CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

AVAP: Automated Verification of Acquirer Properties

Practical Information Flow Verification in a Software Supply Chain

HRL Laboratories LLC
George Kuan, Ph.D.

September 16, 2013

This material is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD), BAA 11-02 and Air Force Research Laboratory Information Directorate via contract number FA8750-12-C-0236 .

Homeland Security

Science and Technology

Team Profile

HRL Laboratories, LLC

George Kuan (PI) Aleksey Nogin

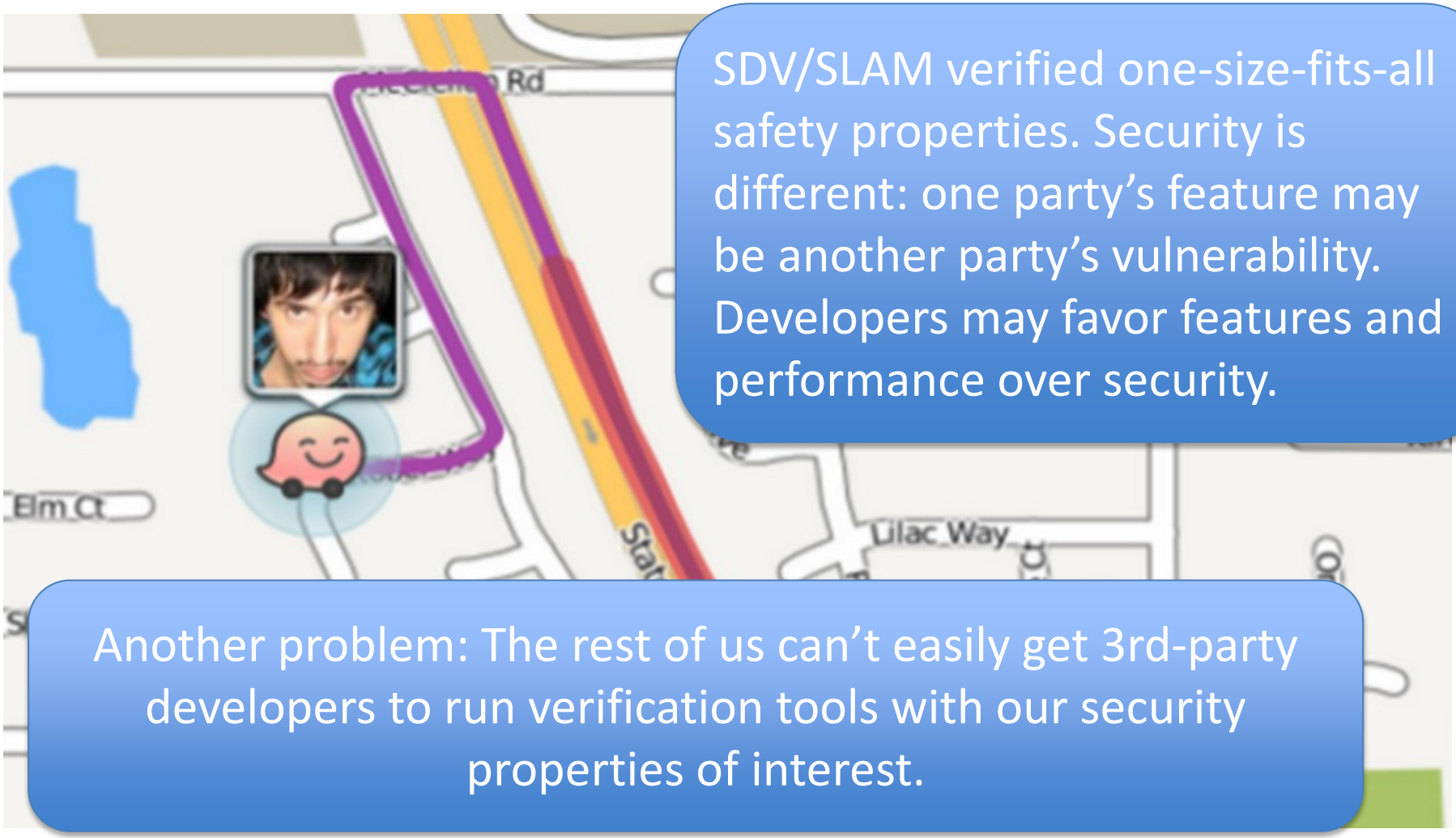
- Formerly Hughes Research Laboratories (est. 1948)
- Formed as a Limited Liability Company (LLC) , 1997
- R&D for The Boeing Company and General Motors
- Government and commercial contracts
- AS9100 accredited / DoD Trusted Foundry
- 250,000 square feet of lab space
- 10,000-square-foot Class 10 clean room
- Located on 72 acres in Malibu, CA

