J. Uudmae, H. Sunkara, D. R. Thompson, S. Bruce, and J. Penumarthi, “MIXNET for radio frequency identification,” in *Proc. IEEE Region 5 Technical Conf.*, Fayetteville, Arkansas, April 20-21, 2007, pp. 382-385.

MIXNET for Radio Frequency Identification

Jaanus Uudmae, Harshitha Sunkara, Dale R. Thompson, Sean Bruce, and Jayamadhuri Penumarthi
Computer Science and Computer Engineering Dept., University of Arkansas
{juudmae, hsunkar, drt, sabruce, jpenuma}@uark.edu

***Abstract* - Privacy concerns have been raised with current and forthcoming implementations of RFID tags. The two main concerns are tracking and inventorying. Cryptosystems are being developed in order to curtail these potential abuses. Conventional cryptosystems that permit re-encryption do so only for a player with the knowledge of the public key corresponding to a given ciphertext. This kind of approach does not scale and is not practical. However, universal re-encryption in a MIXNET can be implemented without the servers holding any knowledge of public keys. Using existing techniques to implement an asymmetric cryptosystem with universal re-encryption in a MIXNET, we examine the ramifications of building such a system and also simulate its behavior with a Java implementation.**

I. INTRODUCTION

Radio frequency identification (RFID) identifies objects using radio signals [1]. The passive form of RFID named the Electronic Product Code (EPC) managed by EPCglobal Inc. is presently used in the supply chain to manage the flow of pallets and cases like the uniform product code (UPC) barcode identification system [2]. Every object is given a unique serial number called an EPC. The flow of individual items is already being tracked providing more detail for distributors and retailers. RFID can provide large economic benefits to users but it can also pose invasive new threats to rights, privacy of individuals, and security of organizations.

RFID has at least the following three privacy threats that need to be addressed: tracking, hotlisting, and profiling [3]. Limiting or preventing tracking the location of individuals is a high priority item. Hotlisting is used by an attacker to single out certain individuals because of the items they possess. Profiling is identifying the items an individual has in their possession. The most important threat to be addressed is tracking.

II. BACKGROUND INFORMATION

Anonymous communication not only hides an individual's true identity but prevents a traffic analysis that would aid in identifying the individual [3]. Traffic analysis is a technique for determining which individuals are communicating and when they communicate. Information can be inferred by knowing that an individual from one organization is communicating with another identified organization. A threat with high risk in wireless communication like RFID is the ability to track the physical location of the tags [5]-[11].

Examples of anonymous communication include the dining cryptographer network [12], MIX network (MIXNET) [3], and onion routing network [13], [14]. The dining cryptographer network is secure but there are scalability issues. The original MIXNET gathers messages from multiple users and sends them out in a different and random order with time delays to hide the sender of the message. In [15], a MIXNET is presented that efficiently integrates the public-key and symmetric-key operations. It provides fast processing speeds and also robustness. MIXNET operates by taking several messages and performing permutations on them before passing them on to the next server. The Onion routing network is a real-time version of the MIXNET that routes connections anonymously from a sender to receiver. Anonymous communication has been suggested for the Internet [6], [8] and cellular communication [7], [9], [10], [11]. A formal asymptotic security model to verify location privacy of a MIXNET in a wireless network is presented in [9].

In [16], several possible solutions for the privacy issue in RFID are discussed. The simplest and most effective approach is to use the 'kill' command on the tag after the customer has purchased the product. This would provide total privacy protection but it would also eliminate the post-purchase benefits like receiptless returns, smart appliances, etc. The second approach is to rename the RFID tag so it has no intrinsic meaning. This approach would hide the identity of the object but it would still be traceable since the serial number of the tag is static. Therefore, it is vital that the unique serial number on the tag be protected from disclosure or changed periodically.

In [17], several solutions are provided to guard against tracking, spoofing and attacking. But those schemes require the tags to have significant computing capability, thus making them more expensive. So for economical reasons it is unlikely that we can solve the privacy problems through the use of more powerful and more expensive tags.

In [18] and [19], a MIXNET is formed in an RFID system by having security agents scattered throughout the system that periodically re-encrypt the tag serial number into pseudonyms that look random and cannot be linked to the original serial number without a secret key. In a traditional re-encryption type MIXNET, the servers rely on both the public keys and the private keys to perform the re-encryption of messages. Managing of keys is very cumbersome for a traditional MIXNET. The big advantage of universal re-encryption is that it enables a MIXNET to be constructed in which servers hold no public or private key material. In addition, universal MIXNETS offer forward-anonymity. If servers in the MIXNET are compromised, the anonymity of previously sent messages is preserved.

