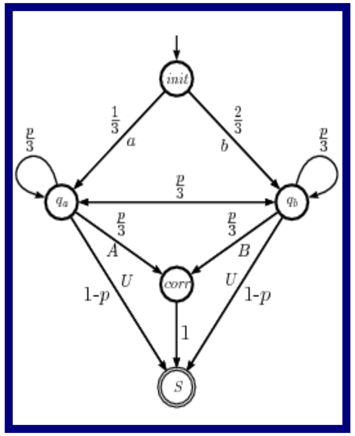
Lema: Let $\mathbf{P}_q(\lambda)$ = Probability of seeing λ ($\in (A_s \cup A_o)^\star$) from state q. Then we have

$$\mathbf{P}_{q_f}(\epsilon) = 1$$
$$\mathbf{P}_{q_f}(\lambda) = 0 \quad \textit{for } \lambda \neq \epsilon$$
$$\mathbf{P}_q(\lambda) = \sum_{h \in \Sigma_\tau} \sum_{q' \in \mathrm{succ}(q)} \alpha(q)(h, q') \cdot \mathbf{P}_{q'}(\lambda) \quad \textit{for } q \neq q_f$$
$$\mathbf{P}_q(\lambda) = \sum_{q' \in \mathrm{succ}(q)} \alpha(q)(\mathrm{first}(\lambda), q') \cdot \mathbf{P}_{q'}(\mathrm{tail}(\lambda)) + \sum_{h \in \Sigma_\tau} \alpha(q)(h, q') \cdot \mathbf{P}_{q'}(\lambda) \quad \textit{for } \lambda \neq \epsilon \textit{ and } q \neq q_f$$

Reachability analysis approach

- Example Notation: $\mathbf{P}_q(\lambda) = x_q^{\lambda}$

$$
\begin{array}{lll}
x_{init}^{aA} = \frac{1}{3} \cdot x_{q_a}^{A}, & x_{q_a}^{A} = \frac{p}{3} \cdot x_{q_a}^{A} + \frac{p}{3} \cdot x_{q_b}^{A} + \frac{p}{3} \cdot x_{corr}^{\epsilon}, & x_{corr}^{A} = x_{S}^{A}, \\
x_{init}^{bA} = \frac{2}{3} \cdot x_{q_b}^{A}, & x_{q_b}^{A} = \frac{p}{3} \cdot x_{q_a}^{A} + \frac{p}{3} \cdot x_{q_b}^{A} + \frac{p}{3} \cdot x_{corr}^{A}, & x_{S}^{A} = 0, \\
x_{init}^{aB} = \frac{1}{3} \cdot x_{q_a}^{B}, & x_{q_a}^{B} = \frac{p}{3} \cdot x_{q_a}^{B} + \frac{p}{3} \cdot x_{q_b}^{B} + \frac{p}{3} \cdot x_{corr}^{B}, & x_{corr}^{B} = x_{S}^{B}, \\
x_{init}^{bB} = \frac{2}{3} \cdot x_{q_b}^{B}, & x_{q_b}^{B} = \frac{p}{3} \cdot x_{q_a}^{B} + \frac{p}{3} \cdot x_{q_b}^{B} + \frac{p}{3} \cdot x_{corr}^{\epsilon}, & x_{S}^{B} = 0, \\
x_{init}^{aU} = \frac{1}{3} \cdot x_{q_a}^{U}, & x_{q_a}^{U} = \frac{p}{3} \cdot x_{q_a}^{U} + \frac{p}{3} \cdot x_{q_b}^{U} + (1-p) \cdot x_{S}^{\epsilon}, & x_{corr}^{\epsilon} = x_{S}^{\epsilon}, \\
x_{init}^{bU} = \frac{2}{3} \cdot x_{q_b}^{U}, & x_{q_b}^{U} = \frac{p}{3} \cdot x_{q_a}^{U} + \frac{p}{3} \cdot x_{q_b}^{U} + (1-p) \cdot x_{S}^{\epsilon}, & x_{S}^{\epsilon} = 1.
\end{array}
$$



$$
\begin{array}{lll}
x_{init}^{aA} = \frac{7}{40}, & x_{init}^{aB} = \frac{3}{40}, & x_{init}^{aU} = \frac{1}{12}, \\
x_{init}^{bA} = \frac{3}{20}, & x_{init}^{bB} = \frac{7}{20}, & x_{init}^{bU} = \frac{1}{6}.
\end{array}
$$

