Sabouri, A., Komninos, N. & Douligeris, C. (2011). User dependent cryptography for security in future mobile telecommunication systems. 18th International Conference on Telecommunications, ICT 2011, pp. 422-427. doi: 10.1109/CTS.2011.5898962

User Dependent Cryptography for Security in Future Mobile Telecommunication Systems

Ahmad Sabouri
Information Networking Institute
Carnegie Mellon University
Pittsburgh, PA, USA
Email: sabouri@cmu.edu

Nikos Komninos
Athens Information Technology
GR-19002, Peania
Athens, Greece
Email: nkom@ait.edu.gr

Christos Douligeris
Department of Informatics
University of Piraeus
GR-18534, Piraeus, Greece
Email: cdoulig@unipi.gr

***Abstract*—In this paper we propose a user dependent scheme for enhancing security of the transmitted content in the future telecommunication systems. In order to achieve a higher level of security we introduce a scheme where the user identity gets involved in the encryption/decryption processes using an additional component for the block cipher which represents the user's behavioural model. Applying such a scheme, in addition to introducing more difficulties to an attacker due to the user dependency of the cipher algorithm, gives the mobile operator the opportunity to ensure that a licensed service has not been shared by the customer.**

To show the feasibility of our approach we use the concept of invertible Boolean functions as an example.

***Index Terms*—Behavioral model box; User dependent cryptography;**

I. Introduction

Third generation (3G) networks represent the recent stage in the evolutionary process of developing and standardizing high speed transmission of data in cellular networks; they provide users with high transmission bandwidths which allow them to transmit both audio and video information. Besides using cell phones for voice communication, we are now able to access the internet, conduct monetary transactions, send text messages etc. using our cell phones, and new services continue to be added [1]. This rapid development of cellular mobile data services has made people increasingly reliant on cellular phones in their daily lives for important and sensitive tasks such as E-shopping and E-banking [2].

The past experiences with security indicate that there are always possibilities for some weak points that have not been taken into account. The lack of physical security for mobile devices imposes these networks to more vulnerability. The attackers could utilize various techniques to crack the secrets embedded in mobile devices. Due to the high price of tamper resistant hardware and software, it does not make sense to consider cell phones with such equipment. So, a compromised device can provide open access to all the secrets associated with the device to the attacker. Therefore all authentication techniques become helpless and result in great damage to the whole system [2]. A simple example is when an attacker clones a SIM card, she can easily enjoy the services which the owner has registered for, until the owner realizes and requests to invalidate the card. The weak point here is that if an intruder can attack the system after the authentication phase, she can abuse the current session and get access to the service provided by the network.

In this paper we describe a scheme which utilizes behavioural model based profiles embedded in cryptographic modules to achieve both authenticity and confidentiality in mobile telecommunication networks. The rest of the paper is organized as follows: Section II provides a brief survey of the current security mechanisms in mobile telecommunication networks and the proposed behavioural model techniques which can be applied to achieve more security. The exact motivation of this work has been clarified in Section III. In section IV we introduce our scheme for behavioural model based ciphers, and provide an example of such a design in section V. Finally, we conclude the paper in section VI.

II. Related Works

In this section we will quickly go through the security mechanisms which have been implemented in existing cellular networks as well as some applications of the user behavioural model in providing security in telecommunication systems.

Global System for Mobile communications or originally Groupe Special Mobile (GSM) [3] and Universal Mobile Telecommunications System (UMTS)[4], [5] are known as the most popular second generation (2G) and third generation (3G) mobile telephony networks, respectively. They have been designed in such a way that they provide some user-related security features for authentication, confidentiality and anonymity [6]. Every subscriber of a GSM network shares a long term secret key K_i with its home network where she has originally subscribed to. Both the authentication in visited network and session key generation is based on this key. In order to perform the authentication, an authentication vector, consisting of a challenge response pair ($RAND_G$, RES_G) and an 64 bits encryption key K_c, will be generated by the Authentication Center in the home network and will be forwarded to the Mobile Switching Center in the visited network. A successful authentication is when the mobile station manages to generate the correct response RES^*_G (comparing to RES_G) and K_c using the challenge $RAND_G$ which was received

from the network and the long term secret key K_i. Then, the base station will receive K_c from the Mobile Switching Center and will be able to initiate a secure communication with the mobile station. Requests for authentication and renewal of the encryption key K_c vary with the network operator [3], [7].

