

Analysis Of SET In CPAL-ES

Presented By : Raja Ramaswamy
Date : 04/22/2002
Advisor : Dr.Alec Yasinsac

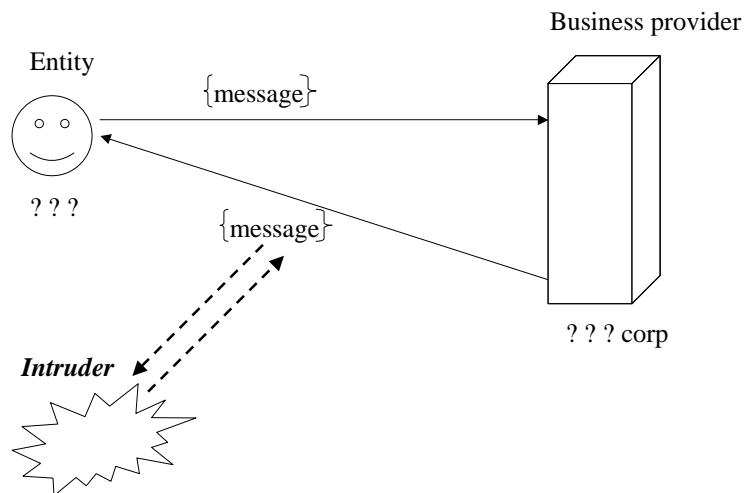
Organization of the presentation . . .

- Project Goal
- Problems in E-Commerce
- CPAL - ES environment
- SET - An Introduction
- Analysis of SET using CPAL - ES
- Conclusion

Project Goal

Analyze the Secure Electronic Transaction (SET) Protocol using the Cryptographic Protocol Analysis Language - Evaluation System (CPAL-ES).

Problems in e-commerce . . . Intruder & Imposter

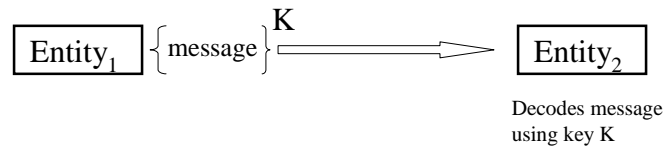


Solving Intrusion

Cryptography

Symmetric Key, Asymmetric Key

→ Symmetric Key Cryptography



Example : Data Encryption Standard (DES)

* 56 bit long key, both party should know the keys

4/22/02

Analysis Of SET Protocol In CPAL-ES

5

CPAL – ES

(Cryptographic Protocol Analysis Language – Evaluation System)

- A formal cryptographic protocol evaluation system.
- It is based on a technique from program verification called Weakest Precondition reasoning
- Allows analyst to give a definitive meaning to the actions of all principals in a protocol run, including intruders.
- Translates syntax to semantics and declarative result that is provable

4/22/02

Analysis Of SET Protocol In CPAL-ES

6

Evaluation of protocols in CPAL-ES is a **three-step process**

1. Encode the protocol actions in CPAL
2. Translate the specification into a Verification Condition
3. Prove the Verification Condition.

4/22/02

Analysis Of SET Protocol In CPAL-ES

7

CPAL (Cryptographic Protocol Analysis Language)

- **expressiveness** to enable protocol designers to specify complex protocols
- allows **analysis** of coded protocols through formal methods
- **superset** of the de facto standard notation (SN)
- simple language
- Some **basic features** include
 - specifying **actions of principals** in a communication session
 - Sending messages
 - encrypting values
 - creating **new** values

4/22/02

Analysis Of SET Protocol In CPAL-ES

8

CPAL

Advanced features of CPAL

- every CPAL action preceded by **identifier of the principal**
- every action in the protocol can be **bound to a specific principal**
- requires **receipt** of messages
- explicit **decryption** of encrypted messages
- **dot notation** is used to identify the address space (ex A.k)
- allowing principals to encode protocol goals and assumptions directly into the specification (**assume & assert**)

