Location-Based Security for ID Document and ID Card Enrollment Stations

Eugene P. Gerety
Khaled M. Elleithy, Ph.D

Computer Science and Engineering Department
University of Bridgeport
{egerety | elleithy}@bridgeport.edu

Keywords: Identity Management Systems, Identity Verification, Location-based Security, Physical Unclonable Functions, RFID

Abstract

Much of today’s security for financial assets, services, facilities, personal information, immigration, employment and travel is provided in the form of a variety of ID instruments such as passports, credit cards, ID badges, access cards, and other similar forms of identification. Staggering costs associated with rampant identity theft are driving ongoing efforts to produce stronger, positive-ID documents and cards through the application of a wide variety of security enhancing techniques such as biometrics, embedded chips, encryption and specialized materials with security features. Each new generation of ID documents and cards becomes more technologically sophisticated and difficult to forge, forcing criminals to resort to increasingly complex and sophisticated forms of attack to circumvent their security mechanisms. Against this backdrop, ID Enrollment systems become particularly enticing targets for theft and unauthorized use, because with their use of authentic security materials, algorithms and production mechanisms, these systems are capable of producing truly undetectable fraudulent ID instruments capable of passing any and all security tests performed by even the most sophisticated ID verification terminals. This paper proposes and presents a practical location-based security framework designed to protect against any attempt to operate an ID production/enrollment system away from its authorized operating location.

1. INTRODUCTION

In calendar year 2009, the (US) Federal Trade Commission’s Consumer Sentinel Network, an online database available only to law enforcement, received over 1.3 million consumer complaints. Of these, the number one complaint category was identity theft, accounting for 21% of all complaints [1]. Many such complaints involve compromised credit card accounts, bank accounts, fraudulent purchases, and other forms of financial fraud. Historically, most identity theft was primarily aimed at fraudulent access to existing bank accounts and credit card accounts, using stolen ID to take out loans and open new accounts, and other forms of financial fraud. More recently, other forms of identity theft such as medical ID theft, immigration and employment fraud have become more common [2]. Often, these forms of identity theft involve forged or copied ID documents and cards.

Then need for truly secure ID cards and documents has driven numerous programs to abandon simple, insecure ID strategies in favor of machine-readable “positive-ID” documents and cards with numerous security enhancing features. For example, in 2004 the International Civil Aviation Organization (ICAO) issued its international standard for machine-readable passports [3]. This new standard includes embedded RFID (Radio Frequency IDentification)1, embedded biometrics (digitized photo required for facial recognition, with fingerprint and iris information optional) and encryption [3][4][5][6]. These features are intended to provide better security for the personal information in the passport and make forgery of the passport itself far more difficult.

Contact and contact-less smart-card technologies (integrated circuit cards) are among the more visible recent security enhancements being made to secure ID cards, particularly the now-common gold-plated contact pattern present on many newer credit cards. These cards, some with embedded processors and embedded biometric templates are being deployed in a wide variety of other identity-verification applications besides credit and debit cards, such as: cruise ship boarding cards, hotel key-cards, employee ID badges, and club membership cards.

In a smart-card security system, a terminal adapted to accessing the functions of the card activates the communications with the card, which responds by providing identifying information. In a truly secure implementation, both sides of the transaction must be considered. From the perspective of the terminal, the main goal is to verify the authenticity of the smart card by confirming the validity of the information it contains. From the perspective of the card and card holder, it is equally important to verify the authenticity of the terminal – i.e., to verify that the terminal is not a “phony” terminal seeking to gain unauthorized

---

1 It has been argued by many that the inclusion of RFID as specified in the ICAO standard actually creates certain security risks, especially when other encryption and security features are implemented only at a basic, minimum level of compliance with the ICAO standard[4][5][6].
access to the information stored on the card. The simplest smart cards with fixed information and without processing capability are incapable of verifying the authenticity of the terminal. Newer, more sophisticated smart cards with embedded processing capability can implement this stronger, two-way verification strategy [7].

