Discussion Notes for the presentation
Dawn Song, Adrian Perrig, and Doantam Phan. Agvi - automatic
generation, verification, and implementation of security protocols. In 13th

Presenter: AliReza Namvar

The discussion was around the content of the paper. It does not seem to be appealing. In order to understand the concepts in the AGVI, we need to study the papers referenced at the bottom of this document. Following points were issued in the discussion:

- How is the belief logic used in the AGVI model? The paper does not address the usage of an adversary model; therefore the beliefs and the access of principals on beliefs are not described in this model. However there is an implicit application of beliefs in the initial setup configuration that defines which cryptographic primitives are available to the principals and what keys each principal possesses.
- The efficiency of the generated code is another issue about the code generator. The authors did not explain it. However there is an inaccessible technical report that probably has some material about that. The reference is: “Adrian Perrig, Doantam Phan, and Dawn Xiaodong Song. ACG-automatic code generation, automatic implementation of a security protocol. Technical Report 00-1120, UC Berkeley, December 2000”.
- The protocol generation and enumeration have a complexity worse than NP, because of infinity of the protocols state space, and the exponential increase in the protocol space, as more requirements are added to the protocol specification.
- The definition of flaw is quite unclear in the paper.
- There is no possible validation for experimenting other protocols interactively. For other protocols, the user needs to re-specify it with different set of selection in the GUI and generate it again. However there is a possibility of finding no protocol for a certain specification.
- Re-factorizing the generated code to find out which part of the code satisfies what specific security protocol would be useful.

References:
