Statement for a Panel on Rigorous Security Analysis of Software

Andrew D. Gordon
Microsoft Research
CSF 2009, Port Jefferson
The Rise of Code Verification

• Re security protocols and the Needham-Schroeder problem:
  – The first 20 years of CSF has seen the **Rise of Model Verification**
  – The next 20 years of CSF will see the **Rise of Code Verification**
• If we can verify code in the languages implementors actually use, we can find and fix security properties as soon as protocols are first implemented
• We may well do better to teach existing software verification tools about the attacker, than to build from scratch
• Into the bargain, we'll detect other security bugs, eg, overruns, using the same tools

(For an earlier version of this position, see my invited paper at LICS'06.)
A Rigorous Foundation

• RCF: a \( \lambda \)-calculus with concurrency and refinement types
  – Examples: \( x: \text{int}\ \{x>0\};\ \ u: \text{string} \star \ p: \text{string} \ \{\text{Req}(u,p) \land \text{Registered}(u)\}\}

• Why refine types?
  – Unifies several prior syntax-heavy type systems using logic
  – Via monadic encoding, obtain Hoare-style reasoning in \( \lambda \)-calculus
  – Implementations (F7, F5, F9) exploit recent advances in SMT solvers

• Why concurrency?
  – Brings \( \pi \)-calculus style modelling into the same unified framework

• Why \( \lambda \)-calculus?
  – Head-to-head comparison with other methods on existing code in ML
  – And because it’s still the “Next 700 Programming Languages”
Some Likely Leads for the Future

• Beyond purely static analysis of security
  – “One document. One. It’s the source code. You learn everything there and you know everything there.”
  – Godefroid “Automated Whitebox Fuzz Testing”

• Cloud computing
  – Enterprises want S&P for work split between cloud and on-premises
  – Opportunity to do multi-tier language compiled to multiple sites

• Domain specific languages
  – Many “little languages” to configure enterprise systems (eg cfengine)
  – Many actual security errors arise from misconfiguration
  – Security tools for specific DSLs useful (eg Policy Advisor). Generalize?