Knowledge Based Security Protocol Verification System

for Bridging Security Primitives and Protocols in IA Courses

Weichao Wang, Aidong Lu, Zhiwei Li, Li Yu (UNC-Charlotte)

http://sis.uncc.edu/~wwang22/Research/Projects/CCLI-I/CCLI-I.html

1. Objectives

• Develop a digital LEGO system to help students better understand relationship among security primitives and protocols, and apply their knowledge flexibly

• Develop corresponding experiments and hands-on exercises for the LEGO system

• Conduct systematic evaluation of the approach in undergraduate and graduate level information assurance courses

2. Motivations

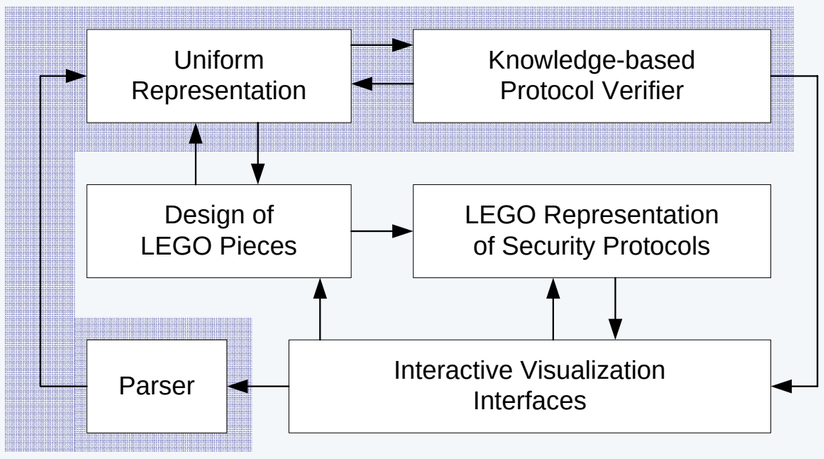
• More and more universities have established their own IA curriculum

• The introductory level and advanced courses demonstrate a gap in teaching security primitives and protocols

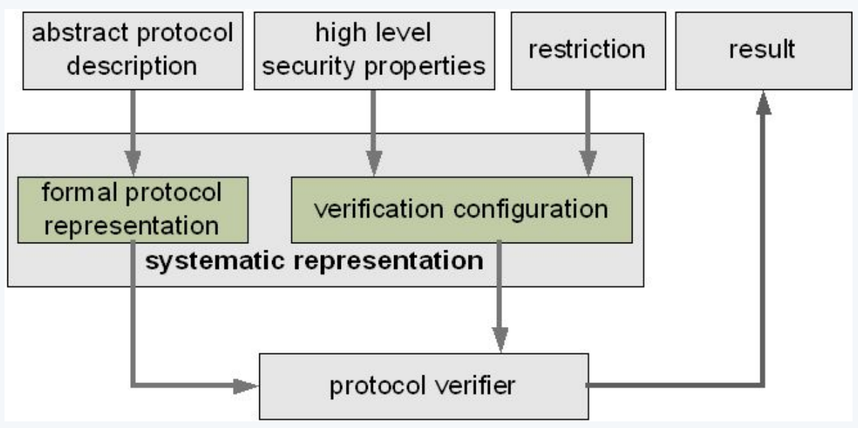
• Has negative impacts on understanding and applying knowledge by students

• Restrict the development of student skills

3. Architecture of Overall Approach



4. Knowledge based Protocol Verifier



5. Formal Treatment of Protocols and Security Properties

Modeling Protocols

• Develop a term syntax to represent the grammar of security protocols

• Define a closure operator to characterize the capability of an entity to construct terms from a term set

• Define the concept of derivable for establishing the knowledge model

• Define the set of rules for instantiation

Modeling Security Properties

• Use strand space model to generate a group of formula to represent the most widely used security properties

• Treat strands of requesters, responders, trusted third parties, and attackers respectively