As security technologies become more complex, so do the attacker’s methods. Faced with “impossible” encryption techniques and sophisticated smart-cards, attackers have resorted to such methods as reverse-engineering and cloning. Once a security mechanism is analyzed successfully, it may be possible to bypass it or to “clone” it [4][8], thereby creating a “working” copy of the cloned ID card (or terminal) and giving the attacker unauthorized access. In certain extreme high-stakes arenas, such as where national security, international travel or global commerce are involved, a cloning-based attack on ID security might come from large teams of highly-skilled individuals with virtually unlimited funds and access to equipment that would ordinarily be prohibitively expensive to procure and operate by anyone other than large institutions and governments[8].

One of the approaches that has been suggested to prevent cloning, is the use of Physically Unclonable Functions (PUFs) to generate secret keys in RFID tags [8][9]. PUFs are manufactured physical structures that feature unique, inherently random characteristics of the materials and processes that produce them. These characteristics can be “read” by suitably adapted apparatus, resulting in a unique “signature” specific that particular instance of that particular physical structure. Due to the inherent randomness, other seemingly identical structures produced in the exactly the same way would have completely different signatures – a truly “uncopyable” (unclonable) function, since any attempt to duplicate it by any means would result in a different signature [10][11]. One of the first references to such structures appears in [10], where they are called “Physical One-Way Functions and employ optical characteristics of a specialized medium. Later developments adapted the PUF concept to silicon devices, permitting PUFs to be embedded in digital devices with relative ease. Although described in [9] with respect to RFID technology, PUFs are readily adapted to other applications [11]. By providing an effectively uncopyable signature, the strategic use of PUFs can be an effective deterrent to cloning.

1.1. Problem Identification

In addition to the data security features described above, most modern ID documents employ a multi-layered security strategy that includes such physical elements as transparent hologram overlay film, specialty papers and plastics, and identifying features visible only at infrared or ultraviolet wavelengths. To produce ID cards and documents of this type, highly-specialized enrollment stations and card or document production systems are required. Some verification terminals are capable of “reading” and verifying the presence of the physical elements in the ID card or document. In combination, these multiple security features make the prospect of producing effective false ID considerably more difficult.

Faced with ID cards and documents that are increasingly difficult to defeat or copy, the potential identity thief is likely to start looking for easier “shortcuts”. To this end, the enrollment stations and materials (e.g., card blanks, passport booklets, overlays films, specialty printers, etc.) used by the issuing authority to create ID cards and documents become particularly attractive targets. With access to an actual ID card production system and materials, a potential identity thief may be able to examine and analyze the system, gain access to secret keys and/or seed values, and produce ID cards or documents that will pass any security test, because they are made using “real” materials, printing techniques, embedded chips, etc..

Three potential areas of vulnerability for ID card or document enrollment systems are: susceptibility to theft, compromised operator, and unauthorized document or card production.

1.1.1. Susceptibility to theft

If an enrollment system is stolen, there is the potential for extensive examination and analysis of the systems security mechanisms, free from observation. This is particularly true in the case of small-scale production setups, like those that one might find at a photo license center, a campus security office, an employer’s security office or a smaller embassy. Many modern ID card and document productions systems are remarkably small, often comprising little more than a camera, a computer, a printer and a few small peripheral devices (e.g., a fingerprint reader or signature pad.) If the enrollment system’s operator security can be successfully breached (perhaps with the willing or unwilling assistance of an authorized operator), then it may be possible to produce false ID that is completely unimpeachable by any ordinary means of ID verification.

1.1.2. Compromised operator

Any enrollment system with reasonably strong security measures in place will require an authorized operator with the proper credentials to operate the system or to provide production materials. Even in multi-level security schemes, there is always someone who has top-level access to the enrollment system. A top-level operator with malicious intent, or an operator who is being coerced could potentially use the system and its associated materials (or be forced to use the system) to produce fraudulent ID cards or documents.

