MIT RFID Privacy Workshop, Boston, November 2003

Enhancing RFID Privacy via Antenna Energy Analysis

Kenneth P. Fishkin
Intel Research Seattle
1100 NE 45th St
Seattle, WA 98105 USA
+1 206 545 2503
kfishkin@intel-research.net

Sumit Roy
Dept. of Electrical Engineering
University of Washington
Seattle, WA 98195
+1 206 221 5261
roy@ee.washington.edu

ABSTRACT
For RFID tags to gain general acceptance, they will have to offer powerful and flexible privacy mechanisms. We propose that a key aspect of RFID communication with passive tags, namely its required energy transference from an external antenna, may offer previously unexamined promise when developing privacy mechanisms. We present two proposals for such mechanisms. In the first mechanism, analysis of the received signal by the tags can be used to estimate reader distance (and hence trust). In the second, antenna energy is used to power a tiered authentication scheme, in which tags reveal more information about themselves to more trusted and/or "energetic" readers.

Keywords
RFID tags, energy, privacy, authentication

INTRODUCTION
RFID technology offers great opportunity. Recent advances have reduced the cost of RFID tags, while increasing their capabilities (detected range, amount of on-tag memory, etc.). These advances have combined to transform RFID from a "boutique" or "fringe" technology, into something which is poised to be deployed in the billions. However, with this explosion of deployment comes an explosion of responsibility – the responsibility to ensure that the data on the tag is only read by desired readers in desired ways. When RFID was a fringe technology, this was not a major issue. However, this issue must now be addressed, or the RFID explosion may not occur, or may occur in a much more limited fashion.

Privacy and authentication mechanisms have been around for many years in other areas, such as file systems, email exchange, and so forth. These mechanisms should not be unthinkingly adopted "as-is" to RFID, however, due to the different constraints of the RFID domain. In particular, the most common RFID tags are powered passively by wireless energy emitted by a reader's antenna. This severely limits the amount and type of processing the RFID tag can do. We propose that this constraint also contains some opportunities – by exploiting the nature of this interchange, by focusing on the properties of the energy received by the tag from a reader antenna, we can have novel privacy-enhancing techniques which have no parallel in "generic" environments such as file systems.

In this paper we present two proposals for such privacy-enhancing techniques. The first is based on the observation that if a set of tags analyze the energy they are receiving from a reader antenna, they can often infer characteristics of that reader, characteristics which may be useful for privacy algorithms. The second is a more general proposal for a tiered authentication scheme, which goes beyond the "kill switch" by suggesting that RFID tags could support a range of disclosures. By looking at *both* the cryptographic guarantees of the reader antenna, *and* the energy received from that antenna, RFID tags can dramatically and flexibly improve the privacy of their data.

We are presently implementing the first technique. The second technique is still in the design phase, we hope its presentation at the workshop will serve to focus and foster the discussion.

DISTANCE IMPLIES DISTRUST
Assume a scenario in which some "hostile" RFID reader wishes to interrogate (or even change) the information on an RFID tag. Note that typically such scenarios involve a reader which is *physically distant* from the receiving tag. This is because the closer the reader is, the more subject it is to scrutiny by the wearers, owners, and/or users of the tagged object. If the tag is located inside a house, for example, it is far more likely that an attack will come from outside the house, than from an intruder inside the house. We therefore argue that RFID privacy mechanisms, unlike other privacy mechanisms, can and should use the physical distance between the information requestor and the information owner as part of their algorithms.

SIGNAL ANALYSIS AND PRIVACY
Assuming, therefore, that it is of interest to distinguish between physically near and far interrogators of RFID information, how can RFID tags be augmented to make that distinction? Our approach is based on exploiting the common received signal from an interrogating reader at a set of proximate tags. There are two possible techniques that can be used, varying in their overhead and their functionality:

Full Signal Analysis
Suppose that we have at least 3 tags, and in addition a local "base station" that they can communicate with. When these tags receive a signal from the interrogating antenna, they forward a copy of their respective received signals to the base station. We further assume that all the tags are time synchronized as a result of the base station sending

out sync pulses (either periodically, or aperiodically when asked to by the tag set).