Solution

	A	B	U
a	21/40	9/40	1/4
b	9/40	21/20	1/4

Channel Matrix

- Complexity
  - O ((|obs| × |Q|)³) In general
  - O (|obs| × |Q|³) Some Scenarios (e.g observables at the end)

Overview

- Motivation
- Information-hiding systems as automata
- Reachability analysis approach
- **Iterative approach**
  - **Regular expressions techniques**
  - **SCC analysis technique**
  - **Identifying high-leakage sources**
- Information-hiding systems with variable a priori
- Interactive information-hiding systems
- Future work

Iterative approach

- Motivation
  - Borrow ideas and tools from prob counterexample generation
  - Provide approximation (with upper and low bounds)
  - It allows to identify high-leak[illegible]

$$\mathbf{P}(\lambda) = \mathbf{P}(\{\sigma \in \mathrm{Paths}(\mathcal{M}) \mid \sigma \models \lambda\})$$

	o_1	...	o_n
s_1	$P(o_1 \mid s_1)$	...	$P(o_n \mid s_1)$
⋮	⋮		
s_m	$P(o_1 \mid s_m)$		$P(o_n \mid s_m)$

- Idea
- Partial Matrices

	o_1	...	o_n
s_1	$P(o_1 \mid s_1)$	...	$P(o_n \mid s_1)$
⋮	⋮		
s_m	$P(o_1 \mid s_m)$		$P(o_n \mid s_m)$

$C_0(o \mid s) = 0$, ... $C_{k+1}(o \mid s) = \begin{cases} C_k(o \mid s) + \mathbf{P}(\sigma_{k+1}) & \text{if } o\text{-trace}(\sigma_{k+1}) = o \text{ and } s\text{-trace}(\sigma_{k+1}) = s \\ C_k(o \mid s) & \text{otherwise} \end{cases}$

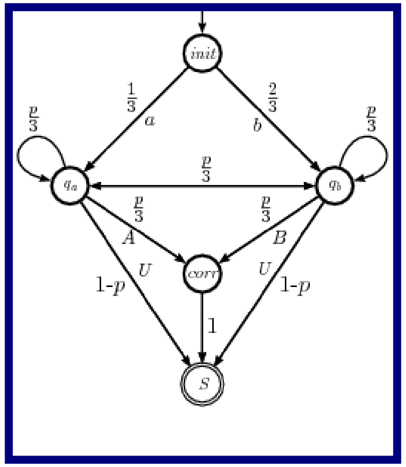
$$\mathbf{P}(\lambda) = \mathbf{P}(\{\sigma \in \mathrm{Paths}(\mathcal{M}) \mid \sigma \models \lambda\})$$

with σ_1, σ_2, … the paths of the system

- Properties
  - $\lim_{k \to \infty} C_k = C$
  - $\lim_{k \to \infty} L(C_k/\pi, \pi) = L(C/\pi, \pi)$
  - $L(C_k/\pi, \pi) \leq L(C/\pi, \pi) \leq L(C_k/\pi, \pi) + g(C_k)$ for all k (g is decreassing)

Iterative approach [regexps]

- Idea: Translate **M** into an ***equivalent*** regular expression $r_M = r_1 + r_2 + \ldots + r_n$
  - Each r_i represents a set of paths ***Paths-r_i*** of M
  - Each r_i has a probability and $\mathbf{P}(r_i) = \mathbf{P}(\textit{Paths-}r_i)$
- Example



