Informal Reasoning

Formal Reasoning

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Belief in Information Flow By M. R. Clarkson, A. C. Myers and F. B. Schneider

Sari Haj Hussein¹

APSIA Breakfast Talk ¹Interdisciplinary Center for Security, Reliability and Trust University of Luxembourg

2011-06-22

Formal Reasoning

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

Introduction

- Information Flow
- Techniques for Information Flow Security
- Quantitative Information Flow Security

Informal Reasoning

- Initial State
- Experiment 1
- Experiment 2
- The Uncertainty Reduction Principle
- The Proposed Principle

3 Formal Reasoning

- Basics
- Attacker-System Interaction
- The Proposed Measure

Formal Reasoning

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Introduction

- Information Flow
- Techniques for Information Flow Security
- Quantitative Information Flow Security

Informal Reasoning

- Initial State
- Experiment 1
- Experiment 2
- The Uncertainty Reduction Principle
- The Proposed Principle

3 Formal Reasoning

- Basics
- Attacker-System Interaction
- The Proposed Measure

Introduction	
000	
Information Flow	

- Information flow analysis determines the amount of information that is leaked about a program's secret inputs during the execution of that program
- Information flow security establishes bounds on information leakage

Introduction ●○○	Informal Reasoning
Information Flow	

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

- Information flow analysis determines the amount of information that is leaked about a program's secret inputs during the execution of that program
- Information flow security establishes bounds on information leakage

Introduction	Informal Reasoning	Formal Reasoning	Summary
000			
Techniques for Information Flow Se	ecurity		

- Qualitative techniques prohibit flow from a program's secret inputs to its public outputs
 Some programs do not function correctly
- Quantitative techniques allow information flow at a certain rate
 At most k bits leak per program execution

Introduction	Informal Reasoning	Formal Reasoning	Summary
000			
Techniques for Information Flow Se	ecurity		

- Qualitative techniques prohibit flow from a program's secret inputs to its public outputs
 - \rightsquigarrow Some programs do not function correctly
- Quantitative techniques allow information flow at a certain rate

 \rightsquigarrow At most k bits leak per program execution

Introduction	Informal Reasoning	Formal Reasoning	Summary
000			
Quantitative Information Flow Sec	urity		

- Treat a program's execution as a channel for transmitting messages
 - \rightsquigarrow Compute the capacity of this channel
- Set bounds on the values of the entropy of input distributions
- Assume that the program input values are independently and uniformly chosen

• Fix a probability distribution on a program's secret inputs ~ Clarkson is here

Introduction	Informal Reasoning	Formal Reasoning	Summary
000			
Quantitative Information Flow	Security		

- Treat a program's execution as a channel for transmitting messages
 - \rightsquigarrow Compute the capacity of this channel
- Set bounds on the values of the entropy of input distributions
- Assume that the program input values are independently and uniformly chosen

• Fix a probability distribution on a program's secret inputs ~ Clarkson is here

Introduction	Informal Reasoning	Formal Reasoning	Summary
000			
Quantitative Information Flo	w Security		

- Treat a program's execution as a channel for transmitting messages
 - \rightsquigarrow Compute the capacity of this channel
- Set bounds on the values of the entropy of input distributions
- Assume that the program input values are independently and uniformly chosen

• Fix a probability distribution on a program's secret inputs ~> Clarkson is here

Introduction	Informal Reasoning	Formal Reasoning	Summary
000			
Quantitative Information Flow Se	curity		

- Treat a program's execution as a channel for transmitting messages
 - \rightsquigarrow Compute the capacity of this channel
- Set bounds on the values of the entropy of input distributions
- Assume that the program input values are independently and uniformly chosen

• Fix a probability distribution on a program's secret inputs ~ Clarkson is here

Formal Reasoning

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

Introduction

- Information Flow
- Techniques for Information Flow Security
- Quantitative Information Flow Security

2 Informal Reasoning

- Initial State
- Experiment 1
- Experiment 2
- The Uncertainty Reduction Principle
- The Proposed Principle

