Team Orange - 46

Storage Server for Adobe

Jerry Wang - 1000009457

Jung Yeon Kwon - 1000924556

Soon Chee Loong – 999295793

Our Client: Adobe

- Nov. 7th, 2013 database hacked.
- 150 million users affected
- Stolen data: Credit card #, personal information, etc.

Agenda: Security VS Efficiency

- Use Case: Credit Card Transaction (Jung Yeon)
- Data Security: Solitaire (Soon)
- Transaction Security: Solitaire (Jerry)
- Performance Evaluation (Jung Yeon)

Use Case Scenario

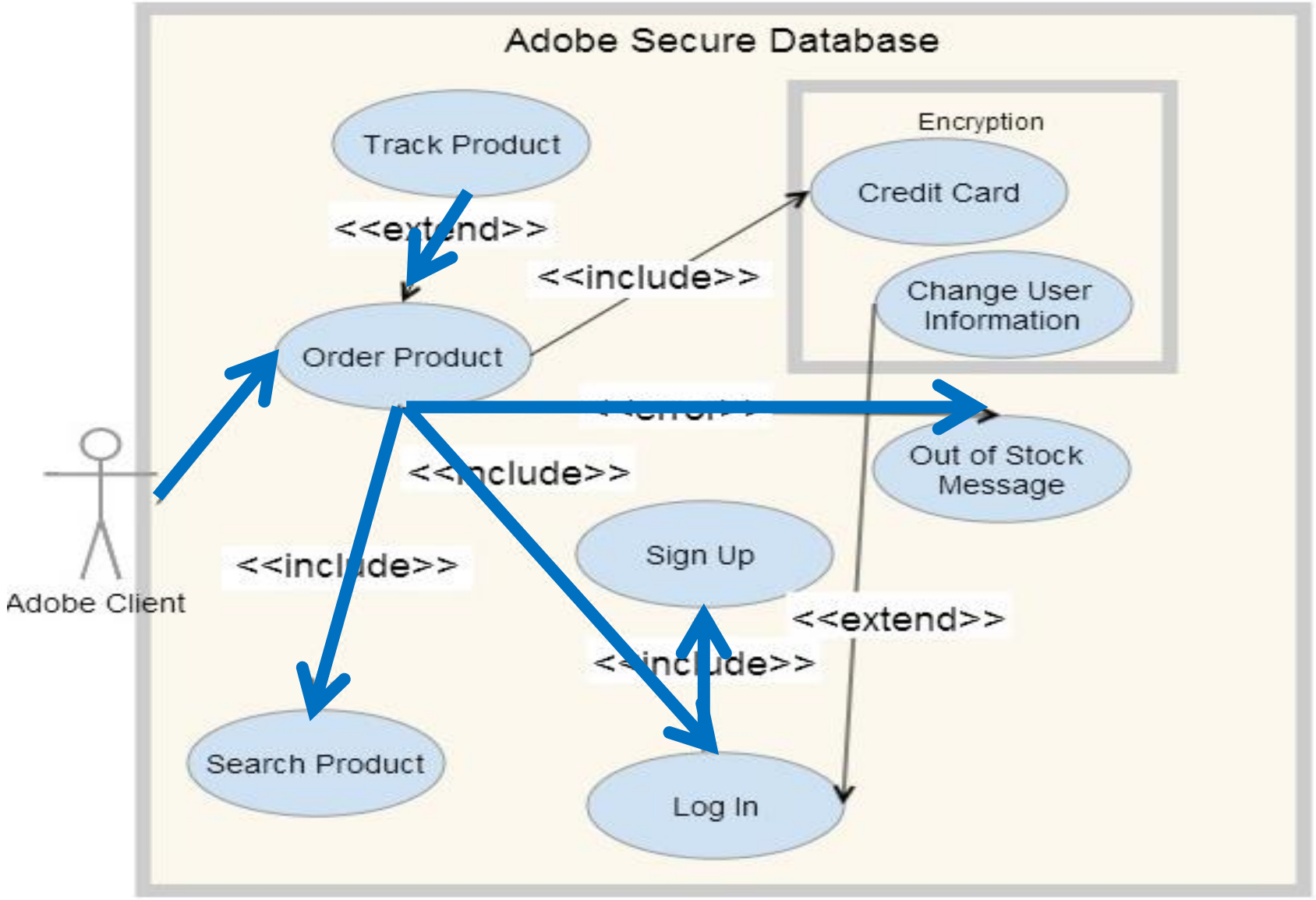

Figure 1: UML Use Case Scenario (Order Product)