≡

$$
\begin{aligned}
r_1 &\triangleq \langle b, \tfrac{2}{3}, q_b\rangle \cdot \hat{r}^\star \cdot \langle B, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle,\\
r_2 &\triangleq \langle b, \tfrac{2}{3}, q_b\rangle \cdot \hat{r}^\star \cdot \langle \tau, 0.3, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle A, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle,\\
r_3 &\triangleq \langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle A, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle,\\
r_4 &\triangleq \langle b, \tfrac{2}{3}, q_b\rangle \cdot \hat{r}^\star \cdot \langle U, 0.1, S\rangle,\\
r_5 &\triangleq \langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle \tau, 0.3, q_b\rangle \cdot \hat{r}^\star \cdot \langle B, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle,\\
r_6 &\triangleq \langle b, \tfrac{2}{3}, q_b\rangle \cdot \hat{r}^\star \cdot \langle \tau, 0.3, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle U, 0.1, S\rangle,\\
r_7 &\triangleq \langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle U, 0.1, S\rangle,\\
r_8 &\triangleq \langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle \tau, 0.3, q_b\rangle \cdot \hat{r}^\star \cdot \langle \tau, 0.3, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot\\
&\quad\ \langle A, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle,\\
r_9 &\triangleq \langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle \tau, 0.3, q_b\rangle \cdot \hat{r}^\star \cdot \langle U, 0.1, S\rangle,\\
r_{10} &\triangleq \langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle \tau, 0.3, q_b\rangle \cdot \hat{r}^\star \cdot \langle \tau, 0.3, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle U, 0.1, S\rangle,
\end{aligned}
$$

where $\hat{r} \triangleq (\langle \tau, 0.3, q_b\rangle^\star \cdot (\langle \tau, 0.3, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^\star \cdot \langle \tau, 0.3, q_b\rangle)^\star)$.

- Partial Matrices (with regexps)

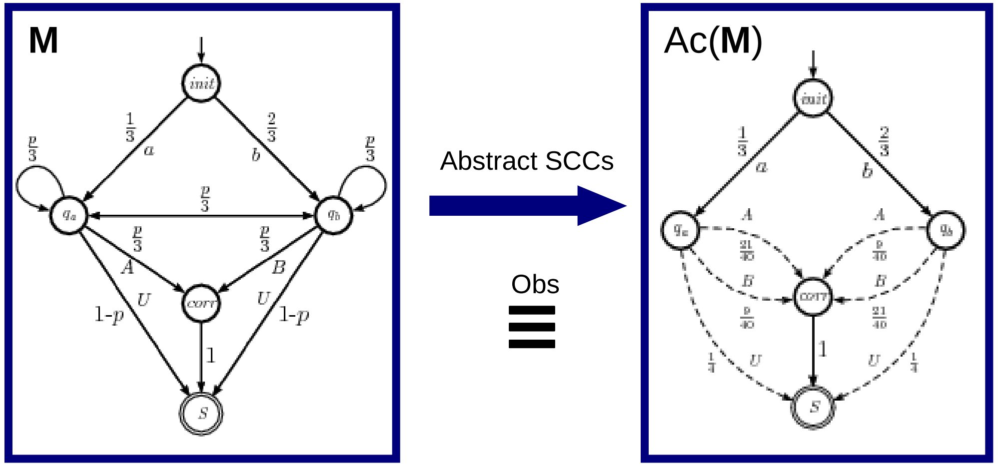
$$
\mathbf{C}_0(o \square s) = 0, \quad \mathbf{C}_{k+1}(o \square s) = \begin{cases} \mathbf{C}_k(o \square s) + \mathbf{P}(r_{k+1}) & \textit{if o-trace}(r_{k+1}) = o \textit{ and s-trace}(r_{k+1}) = s \\ \mathbf{C}_k(o \square s) & \text{otherwise} \end{cases}
$$

where M ≡ $r_1 + \ldots + r_n$

Iterative approach [SCC analysis]