The base station can then analyze the sets of signals so received. For example, by performing pair-wise cross-correlation (or to further robustify the procedure – *generalized* cross correlation) time-difference of arrival information at tag-pairs can be obtained. That can be used to localize the reader, and hence infer its range. The presence of significant additive noise (i.e. low received signal to noise ratios) and other model uncertainty would clearly degrade localization accuracy by enlarging the associated confidence interval; this can be addressed flexibly by adding more collaborating tags as well as enhanced signal processing approaches.

If the outcome of the localization process decides (perhaps in combination with other logic) that the interrogating reader is too far away, it can then instruct the tags not to respond.

RSS Analysis

The preceding algorithm is fairly heavyweight, requiring a base station, time synchronization, and full signal analysis. For a simpler, but less powerful algorithm, the tags can simply analyze the received signal energy/power (RSS). This processing algorithm is based on the observation that the more physically distant the interrogator is from the mean of these (relatively) collocated tags, the *less the variation* in the energy signature received by the tag-set. Conceptually speaking, higher-powered (i.e. distant) interrogators have a lower "curvature" on their energy sphere, and so the different tags will receive more similar amounts of energy. In this case, the tag-sets only transmit their RSS information to a central base station and not the full signal. The processing is also considerably simpler -the lesser the variance, the more powerful (and the more likely distant) the interrogator. Note that in such scenarios, it is not necessary to estimate a range to the interrogator, but rather coarser information – e.g. is the interrogator at a range > 5 feet – may be reliably ascertained by quantizing the variance computation. The processor can therefore quickly tell the tags whether or not they should respond, based on this reasoning. This technique is more feasible for higher-frequency RF techniques: the higher the frequency, the sooner the energy boundary approaches a plane (the Fraunhofer far-field effect).

Noise Analysis

An even simpler technique, that only requires one tag, is to look at the noise in the received signal. As the signal propagates from the antenna, its relative standard deviation increases. A single tag can therefore look at this deviation, and infer distance from it. This technique only requires a single tag, and is immune to Fraunhofer effects. It could be "spoofted" by an antenna which deliberately introduces relative variation into its signal, but this serves only to pretend *greater* distance (and hence less trust) than is actually the case: spoofing to pretend *less* distance (and hence more trust) is not possible; a desirable feature.

Caveats

We are starting to implement the algorithms described above. While it is too early to give a definitive discussion of its strengths and weaknesses, we are well aware that there are many distinctions between the theoretical ideal scenario outlined above, and those found in reality. In particular:

Tag Orientation

The amount of energy a tag receives is affected by many additional factors, most notably the orientation of the tag with respect to the antenna energy field. We believe this can be largely addressed by using commercially available 2D tags. By bending the tag antenna into two right-angle sections (an "L"), the tag can be made roughly invariant in two dimensions. The tags are still sensitive in the 3rd dimension, but this should be much less of an issue.

Imperfections in the reader energy field

The energy field radiated by the reader is not, in practice, perfectly omni. It is affected by a host of environmental considerations, most notably the presence of metal and/or water. The impact of this (unknown) field distortion on the two techniques proposed however should be minimal for clustered tags; in addition various statistical "smoothing" techniques such as data blurring and excision of outliers will help to robustify the method against pathological situations, but this hypothesis must be tested in a laboratory setting.

It is therefore on open question when to employ each of the three techniques described above – each has its own particular advantages and disadvantages. We hope they show, however, that the general technique of inferring distance by looking at the antenna signal is a feasible one, and that it could be helpful as part of mechanisms to improve privacy.

BEYOND KILL – TIERED REVELATION

For historical reasons, most RFID tags have not had a very robust mechanism to govern information disclosure. Indeed, nearly all tags reveal all their information to any interrogator without any mechanism whatsoever. This capability will have to evolve for RFID tags to gain widespread deployment. In this section, we propose a mechanism which leverages some of the unique attributes of RFID to provide a simple, flexible, extensible, secure authentication mechanism.