Stevens Institute of Technology

Dave Naumann (PI)
Andrey Chudnov

- Established 1870
- Located in Hoboken, NJ
- Also online and in DC
- Schools of: Engineering and Science; Technology Management; Systems and Enterprises
- Designated a National Center of Academic Excellence in Information Assurance Education (CAE) and Research (CAE-R)
- DoD National Center of Excellence in Systems Engineering Research
- DHS National Center of Excellence in Port Security
- Ranked #3 among US research universities for high ROI on research investment (Forbes.com)

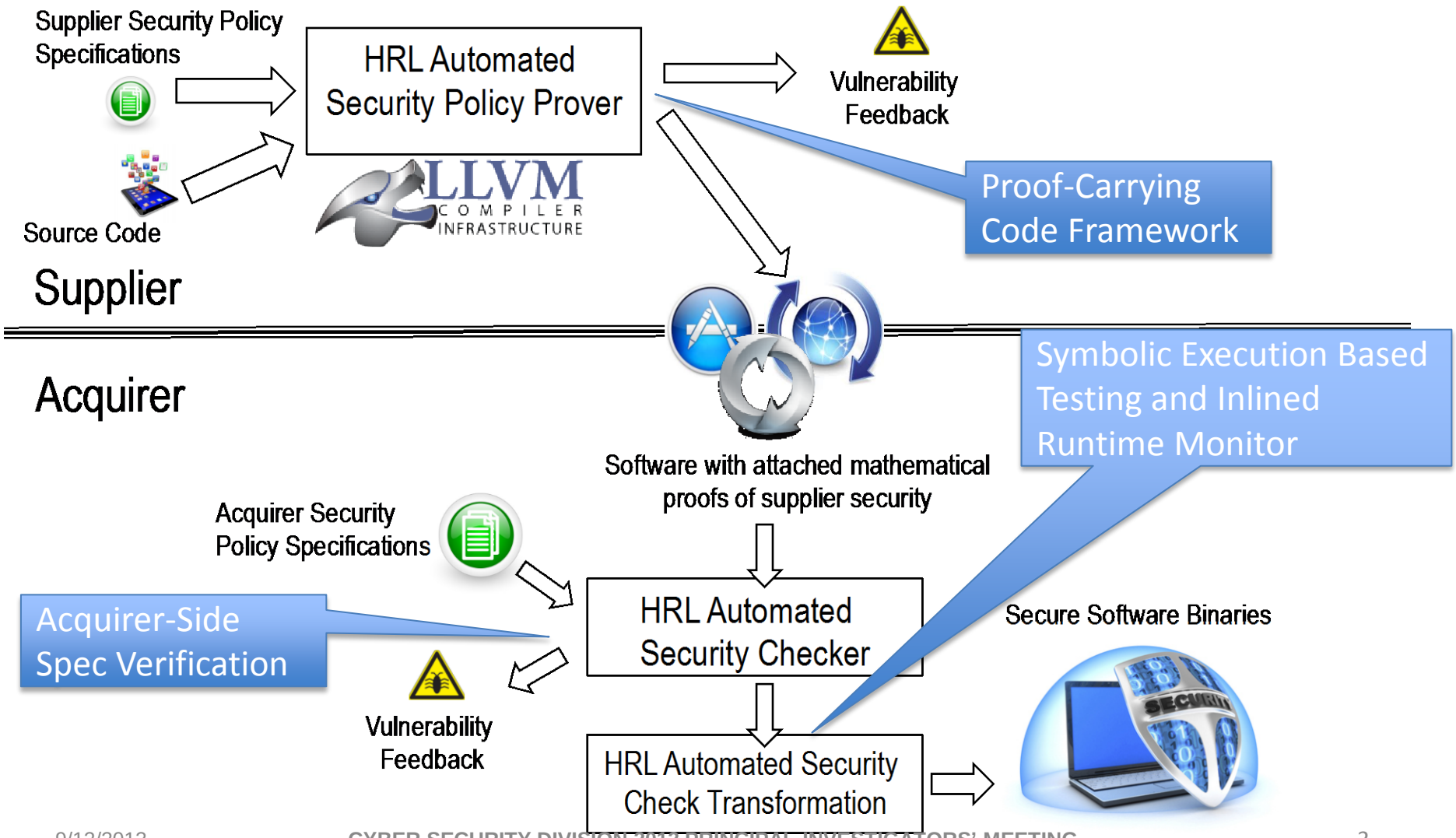
Customer Need



SDV/SLAM verified one-size-fits-all safety properties. Security is different: one party's feature may be another party's vulnerability. Developers may favor features and performance over security.