3 Formal Reasoning

- Basics
- Attacker-System Interaction
- The Proposed Measure





Initial State

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ



Experiment $1 \rightsquigarrow p$ is A

▲□▶ ▲□▶ ▲ □▶ ▲ □▶ □ のへぐ



Experiment 2 \rightsquigarrow p is C

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ ─臣 ─のへで

Introduction	Informal Reasoning	Formal Reasoning	Summary
The Uncertainty Reduction Princip	le		

The Uncertainty Reduction Principle

- A measure of information flow proposed by Denning in the eighties
 - \bullet \uparrow in uncertainty \rightsquigarrow information has flowed
 - \bullet \downarrow in uncertainty \rightsquigarrow information has not flowed
- This principle is unsuitable when input distributions represent attacker beliefs
 - $\bullet\,$ In the initial state \leadsto attacker is almost certain
 - After experiment 2 \rightsquigarrow attacker is somewhat uncertain
 - This is \uparrow in uncertainty \rightsquigarrow information has not flowed

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

• Untrue!

Introduction	Informal Reasoning	Formal Reasoning	Summary
000 The Uncertainty Reduction Princip		0000000	
The oncertainty reduction i men			

The Uncertainty Reduction Principle

- A measure of information flow proposed by Denning in the eighties
 - \bullet \uparrow in uncertainty \rightsquigarrow information has flowed
 - \bullet \downarrow in uncertainty \rightsquigarrow information has not flowed
- This principle is unsuitable when input distributions represent attacker beliefs
 - $\bullet\,$ In the initial state \rightsquigarrow attacker is almost certain
 - After experiment 2 \rightsquigarrow attacker is somewhat uncertain
 - $\bullet\,$ This is \uparrow in uncertainty \rightsquigarrow information has not flowed
 - Untrue!

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

The Proposed Principle

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - \uparrow in accuracy \rightsquigarrow attacker was informed \rightsquigarrow information has flowed
 - \downarrow in accuracy \rightsquigarrow attacker was misinformed \rightsquigarrow information has not flowed
- Based on this principle, we need to devise a measure for information flow...

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

The Proposed Principle

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - \uparrow in accuracy \rightsquigarrow attacker was informed \rightsquigarrow information has flowed
 - \downarrow in accuracy \rightsquigarrow attacker was misinformed \rightsquigarrow information has not flowed
- Based on this principle, we need to devise a measure for information flow...

Formal Reasoning

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Introduction

- Information Flow
- Techniques for Information Flow Security
- Quantitative Information Flow Security

Informal Reasoning

- Initial State
- Experiment 1
- Experiment 2
- The Uncertainty Reduction Principle
- The Proposed Principle

3 Formal Reasoning

- Basics
- Attacker-System Interaction
- The Proposed Measure

Introduction	Informal Reasoning	Formal Reasoning	Summary
000	00000	●000000	
Basics			

• We suppose 4 sets

- Var set of variables
- Val set of values
- *State* set of program states
- *Dist* set of distributions
- A state $\sigma \in \mathit{State}$ is an assignment in $\mathit{Var} \to \mathit{Val}$
- A distribution $\delta \in \textit{Dist}$ is an assignment in $\textit{State} \to \mathbb{R}^+$
- A state mass $\dot{\sigma}$ is a probability distribution that maps σ to 1

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

• With a program S, we use the function [S]: State
ightarrow Dist

Introduction	Informal Reasoning	Formal Reasoning	Summary
000	00000	●000000	
Basics			

- We suppose 4 sets
 - Var set of variables
 - Val set of values
 - *State* set of program states
 - *Dist* set of distributions
- A state $\sigma \in \mathit{State}$ is an assignment in $\mathit{Var} \to \mathit{Val}$
- A distribution $\delta \in \textit{Dist}$ is an assignment in $\textit{State}
 ightarrow \mathbb{R}^+$
- \bullet A state mass $\dot{\sigma}$ is a probability distribution that maps σ to 1

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ● ●

• With a program S, we use the function [S]: State
ightarrow Dist

Introduction	Informal Reasoning	Formal Reasoning	Summary
000	00000	⊙●○○○○○	
Basics			

