Module: RFID Security

9/8/11

Copyright © 2008, 2009, 2011 by Dale R. Thompson {d.r.thompson@ieee.org}

Goal/Assessment

Goal
Where are we going? What is expected? What will the student be able to do, know, and value at the end?

The student will be introduced to general security issues and threats to and by an RFID system. It is expected that the student will be provided with enough security background to perform basic threat modeling and risk analysis. The student will know the definitions of confidentiality, integrity, and availability. The student will be able to choose and apply cryptographic techniques. Finally, the student will be able to perform basic threat modeling and risk analysis.

Assessment
How do we measure? How will the student be assessed in the lessons and at the end of the module?
Use general terms. Present this to the student at the beginning of the module.

A student should:

- Be able to describe the three principles of security.
- Be able to describe threats to and by RFID.
- Be able to list symmetric- and asymmetric-key encryption algorithms, describe the difference between symmetric- and asymmetric-key cryptography, and modify an existing authentication protocol to make it more secure.
- Be able to describe all the STRIDE threat model categories.

Hook
Pique the student’s interest using a case study, interesting story, experiment, or disaster.

Case study: Discuss the hacking of implantable cardiac defibrillators (ICDs).
Lessons

Divide the module into logical lessons (4-5 days). Create lessons, activities, experiments, homework and/or quizzes based on these grain size lessons.

Lesson: Confidentiality, Integrity, and Availability

Lesson: Threats to and by an RFID system

Lesson: Introduction to Cryptography

Lesson: Threat Modeling

Culminating Activity

Tie it all together returning to the big idea. Go full circle. Create a culminating experience that ties lessons back to the module theme. Create module-level rubric and each topic is one of the lessons below.

Perform threat modeling and risk analysis on a given system

Assessment

Assess the results using tools such as paper/pencil, programming, simulation, demonstration, experiments, and projects. Paper and pencil homework assesses what you know. Programming, simulations, demonstrations, and projects assess what you can do.

Assessment:

Use rubric based on lessons. Each lesson is a row in the rubric.
Copyright Notice
This material is Copyright © 2008, 2009, 2011 by Dale R. Thompson. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or incorporated in commercial documents without the written permission of the copyright holder.

Acknowledgment
These materials were developed through a grant from the National Science Foundation at the University of Arkansas. Any opinions, findings, and recommendations or conclusions expressed in these materials are those of the author(s) and do not necessarily reflect those of the National Science Foundation or the University of Arkansas.

Liability Release
The curriculum activities and lessons have been designed to be safe and engaging learning experiences and have been field-tested with university students. However, due to the numerous variables that exist, the author(s) does not assume any liability for the use of this product. These curriculum activities and lessons are provided as is without any express or implied warranty. The user is responsible and liable for following all stated and generally accepted safety guidelines and practices.