1-4244-1280-3/07/$25.00 ©2007 IEEE

In the universal re-encryption scheme a ciphertext on the RFID tag can be digitally signed by a central authority, thereby permitting the reader to verify the authenticity of the associated plaintext. The problem with this approach and any other approach is that it does not protect against swapping of two valid ciphertexts. The adversary could always swap two valid ciphertexts on tags and there would be no way of knowing that the swap took place. In the insubvertible encryption scheme [20], the tags could be periodically re-encrypted without the readers even knowing the identity of the issuing party. The tag would still be intelligible only to the issuing party of the tag. This system does not require the tags to have any other capabilities besides the basic read/write operations. Thus the cost of these tags will be low and that would make them attractive to manufacturers and retailers. Since the tags are basic the attacker will still be able to change the content of the tag but during the next read operation by a 'good' reader the problem will be discovered and the content of the tag will be replaced by new information.

III. UNIVERSAL MIXNET APPROACH

The approach to protect privacy in a passive RFID system such as standardized by EPCglobal Inc. is to use universal re-encryption MIXNET to periodically re-encrypt the serial number on the tag. A simulation of universal re-encryption based on the ElGamal cryptosystem was written in Java. The following sections discuss the ElGamal algorithm and the universal re-encryption MIXNET approach.

A. ElGamal Encryption Scheme

The ElGamal cryptosystem is a successful application of the Diffie-Hellman key agreement. The strength of the ElGamal relies in the difficulty of calculating discrete logarithms. The following steps of ElGamal algorithm is presented in [21]:

Key Setup

Alice has to:

- choose a random prime p
- compute a random multiplicative generator element g of F_p^*
- choose a random number $x \in_U Z_{p-1}$ as her private key
- compute her public key by $y \leftarrow g^x \pmod p$
- make (p, g, y) public, and keeps x as her private key.

Encryption

To send a message m < p to Alice, the sender Bob has to:

- picks $k \in_U Z_{p-1}$ at random and computes a ciphertext pair (c_1, c_2):
  $c_1 \leftarrow g^k \pmod p$
  $c_2 \leftarrow y^k m \pmod p$

Decryption

To decrypt ciphertext (c_1, c_2), Alice has to:

- $m \leftarrow c_2 / c_1^x \pmod p$

As seen in the algorithm, the encryption step creates a ciphertext that needs twice as much space to store compared to the original plaintext.

B. Universal Re-encryption of RFID Tags

Universal re-encryption for RFID tags was proposed in [18]. Universal re-encryption requires encrypting the plaintext and the identity element with ElGamal and sending both so that the user with the correct key can decrypt the serial number but readers without knowledge of the public key can re-encrypt both. The exact steps are as follows:

Key Generation

Alice generates ElGamal public and private keys under a universal prime number p that everyone knows. She then publicizes the public key set (y, g).

Encryption

Bob has a set of RFID tags with plaintext m. This plaintext gets encrypted using Alice's public key y, and a random encryption factor $r = (k_0, k_1) \in Z_q^2$. This results in a ciphertext $C = [(\beta_0, \alpha_0), (\beta_1, \alpha_1)] = [(g^{k0}, my^{k0}), (g^{k1}, y^{k1})]$.

Decryption

Alice reads the ciphertext $C = [(\beta_0, \alpha_0), (\beta_1, \alpha_1)]$ and verifies that $\beta_0, \alpha_0, \beta_1, \alpha_1$ are in G. If not a special symbol # is output. She then computes $m_0 = \alpha_0 / \beta_0^x$ and $m_1 = \alpha_1 / \beta_1^x$. If $m_1 = 1$, the output is $m = m_0$. Otherwise the decryption fails and the special symbol # is output. This last check allows Alice to encrypt only tags meant for her and skip over others.

Re-encryption

Input is ciphertext from a tag in format $C = [(\beta_0, \alpha_0), (\beta_1, \alpha_1)]$. Using a random re-encryption factor $r' = (k_0', k_1') \in Z_q^2$. The resulting output is a ciphertext $C' = [(\beta_0', \alpha_0'), (\beta_1', \alpha_1')] = (\beta_0\beta_1^{k0'}, \alpha_0\alpha_1^{k0'}), (\beta_1^{k1'}, \alpha_1\alpha_1^{k1'})]$, where $k_0', k_1' \in_U Z_q$.

