DYNAMIC ENFORCEMENT OF KNOWLEDGE-BASED SECURITY POLICIES

Piotr (Peter) Mardziel

Joint work with Stephen Magill, Michael Hicks (UMD), and Mudhakar Srivatsa (IBM TJ Watson)
Where is your information?
Bad + Good

Getaways in DC 83% Off
homerun.com

The best Getaways in Washington DC. Huge discounts for our members. Click now to join free!

M.S. – Computer Forensics
online.uab.edu

Become a leader in the rapidly growing field of computer forensics with a Masters degree from UAB!

DC Bucket List
partners.livingsocial.com

365 Things to do in Washington, DC before you die.

Cointreau Noir

Remy Martin Cognac blended with orange liqueur: Cointreau Noir. Do you LIKE it?

Redbeacon gives up to 44% off on local plumbers. Sign up today!

Do you have Anxiety?
healingllc.com

Is your mind spinning with worries and you just want a break? Counseling can help! Email us today at AnotherLook @ HealingLLC.com.
Take back control
out = 24 ≤ Age ≤ 30 ∧ Female? ∧ Engaged?
out = (ssn, ccn, fav-color)
reject
The big problem: how to decide to run a query or not?

Q1
out = 24 ≤ age ≤ 30
∧ female?
∧ engaged?

Q2
out = age

Q3
out = (ssn, ccn, fav-color)
Outline

- Clarkson’s work on quantified information flow
  - (adversary) belief/knowledge and belief revision (Bayesian revision)
  - probability of adversary guessing secret
- Suitable knowledge-based policy formulation
  - maintain bound while revealing query outputs or rejecting queries
- Clarkson’s probabilistic semantics
- Computational feasibility
  - approximation of knowledge
  - abstract interpretation (of probabilistic semantics)
  - soundness in terms of policy
- Experimental results
  - compare to prob-scheme, enumeration-based probabilistic evaluation
Clarkson’s Quantitative Information Flow

= belief (probability distribution) over secret data

- Given belief, query, determine revised belief given the output of the query (Bayesian revision)
  - \( \Pr[\text{gender} = \text{male} \mid \text{output} = o] \)
  - \( \Pr[\text{Bad}] < t = \)
    - adversary holding belief has bounded probability of guessing my secret(s) in one try
      - sufficient: \( \Pr[\text{gender} = \text{male} \mid \text{output} = o] < t \)

- Assumption
  - initial belief is correct
    - our approach might help here (later)
  - adversary guesses by sampling

Ex:
\( \Pr[\text{gender} = \text{male}] = 0.5 \)
\( \Pr[\text{gender} = \text{female}] = 0.5 \)
• More about Clarkson’s semantics later
  • Let us consider an example
  • Flawed initial policy
    • \( \text{Pr}[\text{my secret}] < t \)
    • demonstrate problem with rejection
    • revise policy to address problem
Meet Bob

Bob (born September 27, 1980)
bday = 270
byear = 1980

Secret

0 ≤ bday ≤ 364
1956 ≤ byear ≤ 1992

Policy
Pr[bday] < 0.2
Pr[bday,byear] < 0.05

Currently
Pr[bday] = 1/365
Pr[bday,byear] = 1/(365*37)
```plaintext
bday-query1

today := 260;
if bday ≥ today ∧ bday < (today + 7)
then out := true
else out := false

= (out = false)

Bob
bday = 270
byear = 1980
```
Potentially
Pr[bday] = 1/358 < 0.2
Pr[bday,byear] = 1/(358*37) < 0.05

bday-query1
\[
\text{today} := 260;
\]
\[
\text{if } \text{bday} \geq \text{today} \land \text{bday} < (\text{today} + 7)
\]
\[
\text{then out } := \text{true}
\]
\[
\text{else out } := \text{false}
\]

Bob
bday = 270
byear = 1980
Next day ...

\[
\text{bday-query2} \\
\text{today} := 261; \\
\text{if bday} \geq \text{today} \land \text{bday} < (\text{today} + 7) \\
\text{then out} := \text{true} \\
\text{else out} := \text{false}
\]

\[
\text{out} = \text{false}
\]
Potentially
Pr[bday] = 1/357 < 0.2
Pr[bday, byear] = 1/(357 * 37) < 0.05

bday-query2
today := 261;
if bday ≥ today ∧ bday < (today + 7)
then out := true
else out := false

