On the Logical Verification of Key Exchange Protocols for Mobile Communications

T. Newe & T. Coffey
Data Communications Security Group,
Department of Electronic & Computer Engineering,
University of Limerick,
Ireland.
E-Mail: (Thomas.Newe@UL.ie) (Tom.Coffey@UL.ie)
Fax: 353-61-338176

ABSTRACT

Secure communications are paramount in today's environment, where mobile and fixed networks are trusted with highly sensitive information. Cryptographic protocols are used to provide security services, such as confidentiality, authentication and non-repudiation. Beller, Chang and Yacobi (BCY) proposed three communication protocols capable of providing mobile link security services. These protocols use a combination of asymmetric and symmetric cryptographic algorithms.
In this paper the original BCY basic Modular Square Root (MSR) protocol and the Boyd-Mathuria modified Improved Modular Square Root (IMSR) protocol are discussed. A formal verification of these protocols using the Coffey-Saidha-Newe (CSN) modal logic is given. This verification demonstrates that protocol weaknesses can be readily detected by the use of formal verification methods.

Key-Words: Formal methods, verification, modal logic, wireless communications, 3G mobile, security protocol.

1. Introduction

Wireless communications are being driven by the need for providing network access to mobile or nomadic computing devices. Although the need for wireless access to a network is evident, new problems are presented by this medium. Specifically the wireless medium offers new opportunities for hackers to listen in on private data communications. This kind of eavesdropping is virtually undetectable. In order to prevent this unauthorised access to user's data, secure communications protocols are utilised. These protocols are charged with providing both privacy of data and authentication of users. Such protocols can employ private-key and/or public key cryptographic algorithms. Public-key algorithms hold the promise of simplifying the network infrastructure required to provide privacy and authentication, while symmetric algorithms require less processing power on the mobile device. A popular approach is to use a hybrid protocol which uses the public key algorithm to distribute a secret session key for use with a symmetric algorithm.

Beller, Chang and Yacobi proposed 3 hybrid protocols [1] capable of providing radio link security services. These protocols use a combination of asymmetric and symmetric cryptographic algorithms. The algorithms were chosen so that the computational demands imposed satisfied the imbalance in the computational power of a typical mobile device and base station. Carlsen [3] critically examined these protocols and identified some possible attacks and suggested some protocol modifications to avoid them. Carlsen's suggested improvements were further modified by Boyd and Mathuria [2].

In this paper the BCY basic MSR (Modular Square Root) and the Boyd-Mathuria modified BCY IMSR (Improved Modular Square Root) protocols are discussed. The Coffey-Saidha-Newe (CSN) logic is then presented and a formal analysis of both security protocols is given. This analysis clearly shows the problems that exist in the basis BCY MSR protocol and how they were corrected in the Boyd-Mathuria modified BCY IMSR protocol.

2. The BCY Basic MSR Protocol

The basic MSR protocol operates as follows:

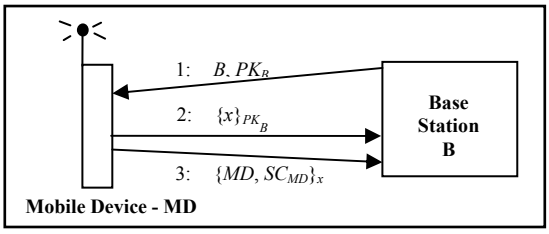

Figure 1 BCY Basic MSR Protocol

Notation used:

B - Base Station
MD - Mobile device
PK_B - Public key of base station.
SC_{MD} - Secret certificate of Mobile device - issued by a trusted central authority.
$\{X\}_K$ - Denotes encryption of X with a key K, where K can be either a symmetric key or a public key depending on the encryption algorithm used.

Upon receiving the public key of B, PK_B, the mobile MD uses it to encrypt a session key x. Then this encrypted message is sent to B. The mobile MD also sends its identity and secret certificate, SC_{MD}, encrypted using x to authenticate x to the base station B. The encryption in step 3 is carried out using a symmetric algorithm. Since the symmetric algorithm operates at a speed far greater than even Rabins public key algorithm used in step 2 the computational effort of the mobile MD is effectively

reduced to that of modulo squaring the session key.

Carlsen [3] identified two weaknesses in the above protocol:

1. The public key of *B* is uncertified, thereby allowing base station masquerading.
2. *B* cannot differentiate between a new protocol run and an old one. Allowing session key replay.

These weaknesses are highlighted in section 5 where the CSN logic is applied in the formal verification of the protocol.

3. The Boyd-Mathuria Modified BCY IMSR Protocol

Carlsen suggested an improvement to the BCY IMSR protocol, figure 2, which includes a challenge-response mechanism, N_B, to allow the base station *B* to detect a session key replay. He also included an expiration time to the contents of the certificate of *B*, *Cert*(*B*), to allow for checks on the certificates validity while at the same time deleting *B*'s certificate from *Cert*(*B*).