1.1.3. Unauthorized or “extra” document or card production

One important key to ensuring that only valid ID cards or documents are produced is positive confirmation that the accuracy and authenticity of the information provided by the recipient of that card or document. In the event that undetected false information is provided (e.g., false name,
false photo, false biometric, etc.) a false document could be produced. For example, consider the scenario where a user enrolls by providing personal information, a photograph and a biometric (e.g., fingerprint image). For example, an identity thief might intercept such a request and substitute his own photo and fingerprint for the real ones, then intercept the card or document when it is sent back by the issuing authority (card or document producer). The thief would then have a completely “valid” ID document, complete with his own photo and biometric information on it.

Another possible scenario whereby a false or fraudulent ID card or document could be produced is where an extra unauthorized record is inserted into a batch job for a secure ID card/document production (enrollment) system. In this case, the operator would likely be completely unaware that anything had happened.

This paper focuses primarily on the problem of a stolen or “borrowed” system being operated away from its intended location. The paper describes a practical location-locking technique that prevents an enrollment terminal from being used when removed from its normal operating location.

2. SYSTEM OVERVIEW

The proposed system is shown generally in Figure 1. The system consists of an ID card/document Production System (IDPS) and a Basepoint Transponder (BPT). The location-based security centers around the BPT and is based on a PUF-based, encrypted, passively-powered RFID transponder. In addition to secure RFID communications, the IDPS and BPT implement a tightly-integrated hardware-based time-of-flight (TOF) secure distance bounding protocol similar to the one described by Hancke, and described below [12].

The BPT communicates only with authorized clients. Authorized clients are created by having a trusted authority (TA) “introduce” them to the BPT using fully authenticated and encrypted communications. At the time of initialization, the BPT recognizes only its manufacturer as a trusted authority and has no clients. The manufacturer can confer TA status upon another entity by means of a secure protocol. To connect with a BPT, an IDPS must first be “introduced” to it by the current TA, after which the IDPS becomes a recognized client and can communicate freely with the BPT. In the event of a compromised system, the TA can also de-authorize a client. When communications with a client suggest security violations, the BPT itself can de-authorize a client.

The BPT acts as a sort of “home base” for the IDPS. It has two main components. The first component is an RFID transponder with PUF-based security and fully encrypted and authenticated communications over a “conventional” RFID channel. The second component implements one side of the distance bounding protocol using an independent bit-wise message exchange via an independent RF communication mechanism. The IDPS and BPT communicate over the “conventional” channel to agree upon an encrypted PUF-generated challenge/response message pair to be exchanged, one bit at a time, to establish an upper limit on the distance between them during a distance bounding sequence.

![Figure 1. General System Configuration](image)

The IDPS is essentially a conventional secure card/document production system that incorporates a “conventional” RFID transceiver, and the other half of the hardware-based TOF distance bounding protocol.

It is intended that the BPT be kept separate from the IDPS, but within its communication range, in a highly secure location. One option would be to embed the BPT into the structure of the building in which the IDPS resides. That is, the BPT could be provided with a strong, well-sealed case and poured right into the concrete of the building or sealed into a hollow cavity in the building’s structure. This is done to guard against theft of both the BPT and IDPS at the same time.

In operation, the IDPS periodically verifies its proximity to the BPT by communicating securely with the BPT to establish its authenticity and verifying the distance between them. If the measured distance between the IDPS and the BPT does not fall within pre-established acceptable limits or if BPT<=>IDS communications fail authentication, the IDPS will prevent further operation. Preferably, in such a case, the IDPS would deactivate itself in a secure, semi-permanent fashion (e.g., by deleting critical files and/or damaging one or more critical components) such that only the manufacturer or a trusted authority would be able to re-activate and/or repair it.