4/22/02

Analysis Of SET Protocol In CPAL-ES

9

Examples :

<i>SN Code</i>	<i>CPAL</i>
A -> B {msg}k	A: =>B(e[msg]k); B: <-(msg'); B: msg := d[msg']k;

Assume & Assert Statements

A: assume(A.k == B.k);

A: assert(A.Na == A.Na');

4/22/02

Analysis Of SET Protocol In CPAL-ES

10

SN and CPAL Specification of a Trivial Protocol

SN

A->B: (A)

B->A: {N}^k

A->B: {N+1}^k

CPAL

global: assume (A.k==B.k);

A: -> B(A);

B: <- (A);

B: -> A(e[n]k);

A: <- (msg);

A: n := d[msg]k;

A: -> B(e[f(n)]k);

B: <- (msg);

B: n' := d[msg]k;

B: assert (n' == f(n));

4/22/02

Analysis Of SET Protocol In CPAL-ES

11

SET Fundamentals

Digital Certificates

- Account Information
- Information about the certificate
- Cryptographic Information (Public key of the customer)
- Its an electronic representation of the card

Trust Chaining

- Root Certifying Authority (RCA)
- Certifying Authority (CA)
- Customer

Digital certificates bind the entity with their public key

4/22/02

Analysis Of SET Protocol In CPAL-ES

12



What is SET (Secure Electronic Transactions)?

- A modern protocol designed to facilitate secure payment transactions in open networks(ex. Internet)
- This open protocol is jointly developed by MasterCard and Visa with support from IBM, Microsoft, GTE, VeriSign, etc.
- To be used mainly in the E-Commerce arena

4/22/02

Analysis Of SET Protocol In CPAL-ES

13



How SET works ?

SET uses encryption technology and digital certificates as the basis for security and authentication.

Several **components** to make SET work are

- **Certificates**
- **Cardholder Wallet and Encryption**
- **Merchant website and server software**
- **Payment Gateway**

4/22/02

Analysis Of SET Protocol In CPAL-ES

14



Cardholder Wallet and Cryptography

- A software that resides in the customers browser
- Contains payment card information such as
 - Card number
 - Digital certificate to identify the user
 - Shipping information
- Performs the necessary encryption of data
- Most recent browser versions from Microsoft and Netscape support wallet technology

4/22/02

Analysis Of SET Protocol In CPAL-ES

15



Merchant website and server software

- A virtual storefront
- A web server
- Software modules such as secure payment, order management, online customer service etc.
- Encryption and decryption

4/22/02

Analysis Of SET Protocol In CPAL-ES

16

Payment Gateway

- Interface between the merchant and the acquirers payment processing system
- validates both merchant and cardholder certificates
- translate the SET message into a format that can be processed by the Acquirers system