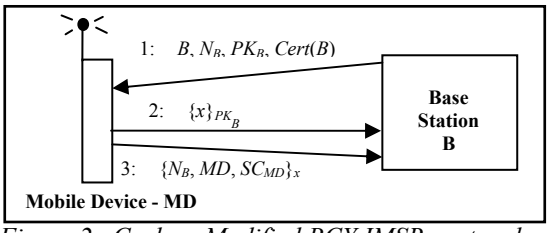

Figure 2. Carlsen Modified BCY IMSR protocol

Although Carlsen identified the replay problem his suggestion for solving it did not work successfully. In figure 2 if *x* is compromised then so is SC_{MD}, thus an attacker can freely masquerade as *MD* as in the original MSR protocol. The solution to this problem as highlighted by Boyd and Mathuria [2] involves sending more information in step 2 of the protocol and less in step 3 as follows:

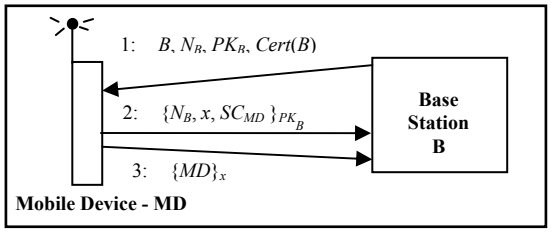

Figure 3. Boyd-Mathuria Modified BCY IMSR protocol

Now if *x* is compromised the mobile's, *MD*'s, secret certificate, SC_{MD}, is not.

In section 6 the Boyd-Mathuria protocol is formally analysed and its operation verified.

4. The Coffey-Saidha-Newe (CSN) Formal Logic

The CSN [4] logic provides a means of verifying hybrid cryptographic protocols. The logic can analyse the evolution of both knowledge and belief during a protocol execution and is therefore useful in addressing issues of both security and trust. The inference rules provided are the standard inferences required for natural deduction and the axioms of the logic are sufficiently low-level to express the fundamental properties of hybrid cryptographic protocols, such as the ability of a principal to encrypt/decrypt based on knowledge of a cryptographic key.

The logic is capable of analysing a wide variety of hybrid cryptographic protocols because the constructs of the logic are general purpose and therefore provide the user with increased flexibility allowing him to develop his own theorems.

4.1 The CSN Logic Language

The language for the CSN logic used to formally express the logical postulates and protocol facts is as follows:

- **a,b,c,...**, general propositional variables
- **Φ**, an arbitrary statement
- **Σ** and **Ψ**, arbitrary entities
- **i** and **j**, range over entities
- **ENT**, the set of all possible entities
- **k**, a cryptographic key. In particular, k_Σ is the public key of entity Σ and k_Σ^{-1} is the corresponding private key of entity Σ
- **t, t', t''...** time
- **e**(x,k_Σ), encryption function, encryption of *x* using key k_Σ
- **d**(x,k_Σ^{-1}), decryption function, decryption of *x* using key k_Σ^{-1}
- ***K***, propositional knowledge operator of Hintikka. $K_{\Sigma,t}\Phi$ means Σ knows statement Φ at time *t*.
- ***L***, knowledge predicate. $L_{\Sigma,t}x$ means Σ knows and can reproduce object *x* at time *t*.
- ***B***, belief operator. $B_{\Sigma,t}\Phi$ means Σ believes at time *t* that statement Φ is true.
- ***C***, 'contains' operator. *C*(x,y) means that the object *x* contains the object *y*. The object *y* may be cleartext or ciphertext in *x*.
- ***S***, emission operator. *S*(Σ,t,x) means Σ sends message *x* at time *t*.
- ***R***, reception operator. *R*(Σ,t,x) means Σ receives message *x* at time *t*.
- $\mathbf{ks_{(\Sigma,\Psi)}}$ Shared secret key for entities Σ and Ψ.
- $\mathbf{KS_{\{\Sigma,\Psi\}}}$ Set of good shared keys for entities Σ and Ψ.
- $\mathbf{ss_{(\Sigma,\Psi)}}$ Shared secret for entities Σ and Ψ (secret can be fresh).
- $\mathbf{SS_{\{\Sigma,\Psi\}}}$ Set of good shared secrets for entities Σ and Ψ.
- **E(x, $\mathbf{ks_{(\Sigma,\Psi)}}$),** Encryption of plaintext message *x* using the shared secret key of entities Σ and Ψ.
- **D(x, $\mathbf{ks_{(\Sigma,\Psi)}}$),** Decryption of ciphertext message *x* using the shared secret key of entities Σ and Ψ.
- **A**, authentication Operator. **A(Σ,t,Ψ)** means that Σ authenticates Ψ at time t.