A stream cipher of the algorithm family A5 is used in GSM. Currently A5/0 (no encryption), A5/1 (standard encryption), A5/2 (weaker version of A5/1) and A5/3 (similar to the KASUMI [5] algorithm used in UMTS) are defined [7]. Right after the authentication phase it is the turn for security setup. During this stage, the base station and the mobile station agree on the encryption algorithm based on the security capabilities of the mobile station and the available choices at the base station. In GSM authentications are carried out between the mobile station and the Mobile Switching Center and the encryption is employed between a mobile station and a base station.

Similar to GSM, in UMTS a shared long term secret key between the subscriber and the home network is used to authenticate the mobile station to the network and to generate the secret session keys. The visited network requests an authentication vector which is generated by the home network to authenticate the mobile station. To provide the ability of authenticating the network and protect the mobile station against attackers trying to impersonate a valid network to the mobile station, a new mechanism called Authentication Token is applied by UMTS. Here the authentication challenge is accompanied with the authentication token. The token contains a sequence number which is checked by the mobile station against a predefined range. If the mobile station verifies the sequence number, it computes the authentication response RES_U and the encryption and integrity protection keys CK and IK and sends RES_U back to the Mobile Switching Center. UMTS uses 128 bits encryption and integrity keys (twice as long as the GSM key). Unlike GSM, in UMTS there are counters for the number of packets that have been encrypted (integrity protected) with the same encryption (integrity) key. As soon as one of the counters exceeds an operator-set limit, a new authentication is enforced immediately before the next connection to a base station [6], [7].

A stream cipher based on the block cipher KASUMI is defined for UMTS as the encryption algorithm. In UMTS the encryption reaches further than GSM, into the backbone network, and namely the Radio Network Controller which is located between the base station and the Mobile Switching Center[7].

A higher level of security can be achieved by trying to detect anomalies in the user's behaviour. Using behavioural model based approaches for user identification in computer systems, has been studied in various works [8], [9]. For instance, when a user types a word, say a password, the keystroke dynamics can be characterized by a "timing vector", consisting of the duration of keystrokes and the time interval between them. Cho *et al.* have proposed an autoassociator neural network that is trained with the timing vectors of the owner's keystroke dynamics and then used to discriminate between the owner and an imposter[10].

In GSM or UMTS, a mobile phone or mobile station uses its subscriber identity module (SIM) to gain network access through authentication. [11] investigates the fraudulent usage of mobile telecommunications services due to cloned SIM. They have shown how quickly the fraudulent usage can be detected under the existing GSM/UMTS mobility management and call setup procedures.

The work in [12] presents an on-line security system for fraud detection by impostors and improper use of mobile phone operations based on a neural network (NN) classifier. It acts solely on the recent information and past history of the mobile phone owner activities, and classifies the telephone users into classes according to their usage logs. Such logs contain the relevant characteristics for every call that was made.

A simple and easy to use anomaly detection scheme on mobile phones is provided in [13]. The scheme records the keystrokes as the phone is operating, and the anomaly detection algorithm calculates a score of similarity, to detect the illegal users.

Exploiting the location history traversed by a mobile user has been used for providing two domain-independent on-line anomaly detection schemes, namely the Lempel-Ziv (LZ)-based and Markov-based detection schemes in [2]. The authors focused on the identification of a group of especially harmful internal attackers. For both schemes, cell IDs traversed by each mobile user are extracted as the feature value.

III. Motivation

There are varieties of block cipher designs aiming to protect the data against different kinds of attacks. All of them try to utilize some mechanisms to introduce enough confusion and diffusion, and achieve an acceptable level of secrecy. The motivation behind this work is to present a scheme, which can be offered by mobile operators in order to achieve a higher level of security, by considering the identity of the customer and her behavioural model in the encryption/decryption process, and thereby ensure that the person who has registered for the service will receive it, and not anyone else. This scheme is made to be easily adapted and utilized in existing encryption algorithms to make them more resilient to attacks. In order to achieve this goal we introduce a new box for block ciphers which affects the encryption/decryption process depending on the user behavioural model.

Another interesting problem that can be addressed by the above scheme is when the mobile operator wants the subscriber to solely use the service. In other words, they want the service to be accessed only by the person that has paid for the license.

For example, access to the IEEE digital library on the cell phone requires a license and the subscriber is not supposed to share this service with the others.

