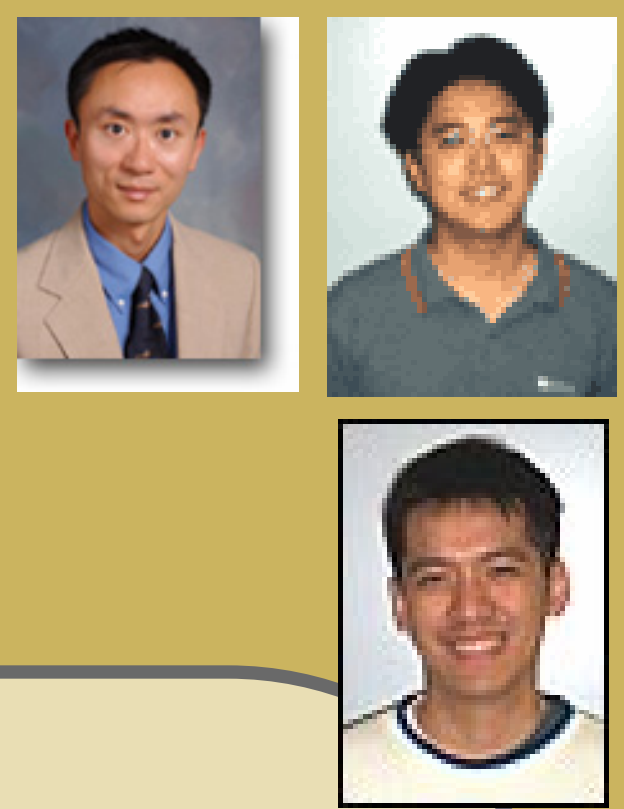


Formal Reasoning about Intrusion Detection Systems



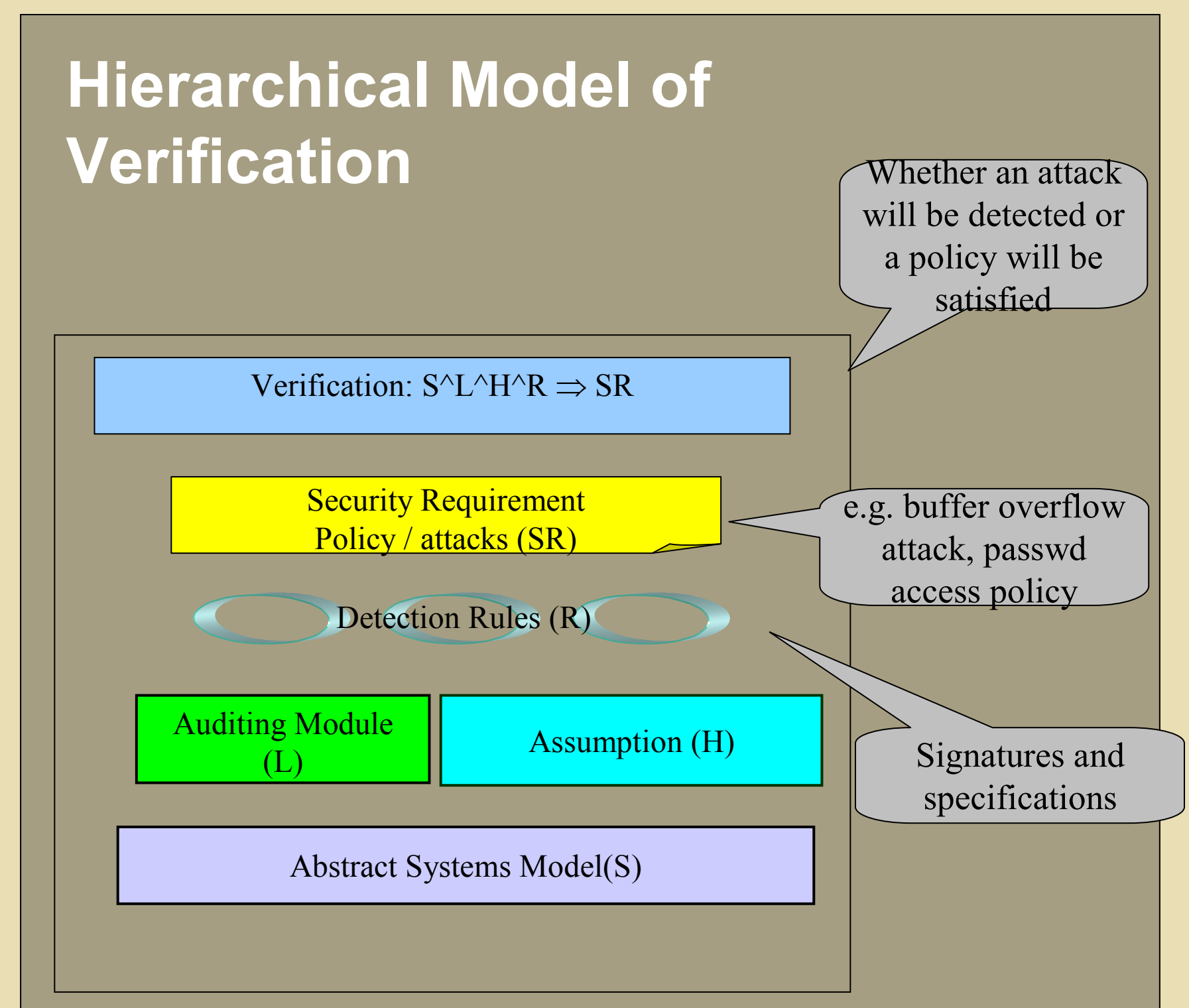
Hao Chen, Jeff Rowe, Tao Song, Henry Tseng, Angelina Wang UC Davis

Proving Security Properties of IDS's

We apply formal verification of the rules of a specification based intrusion detection system.

We prove that, under the assumption that the Unix kernel is secure, either the Unix security policy is maintained or an alert will be generated.

We work on the verification of a specification for monitoring intrusions in Ad-hoc mobile networks, to show that routing protocol messages will result in either correct Ad-hoc routing behavior or the generation of a security alert.



Approach and Impact

- Hierarchical verification model
- Verification in different levels
- Specification and Policy Languages
- Formalization and verification of security policies
- Formal evaluation metric for IDS

Specification-based IDS in Mobile Ad-Hoc Networks

Optimized Link State Routing (OLSR)

Multipoint Relays (MPR) - subset of 1-hop neighbors connecting all 2-hop neighbors

Routing Messages - Hello / 2 sec Topology Control (TC) / 5sec

Routing tables ← Topology tables

Attacker is message originator

Forge 1-hop neighbors in a Hello

Forge MPRs in a Hello

Forge MPR selectors in an initiated TC

Attacker is message forwarder

Forge MPR selectors in a forwarded TC

MANET IDS Specification Constraints

First constraint (C1)	Neighbors in Hello messages must be reciprocal
Second constraint (C2)	MPRs must reach all 2-hop neighbors
Third constraint (C3)	MPR selectors must match corresponding MPRs
Fourth constraint (C4)	Fidelity of forwarded TC messages must be maintained