- We use confidentiality labels to identify secret data
 - $L \rightsquigarrow$ low-confidentiality public data
 - $H \rightsquigarrow$ high-confidentiality secret data
- $\sigma \upharpoonright L \rightsquigarrow$ low projection of the state $\sigma \rightsquigarrow$ the part of σ visible to the attacker
- $\sigma \upharpoonright H \rightsquigarrow$ high projection of the state $\sigma \rightsquigarrow$ the part of σ not visible to the attacker

- $x_L \rightarrow$ a variable that contains low information
- $x_H \rightsquigarrow$ a variable that contains high information

Introduction	Informal Reasoning	Formal Reasoning	Summary
000	00000	⊙●○○○○○	
Basics			

- We use confidentiality labels to identify secret data
 - $L \rightsquigarrow$ low-confidentiality public data
 - $H \rightsquigarrow$ high-confidentiality secret data
- $\sigma \upharpoonright L \rightsquigarrow$ low projection of the state $\sigma \rightsquigarrow$ the part of σ visible to the attacker
- $\sigma \upharpoonright H \rightsquigarrow$ high projection of the state $\sigma \rightsquigarrow$ the part of σ not visible to the attacker

- $x_L \rightarrow$ a variable that contains low information
- $x_H \rightsquigarrow$ a variable that contains high information

Introduction	Informal Reasoning	Formal Reasoning	Summary
000	00000	⊙●○○○○○	
Basics			

- We use confidentiality labels to identify secret data
 - $L \rightsquigarrow$ low-confidentiality public data
 - $H \rightsquigarrow$ high-confidentiality secret data
- $\sigma \upharpoonright L \rightsquigarrow$ low projection of the state $\sigma \rightsquigarrow$ the part of σ visible to the attacker
- σ ↾ H → high projection of the state σ → the part of σ not visible to the attacker

- $x_L \sim a$ variable that contains low information
- $x_H \rightsquigarrow$ a variable that contains high information

Introduction	Informal Reasoning	Formal Reasoning	Summary
		000000	
Attacker-System Interaction			

- PWC: if $p_H = g_L$ then $a_L := 1$ else $a_L := 0$
- The attacker chooses a pre-belief $b_H = (0.98, 0.01, 0.01)$
- The system chooses $\sigma_{H} = (p \rightarrow A)$
- The attacker chooses $\sigma_L = (g
 ightarrow {\it A}, {\it a}
 ightarrow 0)$
- The input to PWC is $\vec{\sigma_L} \otimes \vec{\sigma_H}$
- PWC executes once
- The output is a frequency distribution δ' = [PWC](σ_L ⊗ σ_H) from which one state is chosen σ' = (p → A, g → A, a → 1)

• The attacker observes $o = \sigma' \upharpoonright L = (g \to A, a \to 1)$

Introduction	Informal Reasoning	Formal Reasoning	Summary
		000000	
Attacker-System Interaction			

- PWC: if $p_H = g_L$ then $a_L := 1$ else $a_L := 0$
- The attacker chooses a pre-belief $b_H = (0.98, 0.01, 0.01)$
- The system chooses $\sigma_{H} = (p \rightarrow A)$
- The attacker chooses $\sigma_L = (g
 ightarrow {\it A}, {\it a}
 ightarrow 0)$
- The input to PWC is $\dot{\sigma_L} \otimes \dot{\sigma_H}$
- PWC executes once
- The output is a frequency distribution $\delta' = [PWC](\sigma_L \otimes \sigma_H)$ from which one state is chosen $\sigma' = (p \to A, g \to A, a \to 1)$

• The attacker observes $o = \sigma^{'} \upharpoonright L = (g
ightarrow A, a
ightarrow 1)$

Introduction 000 Informal Reasoning

Formal Reasoning ○○○●○○○ Summary

Attacker-System Interaction

- The attacker generates a prediction of getting authenticated $\delta'_A = [PWC](\sigma_L \otimes b_H)$
- To incorporate the information in o, The attacker conditions $\delta_A'|o$

