Dynamic Leakage
A Need for a New Quantitative Information Flow Measure

Nataliia Bielova

24 October 2016
PLAS’16
Quantitative Information Flow

Private inputs

Program

How much?

Public inputs

Private outputs

Public outputs
How much does the attacker learn when she observes a concrete public output?
if $S = s_1$ then $O = a$ else $O = b$

Secret inputs

$\begin{array}{ccc}
s_1 & s_2 & s_3 \\
\end{array}$

Public outputs

$\begin{array}{c}
a & b \\
\end{array}$

Program

$\begin{array}{ccc}
s_1 & s_2 & s_3 \\
\end{array}$

$\begin{array}{c}
a & b \\
\end{array}$

How much does the attacker learn when she observes output $b$?
if \( S = s_1 \) then \( O = a \) else \( O = b \)

How much does the attacker learn when she observes output \( b \)?
Existing measures of info leakage

- Shannon Entropy
- Min Entropy
- Guessing Entropy
- g-leakage
- Channel capacity

Belief tracking

- Belief Tracking
A need for a new measure

Average measures

Dynamic Leakage?

Belief tracking
if $S = s_1$ then $O = a$ else $O = b$

<table>
<thead>
<tr>
<th>a priori</th>
<th>a posteriori after $a$</th>
<th>a posteriori after $b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pi$</td>
<td>$p_{S</td>
<td>a}$</td>
</tr>
<tr>
<td>$s_1$</td>
<td>0.875</td>
<td>$s_1$ 1</td>
</tr>
<tr>
<td>$s_2$</td>
<td>0.0625</td>
<td>$s_2$ 0</td>
</tr>
<tr>
<td>$s_3$</td>
<td>0.0625</td>
<td>$s_3$ 0</td>
</tr>
</tbody>
</table>
Average measure: Shannon Entropy

Uncertainty about the secret

\[ \mathcal{H}(\pi) = -\sum_{s \in \mathcal{S}} \pi(s) \cdot \log \pi(s) \]

Leakage:

\[ \mathcal{L} = \mathcal{H}(\pi) - \mathcal{H}(p_{S|0}) \]

Entropy for one output

\[ \mathcal{H}(p_{S|o}) = -\sum_{o \in \mathcal{O}} p(o) \cdot \log \mathcal{H}(p_{S|o}) \]

Average for all possible outputs
Average measure: Shannon Entropy

|   | \( \pi \) |   | \( p_{S|a} \) |   | \( p_{S|b} \) |
|---|---|---|---|---|---|
| s1 | 0.875 | s1 | 1 | s1 | 0 |
| s2 | 0.0625 | s2 | 0 | s2 | 0.5 |
| s3 | 0.0625 | s3 | 0 | s3 | 0.5 |

\( \mathcal{H}(\pi) = 0.67 \)

\( \mathcal{H}(p_{S|a}) = 0 \)

\( \mathcal{H}(p_{S|b}) = 1 \)

\( \mathcal{H}(p_{S|O}) = 0.13 \)

\[ \mathcal{L} = 0.67 - 0.13 = 0.54 \]

average information leakage for all possible outputs
Dynamic Leakage for Shannon Entropy

\[
\mathcal{L}_{\text{dynamic}} = \mathcal{H}(\pi) - \mathcal{H}(p_{S|b})
\]

a posteriori for concrete output b
## Dynamic Leakage for Shannon Entropy

<table>
<thead>
<tr>
<th></th>
<th>$\pi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1</td>
<td>0.875</td>
</tr>
<tr>
<td>s2</td>
<td>0.0625</td>
</tr>
<tr>
<td>s3</td>
<td>0.0625</td>
</tr>
</tbody>
</table>

$\mathcal{H}(\pi) = 0.67$

|   | $p_{S|b}$ |
|---|-----------|
| s1| 0         |
| s2| 0.5       |
| s3| 0.5       |

$\mathcal{H}(p_{S|b}) = 1$

$\mathcal{L}_{\text{dynamic}} = 0.67 - 1 = -0.33$

no leakage!
A need for a new measure

Average measures

Belief tracking

Belief tracking

|   | $\pi$   |   | | $p_{S|b}$ |   |   | $p'$ |   |
|---|---------|---|---|---------|---|---|------|---|
| s1 | 0.875   |   |   | s1      | 0 |   | s1   | 0 |
| s2 | 0.0625  |   |   | s2      | 0.5|   | s2   | 1 |
| s3 | 0.0625  |   |   | s3      | 0.5|   | s3   | 0 |

$$\mathcal{L}^{\text{belief}} = \mathcal{D}(\pi \rightarrow p') - \mathcal{D}(p_{S|b} \rightarrow p')$$

**concrete secret input**
**a posteriori for one output**
Belief tracking

| $\pi$ | $p_{S|b}$ | $p'$ |
|-------|-----------|------|
| s1    | 0.875     | 0    |
| s2    | 0.0625    | 0.5  |
| s3    | 0.0625    | 0    |

$D(\pi \rightarrow p') = 4$

$D(p_{S|b} \rightarrow p') = 1$

$\mathcal{L}^{\text{belief}} = 4 - 1 = 3$
Belief tracking is suitable for deterministic programs

Theorem 1. $\mathcal{L}_{\text{belief}} = -\log p(o)$
Belief tracking is suitable for deterministic programs

\[ L^{\text{belief}} = -\log p(b) \]
\[ = -\log (\pi(s2) + \pi(s3)) \]

Initial probabilities of secrets that can produce output b
A need for a new measure

Average measures

Belief tracking

is suitable for deterministic programs
Belief tracking for probabilistic programs?

- **concrete secret s1**
  - $\pi$
    - s1: 0.25
    - s2: 0.75
  - $p_{S\mid b}$
    - s1: 0.75
    - s2: 0.25
  - $p'$
    - s1: 1
    - s2: 0
  - $\mathcal{L}^{\text{belief}} = 1.58$

- **concrete secret s2**
  - $p'$
    - s1: 0
    - s2: 1
  - $\mathcal{L}^{\text{belief}} = -1.58$
Belief tracking for probabilistic programs?

\( \mathcal{L}^{\text{belief}} \neq \mathcal{L}^{\text{belief}} \)
Conclusions

✗ Average measures become negative

✔ Belief tracking is suitable for deterministic programs

❓ Which measure is suitable for probabilistic programs?
   – Operational scenario?
   – Reasonable evaluation criteria?