Puzzle-Based Learning (PBL) to Cyber-Security Education

Dipankar Dasgupta
Center for Information Assurance
Department of Computer Science
The University of Memphis
Cyber Security Puzzles

• Cyber–enabled systems are composed many sw/hw components which interact with each other in a complex way.
• Hackers are finding new ways to exploit these components bypassing security perimeters.
• Need a better understanding of which components are involved in cyber interaction and how to protect and secure these paths
• PBL seems to provide innovative ways to learn security concepts to fight against cyber attacks
PBL for Cyber Security Education

• Create an abstract scenarios based on mathematical logic where the scenario depicts some possible attacks
• Currently using two puzzle design methods: Truth-table based and Decision-Tree based (and their combinations)
• Participants are asked to interpret existing vulnerabilities or best practices and how to avoid or address vulnerabilities being exploited or avoided
• Their responses may lead them to different branches of attack paths/states so to realize whether their responses lead to any exposed state or results in data breaches.
• We considered CVSS, NVD and other updated cyber information for developing different type of dynamic problems.
• Interactive interface to the participants.

• Participants can choose action according to their preference.
Results are summarized by a attack tree.
Evaluation Results

Figure: Classification of responses received from the students before and after the use of puzzles (in a class of 28 students)
Developing Scenarios

Storyline will be built based on some realistic Network (Wing’07) and study possible attack vectors:
Create a puzzle involving similar alternate paths with different servers/Applications with Vulnerabilities in NVD.
Summary

- PBL provokes the *thinking process* by combining mathematical logic with challenges.

- *Interactive process* allows in exploring all possible solutions to a class of security problems in varying environmental situation.

- Participants can review the *consequences* of their *actions*, making the learning process more interesting.

- Several PBL based cyber security assignments/exercises are under development.