Although this location-locking system uses some of the communications mechanisms commonly associated with “conventional” RFID and the BPT has many of the attributes of a RFID “smart card” tag, this system differs from conventional RFID applications in several important ways:

- Both parties (IDPS and BPT) are fixed-location entities
- The BPT, its circuitry and its antenna are not limited in size to what can fit in an ID card
Communications between the BPT and the IDPS are not limited to the “brief encounter” time typically associated with RFID applications. That is, the BPT is not a “passer-by”

There only needs to be one BPT per system, so the BPT represents a one-time cost. As a result, the BPT is not cost-constrained like a conventional RFID smart tag (which represents a recurring cost).

The BPT is not as power-constrained as conventional RFID applications. Although passively powered, it can use energy harvesting techniques (charge and store) to increase available power for compute-intensive operations. Further, IDPS carrier-on time is not arbitrarily limited, so the IDPS can maintain an unmodulated RFID carrier as long as necessary to allow the BPT to complete its functions or to charge up an energy storage cell.

For these reasons, the BPT has a number of advantages over “conventional” cost and power constrained RFID smart-tags. For one thing, with relaxed cost, power and operational constraints (longer communication time, carrier-on time, etc.) the BPT can be designed to accomplish significant computations, such as the math intensive operations necessary for Public Key cryptography. Its fixed location allows the BPT to use larger, more efficient power utilization features such as a larger, more efficient antenna and more efficient power conversion circuitry (for better RF

2.1. Basis for location-based security

One of the first and most important questions in establishing location is to determine the frame of reference, i.e., location relative to what? Considering only the present context of IDPS security, that frame of reference is some fixed point on earth; specifically, the location where the IDPS is supposed to be installed. In the current context, that point is established by the location of the BPT. The maximum distance between the IDPS and the BPT is bounded by a secure distance bounding protocol similar to the one described by Hancke [12]. According to this protocol, a dedicated communication channel specifically designed to accommodate RF pulse transmission and reception is provided. The prover (BPT) and verifier (IDPS) determine a suitable secret challenge/response message to be used only once. This message is then transmitted one bit at a time according to a set of rules previously agreed upon by both sides. These rules are intended to obscure the actual message and make it unpredictable to a would-be attacker. As each bit is received by the prover (BPT), it is immediately transformed (again, according to the pre-determined set of rules) and transmitted back. This echo-back feature is implemented in dedicated hardware to minimize turn-around delay and jitter. The verifier (IDPS) then measures the round-trip time (RTT) between when a challenge bit was sent and the response bit was received and calculates the time-of-flight (TOF) between the IDPS and the BPT, after compensating for any known turn-around and processing delay. With RF signal propagation occurring at approximately the speed of light $c \approx 3 \times 10^8$ m/sec, the distance $d$ between the IDPS and BPT is given by:

$$d = \frac{TOF}{c}$$

which works out to about 1 foot (distance) for every nanosecond of TOF delay.

With hardware mechanisms in the verifier (IDPS) performing the transmission, reception, and timing measurement, and with hardware mechanisms in the prover (BPT) performing bit reception, transformation and re-transmission, a key object of this system is to keep the endpoint delays (i.e., delay time other than actual TOF delay) as close to zero as physically possible, because every nanosecond of processing delay in the BPT represents a distance fraud opportunity for an attacker to exploit by being faster than the BPT. Hancke [12] observes that without foreknowledge of the message stream, the best an attacker can possibly hope for is to achieve zero processing delay. Assuming that an attacker manages to achieve zero delay, a 10 ns BPT endpoint delay gives the attacker approximately 10 feet of distance fraud opportunity to exploit.

The addition of a secure protocol, secret message and bit transformation rules, however, makes this scenario extremely unlikely since to be successful, the attacker would have to send the correct secret message data as processed by the aforementioned set of rules, both of which are presumably unknown to the attacker at the time of distance measurement. In the present application, where a main object of the attack is to move to IDPS from its present location and use it elsewhere, small distances (like the 10 foot example given above) don’t represent much of an opportunity. Any attempt by an attacker to mount a relay attack on this scheme would easily fail the distance test. This is quite different from distance fraud involving conventional RFID applications (passports, ID cards, access control), where even small distance fraud could potentially pose a threat.