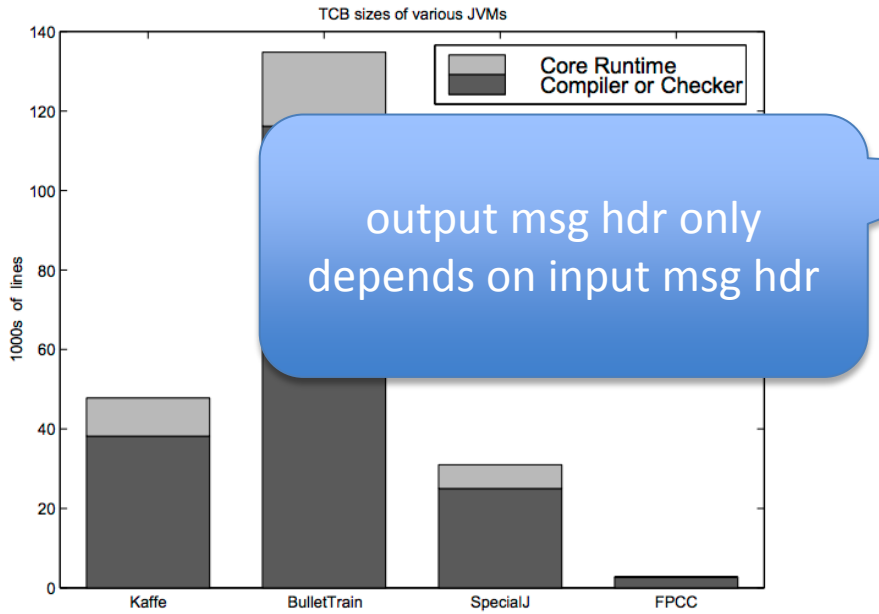
Another problem: The rest of us can't easily get 3rd-party developers to run verification tools with our security properties of interest.

Approach (1) - AVAP



Approach (2)

Proof-Carrying Code (Necula and Lee ’97) takes advantage of the observation that verifying a proof is easier and faster than generating one.