- Idea: Group together paths that only differ in the way they traverse SCC
  1. *Abstract* away *SCC of M* (we do it in such a way that the observable behaviour of the automaton does not change) obtaining an acyclic model Ac(M)
  2. Construct the *partial matrix* of Ac(M) instead of M

- Example



Paths of Ac(**M**)

1. $init \xrightarrow{a} q_a \xrightarrow{A} corr \xrightarrow{\tau} S$
2. $init \xrightarrow{b} q_b \xrightarrow{B} corr \xrightarrow{\tau} S$
3. $init \xrightarrow{a} q_a \xrightarrow{U} S$
4. $init \xrightarrow{b} q_b \xrightarrow{U} S$
5. $init \xrightarrow{a} q_a \xrightarrow{B} corr \xrightarrow{\tau} S$
6. $init \xrightarrow{b} q_b \xrightarrow{A} corr \xrightarrow{\tau} S$

- Partial Matrices (with SCC analysis)

$$\mathbf{C}_0(o \square s) = 0, \quad \mathbf{C}_{k+1}(o \square s) = \begin{cases} \mathbf{C}_k(o \square s) + \mathbf{P}(\sigma_{k+1}) & \text{if } o\text{-trace}(\sigma_{k+1})=o \text{ and } s\text{-trace}(\sigma_{k+1})=s, \\ \mathbf{C}_k(o \square s) & \text{otherwise.} \end{cases}$$

where σ_1 , σ_2 , … , σ_n are the paths of Ac(M)

Iterative approach [Identifying high-leakage sources]

- Goal: Identify sources of high leakage (debugging)
- Idea:

$$L_{\times}(\mathbf{C},\pi) = V(\mathbf{S}|\mathbf{O}) \,/\, V(\mathbf{S}), \qquad L_{+}(\mathbf{C},\pi) = V(\mathbf{S}|\mathbf{O}) - V(\mathbf{S})$$

$$V(\mathbf{S}) = \max_{s} \pi(s), \quad V(\mathbf{S}|\mathbf{O}) = \sum_{o} \max_{s} \mathbf{C}(o|s) \times \pi(s) = \sum_{o} \max_{s} \mathbf{P}(o \,\square\, s)$$

- Example

	A	B	U
a	7/40	3/40	1/12
b	3/20	7/20	1/6

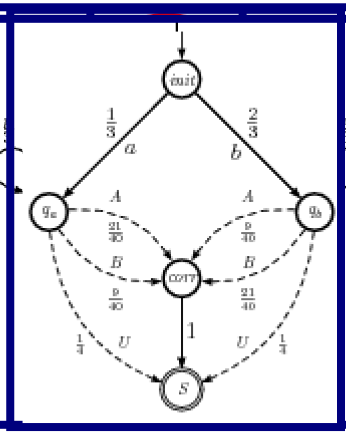
O_1 O_2 O_3

S_1 P( )

S_2 P( )

S_3 P( )

Mat ... ties



- Debugging
  - SCC technique

$$init \xrightarrow{a} q_a \xrightarrow{A} corr \xrightarrow{\tau} S$$

$V(\mathbf{S}|\mathbf{O}) = \mathbf{P}(o_1 \,\square\, s_2) + \mathbf{P}(o_2 \,\square\, s_1) + \mathbf{P}(o_3 \,\square\, s_2)$ $1/3 \times 21/40 \times 1 = 7/40$

  - REGEXPS technique

$$\langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^{\star} \cdot \langle A, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle$$