IV. Design

The assumption by mobile operators that only the subscriber knows the secret keys (or has the secret devices) and that she

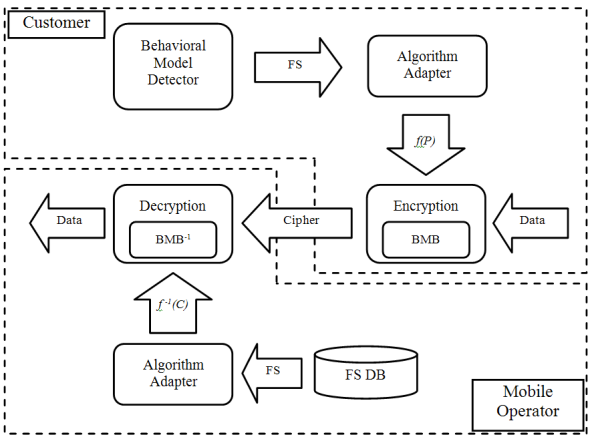

Fig. 1. Architecture of secure communication using behavioural model based encryption/decryption

is responsible to protect them, is considered as the root of our problem. In this case, whoever finds out about them can impersonate the owner and abuse this information to receive services from the operator. But what happens if the operator somehow involves the identity of the user in the encryption mechanisms? Assume the operator knows some specific characteristics of the user which can be examined during the service time and somehow tries to make the encryption process dependent to this characteristic. Then it will become extremely difficult for someone else to use the service even if she knows the secret keys or the secret device.

Assuming such a mechanism is applied in providing network based services, the attacker faces a serious problem. The most essential requirement for her is to know the encryption algorithm over which the communication is based. She cannot blindly try to break a secure communication. In order to know the exact encryption algorithm she requires at least the identity of the user as well as the user's specific characteristics, which are known by the operator and considered in the encryption algorithm. Only when she has her hands on all this information, she can launch different sorts of attacks and hope to find the keys. In the case where the key is stolen (not discovered), the attacker cannot proceed easily because the decryption process of such a secure channel also considers the user's characteristics for retrieving the content. As a result the attacker again needs to find out the specific characteristics of the user and imitate them to have the same encryption procedure that the operator expects. Otherwise, the operator will not be able to decipher the content and it fails to provide the service.

In this section we talk about a proper high level design of a secure system which satisfies the goals described above. The global picture of such a design is shown in Fig 1. It depicts the elements of the system at both the client and operator. Behavioural Model Detector, Algorithm Adapter and Behavioural Model Box are the major modules of this design, and they are collaborating to provide a user dependent secure communication.

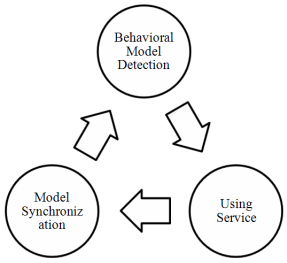

Fig. 2. Process of adaptive behavioural model based secure services

- **Behavioural Model Detector (BMD):** There have been numerous works on different techniques of user characterization based on the pattern of interaction with the machine or the way that she uses the service [14], [8], [15]. It has been shown that a system can be designed to monitor the client's activities and extract a behavioural model which can uniquely identify her. Designing such a detector falls into *Data Mining* and *Profiling* research and it is out of the scope of this work. But the important point is the output parameters of those processes. Similar techniques can be applied here to obtain a *Feature Set (FS)* from the user's behavioural model. Obviously, it takes some time for the operator to come up with such a model by monitoring the pattern of service usage, but when the profiling is done, the operator can offer this high level security to the users. On the user side, there must be a *BMD* software module which tries to extract the *FS* on-line and in a certain amount of time. The initial values may not be accurate enough but it must be in an acceptable level that the operator expects. As time passes, it should get closer to the model that is known to the operator. So, some time periods can be defined in such a way that during each, the system uses a model which is more accurate than the one used in the previous stage. Another key point is that, the *FS* that exists in the operator database will not stay the same forever. After each successful service the operator must update the model with some formulation which takes both the current and previous model into account. This is because the behaviour of client will change with time. This process is clearly shown in Fig 2. The major requirement to make such a module practically feasible is more development in the area of data mining and profiling techniques (which we do expect) to have enough robustness and reliability in BMD.