• Evaluate these formula with causal bundles during verification

6. Knowledge Model Framework

Knowledge Base

• Define the concept of knowledge base

• Develop mechanisms to calculate the knowledge base of a term set

Inference Rules

• Define the set of inference rules to composite and decompose messages

Model Learning

• Define the concept of model learning

• Determine state transition rules during model learning

• Develop state pruning rules to improve the efficiency of the approach

7. Impacts

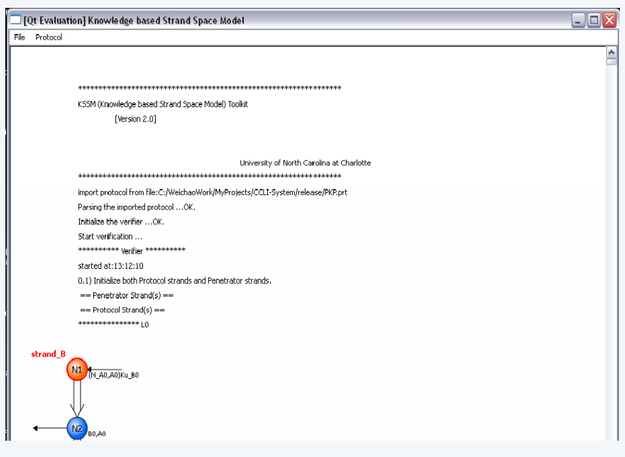
• Bridge the gap between security primitives and protocols in IA education

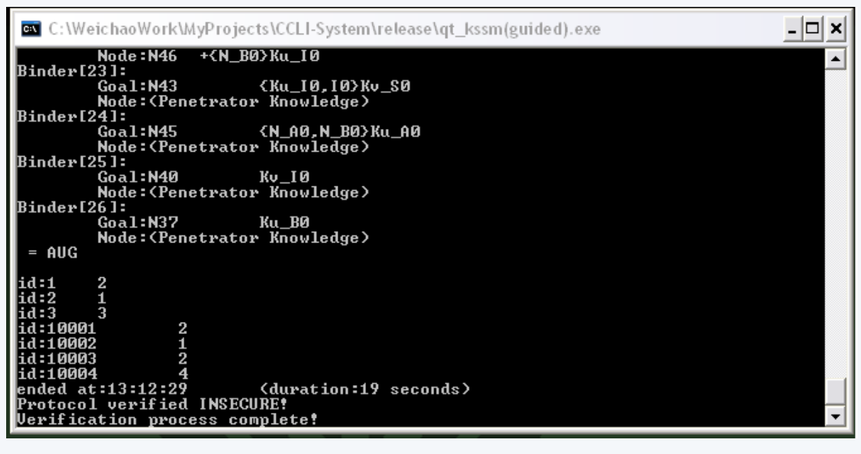
• Construct a platform for protocol verification for the digital LEGO system

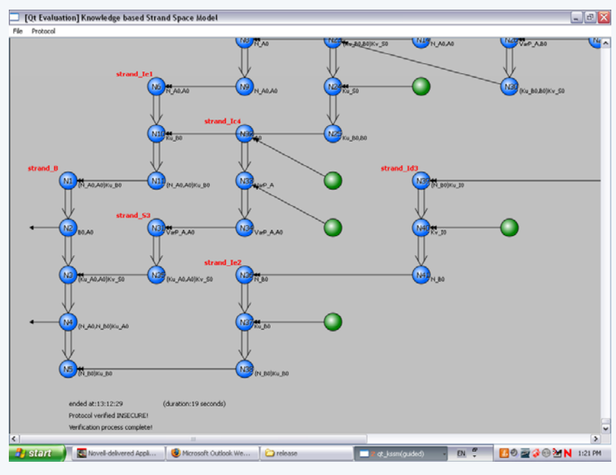
• Enable instructors to design, share, and expand their class materials

• Enable students to conduct hands-on exercises on protocol design

8. System Implementation







Protocol input | **Verification procedure** | **Verification results and attack illustration**

This project is supported by NSF Course, Curriculum, and Laboratory Improvement (CCLI) Program under award DUE 0754592.