The language includes the classical logical connectives of conjunction (∧), disjunction (∨), complementation (¬) and material implication (→). The symbols ∀ and ∃ denote universal and existential quantification

respectively. $\in$ indicates membership of a set and / denotes set exclusion. The symbol $\vdash$ denotes a logical theorem. The logic does not contain specific temporal operators, but the knowledge, belief and message transfer operators are time-indexed.

4.2 Inference Rules

The logic incorporates the following rules of inference:

R1: From $\vdash p$ and $\vdash (p \rightarrow q)$ infer $\vdash q$

R2: **(a)** From $\vdash p$ infer $\vdash K_{\Sigma,t}p$

(b) From $\vdash p$ infer $\vdash B_{\Sigma,t}p$

R1 is the *Modus Ponens* and states that if schema p can be deduced and $(p \rightarrow q)$ can be deduced, then q can also be deduced. R2 consists of the Generalisation rules which state that if p is a theorem, then knowledge and belief in p are also theorems.

The logic also includes the following standard propositional rules of natural deduction:

R3: From $(p \wedge q)$ infer p

R4: From p and q infer $(p \wedge q)$

R5: From p infer $(p \vee q)$

R6: From $\neg(\neg p)$ infer p

R7: From (from p infer q) infer $(p \rightarrow q)$

4.3 Axioms

Two types of axioms are used in this logic, *logical* and *non-logical*. Logical axioms are general statements made in relation to any system, while non-logical are system specific.

4.3.1 Logical Axioms

The logic includes the following standard modal axioms for knowledge and belief:

A1: **(a)** $\exists t\exists p\exists q(K_{\Sigma,t}p \wedge K_{\Sigma,t}(p \rightarrow q) \rightarrow K_{\Sigma,t}q)$

(b) $\exists t\exists p\exists q(B_{\Sigma,t}p \wedge B_{\Sigma,t}(p \rightarrow q) \rightarrow B_{\Sigma,t}q)$

A2: $\exists t\exists p(K_{\Sigma,t}p \rightarrow p)$

The axioms A1(a) and A1(b) are applications of the Modus Ponens to the knowledge and belief operators. The axiom A2 is called the knowledge axiom and is said to logically characterise knowledge. If something is known, then it is true. This property distinguishes between knowledge and belief.

A3: **(a)** $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}x \rightarrow \forall t',t'\geq t\ L_{i,t'}x)$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(K_{i,t}x \rightarrow \forall t',t'\geq t\ K_{i,t'}x)$

(c) $\exists t\exists x\exists i,i\in\{ENT\}(B_{i,t}x \rightarrow \forall t',t'\geq t\ B_{i,t'}x)$

Axioms A3(a), A3(b) and A3(c) relate to the monotonicity of knowledge and belief, which asserts that knowledge and belief, once gained, cannot be lost.

A4: $\exists t\exists x\exists y(\exists i,i\in\{ENT\}L_{i,t}y \wedge C(y,x) \rightarrow \exists j,j\in\{ENT\}L_{j,t}x)$

The final logical axiom is concerned with the C predicate. If a piece of data is constructed from other pieces of data, then each piece of data involved in the construction must be known to some entity:

4.3.2 Non-Logical Axioms

The non-logical axioms (A5-A15) reflect the underlying assumptions of the logic. These assumptions relate to the emission and reception of messages and to the use of encryption and decryption in these messages.

A5: $\exists t\exists x(\ S(\Sigma,t,x) \rightarrow L_{\Sigma,t}x \wedge \exists i,i\in\{ENT/\Sigma\}\exists t',t'>t\ R(i,t',x))$

The emission axiom (A5) states that: if Σ sends a message x at time t, then Σ knows x at time t and some entity i other than Σ will receive x at time t' subsequent to t.

A6: $\exists t\exists x(R(\Sigma,t,x) \rightarrow L_{\Sigma,t}x \wedge \exists i,i\in\{ENT/\Sigma\}\exists t',t'<t\ S(i,t',x))$

The reception axiom (A6) states that: if Σ receives a message x at time t, then Σ knows x at time t and some entity i other than Σ has sent x at time t' prior to t.

A7: **(a)** $\exists t\exists x\exists i,i\in\{ENT\}(\ L_{i,t}x \wedge L_{i,t}k_{\Sigma} \rightarrow L_{i,t}(e(x,k_{\Sigma})))$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}x \wedge L_{i,t}k_{\Sigma}^{-1} \rightarrow L_{i,t}(d(x,k_{\Sigma}^{-1})))$

Axioms A7(a) and A7(b) refer to the ability of an entity to encrypt or decrypt a message when it has knowledge of a public or private cryptographic key.