The idea behind the re-encryption is that the ElGamal possesses a homomorphic property, namely E[a] x E[b] = E[ab], where E[m] denotes ElGamal encryption of plaintext m. This means that the tags can be re-encrypted any number of times and they can still be decrypted in one simple operation. The power of this system is that the readers doing the encryption do not have to know any public key information. Also note that in the MIXNET the space requirement for the ciphertext is 4 times as large compared to the original plaintext.

C. MIXNET Construction in Real World

There are several important things to consider before constructing a large scale universal re-encryption MIXNET. First, everyone has to agree on using the same prime number p as a 'starting point' for the key generation. This also means that everyone has to use the same size tags. For example if the information on the tag needs to be 32 bits then the capacity of the tag has to be at least 128 bits because of the expansion that takes place in the MIXNET.

Once everyone agrees on the standards, it would be easy to implement the MIXNET by placing trusted readers in populated places. For example, there could be readers at airports, restaurants, banks, gas stations, etc. Individuals could

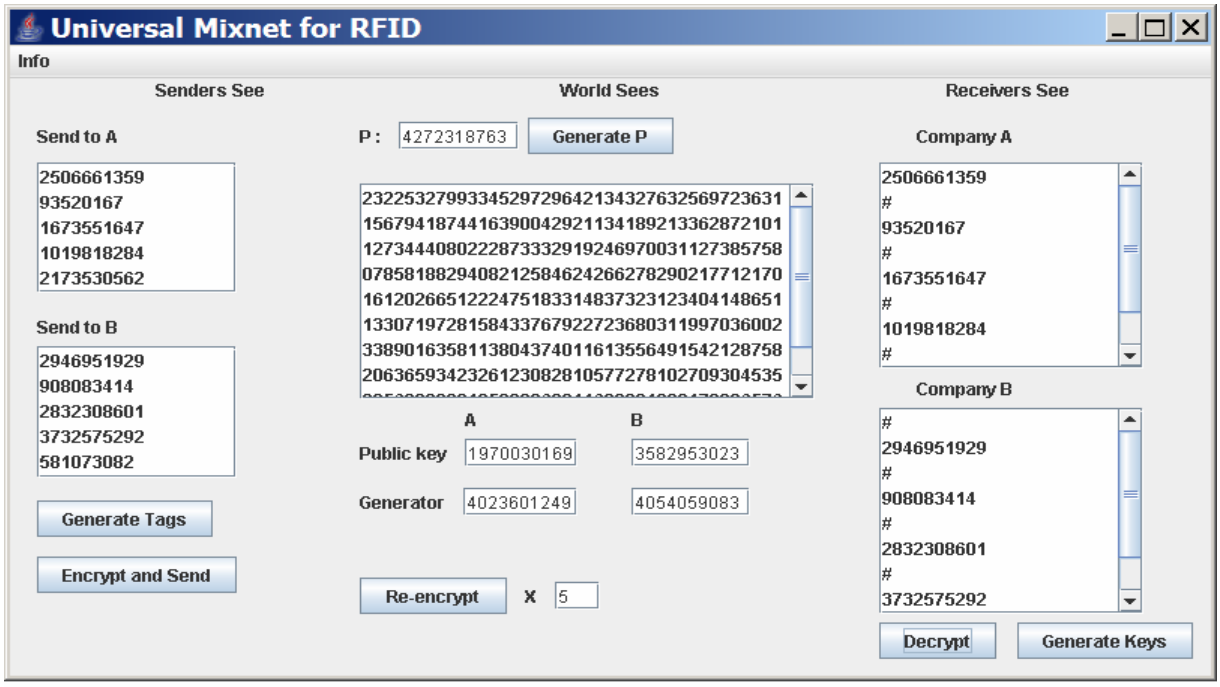

Fig. 1. Screenshot of universal re-encryption prototype

buy a re-encryption device for their car or house that re-encrypts the nearby tags periodically. The frequency of the re-encryption depends on how strong the privacy needs to be.

IV. UNRESOLVED PRIVACY ISSUES

Even though the universal re-encryption MIXNET approach would solve some privacy issues, it is by no means a perfect system. First, there are still some threats to privacy. Let's say that a person carrying a passport equipped with an RFID travels abroad. That particular country might not have a system of trusted readers that perform re-encryption so the person becomes traceable. In addition, in some poorer countries, the total number of RFID tags will be very low. This means that just having an RFID tag becomes a privacy concern. For example, the terrorist could easily identify potential foreigners just by the presence of RFID tags without even having to decipher the numbers. The only way to avoid these situations would be to kill the tag or block it temporarily.