2.2. Basis for PUF-based RFID security

Physically Unclonable Functions of a variety of different types are well known [8-11][13] and their use to provide various types of security for RFID applications has been described. In fact one manufacturer, Verayo, Inc. of San Jose CA, produces a line of uncopyable PUF-based RFID tags [14]. Silicon-based delay-arbiter type PUFs [11][13][15] are of primary interest in the present application, in part because they are easily implemented on FPGAs (although other PUF circuit architectures are readily adaptable to this application). In this type of PUF, various combinations of nearly identical wiring delays on a silicon device are selected and compared to one another.
Figure 2 shows the architecture of a silicon PUF based on wiring delay differences. In this scheme, the PUF characterizes the physical silicon in terms of ‘n’ pairs closely associated, nearly identical wiring delays, represented in the Figure as pairs of delay lines:

$$(D_{1A}, D_{1B}), (D_{2A}, D_{2B}), (D_{3A}, D_{3B}), \ldots (D_{nA}, D_{nB})$$

![Figure 2. A typical Silicon-based delay-arbiter PUF](image)

An ‘n’ bit challenge word C controls ‘n’ crosspoint switches XSW1, XSW2, etc., such that if a challenge bit controlling a crosspoint switch is zero, then connections are made straight across, and if the challenge bit is one, then the connections are swapped. That is, in the case of XSW1, if C1 is zero, then the output of D1A would connect to the input of D2A and the output of D1B would connect to the input of D2B. If C1 is one, however, then the connections would be swapped and the output of D1A would connect to the input of D2B and the output of D1B would connect to the input of D2A. Small variations in manufacturing processes and physical properties of the materials cause the delays in each pair to differ from one another by a very slight amount. On the PUF, a controlled clock signal (CLK) drives the inputs of the first pair of delays, with the outputs of each pair of delays being routed according to the bits of the challenge word C. In this way, the bits of the challenge word configure the pairs of delays together into two cascaded delay paths according to one of 2n possible combinations, ultimately comparing the two delays via an arbiter – in this case, an RS latch made from two NAND gates. When CLK is driven to zero, after all the delays settle out, a pair of zeroes ends up at the inputs to the RS latch. When a zero-to-one transition of CLK occurs, it traverses the two delay paths in parallel, arriving at the arbiter by the faster path first, thereby causing the arbiter to assume a stable state indicative of the result of the delay comparison. For example, if the cascaded delay path leading to the upper input of the arbiter is faster, then the state of the arbiter (at the top output) will be a zero after all of the delays have settled out. Conversely, if the path leading to the arbiter’s lower input is faster, the result will be a one. This logical delay comparison result is effectively a one-bit characterization of the chip containing the PUF for the challenge word C that produced it.

Multi-bit responses can be achieved by using a linear feedback shift register (LFSR). The LFSR acts as a pseudorandom hash function [16] to produce a different challenge to the PUF with each successive clock cycle. The LFSR would be loaded with the initial challenge word and then clocked ‘n’ times to produce an ‘n’ bit response to the ‘n’ bit challenge C in serial fashion.

In order to protect against the remote possibility of the occurrence of two PUFs on different devices having the same signatures an Unique ID value (manufacturer programmed) can be added to the challenge and inserted into the LFSR hash function[13]. This additional step makes each device truly unique.

PUFs, by their nature, are somewhat noisy, and repeatability cannot be guaranteed without some form of fault tolerance. Guajardo et al. [11] note this instability and suggest the use of error correction coding (ECC) (e.g., Reed Solomon or some other similar form of coding). Upon generating a PUF response word to a challenge, a suitable ECC syndrome would be generated and attached to the response word, effectively becoming part of the response. When verifying a response to a challenge, the ECC syndrome would be used to correct any bit errors in the response. As always, there is a trade-off between security and fault tolerance. With a PUF of sufficient bit length, the reduction in security is not significant.