A8: **(a)** $\exists t\exists x\exists i,i\in\{ENT\}(\ \neg L_{i,t}k_{\Sigma} \wedge \forall t',\ t'<t,\ \neg L_{i,t'}(e(x,k_{\Sigma})) \wedge \neg(\exists y(\ R(i,t,y) \wedge C(y,e(x,k_{\Sigma})))) \rightarrow \neg L_{i,t}(e(x,k_{\Sigma})))$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(\ \neg L_{i,t}k_{\Sigma}^{-1} \wedge \forall t',t'<t,\ \neg L_{i,t'}(d(x,k_{\Sigma}^{-1})) \wedge \neg(\exists y(R(i,t,y) \wedge C(y,d(x,k_{\Sigma}^{-1})))) \rightarrow \neg L_{i,t}(d(x,k_{\Sigma}^{-1})))$

Axioms A8(a) and A8(b) refer to the impossibility of encrypting or decrypting a message without knowledge of the correct key. Axiom A8a states that if an entity does not know k_{Σ} at t and does not know, prior to t, the encryption $e(x,k_{\Sigma})$ and also does not receive $e(x,k_{\Sigma})$ at t in a message, then the entity cannot know $e(x,k_{\Sigma})$ at time t. Axiom A8b makes a similar statement for the decryption of a message x without knowledge of the decryption key.

A9: $\forall t(\forall i,i\in\{ENT\}L_{i,t}k_i^{-1} \wedge \forall j,j\in\{ENT/i\}\neg L_{j,t}k_i^{-1})$

The key secrecy axiom (A9) states that the private keys used by the system are known only to their rightful owners.

A10: $\exists t\exists x(\exists i,i\in\{ENT\}(L_{i,t}d(x,k_{\Sigma}^{-1}) \wedge L_{i,t}k_{\Sigma}) \rightarrow L_{i,t}x)) \rightarrow K_{i,t}(\exists t',t'<t\ L_{\Sigma,t'}x)$

Axiom A10 states that if an entity knows and can reproduce $d(x,k_{\Sigma}^{-1})$ and k_{Σ} at time t then it knows and can reproduce x, this implies that this entity knows at time t that Σ knows and can reproduce x prior to t.

A11:

(a) $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}x \wedge L_{i,t}ks_{(\Sigma,\Psi)} \rightarrow L_{i,t}(\ E(x,\ ks_{(\Sigma,\Psi)})))$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(L_{i,t}x \wedge L_{i,t}ks_{(\Sigma,\Psi)} \rightarrow L_{i,t}(D(x,\ ks_{(\Sigma,\Psi)})))$

Axiom 11 refers to the ability an entity has to encrypt or decrypt a message using a symmetric system when it has knowledge of a secret key.

A12:

(a) $\exists t\exists x\exists i,i\in\{ENT\}(\ \neg L_{i,t}ks_{(\Sigma,\Psi)} \wedge \forall t',t'<t,\ \neg\ L_{i,t'}(\ E(x,ks_{(\Sigma,\Psi)})) \wedge \neg(\exists y(R(i,t,y) \wedge C(y,E(x,ks_{(\Sigma,\Psi)})))) \rightarrow \neg L_{i,t}(E(x,ks_{(\Sigma,\Psi)})))$

(b) $\exists t\exists x\exists i,i\in\{ENT\}(\ \neg L_{i,t}ks_{(\Sigma,\Psi)} \wedge \forall t',t'<t,\ \neg\ L_{i,t'}(D(x,ks_{(\Sigma,\Psi)})) \wedge \neg(\exists y(R(i,t,y) \wedge C(y,D(x,ks_{(\Sigma,\Psi)})))) \rightarrow \neg L_{i,t}(D(x,ks_{(\Sigma,\Psi)})))$

Axiom 12 refers to the inability of an entity to encrypt or decrypt data without knowledge of the appropriate shared secret key.

A13:

$\forall t((\forall i,i\in\{ENT/\Sigma,\Psi\}\neg L_{i,t}ks_{(\Sigma,\Psi)} \wedge \exists j,j\in\{\Sigma,\Psi\}\ L_{j,t}ks_{(\Sigma,\Psi)})$
$\rightarrow\ ks_{(\Sigma,\Psi)}\in\{KS_{\{\Sigma,\Psi\}}\}))$

Axiom 13 states that only the rightful owners of a shared secret key know that key and this implies that this key is a good key.

A14:

$\forall t((\forall i,i\in\{ENT/\Sigma,\Psi\}\neg L_{i,t}ss_{(\Sigma,\Psi)} \wedge \exists j,j\in\{\Sigma,\Psi\}L_{j,t}ss_{(\Sigma,\Psi)})$
$\rightarrow ss_{(\Sigma,\Psi)}\in\{SS_{\{\Sigma,\Psi\}}\}))$

Axiom 14 states that only the rightful owners of a shared secret know that secret and this implies that this is a good secret.

