Digital LEGO Sets for Information Assurance Courses

Li Yu, Aidong Lu, Zhiwei Li, Weichao Wang

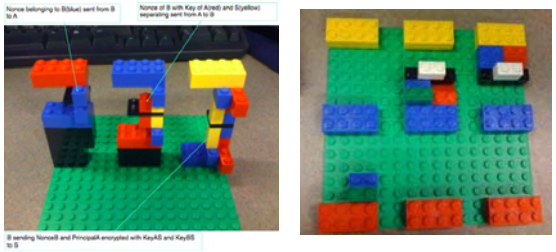
University of North Carolina at Charlotte

Abstract

❖ To bridge the gap between the instruction of security primitives and protocols, we have designed and developed a digital Lego system and supporting course materials.

❖ The digital Lego sets and exercises help to expose the relationship among security primitives and properties, and train students' capabilities to design secure protocols under different requirements.

❖ Our approach applies the pedagogical methods learned from toy construction sets by treating security atomics as Lego pieces and protocols as construction results.



Two Designs of Using Real Legos to Build Security Protocols

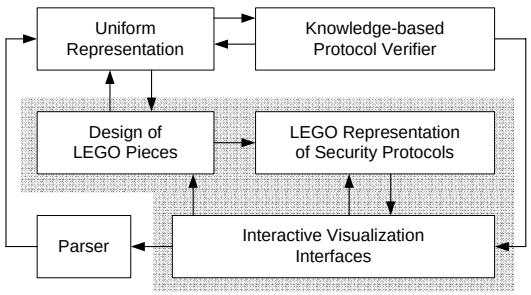
Impacts

❖ Helping students bridge the security primitives and protocols and improving their understanding of the course contents

❖ Providing a friendly and encouraging platform and a group of demonstration and experiment samples to assist instructors to prepare their course materials

❖ Enabling instructors to easily share, expand, and modify their course materials

Overview



Digital Lego Generation

We design digital Legos to represent general security protocols. They simulate concept of Legos for more effective communication.

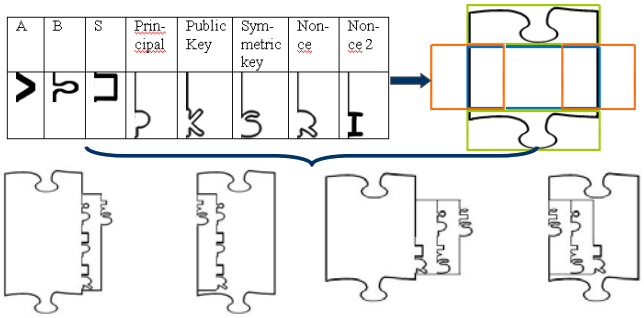
Process

❖ Design basic shapes/images

❖ Construct Legos automatically using message contents

Design

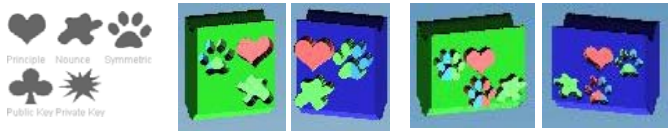
❖ 2D continuous boundaries



A,B:KAS{A,B,NB}

B,S:KBS{A,KAS{NB}}

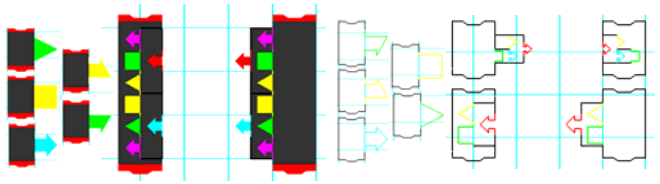
❖ 3D continuous surfaces



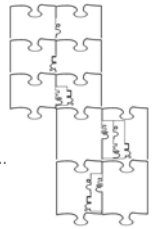
Advantages Over Real Legos

❖ Easy switch among multiple styles

❖ Incorporate visualization techniques for user-friendly demonstration and exercises



Using Digital Lego Sets



Interaction

❖ For constructing and modifying protocols

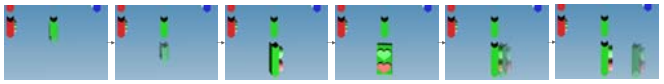
❖ 2D/3D operations: moving, rotating, merging, editing …

Animation

❖ For demonstrating protocols effectively

❖ Important concepts can be assigned by instructors

❖ Animation styles can be adjusted



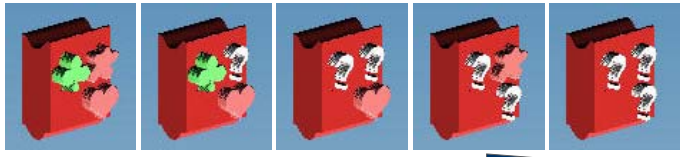
An animation sequence demonstrating a sending activity

Exercise

❖ User friendly exercise system: instant feedbacks based on user interaction

❖ Adopt advanced illustrative visualization techniques

❖ Integrate automatic security components



Increasing difficulty levels / Random Generated exercises

Publication

A Digital Lego Set and Exercises for Teaching Security Protocols, in Proceedings of Colloquium for Information Systems Security Education (CISSE), pp 26-33, Dallas, June 2008.

Acknowledgement

CCLI-0633150 Collaborative Research: Bridging Security Primitives and Protocols: A Digital LEGO Set for Information Assurance Courses

Contact

Aidong Lu, aidong.lu@uncc.edu, http://www.cs.uncc.edu/~alu1
http://sis.uncc.edu/~wwang22/Research/Projects/CCLI-I/CCLI-I.html

UNC CHARLOTTE

National Science Foundation
WHERE DISCOVERIES BEGIN