PUF-based security, as implemented by the present system, relies on having a pre-calculated “stockpile” of challenge/response word pairs. In the proposed system, this “stockpile” would be refreshed (infrequently) as required by the BPT client (IDPS).

3. SYSTEM ARCHITECTURE

Figure 3 is a block diagram showing the BPT’s major functional blocks. The BPT is a passively powered device, with provision for external power in one special case: initialization by the manufacturer. As will be described below, this provision is non-essential, but could prove to be a significant time saver to the manufacturer.

The architecture of the BPT is basically that of a smart RFID transponder, with a control processor, a PUF and a variety of hardware assist functions. Even though power constraints are not as restrictive for the BPT as they are for RFID tags, power is still a consideration and low-power techniques must be employed wherever possible.

The processor is controlled by a program stored in program memory and can access RAM and non-volatile memory during operation. On many modern microcontrollers, there is sufficient built-in program memory (typically flash), RAM and NVM to perform any of the computational functions the BPT is likely to require. Many of these processors are also capable of controlling their power down to extremely low levels by slowing their operating speed and/or shutting down unused functions. The BPT communicates with the IDPS over the RFID channel by means of a modulator and demodulator. Incoming signals are demodulated by the demodulator and...
presented to the processor in serial fashion. In similar fashion the BPT can transmit (respond) to the IDPS via the modulator. (In a typical RFID system, a passive transponder modulates by switching the load impedance presented to the incoming RF carrier signal.)

![Figure 3. BPT Architecture](image)

The BPT implements several hardware assist modules. Of these, the two most important are the PUF function and the prover portion of a Time-Of-Flight distance bounding protocol as described by Hancke[12]. This hardware assist function accepts predetermined PUF-generated challenge/response information from the processor and implements the rapid-fire, single-bit distance bounding protocol. In order to minimize BPT endpoint delays, this function must be implemented completely in hardware.

The PUF function is preferably a delay arbiter type PUF as described above, and includes a hashing function (e.g., the LFSR hashing function described above) and error correction coding (ECC). It produces an ‘n’ bit response word (plus ECC syndrome) in response to any ‘n’ bit challenge in the manner described above. Either the hashing function or the ECC function could be implemented in software as an alternative to a hardware-based implementation.

In an alternative implementation, the IDPS and TA could assume that all PUF response values are noisy and the ECC function could be removed from the BPT and implemented on the IDPS/TA side instead. Two additional hardware assist functions provide acceleration for RSA encryption/decryption (large number and modulo arithmetic functions) and for RSA key generation (prime finding). As with the hash and ECC functions, either or both of these can be implemented in software.

Key generation is only performed once by the BPT – at its time of initialization when it uses the PUF function to produce a seed value for generating its own key.

These hardware assist mechanisms represent would provide considerable performance improvement, and can be enabled (powered) only when they are used, thereby minimizing overall power consumption.

### 3.1. Passive power considerations

One of the main motivations for passively powering the BPT is to allow the BPT to be physically secured, kept away from any direct connection to anything that might require maintenance access. In this way, the BPT can be buried in a building structure or some other ultra-secure location that would make it difficult or impossible to steal.

The BPT receives an RFID signal from the IDPS via its antenna. A voltage multiplier (typically involving a resonant circuit and multi-stage rectifier/multiplier) rectifies the RF signal and boosts its voltage to a level useful for powering the BPT (or at least selected portions of the BPT). As stated before, because the BPT is not as severely cost or size limited as a conventional RFID transponder tag, the antenna and charging system can be designed and optimized for very high energy transfer efficiency.

To prepare the BPT for operation, the IDPS can transmit an unmodulated RFID carrier to allow the BPT some initialization time prior to communicating with it. Further, the IDPS can leave the RFID carrier on while the BPT is performing computations. This allows the BPT to perform lengthy computations when necessary. Because the BPT is not as severely restricted in size as an RFID tag, the BPT can also implement a charging and storage function whereby RFID energy can be “harvested” to slowly charge an energy storage cell (battery). In this way, the BPT can function at higher power levels, when required, by using pre-stored energy.