A15:

(a)$\exists x\exists t(A(\Sigma,t,\Psi) \rightarrow (L_{\Sigma,t}ss_{(\Sigma,\Psi)} \wedge ss_{(\Sigma,\Psi)}\in\ \{SS_{\{\Sigma,\Psi\}}\}\ \wedge R(\Sigma,t,x) \wedge C(x,ss_{(\Sigma,\Psi)}) \wedge \forall t',t' < t\ \neg S(\Sigma,t',x)) \rightarrow K_{\Sigma,t}(S(\Psi,t',x))))$

(b)$\exists x\exists t(A(\Sigma,t,\Psi) \rightarrow (L_{\Sigma,t}k_\Psi \wedge L_{\Sigma,t}x \wedge R(\Sigma,t,y) \wedge C(y,e(x,\ k_\Psi^{-1})))$
$\rightarrow (\forall t',\ t' < t,\ K_{\Sigma,t}(S(\Psi,t',y))))$

Axiom 15 is the authentication axiom and it comes in symmetric and asymmetric form.

A15 (a) states: If Σ knows a secret $ss_{(\Sigma,\Psi)}$ that it shares with Ψ (the secret can be fresh), and this secret is a good secret, and Σ receives a message containing $ss_{(\Sigma,\Psi)}$ at *t* that it did not send, then Σ knows that Ψ sent this message prior to *t*.

A15 (b) states: If Σ knows the public key of Ψ (k_Ψ) and message x, and if Σ receives a message y containing e(x, k_Ψ^{-1}) then Σ knows that Ψ sent message y prior to t.

5. Formal Analysis of BCY Basic MSR Protocol

As discussed in section 2 the BCY basic MSR protocol has a number of weaknesses. In this section the CSN logic is applied to the protocol and these weaknesses are formally highlighted.

5.1 Goals of the BCY Basic MSR Protocol

The goals of the basic MSR protocol are listed in figure 4 and are defined as:

Goal 1 indicates that the mobile *MD* will obtain the public key of the base station *B*, K_B, from *B* prior to the end of step 1.

Goal 2 states that *B* knows it will receive the session key *x* from *MD* prior to the end of step 2. The time indicators of this goal also indicates that *x* should be fresh.

Goal 3 states that base station *B* expects the mobile *MD* to send its secret certificate before the end of step 3 but after step 2. The time indicators indicate that the session key *x* has to arrive first.

Goal 1:	$K_{MD,t1}(\exists t,\ t < t1,\ S(B,\ t,\ K_B))$
Goal 2:	$K_{B,t2}(\exists t,\ t0 < t < t2,\ S(MD,\ t,\ x))$
Goal 3:	$K_{B,t3}(\exists t,\ t2 < t < t3,\ S(MD,\ t,\ Cert_{MD}))$

Figure 4. Goals of the BCY Basic MSR Protocol

5.2 Initial Assumptions of the BCY Basic MSR Protocol

1:	$\forall i,\ i\in\{ENT\}\forall t,\ B_{i,t}K_B$
2:	$\forall i,\ i\in\{ENT\}\forall t,\ Ki,tCert_{MD}$
3:	$L_{MD,t0}x \wedge K_{MD,t0}(\forall i,\ i\in\{ENT/MD\},\forall t,\ t < t2,\ \neg L_{i,t}x)$
4:	$B_{B,t0}(\forall i,\ i\in\{ENT/MD\},\ \forall t,\ t0 < t < t2,\ \neg L_{i,t}x)$

Figure 5. Initial Assumptions of the BCY Basic MSR Protocol

Assumption 1 states that the public key, K_B, of the base station *B* is believed by all entities. No details of ownership are provided and only trust is assumed since the public key, K_B, is uncertified.

Assumption 2 states that all entities know that the secret certificate of the mobile *MD*, $Cert_{MD}$, is good.

Assumption 3 states that the mobile *MD* generates the fresh secret session key *x* and as such it knows that no entity has knowledge of *x* before step 2 of the protocol.

Assumption 4 refers to the fact that the session key *x* is generated entirely by *MD* and not by interaction with *B*. Therefore *B* only believes in the freshness of *x*, as it has no knowledge of it.

5.3 Message Exchanges of the BCY Basic MSR Protocol

Analysing the messages exchanged at each protocol step, we get:

Step 1:

$K_{MD,t1}\ (R(MD,t1,K_B))$

States that the mobile *MD* knows at time t1 that it will receive a message containing K_B.

