

The Need for Collaborative Threat Modeling

To make a logical determination of an RFID system's privacy and security risks, rather than one based on potentially biased perceptions of each individual part, we need to work together to view a security objective in a contextual environment.

By Mike Ahmadi

Dec. 8, 2008—We live in an era in which searching the term "security" on Google brings up a whopping 850 million hits, while the term "contentment" results in only 4.6 million hits. Whether that is prescient is debatable, but I think we can all agree that security (and privacy) weigh heavily on our collective consciousness.

This becomes a cause for concern when the decisions we make regarding security—specifically, RFID security—are based more on perception than on logical reasoning. Yet logical reasoning is somewhat difficult to achieve when there is either a lack of empirical evidence or, perhaps more importantly, available empirical evidence that tends to skew our perspective. If, for instance, it is determined that a secure RFID chip can be hacked by a particular method, we may be led to believe the entire system is fraught with security vulnerabilities, which may or may not be the case.

On the other hand, we may also be led to believe a secure RFID chip can, indeed, solve all problems related to the security of an RFID-based system, which may or may not be true either. In addition, we may fail to realize that simply breaking the security of a single RFID chip, or of a portion of the system, does not necessarily scale to a level where we should be concerned. It soon becomes clear that it is exceedingly important to determine the value we place on both security threats and security countermeasures within a given context.

Jonathan Collins, in an opinion piece he wrote for *RFID Journal* (see [Behind the Headlines](#)) in response to headlines regarding the hacking of Mifare chips by a group of Dutch scientists and researchers, raised this point when he stated that "...a system's security level is based on a number of checks, as well as design choices. One key choice is balancing technology costs with security requirements for each element of the system." He then went on to suggest that the security level [NXP Semiconductors](#) chose for the Mifare system was commensurate with the associated financial risk. This is, indeed, a valid point—and difficult to argue against. Where this view begins to cause me to wrinkle my forehead, however, is when Mr. Collins stated: "All told, that puts the benefits of Mifare ticketing systems ahead of any threat from cloning. In addition, Mifare Plus, with a new strengthened security encryption, is due by year's end."

Can you see where this breaks down? Let me attempt to explain. Consumers who do not truly understand the intricacies of system security might very well be led to believe the empirical evidence surrounding the Mifare chip's clonability (and the reduced clonability of the Mifare Plus chip) is somehow all they need to be concerned with. But as a security professional, I would postulate that it is only one small (yet significant) piece of the entire security equation.

Breaking the security of a Mifare chip does not prove the system is secure or insecure, nor does replacing the Mifare chip with the Mifare Plus chip. The Mifare hack simply demonstrates a hole in the armor, and the

Mifare Plus chip simply represents a patch for that hole. What I want to know is what's happening in the rest of the system. How vulnerable is the interrogator, the database and so forth? Someone attempting to infiltrate a fortified system does not always try to enter through a door that has now been barricaded and is being guarded.

Do we simply adopt a wait-and-see attitude in the hope that we will be able to catch the breach before it becomes a problem, or before a hacker discovers it? Do we simply cease all development of RFID systems until we have this all sorted out? I would say the answer to these questions is no, but how can we perhaps feel a bit more confident in the choices we make when it comes to RFID security, without any knowledge or understanding of the associated threats and risks?

One potential solution is collaborative threat modeling (click [here](#) for an example of a threat model output). The idea behind threat modeling is to view a security objective in a contextual environment, then posit potential threats and countermeasures in a structured manner in which each part of the system is represented, and in which the effect of either a security threat or countermeasure can be understood in terms of how it affects the system. The model's collaborative nature allows for the input of various factions (vendor, security expert, company executives, consultant and consumer), based on what each perceives to be valid points, and enables all collaborators to both view and comment on all inputs. This approach allows every stakeholder to make a logical determination based on a modeled representation of the system, rather than on the potentially biased perceptions of each individual part, which—when taken out of context—may have a tendency to skew judgment.

What is perhaps most important in this exercise is to understand the need to view this situation within a given context. In other words, if a threat model performed on the Mifare technology used in Boston's mass transit system leads us to conclude that the benefits of such technology far outweigh the risks, we cannot necessarily assume the same technology is appropriate for use in an identification system at, for instance, a nuclear power plant. Each context must have its own threat model associated with it.

RELATED_ARTICLES Thalidomide was prescribed in the 1950s and 1960s for use by pregnant women to prevent morning sickness, yet inadequate studies of the drug's potential side effects had not yet been undertaken. As a result, women who took Thalidomide during pregnancy gave birth to children with severe birth defects. In response to these defects, the drug was banned from all use in the United States, and the ban was not lifted until 1997. Recently, however, the drug has been found to be potentially quite beneficial in the treatment of myeloma, a particularly nasty cancer of the plasma cells. How many potential victims of myeloma might have been saved if we had chosen to model the risks of using thalidomide within the context of anything other than as a sedative for pregnant women?

RFID, and its associated Near Field Communications (NFC) and contactless smart card platforms, are remarkable technologies with a vast number of uses, and many more still to be discovered. Let us not allow our lack of understanding to either give us a false sense of security, or create undue distress. We are all better than that. Let's try to work toward understanding the truth.

Mike Ahmadi is the chief operating officer at [GraniteKey](#), a company that provides security technology services. He also heads the [RFID Security Alliance](#), which aims to educate its members, potential users, analysts, educational institutions, the media and others about security and privacy issues related to radio frequency identification.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved