Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 6 (2011) pp. 119-126

A Unified Model for Security, Trust and Privacy (STP) of RFID System

Mohd Faizal Mubarak[1, 2], Jamalul-lail Ab Manan[3] and Saadiah Yahya[4]

[1] Faculty of Computer and Mathematical Science, Universiti Teknologi MARA Malaysia,
40450 Shah Alam, Selangor, Malaysia
myrockib@yahoo.com

[2] Information Communication Technologies (ICT) Division, MIMOS Bhd.,
57000 Technology Park Malaysia, Kuala Lumpur, Malaysia
faizal.mubarak@mimos.my

[3] Advanced Analysis and Modeling Cluster, MIMOS Bhd.,
57000 Technology Park Malaysia, Kuala Lumpur, Malaysia
jamalul.lail@mimos.my

[4] Faculty of Computer and Mathematical Science, Universiti Teknologi MARA Malaysia,
40450 Shah Alam, Selangor, Malaysia
saadiah@tmsk.uitm.edu.my

***Abstract*: RFID technology is a pervasive technology because it is being used in many systems. RFID provides very good solution for non-business areas as well. However, its unprotected data in wireless communication channel and mobility of RFID tags opens up many possibilities of these tags being tracked by unauthorized reader which violates location privacy. It also gives opportunity for unauthorized user to access confidential data. Past works on RFID with privacy-preserving solution have dealt with lots of issues regarding system integrity and availability. In this paper we present A Unified Model for Security, Trust and Privacy (STP) of RFID System. Our proposed model use trusted computing principles and components to solve issues highlighted by previous works in RFID protocols. We combine the strengths of encryption, mutual attestation and privacy enhancement to form a unified model for RFID system. The model provides a holistic protection for RFID system.**

***Keywords*:** RFID, Anonymizer, Privacy, System Trust, Security**.**

I. Introduction

RFID technology is a pervasive technology because it is being used in many systems. The core application by commercial companies and organizations is very diverse, but with specific purpose, i.e. to identify items or products. It creates very positive and encouraging impact for business. RFID provides very good solution for non-business areas as well. For instance, it saves lots of transaction times especially for identifying items in huge warehouse at rates of hundreds per seconds. Another example, it could track the locations and status of any book in the library. A Typical setup of RFID system is as shown in Figure 1.

RFID technology has already become pervasive in many countries in the world because they are being used in numerous systems; its salient feature being able to communicate through wireless radio frequency between RFID reader and tags. However, the pervasiveness of RFID system also comes with emerging security and privacy issues because today's unprotected and unverified RFID system and its components could easily be tracked and/or attacked by adversary. Traceability of its data and location tracking are the two major issues in privacy. RFID tag without any security and privacy protection can easily be tracked by unauthorized reader or adversary can potentially violate user privacy. Other factors are caused by resources limitation, lack of security and mobility of the tag. When tracked by an illegal reader, it will violate privacy of the user who are using or carrying any items with RFID tags.

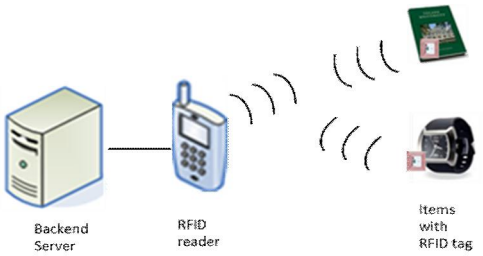

Figure 1. A Typical RFID System.

The most critical challenge for the RFID system is that without data privacy protection, it faces the risk of exposing say, confidential personal information or product sales information. For instance, a private hospital using RFID system for its patients' identities, when used without any privacy protection, will run the risk of exposing patients' drugs usage or prescriptions. This exposure of sensitive data would further exacerbate with the exposure of many more information such as type of sickness, how long has the patient been suffering, etc.

For the privacy protection, what we really need is to provide data anonymity and untraceability. We reviewed past works on RFID systems, particularly on privacy-preserving aspect. However, we noted that they mostly dealt with trust and system availability [1]-[4]. Looking from the overall system solution perspective, we consider them as proposals involving RFID tags only solutions and have not fully considered other system components such as RFID reader and back-end server. As far as our knowledge goes, current RFID products do not provide any privacy solution at all.

From adversary perspective, RFID tag would be an easy target for them to launch attacks on compared to backend server and RFID reader. In the pervasive and ubiquitous systems for future, RFID system would eventually be integrated and interconnected via the network to other systems. For example, current Near Field Communication (NFC) [5] system is a mobile phone that is capable of communicating with RFID reader. In the future, RFID system will eventually be integrated with house appliances and connected to the internet.

From the above discussions, it is apparent that the scope and coverage of security, trust and privacy is crucial as part and parcel of the integrated RFID system that will also be strengthened by more unified Security, Trust & Privacy (STP) Framework as proposed by Ab Manan et al. [6]. A critical review related RFID solution has also been done [7].

From STP systems design point of view, an anonymizer would be good candidate for protecting the entire RFID privacy from being tracked or traced by adversary. Another possible candidate would be the low-cost RFID tag because of the least use of resources [2]. We shall discuss this design consideration further in this paper.

The main contributions of this work are as follows: i) it provides real-time integrity verification for anonymizer and RFID system, ii) it is independent of time, iii) it also combines integrity, security and trust in one solution, and iv) it uses just one single anonymizer (an advantages over other previous solutions which need multiple anonymizers to anonymize tags [2]–[3]).

The rest of this paper is organized as follows: in the next section we discuss previous related works on RFID systems and protocols, followed by a brief discussion on the concept of anonymizer with trusted process. Further on, we present and discuss our proposed solution. Next, is the security analysis on our proposed solution and finally we conclude the paper.

II. Related Work

There are several previous works on RFID protocols that dealt with security and privacy issues [8]-[11]. Their focus was more on protecting RFID tag rather than a unified solution which covers overall security, trust and privacy. In other words, these proposals have considered security, trust and privacy separately. The two solutions provided by [15]–[16] were related to the design of trusted system in RFID reader, but have not proposed any RFID protocol. We proposed an RFID protocol with trust as in Mubarak et al. [17].

There is a protocol used by a hashed-based RFID system proposed by Weis et al. [8]. This solution protects transactions between RFID reader and tag using hash functions, but privacy is not well protected since it is traceable by adversary i.e. the shared key are communicated without being encrypted or protected.

Huang et al. [9] proposed another hash-based RFID protocol to protect secure access control system. This scheme includes timestamp to protect against replay attack which creates randomness through time. However, time stamping is vulnerable to time desynchronization attack. Huang et al. also provided data anonymity through hashing, which as far as our knowledge goes this lacks accuracy.

Lu et al. [10] proposed another RFID protocol that is also related to hash-based authentication system. This solution provided location based privacy which helps resistance against replay attacks. However, replay attack prevention is to the reader and not to the tag which is more crucial because the tag represents identity of the user of the item (which is embedded with the tag). It also has similar issues related to other privacy-preserving solutions which need to regularly update secret information in the system.

Dietrich [11] proposed an anonymous RFID protocol by using Direct Anonymous Attestation (DAA) [12] between NFC terminal and mobile phone. This solution provided anonymity for mobile host but the solution is quite complex and incur heavy burden during authentication process. This is due to the complex eighteen steps in performing authentication protocol between mobile phone and NFC terminal.

Sadeghi et al. [1]–[2] proposed an anonymizer-based RFID protocol that is resistant against impersonation attacks; however, it requires an additional protocol between tags and anonymizers that could also be vulnerable to attack. Moreover, this scheme assumed honest anonymizers to guarantee anonymity of tags and it is very dependent on a number of anonymizers. In a worst case scenario where one or more of these anonymizers is compromised, the whole system could be affected too. It was also noted that the need for several anonymizers can automatically increase overall cost of operation. The diagram in Figure 2 shows that collision could occur between a few anonymizers for anonymizing one tag. Another problem is related to finding the right mechanism that can prevent collision.

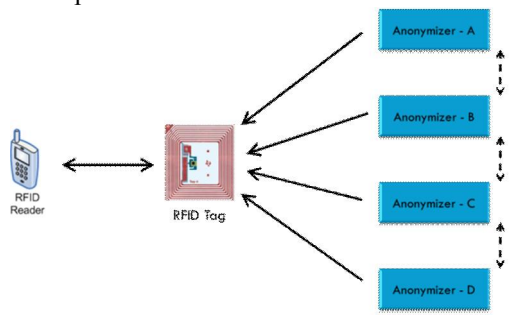

Figure 2. RFID System with Multiple Anonymizers.

An anonymous RFID protocol proposed by Armnecht et al. [3] is based on the modification of DAA protocol which was proposed by Chen et al. [13]. Chen et al. implemented a prototype of the modification type of DAA in RFID system by replacing RSA encryption inside the protocol with Elliptic Curve Cryptography (ECC) [14]. This modification involving a change to a more efficient algorithm also suffers from

problems associated with previous solution. These problems are related to system availability and the need for several anonymizers to anonymize each tag.

As a summary, we can conclude that almost all of the above mentioned RFID protocols still lack the unifying aspects of security, trust and privacy in providing a more integrated solution for future RFID Systems.

III. Building Trusted Anonymizer

The protection of user privacy and data confidentiality is very important to RFID system because it has to be untraceable and anonymous to unauthorized entity. RFID system also has to protect user location privacy from any illegal tracking by unauthorized entity or adversary. Usually, RFID tags and readers are mobile devices and they are more vulnerable to illegal location tracking compared to backend server. Normal backend server needs to be well protected for data privacy because confidential data (related to tags and readers) are stored in the backend system. While RFID tags are vulnerable, they also have very limited resources which mean that few applications could reside inside RFID tag. For example, Public Key Infrastructure (PKI) is not suitable in RFID tag because it requires bigger size resources. Anonymizer (a privacy-preserving tool) is suitable to be used both in RFID system and RFID tag, because it uses fewer resources [2]. Anonymizer protects data and location privacy for users and private data in RFID system by providing anonymity and unlinkability protection of RFID reader, tags and backend server, which could be tracked or traced by adversary. In this section we discuss how trust can be integrated into anonymizer to form trusted anonymizer.

A. Issues on Untrusted Anonymizer

Several anonymizer-based RFID protocols mentioned earlier suffer from almost similar issues, especially on providing honest type of anonymizer and system availability. Most of these anonymizer-based RFID systems have other difficulties such as relying on multiple anonymizers to always refresh tags. It must also be emphasized that anonymizer must have integrity verification so that it could prevent hijacking by adversary and from its component being infected by malicious code or malware [18]. Once the system is hijacked, user will not be able to confirm that it is operating as expected and hence it cannot be trusted any more [15]. A hijacked system is considered dangerous because it could infect RFID system components and could launch further attack by spreading virus to other components in different systems and could work together with the core adversary to track and trace data or user location in a much larger scale.

Another problem which is related to anonymizer-based RFID protocols is system availability, which can potentially disturb the anonymization process if hijacked by adversary. This problem could occur if anonymizer has been corrupted by adversary or it cannot provide anonymization services to tags, which leads to information being directly be exposed and tracked by adversary. A number of previous researchers on privacy-preserving RFID solutions [2]-[3] have tried to solve this issue by using multiple anonymizers. Unfortunately, it could produce others unexpected problems such as collision, logistics and system management issues. Moreover, multiple anonymizers are not cost effective and it would definitely increase the maintenance costs. System collision could occur between two or more anonymizers that are trying to anonymize the same tag. Another issue on system collision is about finding the right location for every anonymizer so that they would not compete with each other in anonymizing tags. This kind of setup is really depending on anonymizers to always anonymize tags regularly. The term “regularly” is related to unclear explanation because we are not really sure which time frequency is the best solution, i.e. whether the time is for every seconds, minutes or hours. If tags anonymization process occurs too frequently, it will be good for anonymity but it will consume lots of computing resources and it is very costly. On the other hand less frequent tag anonymization would give advantage for adversary to track tags.

By applying trusted computing principles to anonymizers, we believe that trusted anonymizers can potentially solve lots of issues mentioned above. Using trusted computing we do system integrity verification for all components including the anonymizer in RFID system to guarantee that they are operating in the expected manner. Any intruders which try to insert alien codes inside any of the trusted RFID system components can easily be detected by integrity monitoring module in the system such as Integrity Measurement Architecture (IMA) [19]-[20].

B. Trusted Process for Anonymizer

Trusted process using trusted computing principles provides trustable platforms or entities, and creates trustable environment within the RFID system. We describe how this is done for the anonymizer within the RFID environment.

The trusted process is first started by measuring properties in the anonymizer or any applications within the RFID system. The measurement process for is configurable. The integrity measurement report which needs to be verified by verifier is created by using integrity measurements (process is described below) which also has to be pre stored in the verifier platform. Any changes of the integrity measurements would definitely change the value of integrity report and would make the integrity verification process to fail. The baseline for integrity report is created after the measurement of the configured properties or components has completed.

The integrity of the booting process from the low level system such as BIOS and boot loader can be measured by using trusted boot application such as Trusted Grub. Every measurement would be extended into Platform Configuration Register (PCR) [21] inside the Trusted Platform Module (TPM) [22]-[23]. TPM is the tamper proof hardware which has already being promoted as trusted computing component by Trusted Computing Group (TCG) [23].

The trusted booting process only measures at the system boot level but not at runtime level. Besides measuring the system booting process, all applications can be measured at runtime by using Integrity Measurement Architecture (IMA) which has been created by IBM Research Group. IMA is the open source software which can be modified openly and reused back by research community. This application is embedded inside the Linux kernel to perform runtime measurement for every executed application and stored the integrity measurement inside the measurement log.

The combination of trusted boot and IMA can guarantee every executed application inside the platform would be measured and verified. Any modification of the application in the platform can be detected by the trusted system because it would produce a different measurement result compared to the legitimate application. Every system application inside the

platform would be measured and extended the measurement inside PCR in the TPM. This measurement can be used as an integrity report in the verification process for attester, which is described next.

C. Integrity Verification Process

The integrity verification process or attestation is like a challenge and response process within the RFID System which proves whether the verified platform or attester can be trusted as a legitimate platform or otherwise. The verifier must first be a trusted entity which can verify other platforms. Our task is to first establish a trusted verifier. It must be cautioned that, if any untrusted platform is able to verify integrity reports of attesters, then automatically we presume that any unauthorized entity can get the integrity report. This means that unauthorized verification process will give advantage to adversary to hijack the legitimate integrity report and launched and impersonation attacks to the system.

The scenario of impersonation attack is as shown in Figure 3 (without trusted process). In this figure an adversary could easily capture the authentication request and relays the message to legitimate backend server. The backend server would not be able to know the identity or integrity of the adversary because no integrity checking has been involved in the system. This shows that the confidential messages can be wrongly routed to adversary.

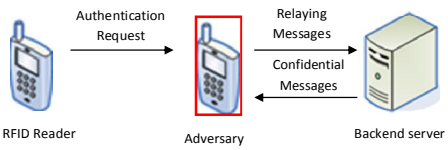

Figure 3. The example of an impersonation attack

In principle, the integrity report from an attester platform has to be protected and must not be sent to any unauthorized system. This can be done by encrypting the message in order to be protected from being exposed to adversary. Our proposal uses sealing key from TPM to seal the encryption key which is previously used to encrypt the integrity report. If the encrypted version of the integrity report has already being hijacked or intercepted by adversary or unauthorized platform, it cannot be decrypted easily because the encryption key is well protected by the sealing key from TPM. Only the rightly associated TPM could unseal the sealed encryption key.

D. Mutual Attestation

The purpose of attestation is to prove that the attester is the genuine, legitimate platform. It is clearly seen that this integrity report is used as trust evidence which comes from the target platform. Generally, the integrity report is any trusted value that can be processed and verified by the verifier platform. Specifically, the outcome of the attestation process (whether trusted or untrusted) depends on the integrity measurement that is collected. Attestation can be done in several ways, which include, i) as binary-based attestation, which has been proposed by TCG, ii) property-based attestation [24], which depends on the property value of attester's platform, and iii) direct anonymous attestation (DAA) [12].

This paper focuses only on using binary-based attestation for trusted process because in term of performance it is lighter and faster compared to property-based and DAA. In RFID system, resource is very limited and has to be utilized efficiently. Attestation could either be done in two ways; one way communication from attester to verifier or mutually as in our earlier work, i.e. Mubarak et al. [17]. Through mutual attestation process, we are essentially creating a trusted communication channel between attester and verifier.

Attestation process starts by the verifier sending nonce or random numbers which is created by using random number generator (RNG) to attester. Then, attester uses the random number as one of the parameter and combined it with Attestation Identity Key (AIK) [21]-[22] to communicate with the TPM. The TPM analyzes every parameter that it receives from attester's application layer. All of these parameters are processed to produce signature, PCR measurement values, and TPM or platform's credential to be sent to verifier. The combination of several integrity parameters in attester's platform creates the required attester integrity report. Then, verifier receives and verifies the integrity report sent by attester by using the verification module. Next, verifier decides whether it can trust the attester platform or the communication with attester would be terminated.

IV. The Proposed Model

The main objective of this paper is to solve and realize the above mitigation process by proposing a solution based on encryption, mutual attestation and anonymization in RFID system. In this paper we propose a Unified Model for Security, Trust and Privacy (STP) of RFID System.

A. The Proposed Model

The proposed Unified Model for Security, Trust and Privacy (STP) of RFID System as shown in Figure 4 is based on the following main principles. For the Trusted Anonymizer, the integrity measurement is extended inside TPM embedded in the RFID reader. This integrity measurement is combined together with all integrity measurements of other components in RFID reader which is then extended inside the PCR of the TPM-embedded RFID reader. The validity of the integrity report will be verified by backend server and RFID tag. This is significant, because the trust is established mutually among its own elements of the RFID system (forming a *chain of trust* within its own local domain). This solution also provides protection for anonymizer so that it would always be in trusted situation.

The proposed model addresses trust and privacy involving all RFID System components such as tag, anonymizer, RFID reader, and backend server. Its core component is the trusted anonymizer and integrity verification module which ensures integrity of every component in this system model is verified by verifier which is another trustable RFID platform. This integrity verification process is done after the mutual attestation has been established amongst the RFID system components, i.e. backend server, RFID reader, RFID tag and anonymizer.

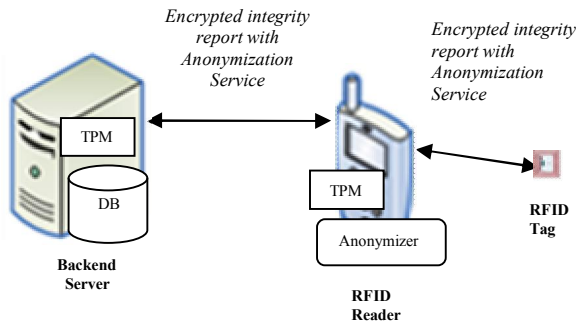

Figure 4. A Unified Model for Security, Trust and Privacy (STP) of RFID System

In the worst case scenario of our proposed Unified Model for Security, Trust and Privacy (STP) of RFID System, if the anonymizer or any RFID component is infected, (i.e. after integrity checks have revealed that integrity measurements have changed), and the whole RFID system would be halted to prevent further damage to the system trustworthiness. Any attempt to do illegal access to the system will be rejected by trusted RFID system. It must be emphasized that the *chain of trust* is very critical in the proposed solution because it protects the system from malicious code [18] or impersonation attacks

B. Attestation Process of System Components

The Trusted Anonymizer inside RFID reader provides anonymization services for identity of RFID tag, identity of RFID reader and confidential data in backend server. This means that any unauthorized system will be unable to trace or track RFID tag associated to any specific user and will be able to retrieve any confidential data from backend server. Anonymity also means that even if the backend server is compromised, no confidential data can be linked to any specific user.

Notations for the proposed STP Model

Notation	Descriptions
N_B, N_R	Random numbers (nonces)
A_Z [ID_T]	Anonymous value of tag ID
A_{Znew}[ID_T]	New anonymous value of tag ID
E_A[IR_R]	Encrypted value of integrity report from RFID reader
A_Z[IR_B]	Anonymous value of integrity report from backend server
A_{Znew}[IR_B]	New anonymous value of integrity report from backend server
SK_B	Sealing key from backend server

Table 1. Notations.

Referring to the Figure 5 below, every component including the anonymizer has to be measured and extended inside PCR in TPM before the attestation process is started. The integrity measurement of anonymizer is to make sure that anonymizer is a trusted component. Please refer to Table 1 for the description of the notations used in Figure 5 and Figure 6. The pre-condition is that the backend server must have the encrypted integrity measurement of RFID reader (E_A[IR_R]) stored inside the storage of the backend server. Anonymizer inside RFID reader first anonymizes integrity measurement of backend server (A_Z[IR_B]) and stores them inside RFID reader and backend server. The anonymized identity of RFID tag (A_Z[ID_T]) which has been anonymized by the anonymizer in RFID reader will also be stored inside RFID reader and tag.

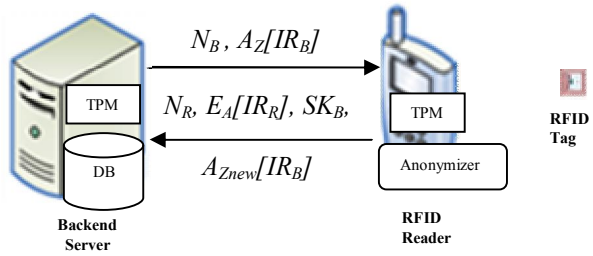

Figure 5. Attestation process of Anonymizer and RFID reader.

The mutual attestation process is first started by the backend server sending nonce (N_B) i.e. a random number and anonymous integrity measurement value of the backend server (A_Z[IR_B]) to RFID reader. The nonce (N_B) which is received by RFID reader will be used to retrieve integrity measurement in the TPM. The anonymous value of (IR_B) is extracted by using the anonymizer to verify the validity of the integrity measurement from backend server. If the integrity measurement of RFID reader is found to be valid, RFID reader will send its integrity report to be verified by backend server.

Next, the RFID reader will use nonce (N_B) to populate the integrity report using integrity measurement (IR_R) of the platform, Attestation Identity Key (AIK), which represents identity of the platform and signature of the key and sealing key of the backend server (SK_B). The integrity measurement is encrypted by using lightweight-based encryption (E_A[IR_R]). The encryption key which was used to encrypt integrity measurement of RFID reader is sealed by using sealing key which has been retrieved earlier from the TPM in backend server. The encryption key is stored inside backend server. The encrypted integrity measurement of RFID reader can only be decrypted by using backend server because only backend server could unseal the encryption key through the TPM.

This populated integrity report from RFID reader is send to backend server to be verified. If the integrity report of RFID reader with anonymizer is invalid (cannot be verified), the backend server will stop any communication with RFID reader. Otherwise, if otherwise (i.e. valid), backend server will continue the communication with RFID reader. The new anonymous integrity measurement value of backend server (A_{Znew}[IR_B]) is created by anonymizer to update the anonymous value to a new value.

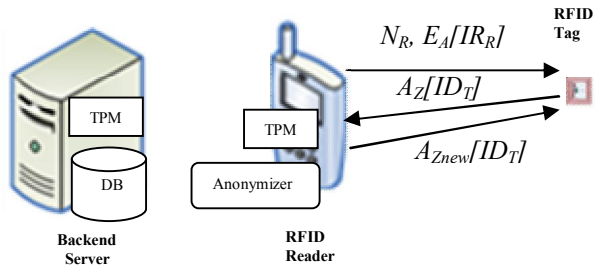

Figure 6. Integrity verification process of RFID tag.

C. *Integrity Verification Process of System Components*

The integrity verification process of RFID tag is as shown in Figure 6. RFID reader starts RFID tag's integrity verification process by sending nonce (N_R) and encrypted integrity measurement value of RFID reader ($E_A[IR_R]$) to RFID tag. Next, RFID tag needs to decrypt the encrypted integrity report from RFID reader and verifies the validity of the integrity report. If the integrity report is found to be invalid, RFID tag will stop the communication with RFID reader. Otherwise, if otherwise it is valid, RFID tag will send an anonymous identity value of the tag to be verified by RFID reader. Then, anonymizer inside RFID reader retrieves the real value of identity tag and verifies the validity of the identity of the tag. If the tag identity is found to be invalid RFID reader will stop the communication with RFID tag. Otherwise, if tag identity is found to be valid, RFID reader provides new anonymous ID to RFID tag.

V. Security Analysis of Model

A. *Integrity (Trust)*

The proposed model is analyzed from trust perspective. From trust point of view, the proposed model satisfies the key element in trust by providing much needed integrity measurements, reports between backend server, RFID reader, and tags. The mutual attestation process between RFID reader and backend server fulfills this need for trust (integrity verifications) for both platforms. The current passive RFID tag could not be embedded with TPM; it is envisage that future NFC type of mobile phone will be able to be embedded with TPM or mobile trusted module (MTM) [25]. The future trend of RFID system such as NFC mobile phone should enable mutual attestation with RFID reader. In the proposed model, identity verification is more than enough for RFID tag.

The much needed hardware based, tamper proof protection necessary to store secret information used by the proposed RFID System model is provided by the TPM which stores encryption key, AIK, sealing keys and etc. Any intruders or adversary would not be able to retrieve any integrity measurement or AIK from the TPM without physically hacking it, which is actually difficult. Hence, the integrity reports in our proposed model are well protected.

To further strengthen our proposed model, integrity reports are protected by using lightweight-based encryption such as ECC and anonymized by using anonymizer. The RFID tag identity is also anonymized by the trusted anonymizer. The combination of integrity verification, anonymization and encryption provides protection for "*data in motion*" and "*data at rest*". IMA provides a runtime based protection for every executed application in the system. Any malicious code attempts and data changes will be detected by IMA. Therefore, this solution also provides "*data in use*" protection which has never been discussed before in RFID system research. The IMA detection process for any changes in the system is as shown in Figure 7. In the attack scenario shown here, we know that the index.html file has been hacked. It shows that its measurement value has changed from '73b7fc43ee60fa0bdb0c8cbd8ee9812e1a4e8baf' to a different value 'fe7d33abe968fe09bc2f4cbcd6480db37779816a'. In this example, the IMA detects the changes automatically in real time, after the file had been changed.

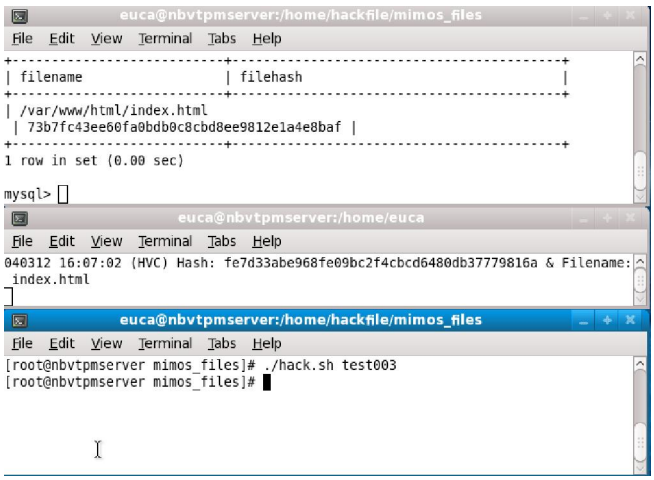

Figure 7. IMA detection process for any changes in the system.

B. *Security*

We also analyzed the proposed model from security perspective. From security point of view, the proposed model satisfies the security requirement by providing a lightweight-based encryption to protect data in RFID system. Data in the communication channel between RFID reader, tag and backend server is encrypted by using ECC. Passive RFID tag cannot use Public Key Infrastructure (PKI) because of resource limitation and complexity in key management. Hence, only lightweight-based encryption such as ECC can be used with RFID tag.

Any eavesdropper trying to retrieve the integrity report and messages via the communication channel would only get encrypted messages. They need to have encryption key in order to decrypt the message which will be in vain because encryption keys are well protected by using sealing key from TPM. The only way they can get the encryption key is by physically hacking the tamper proof TPM which will be difficult. Hence, the eavesdropper will fail to retrieve any information from the system. The combination of security (encryption key) and trusted platform (sealing key) provides protection for data in the network (*data in motion*).

Any data inside the platform also can be encrypted by using encryption key from lightweight-based encryption and sealed the encryption key by using sealing key. This part of combination between security and trust also provides protection for *data at rest* in the backend server.

C. *Privacy*

The proposed model is also analyzed from privacy perspective. From privacy point of view, the proposed model

satisfies the privacy-preserving part by providing anonymizer to provide anonymity services for the system. Several integrity reports and tag identity is being anonymized by using anonymizer. The anonymizer inside RFID reader provides data and location privacy for user and RFID system. Anonymity and unlinkability functionalities of the anonymizer protects privacy of confidential data and location privacy of RFID reader, tags and back-end server from being tracked or traced by adversary.

The combination between privacy preservation (via anonymizer) with integrity verification (via integrity report) provides complete privacy for data at network level and at storage level. Anonymized data is well protected by trusted anonymizer inside RFID reader. IMA tool in RFID reader monitor any unauthorized changes to the data or system.

VI. Conclusion

In this paper we presented our proposed Unified Model for Security, Trust and Privacy (STP) of RFID System. Our proposed model use trusted computing principles and components to solve issues highlighted by previous works in RFID protocols. We combine the strengths of encryption, mutual attestation and privacy enhancement to form a unified model for Security, Trust and Privacy (STP) of RFID system. The model provides a holistic protection for RFID system.

References

[1] A. R. Sadeghi, I. Visconti, C. Wachsmann, -"Location Privacy in RFID Applications," In: C. Bettini, S. Jajodia, P. Samarati, X. S. Wang, (eds.) Privacy in Location-Based Applications, volume 5599 of LNCS, Springer, Heidelberg, 2009, pp. 127-150.

[2] A. R. Sadeghi, I. Visconti, C. Wachsmann, -"Anonymizer-Enabled Security and Privacy for RFID," In: J. A. Garay, A. Miyaji, A. Otsuka (eds.) CANS 2009, volume 5888 of LNCS, Springer, Heidelberg, 2009, pp. 134-153.

[3] F. Armknecht, L. Chen, A. R. Sadeghi and C. Wachsmann, "Anonymous Authentication for RFID Systems", In 6th Workshop of RFID Security-RFIDSec 10', Istanbul, Turkey, June 2010.

[4] F. Armknecht, A. R. Sadeghi, I. Visconti, C. Waschmann, "On RFID Privacy with Mutual Authentication and Tag Corruption. In: Zhou, J. (ed.) ACNS 2010. LNCS, vol. 6123, Springer, Heidelberg, 2010, pp. 493-510.

[5] V. Kostakos and E. O'Neill. NFC on mobile phones: Issues, lessons and future research. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07*., pages 367-370, 2007.

[6] J. Ab Manan, M. F. Mubarak, M. A. M. Isa, Z. A. Khattak, "Security, Trust, Privacy – A New Direction for Pervasive Computing," In *Conference on Communication and Information Technology, WSEAS*, Corfu Island, Greece, 14th – 16th July 2011.

[7] M. F. Mubarak, J. Ab Manan, S. Yahya, "A Critical Review on RFID System towards Security, Trust, and Privacy (STP)", 7th International Colloquium on Signal Processing & Its Applications, Penang, Malaysia, 4th-6th March 2011.

[8] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *in 1st Intern. Conference on Security in Pervasive Computing (SPC)*, Springer-Verlag, Germany, 2003, pp. 454-469.

[9] Y. C. Huang and W. C. Kuo, "Secure Access Control Scheme of RFID System Application", Journal of Information Assurance and Security, Volume 5, 2010, pp. 240-245.

[10] J. C. Lu, Y. Y. Chen, S. I. Chen, J. K. Jan, "A Low-cost RFID Authentication Protocol with Location Privacy Protection", Journal of Information Assurance and Security, Volume 5, 2010, pp. 179-186.

[11] K. Dietrich, "Anonymous RFID Authentication Using Trusted Computing Technologies", In the Workshop on RFID Security 2010, Istanbul, Turkey, June 2010.

[12] E. Brickell, J. Camenisch and L. Chen, "Direct Anonymous Attestation," In Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, pp. 132-145.

[13] L. Chen, D. Page, N. P. Smart, "On the Design and Implementation of an Efficient DAA Scheme", CARDIS 2010, pp. 223-237.

[14] D. Hein, J. Wolkerstorfer, N. Felber, "ECC is Ready for RFID – A Proof in Silicon," In: *Conference on RFID Security*, Budapest, Hungary (July 2008).

[15] A. Soppera, T. Burbridge, V. Boekhuizen, "Trusted RFID Readers for Secure Multi-Party Services," *EU RFID Forum*, March 2007.

[16] D. Molnar, A. Soppera and D. Wagner, "Privacy for RFID Through Trusted Computing," *WPES*, USA, November 2005.

[17] M. F. Mubarak, J. Ab Manan and S. Yahya, "Mutual Attestation Using TPM for Trusted RFID Protocol," In *2nd International Conference on Network Applications, Protocols and Services-NETAPPS 2010*, Kedah, Malaysia, September 2010.

[18] M. R. Rieback, P. N. D. Simpson, B. Crispo and A. S. Tanenbaum, "RFID malware: Design principles and examples," In *Pervasive and Mobile Computing* In Special Issue on PerCom 2006, Vol. 2, No. 4. (November 2006), IEEE, 2006, pp.405-426.

[19] T. Jaeger, R. Sailer and U. Shankar, "PRIMA: Policy-Reduced Integrity Measurement Architecture," SACMAT '06, ACM Press,2006, pp. 19-28.

[20] R. Sailer, X. Zhang, T. Jaeger, L. V. Doorn, "Attestation-based policy enforcement for remote access," In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, 2004, pp. 308–317.

[21] D. Challener, K. Yoder, R. Catherman, D. Safford and L. V. Doorn, "A Practical Guide to Trusted Computing," IBM Press, 2008.

[22] A. Sadeghi, "Trusted Computing – Special Aspects and Challenges," *SOFSEM 2008, High Tetras*, volume 4910 of LNCS, January 2008, Springer, Slovakia, pp. 98-117.

[23] Trusted Computing Group (2007, August 2nd). TCG Specification Architecture Overview, Specification Revision 1.4.

[24] L. Chen, R. Landfermann, H. Löhr, M. Rohe, A. R. Sadeghi and C. Stüble, "A Protocol for Property-based Attestation," In *Proceedings of the first ACM workshop on Scalable Trusted Computing,* 2006, pp. 7-16.

[25] A. Schmidt, N. Kuntze, M. Kasper, "On the deployment of Mobile Trusted Modules," Arxiv preprint arXiv:0712.2113, 2007.

Author Biographies

Mohd Faizal Mubarak graduated from the Universiti Sains Malaysia (USM), Penang, Malaysia with a Bachelor in Computer Science (Hons.). He then joined several software development companies and later works as a Staff Researcher at Advanced Information Security Cluster, MIMOS Bhd. He then obtained a Master of Science (M. Sc.) in Information Technology and Quantitative Science from Universiti Teknologi MARA (UiTM). He is currently doing PhD in Information Technology at Universiti Teknologi MARA. He has 14 years of experience as Software Developer in several software integrators to telecommunication-based companies. In MIMOS Bhd, his current research focus is Information Security, particularly in Trusted Computing, Security, Trust and Privacy for RFID System and Privacy Enhancing Technologies.

Jamalul-lail Ab Manan graduated from the University of Sheffield, UK with a Bachelor in Electrical Engineering (B.Eng). He pursued his Master of Science (MSc) in Microprocessor Engineering from University of Bradford, UK and PhD in Communications Engineering from University of Strathclyde, Glasgow, UK. He is currently a Principal Researcher at Advanced Analysis and Modeling Cluster, MIMOS Berhad. He has 17.5 years of experience in teaching Electrical & Electronics Engineering, Microprocessor Engineering and Network Security. He has many years of industrial experience as Network Engineer, Senior Manager and Senior Vice President in ICT based government linked companies in Malaysia. In MIMOS Berhad, his current research focus is Information Security, particularly in Trusted Computing and Privacy Enhancing Technologies.

Saadiah Yahya is a Professor of Computer Sciences at MARA University of Technology, Malaysia. She has been lecturing in the University for 30 years in the area of Internet Technology, Information Technology Security, and Management of Information System. She has a Ph. D. in Computer Science specializing on computer networking from Putra University, Malaysia. She has published 10 (7 main author and 3 co-author) academic books in the area of computer sciences and IT, written many refereed journal and refereed international proceedings in the area of computer networking. She is active in doing research in the area of computer networking and IT where seven of those researches has participated in the innovation, invention, and design competition at the university and international level and won numerous medals (1 gold, 5, silver, 4 bronze and a Special Award: best presenter). She supervises many PhD students in the area of computer networking and it's related.