Apply Axiom A2 to reduce the formula: $R(MD,t1,K_B)$

Apply Axiom A6, the reception axiom:

$L_{MD,t1}K_B \wedge \exists i,\ i \in\{ENT/MD\},\ \exists t,\ t < t1,\ S(i,t,K_B)$

Inference rule R2:

$L_{MD,t1}K_B \wedge K_{MD,t1}\ (\exists i,\ i \in\{ENT/MD\},\ \exists t,\ t < t1,\ S(i,t,K_B))$

Inference rule R3 to reduce:

$K_{MD,t1}\ (\exists i,\ i \in\{ENT/MD\},\ \exists t,\ t < t1,\ S(i,t,K_B))$

Using assumption 1, which expresses belief in the public key of *B*, K_B, we get:

$B_{MD,t1}\ (\exists t,\ t < t1,\ S(B,t,K_B))$ **:!Goal 1**

Only belief achieved, not knowledge!

This tells us that only belief in the sender of the public key of *B*, K_B, is achieved due to the non-certification of K_B. This can allow masquerading of *B* by an intruder.

Step 2:

$K_{B,t2}\ (R(B,t2,Y) \wedge C(Y,\ e(x,\ K_B)))$

This states that *B* knows at time t2 that it will receive a message *Y* and *Y* contains the session key *x* encrypted using the public key of *B*, K_B.

Applying Axiom A2 to reduce the formula:

$R(B,t2,Y) \wedge C(Y,\ e(x,\ K_B))$

Apply Axiom A6:

$L_{B,t2}Y \wedge \exists i,\ i \in\{ENT/B\},\ \exists t,\ t<t2,\ S(i,t,Y)\wedge C(Y,\ e(x,\ K_B))$

Inference rule R2:

$L_{B,t2}Y \wedge K_{B,t2}\ (\exists i,\ i \in \{ENT/B\},\ \exists t,t<t2,\ S(i,t,Y) \wedge C(Y,\ e(x,\ K_B)))$

Using Inference rule R3 to reduce:

$K_{B,t2}\ (\exists i,\ i \in \{ENT/B\},\ \exists t,\ t < t2,\ S(i,t,Y) \wedge C(Y,\ e(x,\ K_B)))$

Applying Axioms A4 and A10:

$K_{B,t2}\ (\exists i,\ i \in \{ENT/B\},\ \exists t,\ t < t2,\ S(i,t,x))$

Using assumption 3 which states that the mobile *MD* generates *x*:

$K_{B,t2}\ (\exists t,\ t < t2,\ S(MD,t,x))$

Using assumption 4 which expresses the belief of *B* in the freshness of *x*:

$B_{B,t2}\ (\exists t,\ t0 < t < t2,\ S(MD,t,x))$ **:!Goal 2**

Only belief achieved, not knowledge!

This indicates that only belief in the freshness of *x* is achieved by *B* and not knowledge due to the fact that *B* has no role in the creation of *x*, *x* is not time stamped and nonces are not used.

Step 3:

$K_{B,t3}\ (R(B,t3,Y) \wedge C(Y,\ E(Cert_{MD},\ x)))$

Applying Axiom A2 to reduce the formula:

$R(B,t3,Y) \wedge C(Y,\ E(Cert_{MD},\ x))$

Apply Axiom A6:

$L_{B,t3}Y \wedge \exists i,\ i \in \{ENT/B\},\ \exists t,\ t<t3,\ S(i,t,Y) \wedge C(Y,\ E(Cert_{MD},\ x))$

Inference rule R2:

$L_{B,t3}Y \wedge K_{B,t3}(\exists i, i \in \{ENT/B\}, \exists t,t<t3, S(i,t,Y) \wedge C(Y, E(Cert_{MD},\ x)))$

Inference rule R3 to reduce formula:

$K_{B,t3}\ (\exists i,\ i \in \{ENT/B\},\ \exists t,\ t < t3,\ S(i,t,Y) \wedge C(Y,\ E(Cert_{MD},\ x)))$

Using assumption 3 which states that only *MD* has knowledge of *x* before t2:

$K_{B,t3}\ (\exists t,\ t2 < t < t3,\ S(MD,t,Y) \wedge C(Y,\ E(Cert_{MD},\ x)))$

Using Axioms A11 and A12, which reflect the ability of an entity to decrypt a message when it has knowledge of the secret key and assumption 4 which states that *B* has belief of *x* after t2 we get:

$B_{B,t3}\ (\exists t,\ t2 < t < t3,\ S(MD,t,Cert_{MD}))$ **: !Goal 3.**

Only belief achieved, not knowledge!

The goal of the timely arrival of the secret certificate $Cert_{MD}$ from *MD* is not achieved. This is due to the fact that the certificate itself could be compromised because only trust and not knowledge in the freshness of *x* is established by assumption 4. This leaves the protocol open to a masquerade attack.

6. Formal Analysis of the Boyd-Mathuria Modified BCY IMSR Protocol

The Boyd-Mathuria modified BCY IMSR protocol discussed in section 3 is now formally analysed.

