Digital Lego Set: Design and Exercises Teaching Security Protocol

Lane Harrison, Dr. Aidong Lu, Li Yu
{ltharri1, aidong.lu, lyu8, }@uncc.edu

Lane at a Lego - laden desk

Introduction

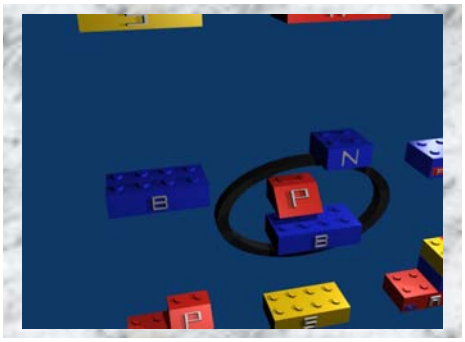
It is well known that learning security protocols is difficult. In the past, protocols were only discussed in graduate level courses. Part of the reason for this difficulty is the use of specialized relational algebra to represent the protocol process. Another difficulty is communicating the connection between security primitives (pseudo-random numbers, identification principals, time-stamps, etc.) and the processes taking place in the protocol.

We have developed a Digital Lego Set to address some of these problems. It has been shown that students learn information security by “doing it”. By using digital Lego bricks, students will be able to construct both classic and new protocols as well as see the effects of their interactions on the protocol’s outcome. We also have designed a set of exercises and demos that can be used in a classroom setting which use the Digital Lego Set while incorporating different learning styles and viewpoints of security protocols.

Background

Various tools have been developed to aid in the teaching of security protocols. Bill Chu (UNC-Charlotte) and faculty from NCA&T developed an interactive animation to help teach the complex Kerberos V.5 protocol. Dr. Leonard Hamey (Macquarie University, Australia) developed a game using envelopes, colored paper, and other common office supplies to teach protocols and attacks on protocols.

Protocol development is a constructive process. An example would be Woo & Lam pi protocol being “deconstructed” and simplified in 4 steps to produce the simple Woo and Lam pi f protocol for which no attacks are known. Lego bricks are easily seen as constructive tools.



Exploded View

Research

My contributions are in two main areas--the design of the digital Legos and the design of the exercises and demos using the Digital Lego Set. In the following points I will attempt to briefly outline what I did:

Digital Lego Design:

•Generated multiple prototypes of protocol representations using real Lego sets

•Generated multiple prototypes of protocol representation using digital Legos (made using Blender)

•Designed alternate symbols and shapes to represent security primitives to accommodate student and/or teacher preferences.

•Generated various animation prototypes to represent processes and key concepts in a security protocol.

Exercises and Demos using the Digital Lego Set (DLS):

•Designed and implemented various random removal methods based on a difficulty level:

- Random removal from a set of specified "important" pieces of a security protocol.
- Random removal of only a type of primitive.

•Wrote identify questions and feedback using the DLS as a visual aid:

- Questions are based on current security/security protocol education research.
- Use animations to highlight the part/process of the protocol relevant to the current question (not yet implemented).

Impact

Materials produced not mentioned in Research are as follows:

- Annotated bibliography of selected security education research
- Various prototype documents

Conclusions

The following is a brief list of the things I learned (or did) this summer:

•Learned to make 3D models in Blender.

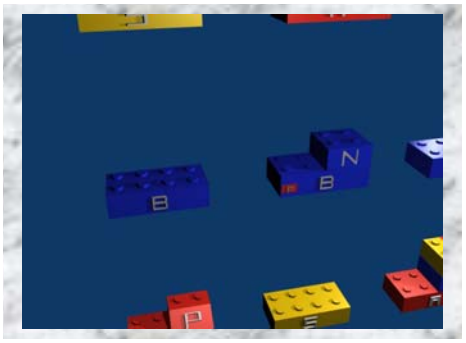
•Learned some Python and Panda3D game engine to make a simple animation.

•Read 10+ papers on information security education and security protocols.

•Learned to quickly prototype design and animation ideas and to communicate them effectively through design documents.

•Learned to edit and work with other's code.

•Worked on a team made up of members from different departments.



Visual Knowledge Retention

Future Work

The following list will outline future work plans:

•Expand questions set to include more protocols.

•Generate more alternate shapes to represent security primitives.

•Design an automatic animation generator for simulating protocols according to user's specifications.

•Finish implementing exercises into the Digital Lego Set software.

•Complete a user study using the exercises and demos.

•Submit a paper to SIGCSE by August 31, 2008.