4/22/02

Analysis Of SET Protocol In CPAL-ES

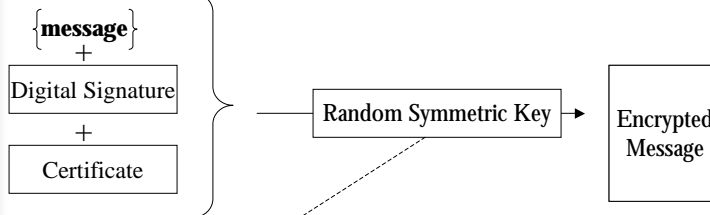
17

Customer Side activities

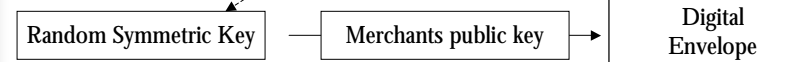
Step I



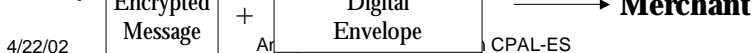
Step II



Step III



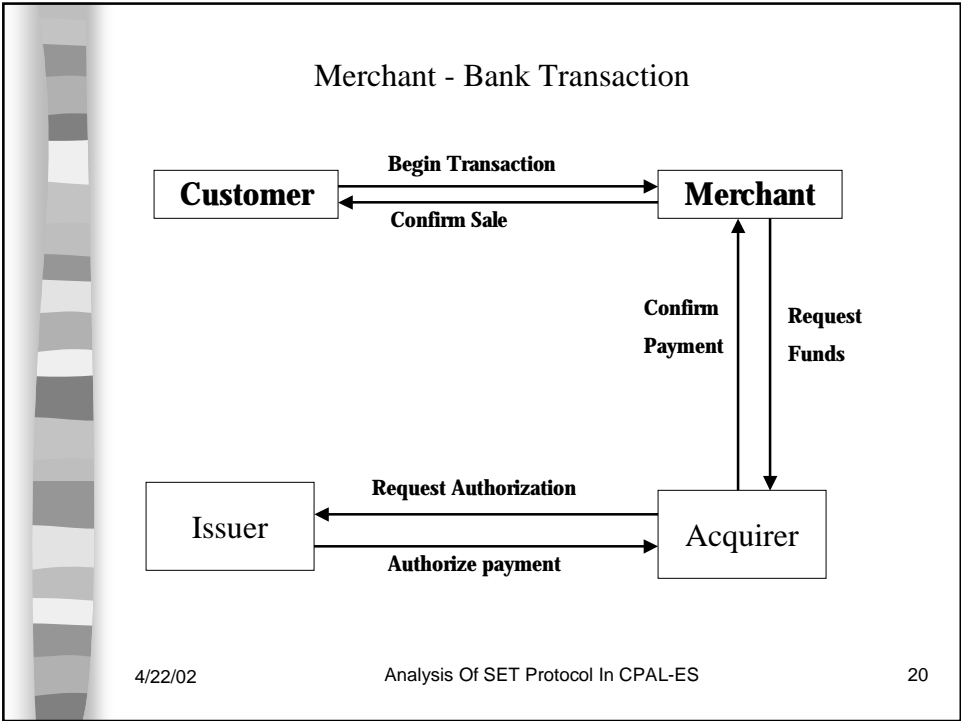
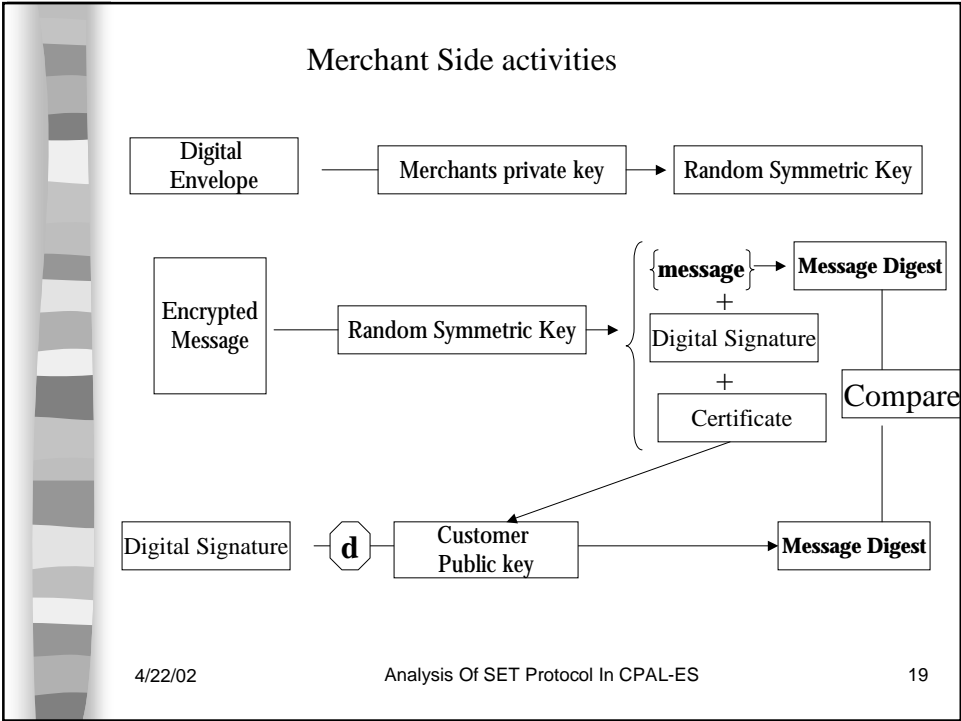
Finally