р	g	а	$\delta'_{\mathcal{A}}$	$\delta'_{A} o$
A	A	0	0	0
A	A	1	0.98	1
В	A	0	0.01	0
В	A	1	0	0
С	A	0	0.01	0
С	A	1	0	0

- The attacker projects on the high state to obtain her post-belief b'_H = (δ'_A|o) ↾ H = (1, 0, 0)
- This matches with the informal reasoning

The Proposed Measure

Formal Reasoning

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

The Proposed Principle

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - \uparrow in accuracy \rightsquigarrow attacker was informed \rightsquigarrow information has flowed
 - \downarrow in accuracy \rightsquigarrow attacker was misinformed \rightsquigarrow information has not flowed

• How can we use that?...

The Proposed Measure

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

The Proposed Principle

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - \uparrow in accuracy \rightsquigarrow attacker was informed \rightsquigarrow information has flowed
 - \downarrow in accuracy \rightsquigarrow attacker was misinformed \rightsquigarrow information has not flowed
- How can we use that?...

Formal Reasoning ○○○○○●○

The Proposed Measure

The Proposed Measure

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - Accuracy of attacker's pre-belief b_H is $D(b_H \rightarrow \vec{\sigma_H})$ (Kullback–Leibler divergence)
 - Accuracy of attacker's post-belief b'_H is $D(b'_H o \dot{\sigma_H})$

•
$$\Delta = D(b_H \to \sigma_H) - D(b'_H \to \sigma_H)$$

•
$$= \dot{\sigma}_H \bullet \log \frac{\dot{\sigma}_H}{b_H(\sigma_H)} - \dot{\sigma}_H \bullet \log \frac{\dot{\sigma}_H}{b'_H(\sigma_H)}$$
(Kullback-Leibler)
•
$$= 1 \bullet \log \frac{1}{b_H(\sigma_H)} - 1 \bullet \log \frac{1}{b'_H(\sigma_H)}$$
(Definition of state mass)
•
$$= -\log b_H(\sigma_H) + \log b'_H(\sigma_H)$$

•
$$= -\log b_H(\sigma_H) + \log b_H(\sigma_H) \bullet \frac{\delta_S(o)}{\delta_A(o)}$$
(proved in the paper)
•
$$= -\log b_H(\sigma_H) + \log b_H(\sigma_H) + \log \frac{\delta_S(o)}{\delta_A(o)}$$

•
$$= -\log b_H(\sigma_H) + \log \delta_S(o)$$

•
$$= -\log Pr_{\delta_A}(o) + \log Pr_{\delta_S}(o)$$

Formal Reasoning ○○○○○●○

The Proposed Measure

The Proposed Measure

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - Accuracy of attacker's pre-belief b_H is $D(b_H \rightarrow \sigma_H)$ (Kullback–Leibler divergence)
 - Accuracy of attacker's post-belief $b_{H}^{'}$ is $D(b_{H}^{'}
 ightarrow ec{\sigma_{H}})$

•
$$\Delta = D(b_H \to \dot{\sigma_H}) - D(b'_H \to \dot{\sigma_H})$$

•
$$= \dot{\sigma}_H \bullet \log \frac{\dot{\sigma}_H}{b_H(\sigma_H)} - \dot{\sigma}_H \bullet \log \frac{\dot{\sigma}_H}{b'_H(\sigma_H)}$$
 (Kullback-Leibler)
•
$$= 1 \bullet \log \frac{1}{b_H(\sigma_H)} - 1 \bullet \log \frac{1}{b'_H(\sigma_H)}$$
 (Definition of state mass)
•
$$= -\log b_H(\sigma_H) + \log b'_H(\sigma_H)$$

•
$$= -\log b_H(\sigma_H) + \log b_H(\sigma_H) \bullet \frac{\delta_S(o)}{\delta_A(o)}$$
 (proved in the paper)
•
$$= -\log b_H(\sigma_H) + \log b_H(\sigma_H) + \log \frac{\delta_S(o)}{\delta_A(o)}$$

