Lesson Title: Reader Layer Threats, Risks, and Mitigation

7/15/09
Copyright © 2008, 2009 by Dale R. Thompson {d.r.thompson@ieee.org}

Rationale
Why is this lesson important? Why does the student need this lesson? How does this lesson fit in the larger module?

The lesson addresses the security issues of the reader layer. RFID readers are a combination of software-defined radios and computers with operating systems. They have OSI data link interfaces such as Ethernet or wireless IEEE 802.3b that are connected to a computer network. Therefore, readers have the same security threats as any computer that is connected to a network including threats to the operating system and threats from the network. The student needs this lesson to understand the security threats to networked computers, techniques to mitigate these threats, and risks.

Objective(s)
What will the student know, be able to do, and value at the end of this lesson? This is smaller amounts of information than the module objectives.

The student will be able to list some common threats, evaluate risk using the STRIDE and DREAD models, and synthesize a new threat.

Exploration
Explicit concepts related to the Module goal are explored. It is at this point that the student will be provided basic information about the topic and the chance to explore some basic concepts about the topic. This is where the instructor imparts information.

- Review confidentiality, integrity, and availability.
- Review definition of threat and risk.
- Apply the STRIDE threat model.
  - How can you spoof the system?
  - How can you tamper with data?
  - How can you repudiate your actions?
  - How can you cause the system to disclose information (information disclosure) that should be confidential?
  - How can you deny service to authorized users?
  - How can you elevate your privilege?
- Which threat seems the most important?
- Apply the DREAD risk model to the chosen threat.
  - What is the damage potential?
  - How easy is the threat to reproduce?
  - How easy is the threat to exploit?
  - Rank the number of affected users that the threat affects.
  - How easy is it for the threat to be discovered?
- Review general techniques to mitigate threats in each of the six categories of the STRIDE model.
- Discuss general and specific techniques to mitigate the some of the threats categorized with the STRIDE model.
Reflection
Several questions are posed to the student to answer and then often discuss as a class. This is an attempt to determine whether the student "gets" the basic concepts delivered above. If they do get it, move on to engagement. If they do not get it, go back to exploration above. It could be as simple as asking a few probing questions or as complex as asking the student to write a paper.

- Rank threats to confidentiality, integrity, and availability from the easiest to the hardest to exploit.
- Can you think of a threat not discussed yet?
- Of all the six threat categories in the STRIDE threat model, which is easiest to exploit?
- Is the STRIDE threat model or DREAD risk model easier to apply? Why?
- What criteria can be used for assigning a value to damage potential?

Engagement
Concepts learned in the Exploration are further developed by conducting experiments, designing and building solutions, and solving problems. This is an attempt to cause the student to apply the new knowledge. By applying the new knowledge, the student is much more likely to retain this information. This engagement could be accomplished through a debate, an experiment, a problem solving activity, or anything else that would cause the student to demonstrate understanding and competence.

- Homework assignment
  - Apply STRIDE threat model to a system.
  - Apply DREAD risk model to a particular threat of the system.

Expansion
Provide opportunities for students to expand the concepts to more general or global situations including connection to the Module goal. Expand back to the big ideas of the module and prepare for the next lesson.

- Name two mitigation techniques a reader could use to prevent denial of service.

Lesson Assessment
Assess student understanding of the lesson content. This does not have to be a full-blown examination. It could be a graded homework assignment, a quiz, a performance examination, a graded problem solving activity, or something similar.

- Homework assignment

Equipment
- None

Software
- None

References
- Neeraj Chaudhry, Dale .R. Thompson, and Craig Thompson, RFID Technical Tutorial and Threat Modeling, ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering,

Copyright Notice
This material is Copyright © 2008, 2009 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.