4/22/02

CPAL-ES

18



CPAL Specification for SET

- Sequential flow of messages
- Identify the flow of messages between different entities
- Categorize them
- Convert them to CPAL
- Analyze CPAL specification in CPAL-ES

4/22/02

Analysis Of SET Protocol In CPAL-ES

21

Categories of SET messages

- 1. Certificate Management messages*
- 2. Cardholder-Merchant messages*
- 3. Merchant-Payment Gateway messages*

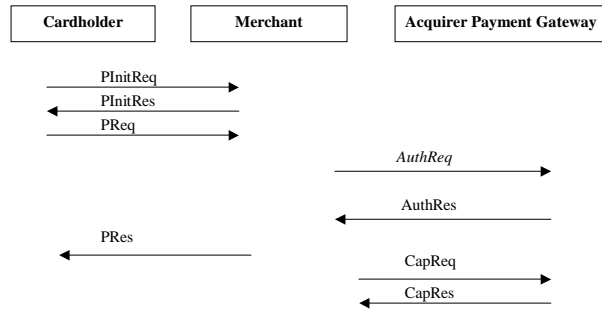
4/22/02

Analysis Of SET Protocol In CPAL-ES

22

Cardholder-Merchant messages

- * Purchase Initialization Request (*PInitReq*)
- * Purchase Initialization Response (*PInitRes*)
- * Purchase Request (*PReq*) & Payment Response (*Pres*)



4/22/02

Analysis Of SET Protocol In CPAL-ES

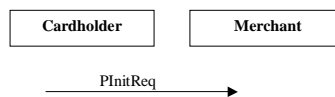
23

Purchase Initialization Request (*PInitReq*) – Generation Process

PInitReq {RRPID, Language, LID_C, LID_M, Chall_C, BrandID, BIN}

MWPInitReq {Version, Revision, Date, *PInitReq*, SWIdent}

1. Generate RRPID for matching the message and the matching response message.
2. Populate language of the cardholder's choice.
3. Generate LID_C, Local Identification for Cardholder
4. If Merchant has already supplied a LID_M in the SET initiation process then copy it into the message.
5. Generate a fresh Chall_C
6. Populate BIN (first 6 digits of the cardholder's account number)
7. Save RRPID, LID_C, LID_M (if available) and Chall_C
8. Invoke Compose Message Wrapper to send the message to Merchant.



4/22/02

Analysis Of SET Protocol In CPAL-ES

24

CPAL specification of the PInitReq message

1. -- Action : *Initiate Transaction*
2. -- Message : *Purchase Initialization Request (PInitReq)*
3. -- Initiated by : *Customer*
4. C: *RRPID* = *new*;
5. C: *Chall_C* = *new*;
6. C: *PInitReq* = <*RRPID, Language, LID_C, LID_M, Chall_C, BrandID, BIN*>
7. C: *TransRec* = <*RRPID, LID_C, LID_M, Chall_C*>;
8. C: *MWPInitReq* = <*Version, Revision, Date, PInitReq, XID*>;
9. C: => M (*MWPInitReq*);
10. M: <- (*MWPInitReq*);
11. M: (*Version, Revision, PInitReq, XID*) = *MWPInitReq*;
12. M: (*RRPID, Language, LID_C, LID_M, Chall_C, BrandID, BIN*): =
PinitReq;