•
$$= -\log \delta_A(o) + \log \delta_S(o)$$

•
$$= -\log Pr_{\delta_A}(o) + \log Pr_{\delta_S}(o)$$

Formal Reasoning ○○○○○●○

The Proposed Measure

The Proposed Measure

- Information flow corresponds to an improvement in the accuracy of an attacker's belief
 - Accuracy of attacker's pre-belief b_H is $D(b_H \rightarrow \vec{\sigma_H})$ (Kullback–Leibler divergence)
 - Accuracy of attacker's post-belief $b_{H}^{'}$ is $D(b_{H}^{'}
 ightarrow ec{\sigma_{H}})$

•
$$\Delta = D(b_H \to \dot{\sigma_H}) - D(b'_H \to \dot{\sigma_H})$$
•
$$= \dot{\sigma}_H \bullet \log \frac{\dot{\sigma}_H}{b_H(\sigma_H)} - \dot{\sigma}_H \bullet \log \frac{\dot{\sigma}_H}{b'_H(\sigma_H)}$$
(Kullback-Leibler)
•
$$= 1 \bullet \log \frac{1}{b_H(\sigma_H)} - 1 \bullet \log \frac{1}{b'_H(\sigma_H)}$$
(Definition of state mass)
•
$$= -\log b_H(\sigma_H) + \log b'_H(\sigma_H)$$
•
$$= -\log b_H(\sigma_H) + \log b_H(\sigma_H) \bullet \frac{\delta_S(o)}{\delta_A(o)}$$
(proved in the paper)
•
$$= -\log b_H(\sigma_H) + \log b_H(\sigma_H) + \log \frac{\delta_S(o)}{\delta_A(o)}$$
•
$$= -\log \delta_A(o) + \log \delta_S(o)$$
•
$$= -\log Pr_{\delta_A}(o) + \log Pr_{\delta_S}(o)$$
•
$$= l_{\delta_A}(o) - l_{\delta_S}(o)$$
(a result from information theory)

000	00000
Introduction	Informal R

Formal Reasoning ○○○○○○●

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

Flow in Experiment 1

•
$$\Delta_1 = -\log \Pr_{\delta_A}(o_1) + \log \Pr_{\delta_S}(o_1) = -\log 0.98 + \log 1 = 0.0291$$
 bit.

Flow in Experiment 2

• $\Delta_2 = -\log Pr_{\delta_A}(o_2) + \log Pr_{\delta_S}(o_2) = -\log 0.02 + \log 1 = 5.6439$ bit.

- Thus the flow in Experiment 2 is larger than it is in Experiment 1
- Again, this matches with the informal reasoning

Introduction	Informal Reasoning	Formal Reasoning	Summ
000	00000	○○○○○○●	
The Proposed Measure			

Flow in Experiment 1

•
$$\Delta_1 = -log Pr_{\delta_A}(o_1) + log Pr_{\delta_S}(o_1) = -log 0.98 + log 1 = 0.0291$$
 bit.

Flow in Experiment 2

•
$$\Delta_2 = -\log Pr_{\delta_A}(o_2) + \log Pr_{\delta_S}(o_2) = -\log 0.02 + \log 1 = 5.6439$$
 bit.

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

- Thus the flow in Experiment 2 is larger than it is in Experiment 1
- Again, this matches with the informal reasoning

Introduction 000	Informal Reasoning 00000	Formal Reasoning	
The Proposed Measure			

Flow in Experiment 1

•
$$\Delta_1 = -\log Pr_{\delta_A}(o_1) + \log Pr_{\delta_S}(o_1) = -\log 0.98 + \log 1 = 0.0291$$
 bit.

Flow in Experiment 2

•
$$\Delta_2 = -\log Pr_{\delta_A}(o_2) + \log Pr_{\delta_S}(o_2) = -\log 0.02 + \log 1 = 5.6439$$
 bit.

- Thus the flow in Experiment 2 is larger than it is in Experiment 1
- Again, this matches with the informal reasoning

- The Uncertainty Reduction Principle cannot satisfactorily explain information flow when input distributions represent attacker beliefs
- Accuracy is the appropriate measure for information flow in the presence of attacker beliefs

Introduction 000 Informal Reasoning

Formal Reasoning

Summary

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

Thank you!