I want Alice’s password.

@lice!

Great.

HotCRP server

Why is security so hard?

Email Preview

Compose Mail

$User

$Password
How can we have secure rapid development?
How we do specify and enforce policies?
Programming

This talk:
- Programming model
- Execution strategy
- Why is security so hard?
- Secure rapid development?
- Specifying and enforcing policies?
Why is security so hard?
Why is security so hard?

Only my friends can see my photo tags.
No one can see where I am tagged.

Only my friends can see my photo tags.

Why is security so hard?
Policy

Only friends can see my photo tags.

Program

No one can see where I am tagged.

Policy?

Why is security so hard?

1

Meaning in context?

2
1. Delegated expressions

Symbolic execution

Oracle

Secure rapid development?
Implicit contexts

Symbolic execution

Oracle

Secure rapid development
let result : int =
let b : int = 4 in
let a : deferred int =
defer a' { a' > 0 } in
concretize (a + b)
data ctxt = { isPos : bool }

let result : int =
let b = 4 in
let a : deferred ?ctxt int =
defer a'
{ if context.is Pos
 then a' ≥ 0
 else a' < 0 } in
concretize
{ isPos = true} (a + b)
let add_tag_policy (tag : user) : user =
  defer tag'
  { (can_view tag context.viewer) ?
    (tag' == tag) : (tag' == null) }

let can_view (u : user_id) (v : user_id) : bool =
  defer cv {
    is_friends u v
    implies cv == true }
  default { cv == false }
Interpreter loop (OCaml)

Environment (C++)

Solver (Yices)

Eager optimizations and garbage collection.

Constraint resolution: simple linear and boolean constraints.
<table>
<thead>
<tr>
<th># users</th>
<th>Input proc. (s)</th>
<th>Evaluation (s)</th>
<th>Solving (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>0.008</td>
<td>0.004</td>
<td>0.000</td>
</tr>
<tr>
<td>256</td>
<td>0.020</td>
<td>0.008</td>
<td>0.000</td>
</tr>
<tr>
<td>512</td>
<td>0.084</td>
<td>0.012</td>
<td>0.000</td>
</tr>
<tr>
<td>1024</td>
<td>0.340</td>
<td>0.014</td>
<td>0.000</td>
</tr>
<tr>
<td>2048</td>
<td>1.460</td>
<td>0.048</td>
<td>0.000</td>
</tr>
<tr>
<td>4096</td>
<td>6.000</td>
<td>0.104</td>
<td>0.004</td>
</tr>
<tr>
<td>8192</td>
<td>28.533</td>
<td>0.265</td>
<td>0.000</td>
</tr>
</tbody>
</table>

**Evaluation time**

Times for accessing symbolic photo tags.
Why is security so hard?

*Security is a cross-cutting concern.*

How can we have secure rapid development?

*Separate the core program from cross-cutting concerns.*

How do we specify and automatically enforce policies?

*Constraints, contexts, and symbolic execution.*