6.1 Goals of the Boyd-Mathuria Modified BCY IMSR Protocol

The goals of the Modified/Improved IMSR protocol are listed in figure 6.

Goal 1:	$K_{MD,t1}(\exists t,\ t < t1,\ S(B,\ t,\ (N_B,\ K_B,\ Cert_B)))$
Goal 2:	$K_{B,t2}(\exists t,\ t0 < t < t2,\ S(MD,\ t,\ (x,\ N_B, Cert_{MD})))$
Goal 3:	$K_{B,t3}(\exists t,\ t2 < t < t3,\ S(MD,\ t,\ MD))$

Figure 6. Goals of the Boyd-Mathuria Modified BCY IMSR Protocol

Goal 1 indicates that the mobile *MD* will obtain N_B, K_B and $Cert_B$ from *B* prior to the end of step 1.

Goal 2 states that *B* knows it will receive the session key *x*, nonce N_B and the certificate of the mobile $Cert_{MD}$ before the end of step 2 from *MD*. This certificate allows the mobile to be authenticated. The time indicators of this goal indicate that *x* should be fresh.

Goal 3 states that base station *B* expects the mobile to send its public ID, *MD*, before the end of step 3 but after step 2. The time indicators indicate that the session key *x* has to arrive at the base station *B* first. The encryption of *MD* by *x* achieves user confidentiality for this session.

6.2 Initial Assumptions of the Boyd-Mathuria Modified BCY IMSR Protocol

1:	$\forall i,\ i \in \{ENT\}\ \forall t,\ t < t_{CertB},\ L_{i,t}K_B$
2:	$\forall i,\ i \in \{ENT\}, \forall t,\ t1 < t < t_{CertB},\ L_{i,t}Cert_B$
3:	$\forall i,\ i \in \{ENT\}\ \forall t,\ K_{i,t}Cert_{MD}$
4:	$L_{MD,t0}x \wedge K_{MD,t0}(\forall i,\ i \in \{ENT/MD\}, \forall t,\ t < t2,\ \neg L_{i,t}x)$
5:	$K_{B,t0}(\forall i,\ i \in \{ENT/MD\},\ \forall t,\ t0 < t < t2,\ \neg L_{i,t}x)$
6:	$K_{B,t0}(\forall i,\ i \in \{ENT/B\}, \forall t,\ t < t1,\ \neg L_{i,t}N_B)$

Figure 7. Initial Assumptions of the Boyd-Mathuria Modified BCY IMSR Protocol

Assumption 1 states that the public key, K_B, of the base station *B* is known to all entities. K_B is certified up to time t_{CertB}.

Assumption 2 indicates that the certificate of *B*, $Cert_B$, is known to all entities after step 1 and this certificate is only valid up to time t_{CertB}, after which its validity expires.

Assumption 3 states that all entities know that the secret certificate of the mobile *MD*, $Cert_{MD}$, is good.

Assumption 4 states that the mobile *MD* generates the fresh secret session key *x* and as such it knows that no entity has knowledge of *x* before step 2 of the protocol.

Assumption 5 states that *B* knows that *x* is fresh. This is due to the inclusion of N_B in the encrypted message of step 2. The ID of the mobile is established by the inclusion of its secret certificate $Cert_{MD}$.

Assumption 6 indicates that only *B* knows and can reproduce the random nonce, N_B, prior to step 1. This indicates its freshness.

6.3 Message Exchanges of the Boyd-Mathuria Modified BCY IMSR Protocol

Analysing the messages exchanged at each protocol step, we get:

Step 1:

$K_{MD,t1}\ (R(MD,t1,Y) \wedge C(Y,\ (N_B,\ K_B,\ Cert_B)))$

States that the mobile *MD* knows at time t1 that it will receive a message *Y* containing N_B, K_B and the certificate of *B*, $Cert_B$.

Apply Axiom A2 to reduce the formula:

$R(MD,t1,Y) \wedge C(Y,\ (N_B,\ K_B,\ Cert_B))$

Apply Axiom A6, the reception axiom:

$L_{MD,t1}Y \wedge \exists i, i \in \{ENT/MD\}, \exists t, t<t1, S(i,t,Y) \wedge C(Y,(N_B,K_B, Cert_B))$

Inference rule R2:

$L_{MD,t1}Y \wedge K_{MD,t1}(\exists i, i \in \{ENT/MD\}, \exists t, t < t1, S(i,t,Y) \wedge C(Y,(N_B,K_B, Cert_B)))$

Inference rule R3 to reduce:

$K_{MD,t1}(\exists i, i \in \{ENT/MD\}, \exists t, t < t1, S(i,t, (N_B, K_B, Cert_B)))$

Assumption 1 expresses knowledge by all entities of the public key of B, K_B, prior to time t_{CertB} and assumption 2 shows that $t_{CertB} > t1$. Applying assumptions we get:

$K_{MD,t1}(\exists t, t < t1, S(B,t, (N_B, K_B, Cert_B)))$ **:Satisfies Goal 1**

Step 2:

$K_{B,t2}(R(B,t2,Y) \wedge C(Y, e((x, N_B,Cert_{MD}), K_B)))$

This states that B knows at time t2 that it will receive a message Y, and Y contains the session key x, random nonce N_B and secret certificate of the mobile, $Cert_{MD}$, encrypted using the public key of B, K_B.