Bob
bday = 270
byear = 1980
Meet Bob'

Bob'
bday = 267
byear = 1980

bdays-query2

\[ \text{today} := 261; \]
\[ \text{if } \text{bday} \geq \text{today} \land \text{bday} < (\text{today} + 7) \]
\[ \text{then out := true} \]
\[ \text{else out := false} \]

So reject?
Querier’s perspective

Assume querier knows policy

if bday ≠ 267

will get answer

if bday = 267

will get reject
Querier’s perspective

- **Solution?**
  - Decide policy independently of secret
  - Revised **policy**
    - For every possible output \( o \), for every possible bday, \( \Pr[bday \mid out = o] < t \)
    - So the real bday in particular
    - Therefore \( \Pr[bad] < t \)
bd*ay-query2

today := 261;
if bday >= today ∧ bday < (today + 7)
    then out := true
else out := false

reject

(regardless of what bday actually is)
Clarkson’s Probabilistic Interpretation

- Given $\delta : \text{States} \rightarrow \mathbb{R}$
  - probability distribution on program states (including secrets)
  - $\delta(\sigma) = \text{probability of state } \sigma$
- Given program S
- Compute
  - $[S]\delta$
    - probability distribution on resulting program states
  - $\delta \wedge B$
    - (sub)probability distribution of $\delta$ only on states consistent with $B$
  - $\delta \mid (\text{out} = \text{true})$
    - Bayesian revision, post belief
Probabilistic Interpretation

- **Semantics**
  - $[[\text{skip}]]\delta = \delta$
  - $[[S_1;S_2]]\delta = [[S_2]][[S_1]]\delta$
  - $[[\text{if } B \text{ then } S_1 \text{ else } S_2]]\delta = [[S_1]](\delta \land B) + [[S_2]](\delta \land \neg B)$
  - $[[\text{pif } p \text{ then } S_1 \text{ else } S_2]]\delta = [[S_1]](p^*\delta) + [[S_2]]((1-p)^*\delta)$
  - $[[x := E]]\delta = \delta[x \rightarrow E]$
  - $[[\text{while } B \text{ do } S]]\delta = \text{lfp}(\lambda \delta \cdot F([[S]](\delta \land B)) + (\delta \land \neg B))$

- **Operations**
  - $p^*\delta$ – scale probabilities by $p$
  - $\delta \land B$ – remove mass inconsistent with $B$
  - $\delta_1 + \delta_2$ – combine mass from both
  - $\delta[x \rightarrow E]$ – transform mass
Subdistribution operations

\( \delta \land B \) – remove mass inconsistent with \( B \)
\( \delta \land B = \lambda \sigma. \text{if } [B] \sigma = \text{true then } \delta(\sigma) \text{ else } 0 \)

\( \delta_1 + \delta_2 \) – combine mass from both
\( \delta_1 + \delta_2 = \lambda \sigma. \delta_1(\sigma) + \delta_2(\sigma) \)

\( \delta \land x \leq 5 \)
\( [y := y + 3] (\delta \land x \leq 5) \)

\( \delta \land x > 5 \)
\( [y := y - 3] (\delta \land x > 5) \)

\( [\text{if } x \leq 5 \text{ then } y := y + 3 \text{ else } y := y - 3] \delta = [y := y + 3](\delta \land x \leq 5) + [y := y - 3](\delta \land x > 5) \)
Infeasibility

- **Computational trouble**
  - $\delta[x \rightarrow E] = \lambda \sigma \cdot \sum_{\tau} \mathbb{1}[x \rightarrow [E]] = \sigma \delta(\tau)$
  - $\max_{\sigma} \delta(\sigma) = ?$ (for policy check)
    - enumeration?