In addition to privacy issues, there are also other potential issues with universal re-encryption MIXNETs that would have to be dealt with before large scale implementation. One of them is the issue with the reliability of trusted readers performing the re-encryption. If one of them fails and writes the wrong data on the tag, the decryption will fail and the tag becomes useless. This might happen by mistake or due to malicious readers. If these issues could be addressed, then the universal re-encryption MIXNET for RFID tags would be effective in eliminating the threats to privacy. Future work includes implementing the protocol on an RFID reader or as a plug-in feature for middleware that manages one or more readers.

REFERENCES

[1] N. Chaudhry, D. R. Thompson, and C. Thompson, *RFID Technical Tutorial and Threat Modeling*, ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering.

[2] EPCglobal Inc., http://www.epcglobalinc.org/.

[3] S. Karthikeyan and M. Nesterenko, "RFID security without expensive cryptography," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN),* Alexandria, VA, USA, Nov. 2005, pp. 63-67.

[4] D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms," in *Communications of the ACM*, vol. 24, no. 2, pp. 84-88, 1981.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "RFID privacy issues and technical challenges," in *Communications of the ACM*, vol. 48, no. 9, pp. 66-71, Sep. 2005.

[6] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "P^5: A protocol for scalable anonymous communication," in *Proc. IEEE Symposium on Security and Privacy*, 2002, pp. 58-70.

[7] W.-S. Juang, C.-L, Lei, and C.-Y. Chang, "Anonymous channel and authentication in wireless communications," in *Computer Communications*, vol. 22, pp. 1502-1511, 1999.

[8] L. Korba and R. Song, Investigation of Network-based Approaches for Privacy, tech. report, NRC/ERB-1091, NRC 44900, Institute for Information Technology, National Research Council Canada, Nov. 2001. Available: http://iit-iti.nrc-cnrc.gc.ca/publications/nrc-44900_e.html.

[9] J. Kong, D. Wu, X. Hong, and M. Gerla, "Sensor networks (work in progress): mobile traffic sensor network versus motion-MIX: tracing and protecting mobile wireless nodes," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN),* Alexandria, VA, USA, Nov. 2005, pp. 97-106.

[10] C.-H. Lee, M.-S. Hwang, and W.-P. Yang, "Enhanced privacy and authentication for the global system for mobile communications," in *Wireless Networks*, vol. 5, no. 4, pp. 231-243, July 1999.

[11] G. M. Køien, "Privacy enhanced cellular access security," in *Proc. ACM Workshop on Wireless Security (WiSe)*, Cologne, Germany, Sep. 2005, pp. 57-66.

[12] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," in *Journal of Cryptography*, vol. 1, no. 1, pp. 65-75, 1988.

[13] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private Internet connections," in *Communications of the ACM*, vol. 42, no. 2, pp. 39-41, Feb. 1999.

[14] M. Reed, P. Syverson, and D. Goldschlag "Anonymous connections and onion routing," in *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482-494, May 1998.

[15] M. Jakobsson and A. Juels, "An Optimally Robust Hybrid Mix Network," in *Proceedings of the twentieth annual ACM symposium on principles of distributed computing*, Aug. 2001.

[16] A. Juels, "RFID Security and Privacy: A Research Survey," in *IEEE Journal in Selected Areas in Communication*, 2006.

[17] L. Zhang, H. Zhou, R. Kong, and F. Yang, "An Imporved Approach to Security and Privacy of RFID Application System," in *Wireless Communications, Networking and Mobile Computing 2005*, Proceedings 2005, International Conference on, Vol. 2, 23-26 Sept. 2005. p. 1195-1198.

[18] P. Golle, M. Jakosbsson, A. Juels, and P. Syverson, "Universal re-encryption for mixnets," in *The Cryptographers's Track at the RSA Conf. (CT-RSA)*, LNCS, T. Okamoto, Ed., Springer-Verlag, 2004, pp. 163-178.

[19] T. Hjorth, *Supporting Privacy in RFID Systems*. Master Thesis, Technical University of Denmark, Lyngby, Denmark, Dec. 2004.

[20] G. Ateniese, J. Camenisch, and B. de Medeiros, "Untraceable RFID Tags via Insubvertible Encryption," *CSS'05,* November 7-11, 2005.

[21] W. Mao, *Modern Cryptography Theory and Pracitce*, Prentice Hall, Upper Saddle River, NJ, 2003.