Lesson Title: Threats to and by an RFID system

9/8/11
Copyright © 2008, 2009, 2011 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?

It is important to know the types of threats to and by an RFID system. The student needs this lesson to be able to mitigate the threats. This lesson provides the student with an overview of several threats.

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 describe threats to and by RFID.

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.

- Threats to RFID system
  - Tag cloning – Duplicating tag data to another equivalent tag.
  - Reader cloning – Duplicating an authorized reader.
  - Replay attack – Recording signals and replaying them later to attack the system.
  - Tag spoofing – Duplicating tag signals with unauthorized tag or system made to look like one or more tags and transmitting them to a reader and/or back-end system to mimic an authorized tag. A spoofed tag could act like thousands of tags performing a denial of service attack.
  - Reader spoofing – Duplicating reader signals with unauthorized reader or system made to look like a reader and transmitting them to a tag and/or back-end system to mimic an authorized reader.
  - Modifying tag data – Modifying, adding, or reordering data on tags.
  - Deleting tag data – Erasing data or locking memory to render the tag useless.
  - Skimming (also called scanning) – Unauthorized primary access or reading of tag data using an interrogator. Signal which addresses the tag to get information from the tags.
  - Eavesdropping (passive) – Unauthorized listening / intercepting through the use of radio receiving equipment.
  - Relay attack or Man-in-the-middle attack (Parasitic Eavesdropping) (active) – Unauthorized listening through the use of a separate reader system at distance, while tag is powered by a nearby reader. For example, a device sometimes called a ghost can be placed near the authorized reader to eavesdrop and then retransmit the signal over radio waves to a different reader sometimes called a leech at another location that is near authorized tag. (Note that this can be used to extend the range for skimming. The device near the authorized reader eavesdrops and tricks the authorized reader to do a
“read” command, which is retransmitted over radio waves to a different reader at another location that is near the tag to be skimmed.)

- **Jamming** – Using of an electronic device to disrupt all tag/reader communication within its range.
- **Shielding** – Placing an object between the reader and tag to prevent reading of a tag. The object could absorb the signal like water or reflect the signal like a Faraday cage made of aluminum foil.
- **Coupling** – Placing an object near the tag or reader that detunes the circuit enough to disrupt communication. Ferrous material can be placed near a tag such that the frequency of the circuit changes.
- **Blocker tag** – Carrying a blocker tag that disrupts reader communication. The blocker tag is used against the anti-collision protocols. An attacker can simulate many RFID tags simultaneously causing the anti-collision to perform singulation on a large number of tags making the system unavailable to authorized use.

**Threats by RFID system**

- **Tracking** – Determine where individuals are located
- **Tracing** – Determine where individuals have been
- **Hotlisting** – Single out certain individuals because of the items they possess
- **Profiling** – Identifying the items an individual has in their possession
- **Identification by constellations** – Identifying an individual by the group of tag identifiers that they carry. This threat requires profiling the individual first.

**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.

- What is a replay attack?
- What is skimming?
- What is a man-in-the-middle attack and what is another name for it?
- What does jamming, shielding, coupling, and a blocker tag have in common?
- Why would some people not want the RFID-enabled objects that they carry to be inventoried by a reader?

**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.

- Given the threats discussed, as a class, group them into categories.

**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.
• Choose one threat and determine a way to mitigate it.

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

Equipment
• None

Software
• None

References
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.