Security RE in Online Payment

By Ying(Irene) Yu

July 11th, 2017
Outline

● Security in RE
● Online payment methods
● Security issues
● Methodology for modelling
● Examples and scenarios
● Lessons learned
● Reference
Security in RE

Security requirements:

- Constraints on system’s functional requirements
- Express system’s security goals
- Precise, prescriptive and iterative
Security Goals

General Assets:

- Confidentiality
- Integrity
- Availability

List threats of these assets

Combine management control principles and organization security policies

Consider goals of attackers
Online Payment Methods

E-commerce payment system: Accelerates the popularity of electronic payment for online transactions.

- Credit cards
- Debit cards
- Wallets like PayPal, Apple Pay, Alipay, Google Wallet
Credit card & Debit card

Card issuer (usually a bank, VISA, Mastercard): creates a revolving account, grants credit

Card holder: borrow money for payment, use as a cash advance.

Security Mechanism:

- Personal identification number (PIN)
- Electronic verification systems: Terminal, POS, using magnetic stripe or chip
- Card not present transactions: security code
- Electronic authorization of every transaction (for debit)

Smart cards
Other Online payment

Wallets: paypal, alipay, etc

Wallets like PayPal act as acquirer, a performing payment processing for online vendors and other commercial users.

Security mechanism:

- Login and password
- Mobile phone security(SMS)
- Real name certification
- Digital certificate
- Consumer behavior detection
Security Issues

- Fraudulent purchases & chargebacks
  - Merchants
  - Customers
  - Hackers
- Cross-border transactions
- Card data security: personal info leaks
Methodology for modeling

Tropos/i* Methodology:

- Agent-oriented software system development
- methodology
- Adopts the i* modelling framework
  - actor, goal, soft goal, task, resource, etc.
  - social dependency of dependees AND dependers
Characteristics:

- Well suited to model business security requirements
- Deeper understanding of the environment and interactions
- Refinement analysis and rationale diagrams that explains dependencies.
Scenario

E.g. The Cardholder depends on the Merchant for obtaining some goods and the Merchant depends on the Cardholder for obtaining the payment.

Fig1. Merchant-Cardholder Basic Dependencies
Actor diagram for certification

Fig2. Certification actor diagram
Rationale diagram

From Fig 2. in the example, it can be decomposed into three subgoals:

1. Request of personal data from the cardholder
2. Checking the authorization at the issuer
3. Generating and sending back the certificate.
Modelling using Tropos

Fig 4. Payment actor diagram
Refinement of the actor diagram

1. Add actors in online transaction setting

Fig5. Payment2 actor diagram
Refinement of the actor diagram

2. Clarifies the relations between various actors in the financial setting of the transaction.

[Diagram showing the relationships between various actors in the financial setting of a transaction, including Cardholder, Merchant, Merchant Bank, Local Bank, Issuer, and Acquirer, with labeled arrows indicating interactions such as goods, charge payment, credit card services, manage customer relations, authorize billing credit card transaction, financial credit data, financial debit data, authorize crediting credit card transaction, and manage customer relations.]

Fig6. Payment3 actor diagram
Security-Enhanced Tropos

3. Security enhanced makes it possible to analyze the trust relationship

   e.g. If the owner does not trust the storage server, we can change the model and encrypt the data

Fig7. Payment Dependency with Ownership of Data
Online transaction

Fig8. Old Online transaction
Online transaction using secure protocols

Using Secured hypertext transaction protocol (S-HTTP)

Fig8. Old Online transaction
Online transaction using secure e-transactions

![Diagram of online transaction process](image)

Fig9. Secure Online transaction
Security integrated with SMS

Fig9. Secure Online transaction
Lesson Learned

Clear separation of roles and dependency relations

- Who owns the data
- Who request service
- Who offer service

Capture high level requirements, instead of digging into cryptographic algorithms in the beginning

- Encryption
- Authentication
- Access control
Lessons Learned Cont’d

During the modelling processes for security in RE:

1. We can get the idea that we need some secure methods (like encryption, etc) at a certain step, without thinking in advance.

2. A good security requirement will be easily modified and to add new features without impacting the system a lot.

3. Challenges are that how to integrate these processes with other phases, and how to reduce the cost for modification of system requirements.
Thanks!

Questions?
References