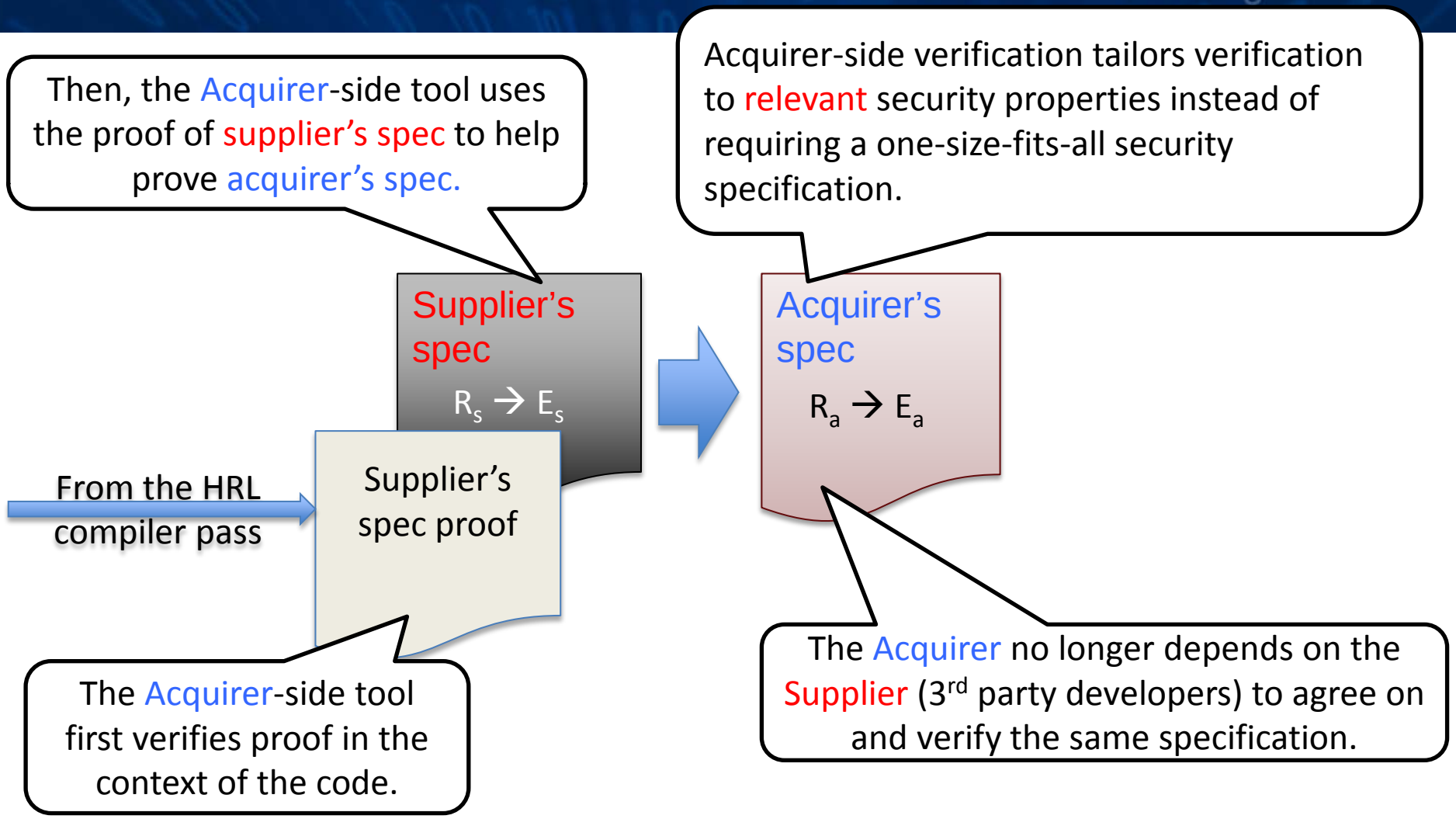


output msg hdr only depends on input msg hdr

- Security Properties
- Machine Semantics
- Proof Rules
- Proof Checker Core

Source: Appel et al ‘03

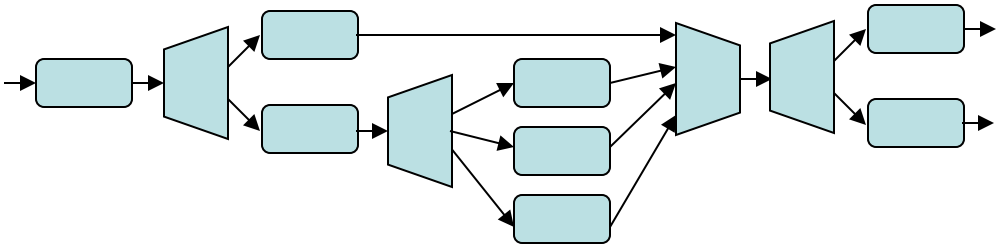
Approach (3)



Approach (4)

Control Flow Analysis

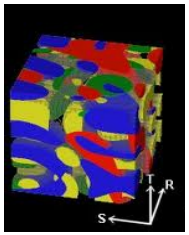
Representation

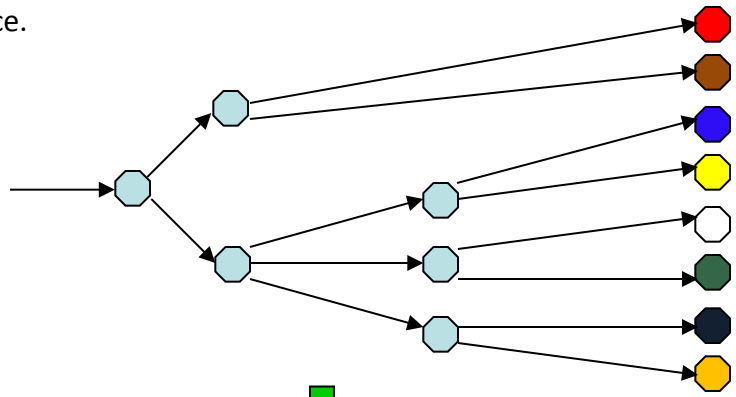


Static Semantic Representation
Control Flow Graph

(X,Y,Z)
Input space is divided into a set of equivalence classes, each defined by the region of input space that travels the same path through execution state space.