$1/3 \quad \times \quad [\,3/7\,] \quad \times \quad 1 \quad = 1/7$

$$\langle a, \tfrac{1}{3}, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^{\star} \cdot \langle \tau, 0.3, q_b\rangle \cdot \hat{r}^{\star} \cdot \langle \tau, 0.3, q_a\rangle \cdot \langle \tau, 0.3, q_a\rangle^{\star} \cdot \langle A, 0.3, corr\rangle \cdot \langle \tau, 1, S\rangle$$

Overview

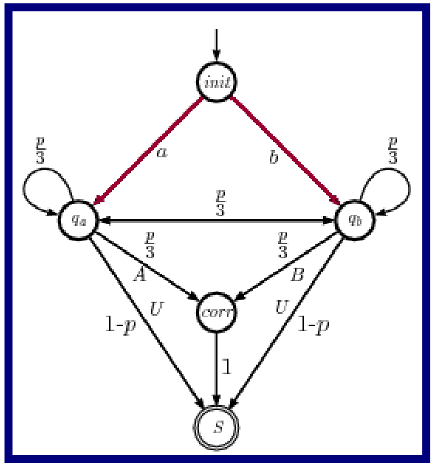
- Motivation
- Information-hiding systems as automata
- Reachability analysis approach
- Iterative approach
  - Regular expressions techniques
  - SCC analysis technique
  - Identifying high-leakage sources
- **Information-hiding systems with variable a priori**
- Interactive information-hiding systems
- Future work

Information-Hiding Systems with variable a priori

- IHS with variable a priori

  $\mathcal{I} = (\mathcal{M}, A_s, A_o, A_\tau)$ where

  - $\mathcal{M} = (Q, A, \delta)$ is a ***non-deterministic*** automaton
  - A_s, A_o, and A_τ are disjoint sets of *secret*, *observable*, and ***internal*** actions
  - δ *satisfies:*
    - ***Non-determinism*** can occur only at the ***beginning***
    - *Secret actions* can occur only at the *beginning*
    - Only *internal actions* can occur in *cycles*



- Lemma (The channel matrix is independet of π)

  For all $\pi, \rho \in \mathcal{D}(S)$ we have: $\mathbf{P}_\pi(o \mid s) = \mathbf{P}_\rho(o \mid s)$, for all secrets s and observable o

- Maximum leakage Computation

$$ML_\times(C) = \max_{\pi \in \mathcal{D}(S)} L_\times(C, \pi) \quad \text{and} \quad ML_+(C) = \max_{\pi \in \mathcal{D}(S)} L_+(C, \pi)$$

  - Multiplcative Leakage: easy taking π uniform distribution
  - Additive Leakage: More difficult, we have to consider all corner points distribution
    - Lemma: Computing maximum additive leakage is NP-complete

Overview

- Motivation
- Information-hiding systems as automata
- Reachability analysis approach
- Iterative approach
  - Regular expressions techniques
  - SCC analysis technique
  - Identifying high-leakage sources
- Information-hiding systems with variable a priori
- **Interactive information-hiding systems**
- Future work

Interactive Information-Hiding Systems

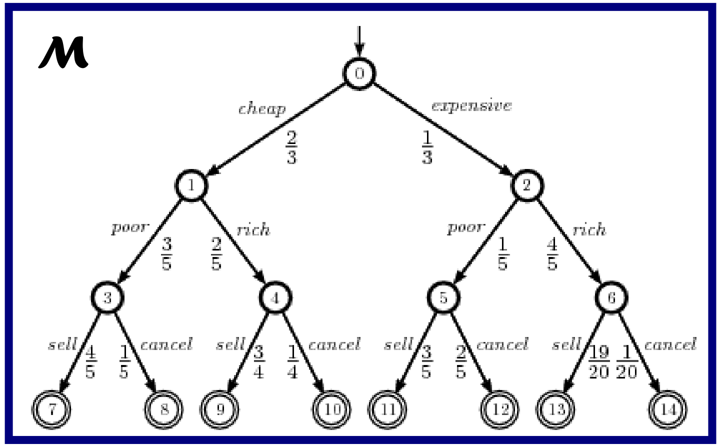
- Idea: Secrets and observables can alternate
- Interactive IHS

