Lifecyle Attestation:

Maintaining Appraisal Over System Changes

Perry Alexander and Adam Petz
The University of Kansas, Lawrence, KS

David Hardin and Amer Tahat
Collins Aerospace, Cedar Rapids, IA

Background

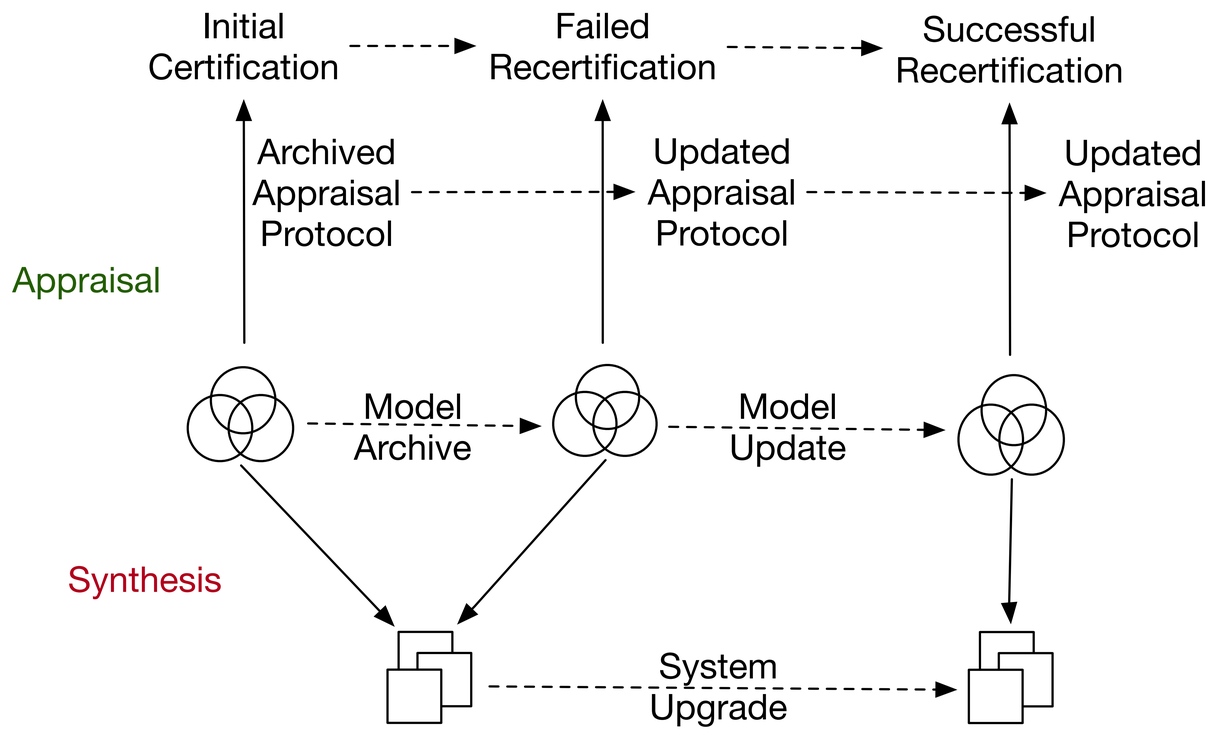
Semantic Remote Attestation provides mechanisms for measuring and appraising systems. The basic approach mimics any system appraisal or certification process:

- Appraiser requests an attestation
- Target produces bundled evidence
- Appraiser assesses evidence

An *attestation protocol* governs interactions and the gathering of evidence.

Research Questions

- Can we use an attestation protocol more generically as an *appraisal protocol*?
- Can we use the appraisal protocol to maintain evidence over system lifecycle?
- Can we use synthesis and ML techniques to repair protocols over system lifecycle?



Methods and Materials

- GPT for machine learning of Copland proofs in Coq
- Existing Copland proof-base for learning corpus
- Used Copland attestation protocol representation for appraisal protocols
- Copland semantics and Coq sigma types for evidence representation
- Eventually use Coq Cakeml extraction for system synthesis

Initial Results

- CoqDog GPT-based learning demonstrations for repairing and adapting proofs
  - Automatically generate proof snippets in Coq, Isabelle and Lean
  - Learning from proofs over Copland protocol verification
- Highly parameterized attestation manager for running appraisal protocols
  - General purpose mechanism for integrating attestation services
  - Enhance traditional measurements with proofs and tests
- Dependently typed theory for maintaining systems and evidence
  - Record observations made by individual appraisal actions
  - Record if and how evidence supports conclusions

Future Work

- Deeper ML for proof repair in the context of appraisal protocols
- ML for refining and adapting appraisal protocols
- ML informed synthesis techniques that mix ML with traditional program synthesis
- Tighter integration with appraisal and certification workflows
- Synthesis of artifacts from specifications

References

- V. Haldar, D. Chandra, and M. Franz. “Semantic remote attestation – a virtual machine directed approach to trusted computing.” *In Proceedings of the Third Virtual Machine Research and Technology Symposium,* San Jose, CA, May 2004
- G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O’Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. “Principles of remote attestation.” *International Journal of Information Security,* **10**(2):63–81, June 2011.

Acknowledgements

This work is supported by DARPA contract HR00111890001. We gratefully acknowledge their continuing support.