- **Sampling (prob-scheme, IBAL, …)**
  - evaluate statement for some set of input states
  - poor probability bounds if evaluated on small subset of possible states (later)
  - prohibitive (time, memory) for large state space

- Let’s try an approximation
Abstraction

• **Approximate representation** $P$
  - $P$ abstracts a set of distributions, $\gamma(P)$
  
  • sound probability bound
  - if $\delta \in \gamma(P)$ then $\max_{\sigma} \delta(\sigma) \leq \maxprob(P)$

• $((S)) \ P$ – **abstract interpretation**
  - if $\delta \in \gamma(P)$ then $[[S]]\delta \in \gamma( ((S))P )$

• $P \mid (\text{out} = X)$ – **abstract conditioning**
  - if $\delta \in \gamma(P)$ then $(\delta \mid (\text{out} = X)) \in \gamma(P \mid (\text{out} = X))$

• (more) computationally feasible

• let us revisit Bob to motivate a suitable abstraction
Representation

$P_1$: $0 \leq \text{bday} \leq 364$, $1956 \leq \text{byear} \leq 1992$

- $p = 0.000074$
- $s = 13505$ (# of points)
- $m = 1$ (total mass)

$P_2$: $267 \leq \text{bday} \leq 364$, $1956 \leq \text{byear} \leq 1992$

- $p = 0.000074$
- $s = 3626$
- $m = 0.268$

Can determine ($\wedge$ out = false)
\textbf{spec-byear-query}

\begin{verbatim}
  age := 2011 – byear;
  if age = 20 \lor \ldots \lor age = 60
      then out := true
    else out := false;
  pif 0.1 then out := true
\end{verbatim}

\textbf{pif p then }S_1\textbf{ }
- evaluate }S_1\textbf{ with probability }p
Approximation

\[ \land \text{out} = \text{true} \]

\[ P_1 : 0 \leq \text{bday} \leq 259, \ 1992 \leq \text{byear} \leq 1992 \]
\[ p = 0.0000074 \]
\[ s = 260 \]
\[ m = 0.0019 \]

\[ P_2 : 0 \leq \text{bday} \leq 259, \ 1991 \leq \text{byear} \leq 1991 \]
\[ p = 0.0000074 \]
\[ s = 260 \]
\[ m = 0.019 \]

\[ P_1 : 0 \leq \text{bday} \leq 259, \ 1956 \leq \text{byear} \leq 1992 \]
\[ p \leq 0.0000074 \]
\[ s = 9620 \]
\[ m = 0.141 \]

\[ P_2 : 267 \leq \text{bday} \leq 364, \ 1956 \leq \text{byear} \leq 1992 \]
\[ p \leq 0.0000074 \]
\[ s = 3626 \]
\[ m = 0.053 \]

...
Approximation

P₁: 0 ≤ bday ≤ 259, 1992 ≤ byear ≤ 1992
   p = 0.000067
   s = 260
   m = 0.019

P₂: 0 ≤ bday ≤ 259, 1982 ≤ byear ≤ 1990
   p = 0.000067
   s = 2340
   m = 0.173

P₂: 267 ≤ bday ≤ 364, 1956 ≤ byear ≤ 1992
   p = 0.000067
   s = 3234 ≠ size of region
   m = 0.215

p and s only refer to possible (non-zero probability) points in region
Approximation

For each $P_i$, store
- region (polyhedron)
- upper bound on probability of each possible point
- upper bound on the number of points
- upper bound on the total probability mass (useful)

Also store
- lower bounds on the above

$$\Pr[A | B] = \frac{\Pr[A \land B]}{\Pr[B]}$$
Approximation

\[ \delta \in \gamma(P) \text{ iff } \]

\[ \text{support}(\delta) \subseteq \gamma(C) \]
\[ p_{\text{min}} \leq \delta(\sigma) \leq p_{\text{max}} \text{ for every } \sigma \in \text{support}(\delta) \]
\[ s_{\text{min}} \leq |\text{support}(\delta)| \leq s_{\text{max}} \]
\[ m_{\text{min}} \leq \text{mass}(\delta) \leq m_{\text{max}} \]

\[ \max_\sigma \delta(\sigma) \leq p_{\text{max}} \]
Abstract Interpretation

- **Need**
  - \( ((S)) P \)
    - define identically to \([S] P\) but using abstract operations
    - if \( \delta \in \gamma(P) \) then \([S] \delta \in \gamma( ((S))P )\)

- **Need Abstract operations**
  - \( P_1 + P_2 \)
    - if \( \delta_i \in \gamma(P_i) \) for \( i = 1,2 \) then \( \delta_1 + \delta_2 \in \gamma(P_1 + P_2) \)
  - \( P \land B \)
    - if \( \delta \in \gamma(P) \) then \( \delta \land B \in \gamma(P \land B) \)
  - \( p^*P \)
    - if \( \delta \in \gamma(P) \) then \( p^* \delta \in \gamma(p^*P) \)
  - ...