4/22/02

Analysis Of SET Protocol In CPAL-ES

25

Assertions

Encode protocol goals and assumptions directly into the specification

- C*: *assume* (*C.RRPID_MWREQ* == *C.RRPID_REQ*);
- C*: *RRPID* := *new*;
- C*: *LID_E* := *new*;
- C*: *Chall_EE* := *new*;
- C*: *CardCInitReq* := <*RRPID, LID_EE, Chall_EE, BrandID*>;
- C*: *MWCardCInitReq* := <*Version, Revision, Date, RRPID, SWIdent, CardCInitReq, XID*>;
- C*: => *CCA*(*MWCardCInitReq*);
- CCA*: <- (*MWCardCInitReq*);
- CCA*: (*Version, Revision, Date, RRPID_MW, SWIdent, CardCInitReq, XID*) :=
MWCardCInitReq;
- CCA*: (*RRPID_C, LID_EE, Chall_EE, BrandID*) := *CardCInitReq*;
- CCA*: *TransRec* := <*RRPID, LID_EE, Chall_EE, BrandID*>;
- CCA*: *assert* (*RRPID_MW* == *RRPID_C*);

4/22/02

Analysis Of SET Protocol In CPAL-ES

26

Encoded CPAL file

- **cpal-set.cpa** → contains the CPAL specification of the SET protocol

Generated Files

- **protocol.out** → contains the encoded protocol, Initial WP predicate, Basic simplification and the simplified predicate
- **assume.out** → contains assume statements
- **tst.out** → information to debug

4/22/02

Analysis Of SET Protocol In CPAL-ES

27

Initial Predicate list

***** Initial WP predicate follows.

```
(((not ((unique.v17 ==
<<C.Version,C.Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,unique.v15,C.BrandID>,C.XID>.1,<
C.Version,C.Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,unique.v15,C.BrandID>,C.XID>.2,<C.
RPID_RES,<C.Version,C.Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,unique.v15,C.BrandID>,C.XID>.3,CCA.R
RPID_RES,<C.Version,C.Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,unique.v15,C.BrandID>,C.
XID>.5,f.S(CCA.CA,<CCA.RRPID,<C.Version,C.Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,uni
ue.v15,C.BrandID>,C.XID>.6.2,<C.Version,C.Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,uni
ue.v15,C.BrandID>,C.XID>.6.3,unique.v14,unique.v13,CCA.RequestType,CCA.RegFormORReferral}),<C.Version,C.
Revision,C.Date,unique.v17,C.SWIdent,<unique.v17,C.LID_EE,unique.v15,C.BrandID>,C.XID>.7>.4))
```

or

```
(not ((unique.v12 ==
f.S(CCA.CA,<CCA.RRPID,<unique.v12,unique.v11,unique.v10,M.RequestType,<<M.MerchantBIN,M.MerchantID>,<M.A
cqBIN,M.AcqBusinessID>,<M.BrandID,M.Language>.2,<unique.v12,unique.v11,unique.v10,M.RequestType,<<M.Merc
hantBIN,M.MerchantID>,<M.AcqBIN,M.AcqBusinessID>,<M.BrandID,M.Language>.3,unique.v9,CCA.RegType,<<CCA.R
egFormID,CCA.BrandLogoURL,CCA.CardLogoURL,CCA.RegFieldSeq,CCA.PolicyText>,<CCA.Reason,CCA.ReferralURLe
q>>>.1))
```

Final Simplified Predicate

***** Simplified predicate follows.


TRUE

***** NO MORE PREDICATE

4/22/02

Analysis Of SET Protocol In CPAL-ES

28



Demonstration

- Modules in CPAL file
- Assume and Assert statements
- Final simplified predicate

4/22/02

Analysis Of SET Protocol In CPAL-ES

29



Conclusion

- Learn SET protocol and CPAL
- Convert the SET protocol into a CPAL specification
- Analyze the CPAL specification against the CPAL-ES environment

Thank You & Questions??

4/22/02

Analysis Of SET Protocol In CPAL-ES

30