- **Algorithm Adapter:** After successful detection of the behavioural model of the user, there will be some values which are the elements of the *Feature Set*. The next step is to somehow combine these values and convert them to a module that can be used in the encryption algorithm. On the user side, the *Algorithm Adapter* will be a function $G(FS)$ which produces a unique function

$f(P)$, that can be utilized in the encryption process, as representative of the user's identity. Therefore, this is the part that defines the uniqueness of the encryption process, with respect to the user. As a result, when the user shares his service or when an attacker wants to abuse the stolen secrets to enjoy the service, this module produces different $f(P)$ as long as she is not able to imitate the actual user. It is important to note that the function $f(P)$ must be invertible since on the operator side, the *Algorithm Adapter* uses the existing *FS* in her database to determine $f^{-1}(C)$ and decrypt the incoming data.

- **Behavioural Model Box (BMB):** Cipher blocks are usually designed in components where each component is responsible to provide some confusion or diffusion to the cipher. The *Behavioural Model Box* is a new component that we introduce to the existing encryption techniques to achieve the user dependency that we previously discussed. Actually, the *BMB* is the part that is attached to the encryption procedure, and which is responsible to apply the function $f(P)$, coming from the *Algorithm Adapter*. The most important issue regarding the *BMB* is where to place it. Typical encryption algorithms follow a repeating procedure where there are rounds, and during each, the existing blocks apply their effects on the cipher. In order to have a correct cryptographic procedure, it is important to place the *BMB* correcly, in such a way that there exists a counterpart in the decipher block, where *BMB Inverse* is to be put, which in turn, is responsible to apply $f^{-1}(C)$ to retrieve the original data.

V. Security Analysis by Example

In order to show the feasibility of our design we present a sample implementation of such a scheme. We describe how *Algorithm Adapter* and *BMB* can be designed and attached to an arbitrary cipher such as *Advanced Encryption Standard* using *Invertible Boolean Functions* [16]. As we said before, the design and implementation of *BMD* is not in the scope of this work.

A Boolean function has an inverse when every output is the result of one and only one input. The Boolean function $F(x_1, x_2, x_3) = (f_1, f_2, f_3)$ such that

$$f_1 = x_1$$
$$f_2 = x_2 \oplus x_3$$
$$f_3 = x_1 x_2 \oplus x'_1 x_3$$

has the inverse function $F^{-1}(f_1, f_2, f_3) = (x_1, x_2, x_3)$ such that

$$x_1 = f_1$$
$$x_2 = f_3 \oplus f'_1 f_2$$
$$x_3 = f_3 \oplus f_1 f_2$$

where $x_1 \oplus x_2$ is "modulo 2" or "eXclusive OR" operation. The function can be used uniquely in either direction. The input or output is uniquely specified, in terms of the output or input, respectively. This function is said to have an inverse F^{-1}. Other equivalent functions can be obtained by a non-singular transformation of the x's and f's [16] .

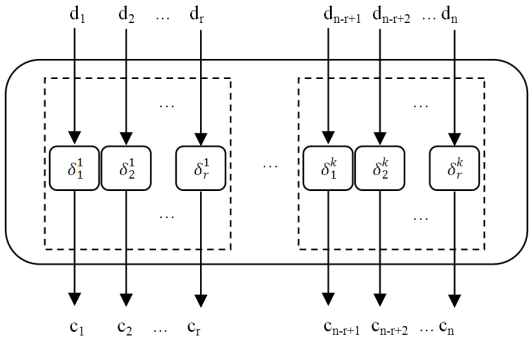

Fig. 3. Behavioral Model Box design (BMB)

Let say Ψ^r is the set of invertible Boolean functions $F(x_1, x_2, ..., x_r)$ using r variables. The number of distinct invertible Boolean functions for r variables is equal to:

$$|\Psi^r| = 2^r! \tag{1}$$

corresponding to the $2^r!$ ways the truth table can be completed with the 2^r distinct entries of F. Since the truth table for F is a complete listing of the 2^r r-digit binary numbers, each output variable f_i of F has an equal number of 0's and l's [16]. That is, every output variable f_i is a balanced Boolean function. It is important to have these functions balanced because it makes the cipher more resilient to cryptographic attacks.