Abstract operation example

\( \delta_1 + \delta_2 \) – combine mass from both
\( \delta_1 + \delta_2 = \lambda \sigma. \delta_1(\sigma) + \delta_2(\sigma) \)

What is the maximum number of possible points in the sum?
• determine minimum overlap (10)

\[ |C_1 \cap C_2| = 20 \]

\[ P_1 \]

\[ P_2 \]

\[ C_2 \]

\[ |C_1| = 100 \]

\[ |C_2| = 40 \]

\[ s_1^{\text{max}} = 100 \]

\[ s_2^{\text{max}} = 30 \]

\[ P_3 = P_1 + P_2 \]

\[ s_3^{\text{max}} \leq s_1^{\text{max}} + s_2^{\text{max}} = 130 \]

\[ |C_1| = 100 \]

\[ |C_2| = 40 \]

\[ s_3^{\text{max}} = 120 \]
Operations

- $P_3 = P_1 + P_2$
  - $C_3$ – convex hull of $C_1$, $C_2$
  - $s_3^{\text{max}}$ – what is the smallest overlap?
  - $s_3^{\text{min}}$ – what is the largest overlap?
  - $p_3^{\text{max}}$ – is overlap possible?
  - $p_3^{\text{min}}$ – is overlap impossible?
  - $m_3^{\text{max}}$ – simple sum $m_1^{\text{max}} + m_2^{\text{max}}$
  - $m_3^{\text{min}}$ – simple sum $m_1^{\text{min}} + m_2^{\text{min}}$

- Other operations, similar, complicated formulas abound

- Need to
  - count number of integer points in a convex polyhedra
    - Latte
  - maximize a linear function over integer points in a polyhedron
    - Latte
  - convex hull, intersection, affine transform
    - Parma
Precision

- Extend abstraction to a set of Probabilistic Polyhedrons
  - $\delta \in \gamma(\{P_1, P_2\})$ iff $\delta = \delta_1 + \delta_2$ with $\delta_1 \in \gamma(P_1)$ and $\delta_2 \in \gamma(P_2)$
  - similarly for more than two
  - $\max_{\sigma} \delta(\sigma) \leq \sum_i p_i^{\max}$
    - can do better with a bit more work

- performance / precision tradeoff
Implementation and Results

\[ 0 \leq \text{bday} \leq 364 \]
\[ 1956 \leq \text{byear} \leq 1992 \]
Policy

$\Pr[bday, byear] \leq 0.05$

**bday-query1**

today := 260;
if bday $\geq$ today $\land$ bday < (today + 7)
then out := true
else out := false

1. **prob** (our implementation)
2. **prob-scheme** (sampling/enumeration)
   - provides sound estimation after partial enumeration
   - measure time and bound on $\max_\sigma \delta(\sigma)$ produced
Implementation and Results

1 pp

\[
0 \leq \text{bday} \leq 364 \\
1956 \leq \text{byear} \leq 1992
\]

> 1 pp

\[
0 \leq \text{bday} \leq 364 \\
1910 \leq \text{byear} \leq 2010
\]
Limiting number of prob. polyhedra requires merging two into one at various points
Deciding which ones to merge is troublesome
  • likely reason for the strangeness above
Conclusions

• Knowledge-based policies
  • quantitative information flow, probabilistic semantics
  • bound on probability of specific bad events (guess of secret)

• Dynamic enforcement, via abstract interpretation
  • policy formulation safe for rejection
  • resistant to state space explosion
  • can be sound in respect to many initial distributions
    • alleviates the problem of determining what is the correct initial distribution

• Drawback
  • restricted language, integer linear expressions

• Potential (future work)
  • simpler domains (Octagons) can replace Polyhedra
    • increased performance?
Thank you!

Go back.