Tiered Revelation

Our proposed revelation scheme moves from a "flat" data space (where either all bits are transmitted or none), to a *tiered* data space. Every level of disclosure is assigned to a certain tier. When an antenna requests information, it requests a certain tier level. All information at that level and below is transmitted in response. In this way, different readers can be provided with differing amounts of detail, the detail required for their functionality. The more detail the reader requests, the greater its authentication burden, as discussed in the next section.

For example, to show how this tiered revelation might work in practice, let's consider an RFID tagged object such

as a shirt made by Benetton. Its tiered information might be structured as follows:

Level 0 – reports that it is an object. This is useful for baseline testing of a functioning reader.

Level 1 – additionally reports that it is a shirt, its fabric, and its color. This is useful for a reader integrated with a washer or dryer – with this information it can tailor its behavior depending on the set of clothes placed in it.

Level 2 – additionally reports its purchase cost. Now we start to enter the realm of more skeptically granted information. This level would be useful to, for example, an insurance adjuster. By walking through a house with an RFID reader equipped with level 2 authority, it could quickly ascertain the proper amount of insurance needed to cover the objects in the home.

Level 3 – additionally reports which factory it was made at, and at which date. This level is useful to determine if the shirt requires a recall.

Level 4- additionally reports which store it was bought at, and at which date. This level is useful to determine if the shirt qualifies for a refund/return.

The details of course will vary in practice, this is simply intended as an illustrative example that different levels of information disclosure are needed in different scenarios for the same object.

Tiered Authentication

This tiered information structure is naturally married to a tiered authentication structure; a reader is provided the information at a given level if and only if it passes an authentication protocol for that level – the higher the level, the more rigorous the authentication protocol.

One method (though by no means the only method) is for the tag and reader to communicate using public-key cryptography, where the number of bits employed is variable, and a function of the desired level of information. In this way, higher and higher amounts of revelation are naturally associated with higher and higher amounts of computation and data transmission.

Therefore, under this protocol, a reader changes its initial request from a blanket request, to a request which indicates:

1. The desired level of revelation
2. The reader public key
3. The number of bits of encryption desired, C
4. The amount of energy received by the tag.

If C (the number of bits of encryption desired) is less than the number of bits the tag requires for that level of revelation, the tag makes no response. Similarly, if the amount of energy received is insufficient, again the tag makes no response; as mentioned below, this provides the advantage of automatically increasing the burden on more physically distant readers. Assuming both of these tests have been passed, the tag responds with a cryptographic challenge-response protocol, keyed to a C-bit encryption.

Energy-Sensitive Authentication

Our proposed algorithm requires that the reader provide the tag with a minimum amount of energy, and that that amount of energy can be a function of the level of information disclosure required. This requirement can exist even for tags which are *not* passive, i.e. ones which don't need that extra energy. By still requiring a certain minimal amount of energy to reach them, we can again tie the notion of trust to the notion of physical proximity. Further readers, being less trusted by nature, will have to transmit a greater amount of energy than nearby readers, *even if* they pass cryptographic muster on the other criteria. Therefore, a distant hostile interrogator, even one which has cracked the authentication mechanism, may have to increase their energy level to unattainable levels, or at least levels which can be easily detected by mechanisms such as that discussed in the previous section. Again, the essential idea is that the tag reveals the desired information only if the energy signal passes cryptographic muster, *and* if the received energy is sufficient.

In this protocol, then, a reader conceptually offers up a 3-tuple: the desired level of revelation R, the encryption level C, and the energy level E. We point out two special-cases of this:

1. ***C=0***. In this case, the tag is not being asked to perform any encryption whatsoever. However, we are still achieving at least *some* security, by using the required energy level E. By requiring higher levels of energy, we may at least partially satisfy the goal of requiring greater proximity for greater revelation, without requiring any sort of encryption/decryption circuitry on the tag itself.
2. ***E=0***. In this case, the tag is not requiring any particular energy level. In this special case, tag authentication collapses to existing standard methods for tiered information interchange.

ACKNOWLEDGMENTS

We thank Bing Jiang for his dilligent investigations of the signal analysis technique