Assume we want to use r variable functions with n bit message blocks. Then we have $k = n/r$ groups of bits. A schematic of a *BMB* has shown in Fig 3 where d_i and c_i represent the input bits and the output bits of the *BMB*, respectively. As it is shown the bits are grouped into k parts and each part is assigned a function:

$$\Delta_i^r = \left(\delta_1^i, \delta_2^i, ..., \delta_r^i\right) \tag{2}$$

where

$$\Delta_i^r \in \Psi^r$$

Since there is $2^r!$ possible values for Δ_i^r, totally there exist $(2^r!)^k$different *BMB*s. Assuming two variables for a Boolean function, there are $2^2! = 24$ different invertible functions. So, having a 32 bit input, there will be $32/2 = 16$ groups of inputs and each group can take any of the 24 possible function sets. As a result $24^{16} = 2^{48}.3^{16}$ different *BMB* can be defined using this approach. This provides enough uncertainly for an attacker who wants to find the structure of a *BMB*.

In this implementation, the *Algorithm Adapter* maps the given *FS* to the selected set of Δ_i^rs. In order to choose of Δ_i^r we need a l bit number where

$$l = log_2(2^r!) \tag{3}$$

Since we need $k = n/r$ number Δ_i^rso we require a $k \cdot l$ bit number to be able to select the functions for a *BMB*. So the

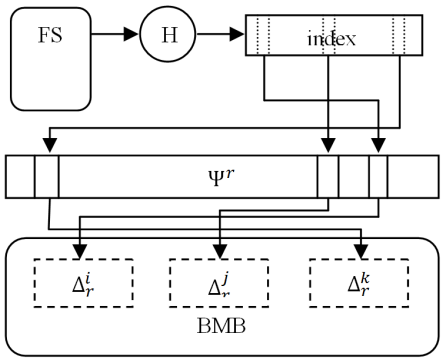

Fig. 4. Function mapping procedure using Hash Algorithm Adapter

Algorithm Adapter can be considered as a hash function which takes a *FS* and produces a $k \cdot l$ number index.

$$index = H(FS)$$
$$H : N^M \rightarrow N \tag{4}$$

where M is the size of *Feature Set*. The global picture of this procedure is depicted in Fig 4.

Assuming *Advanced Encryption Standard (AES)* is used for the next generation of mobile cellular networks, we show how a *Behavioural Model Box* can be embedded in the algorithm. *AES*, also known as the *Rijndael* algorithm [17], is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The *AES* cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps (SubBytes, ShiftRows, MixColumns and AddRoundKey). A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key [18].

A *BMB* can be either considered as a one time usage component which affects only the input or the output of the block cipher, or applied as a round operation component which performs its effect in each round of *AES*. Obviously, the latter case needs a careful design regarding the placement of the *BMB*s and the corresponding *BMB Inverse*s. We have shown in Fig 5 an example of a correct installation of *BMB*s and *BMB Inverse*s in the encryption and decryption process of *AES*. In this example, a *BMB* has been inserted after MixColumns and before AddRoundKey operation. Hence, the *BMB Inverse* must be considered after AddRoundKey and before InverseMixColumns operation in the decryption part. So a *BMB* operation is included in each round except the last one.

Another issue which might be of interest is that by using a stronger *Algorithm Adapter*, we can define different *BMB*s for each round. In this case, the same flow must be taken into account in the deciphering part.

VI. Conclusion

Employing the user's behavioural model is a concept that can enhance the security level of the next generation mobile telecommunication networks. In this work we have presented a scheme which allows the features extracted from the user's behaviour, to get involved in the encryption/decryption algorithms using *Behavioural Model Box (BMB)*. In this case, there will be a higher level of confidence that only the person who has subscribed for a service will be able to receive it. Since the encryption mechanism works differently depending on the user, an attacker will not be able to apply many of the known attacks which rely on the knowledge of the encryption algorithm, unless she recongnizes the identity and behavioural characteristics of the user. Furthermore, if a user wants to intentionally share a licensed service with someone else, the service will fail because the operator side deciphering mechanisms are extracted from the genuine user's behaviour.

We have also shown a sample implementation of *BMB* using *Invertible Boolean Functions*, and described how *AES*, being a potential encryption mechanism for the future mobile telecommunication networks, can be adapted to take the behavioural model into account during encryption/decryption processes.