Applying Axiom A2 to reduce the formula:

$R(B,t2,Y) \wedge C(Y, e((x, N_B,Cert_{MD}), K_B))$

Apply Axiom A6:

$L_{B,t2}Y \wedge \exists i, i \in \{ENT/B\}, \exists t, t < t2, S(i,t,Y) \wedge C(Y, e((x,N_B,Cert_{MD}), K_B))$

Inference rule R2:

$L_{B,t2}Y \wedge K_{B,t2}(\exists i, i \in \{ENT/B\}, \exists t, t < t2, S(i,t,Y) \wedge C(Y, e((x, N_B,Cert_{MD}), K_B)))$

Using Inference rule R3 to reduce:

$K_{B,t2}(\exists i, i \in \{ENT/B\}, \exists t, t<t2, S(i,t,Y) \wedge C(Y,e((x,N_B,Cert_{MD}),K_B)))$

Applying Axioms A4 and A10:

$K_{B,t2}(\exists i, i \in \{ENT/B\}, \exists t, t < t2, S(i,t, (x, N_B,Cert_{MD})))$

Using assumption 4 which states that the mobile MD generates x and x is not known before time t2 to any other entity:

$K_{B,t2}(\exists t, t < t2, S(MD,t, (x, N_B,Cert_{MD})))$

Using assumptions 6 which states that B knows that N_B is fresh for this protocol cycle, we get:

$K_{B,t2}(\exists t, t0<t<t2, S(MD,t, (x, N_B,Cert_{MD})))$ **:Satisfies Goal 2**

The freshness of x is established by assumption 5 and the identity of the mobile is known due to the inclusion of $Cert_{MD}$ in the encrypted message.

Step 3:

$K_{B,t3}(R(B,t3,E(MD, x))$

Applying Axiom A2 to reduce the formula:

$R(B,t3, E(MD, x))$

Apply Axiom A6:

$L_{B,t3}E(MD, x) \wedge \exists i, i \in \{ENT/B\}, \exists t, t < t3, S(i,t, E(MD, x))$

Inference rule R3 to reduce formula:

$\exists i, i \in \{ENT/B\}, \exists t, t < t3, S(i,t, E(MD, x))$

Inference rule R2:

$K_{B,t3}(\exists i, i \in \{ENT/B\}, \exists t, t < t3, S(i,t, E(MD, x)))$

Using assumption 4 which states that only MD has knowledge of x before t2 and assumption 5 establishes the freshness and timeliness of x from the base stations B's perspective to give:

$K_{B,t3}(\exists t, t2 < t < t3, S(MD, t, E(MD, x)))$

Using Axioms A11/A12 and A13, which reflect the ability of an entity to decrypt a message when it has knowledge of a shared secret key:

$K_{B,t3}(\exists t, t2 < t < t3, S(MD,t, MD))$ **: Satisfies Goal 3.**

7. CONCLUSIONS

In this paper two hybrid mobile security protocols were discussed, the BCY basic MSR and the Boyd-Mathuria BCY IMSR protocols.

The verification of the basic MSR protocol presented in this paper highlighted a number of weaknesses in the protocol. The analysis of the Boyd-Mathuria BCY IMSR protocol shows that the corrected and improved protocol is free of these weaknesses.

REFERENCES

[1] Beller M.J., Chang L.-F. and Yacobi Y., "Privacy and Authentication on a Portable Communications System", IEEE Journal on Selected Areas in Communications, vol. 11, pp. 821-829, 1993.

[2] Boyd C. and Mathuria A., " Key establishment protocols for secure mobile communications: A selective survey", Information Security and Privacy '98, vol. 1438, pp. 344-355, 1998.

[3] Carlsen U., "Optimal Privacy and Authentication on a Portable Communications System", ACM Operating Systems Review, vol. 28, No. 3, pp. 16-23, 1994.

[4] Newe, T. and Coffey, T., "Formal Verification Logic for Hybrid Security Protocols". International Journal of Computer Systems Science and Engineering, Vol. 18 no 1, pp. 17-25, January 2003. ISSN 0267 6192

[5] Coffey T. and Saidha P. "Logic for verifying public-key cryptographic protocols". IEE Proceedings - Comput. Digit. Tech., Vol. 144, No. 1. pp. 28-32 , January 1997