Alternatively, the BPT can be powered by an entirely separate RF charging signal (at a different frequency from the RFID communication frequency) that continually charges the RFID’s energy storage cell. In this way, the BPT can sporadically operate at much higher power levels while remaining passively powered (e.g., to perform numerically intensive operations or the operate hardware assist mechanisms beyond the capability of an RFID signal driven power source).

A special direct-power facility is provided for the manufacturer to directly power the BPT when initializing it at time of manufacture. The BPT can detect this form of powering and allow itself to operate at a faster clock rate and with more resources active than it would ordinarily do under passive power conditions. Upon powering up for the first time, the uninitialized BPT queries the PUF with a predetermined challenge to produce a seed value for RSA
key generation. It then proceeds to generate and store its own public and private RSA keys. Once accomplished, this process will never be repeated. (This initialization and key generation process could also be done under passive power, but it would require arbitrary limitations on speed and available resources that could considerably slow down the operation.)

3.2. Use of Public Key Cryptography

The location-based security system employs public key (asymmetric) cryptography to provide two-way encryption and authentication throughout its operations. While this form of cryptography tends to be considerably more compute intensive than symmetric key encryption, it does not require a secret key to be kept on by both sides of an exchange. The strength of the RSA form of asymmetric key encryption/decryption is well established, and authentication is inherent when encryption is performed using a private key.

When the alternative possibility of a session key is considered, there are several disadvantages. First, a very high level of security for session key generation would have to be maintained for the session key generation process, so a secondary high-security scheme would still be required. Second, since the BPT is passively powered, it cannot reasonably provide time-based control of session limits, thereby opening up an avenue for attacks.

Lu et al [15] describe an approach to fast RSA key generation in the resource limited smart cards environment. The biggest and most compute intensive task in RSA key generation is that of prime finding. The remaining operations, including modulo exponentiation, are relatively simple and easily implemented [15]. Likewise, encryption and decryption, which is based on modulo exponentiation, is relatively simple and easily implemented.

In the present PUF-based system, the PUF’s response to a particular challenge would be used to seed the prime finding operations of key generation, thereby generating a unique public/private key pair for the BPT. Since this process is performed only once, the computational load associated with RSA key generation is not a concern under normal operating conditions.

To minimize the computing load using RSA encryption, messages should be kept as short as possible.

3.3. System Functions and Messages

All communications with the BPT are fully encrypted and authenticated in both directions using conventional asymmetric encryption operations. Authentication is accomplished by encrypting an authentication message with the sender’s private key. Each party to a communication has an ID and must identify itself and the intended recipient’s ID as part of the exchange. Message security and privacy is accomplished by encrypting using the intended receiver’s public key. Within that framework, the proposed location-based security system implements the following functions:

BPT Factory Initialization Sequence (KeyGen)

The manufacturer powers up BPT circuitry using the direct external power connection. This special case is detected by the BPT. (The BPT will also recognize its uninitialized NVM tables). The BPT initializes its table will all known, pre-stored values. The manufacturer identifies itself with an authenticated communication, after which the BPT queries the PUF function to obtain a seed for public/private key generation. It generates and stores the keys, finishing by transmitting its public key to the manufacturer along with an initial set of challenge/response pairs. The PUF is also used to generate a unique BPT ID.

Verify distance

A client (which can be the manufacturer, the TA, or any already-introduced IDPS) sends a verify command along with a challenge word and a random nonce. The BPT uses the challenge word to produce an initial challenge with a known response to the PUF. The PUF function returns a response, which is then hashed with the nonce according to a predetermined algorithm. The hashed response is then transmitted back to the client, which verifies its accuracy. A different hash of the response (according to a known set of rules) is generated in the BPT. The client then generates a random word performs single-bit distance verification as described by Hancke[12]. If the measured distance falls within expected bounds, then the client knows that it is within the expected distance of the authentic BPT.