Symbolic Execution



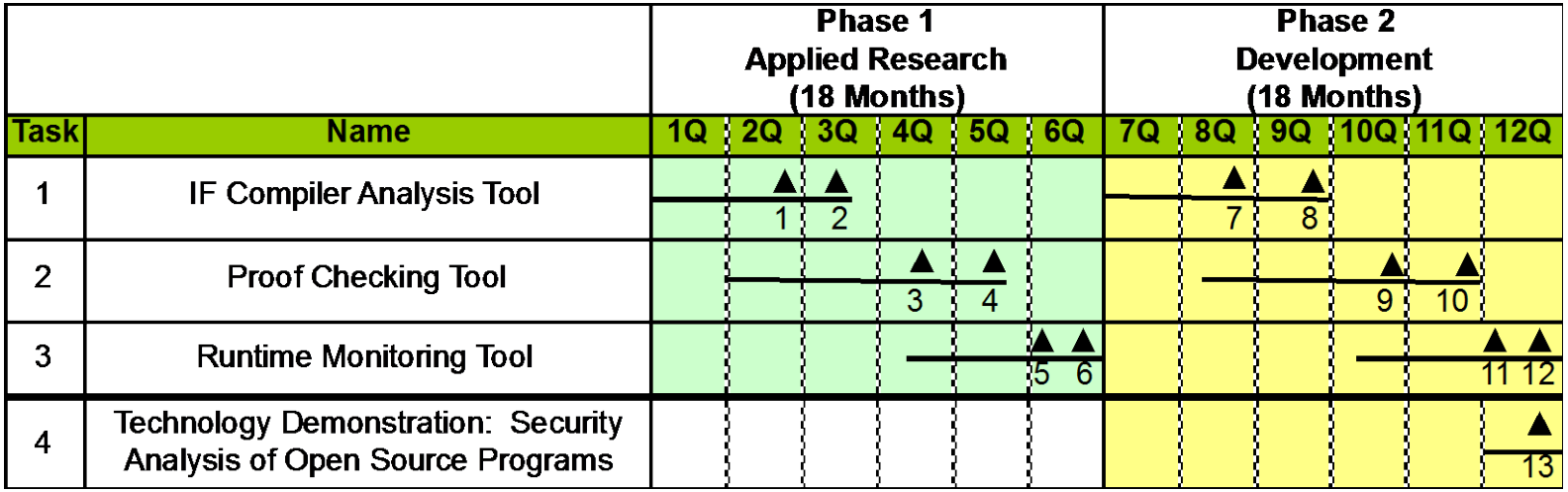


Dynamic Semantic Representation
Execution State Tree

Benefits

- For the Software Assurance community, Tunable Info Flow enables verification of Acquirer specs by the Acquirer without having to divulge the specs to the Supplier or a 3rd-party
- It empowers the Acquirer to check the most relevant information flow security spec and simultaneously simplify verification by taking into account the Acquirer's implicit assumptions
- Highly expressive framework for encoding properties
- Can help enable information flow-preserving compilation
- Portable across virtual machines and just-in-time compilers
- Takes advantage of existing compiler optimizations

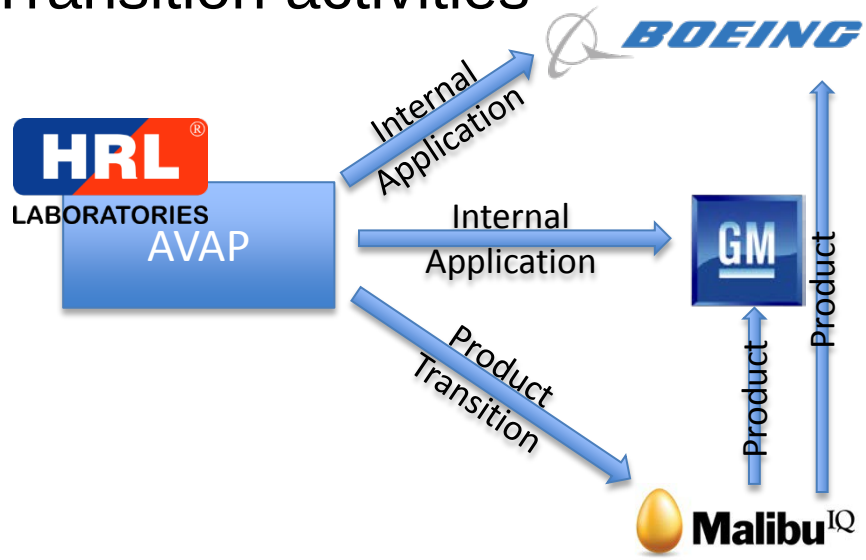
Current Status



- We have designed and implemented prototypes for the Compiler Pass and Proof Checking Tools.
- We have also designed the Runtime Monitoring Tool and adapted a symbolic executor to propagate information flow security tags.
- Designed an information flow specification contract language with novel features motivated by our analysis of vulnerabilities
- Theory and implementation technique for checking specification contract refinement

Next Steps

- Runtime Monitoring for Information Flow
- Larger-scale performance analysis
- Automated feedback mechanisms
- Transition activities



Contact Information

For more information:
George Kuan
gkuan@hrl.com