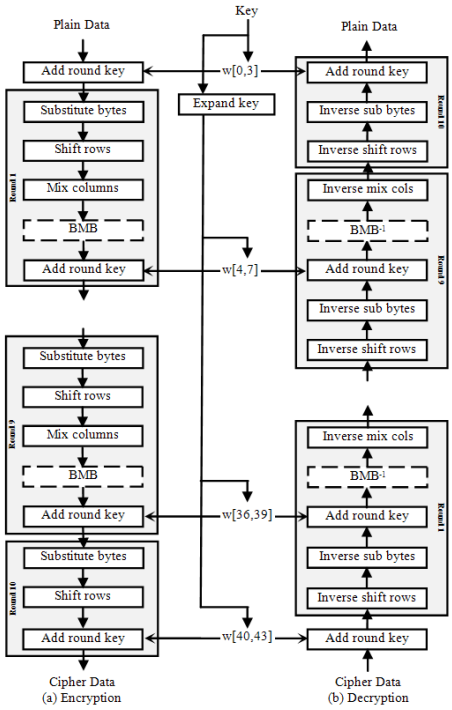

Fig. 5. Extended AES design using BMB

References

[1] Technical Report: Security Architecture in UMTS Third Generation Cellular Networks, 2004, http://ccc.inaoep.mx/Reportes/CCC-04-002.pdf.

[2] B. Sun, F. Yu, K. Wu, Y. Xiao, S. Member, and V. C. M. Leung, "Enhancing security using mobility-based anomaly detection in cellular mobile networks," *IEEE Transaction on Vehicular Technology*, vol. 55, no. 4, pp. 1385–1396, 2006.

[3] ETSI Technical Specification, "ETSI TS 100.929, V8.0.0, Digital Cellular Telecommunications System (phase 2+)(GSM); Security related network functions,"2000.

[4] 3GPP Technical Specification, "3GPP TS 35.201 V9.0.0, Third Generation Partnership Project; Technical Specification Group; 3G Security; specification of the 3GPP confidentiality and integrity algorithms; document 1: f8 and f9 specification," Dec 2009.

[5] 3GPP Technical Specification, "3GPP TS 35.202 V9.0.0, Third Generation Partnership Project; Technical Specification Group; 3G Security; specification of the 3GPP confidentiality and integrity algorithms; document 2: Kasumi algorithm specification," Dec 2009.

[6] P. H. K. Boman, G. Horn and V. Niemi, "Umts security," *Electronics & Communications Engineering Journal*, vol. 14, no. 5, pp. 191–204, 2002.

[7] U. Meyer and S. Wetzel, "On the impact of gsm encryption and man-in-the-middle attacks on the security of interoperating gsm/umts networks," in *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2004)*, 2004.

[8] Y. C. Yang, "Web user behavioral profiling for user identification," *Decis. Support Syst.*, vol. 49, pp. 261–271, June 2010. [Online]. Available: http://dx.doi.org/10.1016/j.dss.2010.03.001

[9] M. Choraś and P. Mroczkowski, "Keystroke dynamics for biometrics identification," in *Proceedings of the 8th international conference on Adaptive and Natural Computing Algorithms, Part II*, ser. ICANNGA '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 424–431.

[10] S. Cho, C. Han, D. H. Han, and H. il Kim, "Web based keystroke dynamics identity verification using neural network," *Journal of Organizational Computing and Electronic Commerce*, vol. 10, pp. 295–307, 2000.

[11] Y.-B. Lin, M.-F. Chen, and H. C.-H. Rao, "Potential fraudulent usage in mobile telecommunications networks," *IEEE Transactions on Mobile Computing*, vol. 1, pp. 123–131, 2002.

[12] A. Boukerche and M. S. M. A. Notare, "Behavior-based intrusion detection in mobile phone systems," *J. Parallel Distrib. Comput.*, vol. 62, pp. 1476–1490, September 2002. [Online]. Available: http://portal.acm.org/citation.cfm?id=634525.634534

[13] Takamasa Isohara, Keisuke Takemori and Iwao Sasase: "Anomaly Detection on Mobile Phone Based Operational Behavior", Information and Media Technologies, Vol. 3, No. 1, pp.156-164, (2008) .

[14] Thomas A. Gerace, Method and apparatus for determining behavioral profile of a computer user, United States Patent 5848396.

[15] T. S. Raghu, P. K. Kannan, H. R. Rao, and A. B. Whinston, "Dynamic profiling of consumers for customized offerings over the internet: a model and analysis," *Decision Support Systems*, vol. 32, no. 2, pp. 117–134, 2001.

[16] C. S. Lorens, "Invertible boolean functions," *Electronic Computers, IEEE Transactions on*, vol. EC-13, no. 5, pp. 529 –541, 1964.

[17] J. Daemen, J. Daemen, J. Daemen, V. Rijmen, and V. Rijmen, "Aes proposal: Rijndael," 1998.

[18] Federal Information Processing Standards Publication 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", 2001.