Transfer TA Status to a new entity

The TA verifies the BPT (Verify distance). Confirming the BPT, it transmits a transfer message that includes the new TA’s ID, public key and a random nonce. The BPT responds with by retransmitting the new TA’s ID and public key along with a hash of the random nonce according to a predetermined function. To accept and execute or to reject and discard the transfer, the current TA sends an ACK or NAK message. If an acknowledgement is not received before the current TA stops communicating, the transfer of authority is discarded.

Introduce new Client System to BPT (TA)

In a manner similar to transfer of authority, the TA verifies the BPT, then transmits a command to add a new client that includes the new client’s ID, public key and a random nonce. The remainder of the transaction is the same as for transfer of TA authority. After introduction, the client may communicate with the BPT.

Invalidate Client System to BPT (TA)

The client is invalidated in exactly the same manner as it is introduced. After invalidation, the client can no longer communicate with the BPT.

Generate Challenge/Response Pair

The client, TA or manufacturer transmits a challenge message to the BPT requesting a response to the challenge along with a
3.4. Values Stored in BPT Non-Volatile Memory

- Manufacturer’s ID (pre-programmed)
- Manufacturer’s Public Key (pre-programmed)
- BPT ID (calculated at initialization)
- BPT public and private key (calculated at initialization)
- Current TA’s ID
- Current TA’s Public Key (by TA transfer)
- Client 1 ID and Public Key (by TA introduction)
- Client 2 ID and Public Key (by TA introduction)
- ... (other clients)
- Value related to challenge/response generation requests by manufacturer (to prevent duplication/reuse)
- Value related to challenge/response generation requests by current TA (to prevent duplication/reuse)
- Value related to challenge/response generation requests by each client (to prevent duplication/reuse)

4. CONCLUSIONS

The system proposed in this paper represents a framework for a practical location-based security scheme for protecting ID card/document production systems (or any system with similar requirements) against theft and operation away from their intended installation site. The framework is advantageous in that it provides a highly-secure, fully automatic mechanism for location-based security. Although this paper describes the system only in the context of ID document and card production, it can easily be applied anywhere a computing system of any type needs to be protected against theft or otherwise secured to a fixed location.

The development of the messaging protocols, development of a hardware implementation, and experimental verification of results are all subjects of ongoing research that will be discussed in different publications.

References


Biographies

Eugene P. Gerety received BSEE and MSEE degrees from the University of Bridgeport in 1981 and 1984, respectively, and is currently pursuing a Ph.D in Computer Engineering and Computer Science at the University of Bridgeport. He is currently a Senior Staff Systems Engineer at Philips/Respironics, and has previously held positions as Vice President of Research and Development for Datastrip, Inc., Chief Principal Engineer at CooperSurgical, Inc., Manager of Hardware Engineering at Paragon Networks, and senior engineering positions with Pitney Bowes and ITT Corp.

Dr. Khaled M. Elleithy is the Associate Dean for Graduate Studies in the School of Engineering at the University of Bridgeport. He has research interests are in the areas of network security, mobile communications, and formal approaches for design and verification. He has published more than one hundred twenty research papers in international journals and conferences in his areas of expertise.

Dr. Elleithy is the co-chair of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). CISSE is the first Engineering/Computing and Systems Research E-Conference in the world to be completely conducted online in real-time via the internet and was successfully running for four years.

Dr. Elleithy is the editor or co-editor of 10 books published by Springer for advances on Innovations and Advanced Techniques in Systems, Computing Sciences and Software.

Dr. Elleithy received the B.Sc. degree in computer science and automatic control from Alexandria University in 1983, the MS Degree in computer networks from the same university in 1986, and the MS and Ph.D. degrees in computer science from The Center for Advanced Computer Studies in the University of Louisiana at Lafayette in 1988 and 1990, respectively.