  $\mathcal{I} = (\mathcal{M}, A_S, A_O, A_\tau)$ where

  - $\mathcal{M} = (Q, A, \delta)$ is a ***probabilistic*** automaton
  - A_S, A_O, and A_τ are disjoint sets of *secret*, *observable*, and ***internal*** actions
  - δ *satisfies:*
    - ***Transitions*** are either ***secret or observable*** (not both)
    - Only *internal actions* can occur in *cycles*

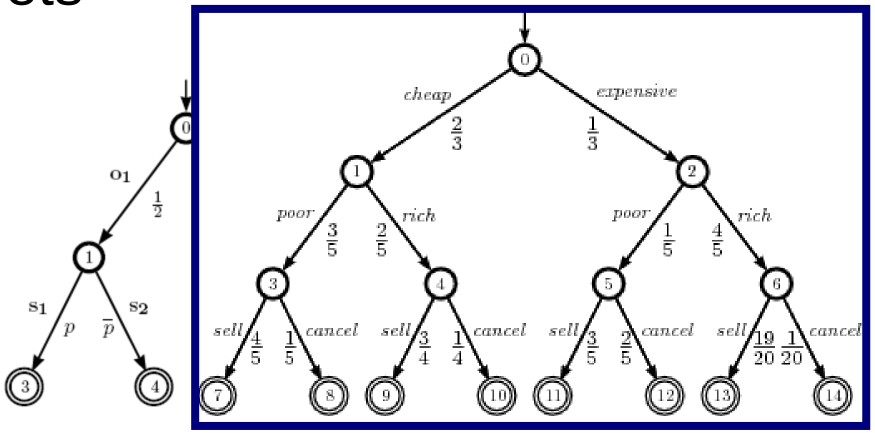
- Example (eBay Protocol)

  - A_S={*poor, rich*}
  - A_O={*cheap, expensive, sell, cancel*}
  - A_τ ={}



Interactive Information-Hiding Systems

- Observation: The channel matrix depends on the distribution over secrets
  - Why?



Channel Matrix

	o1	o2
s1	a	$\bar{a}$
s2	b	$\bar{b}$

Depends on ***p*** and ***q*** !!!

- Consequence: We cannot model Interactive protocols as noisy channels. However we can still compute leakage
  - Recall $V(\boldsymbol{S}) = \max_{s} \boldsymbol{\pi}(s)$, $\quad V(\boldsymbol{S}|\boldsymbol{O}) = \sum_{o} \max_{s} \boldsymbol{C}(o|s) \times \boldsymbol{\pi}(s) = \sum_{o} \max_{s} \mathbf{P}(o \,\square\, s)$
  - Then we compute
    - A priori distribution

      π(***poor***)=**P**(***poor***)= *7/15*
      π(***rich***) =**P**(***rich***) = 8/15

    - Matrix of Joint Probabilities

	cheap sell	*cheap cancel*	*expensive sell*	*expensive Cancel*
poor	**8/25**	**2/25**	**1/25**	**2/75**
rich	**1/5**	**1/15**	**19/75**	**1/75**

Overview

- Motivation
- Information-hiding systems as automata
- Reachability analysis approach
- Iterative approach
  - Regular expressions techniques
  - SCC analysis technique
  - Identifying high-leakage sources
- Information-hiding systems with variable a priori
- Interactive information-hiding systems
- **Future work**

Future work

- Use tools from counterexamples generation to compute/approximate leakage of large scale protocols
- Try to identify flaws in protocols
- Extend the notion of noisy channel to capture the dynamic nature of interactive protocols
  - Lift channel inputs from secrets to schedulers on secrets
  - Use channels with history and/or feedback

Questions

Thanks for your attention!

Questions