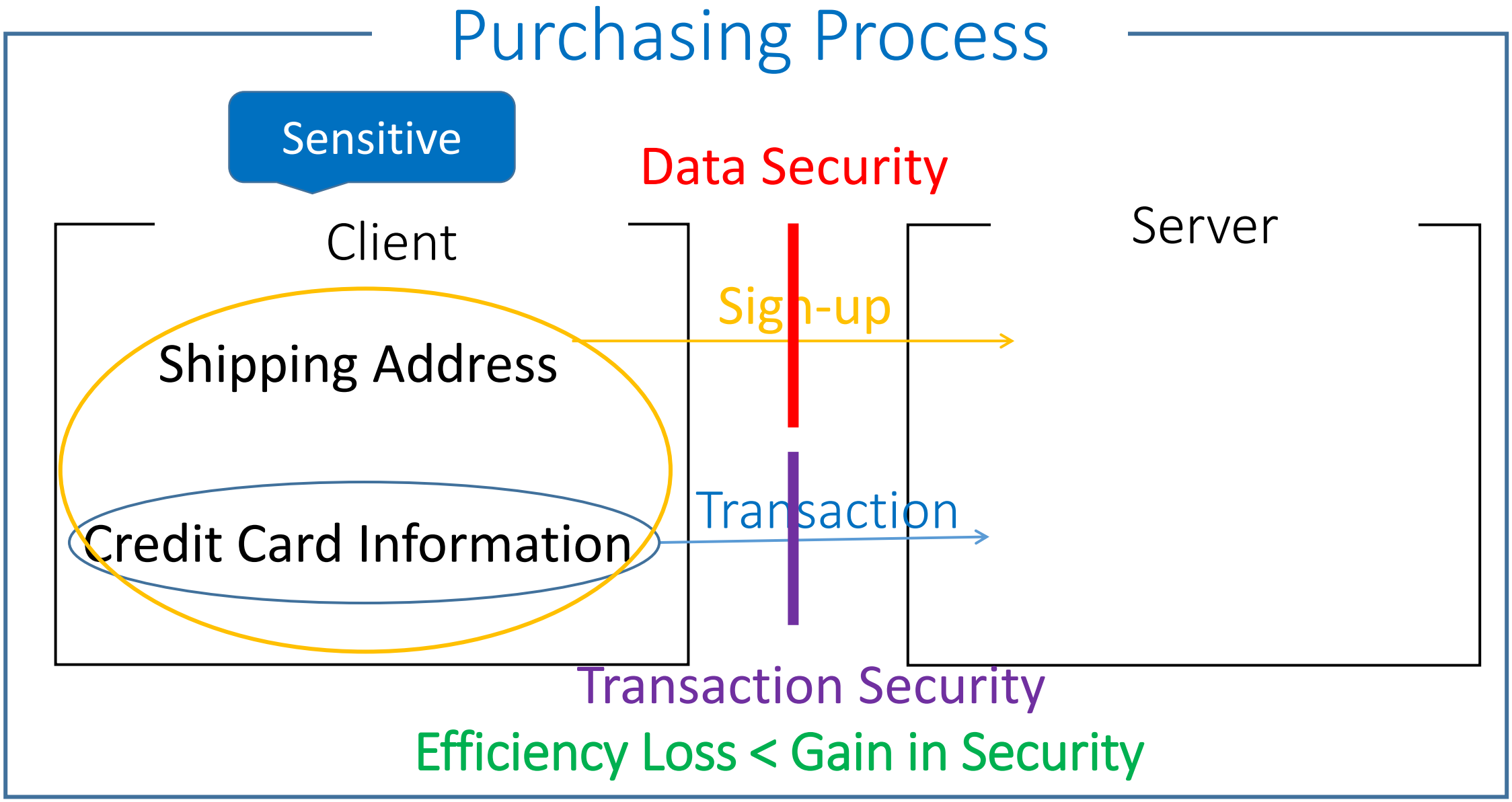

Figure 2: Purchasing Process (Addition of Security Layer)

Data Security

Solitaire Encryption [1]

- 1. Created by Bruce Schneier (Famous Cryptographer)
- 2. Symmetric Key Encryption
- 3. Deck can be configured to be any private key

Based on product

[1] B. Schneier. (1999, May 26). *The Solitaire Encryption Method.* [Online].

Available: https://www.schneier.com/solitaire.html

Data Security: Solitaire

1234 5678

[2]

AEF^ 5*3_

Database

[2]

1234 5678

Credit Card Number

[2] http://boardgaming.com/games/card-games/locke-and-key-the-game

Data Security

Data Security: Solitaire

1234 5678

[2]

1234 5678

[2]

Credit Card Number

AEF^ 5*3_

DFG- 7!8+

Database

[2]

1234 5678

[2]

1234 5678

[2] http://boardgaming.com/games/card-games/locke-and-key-the-game

Data Security

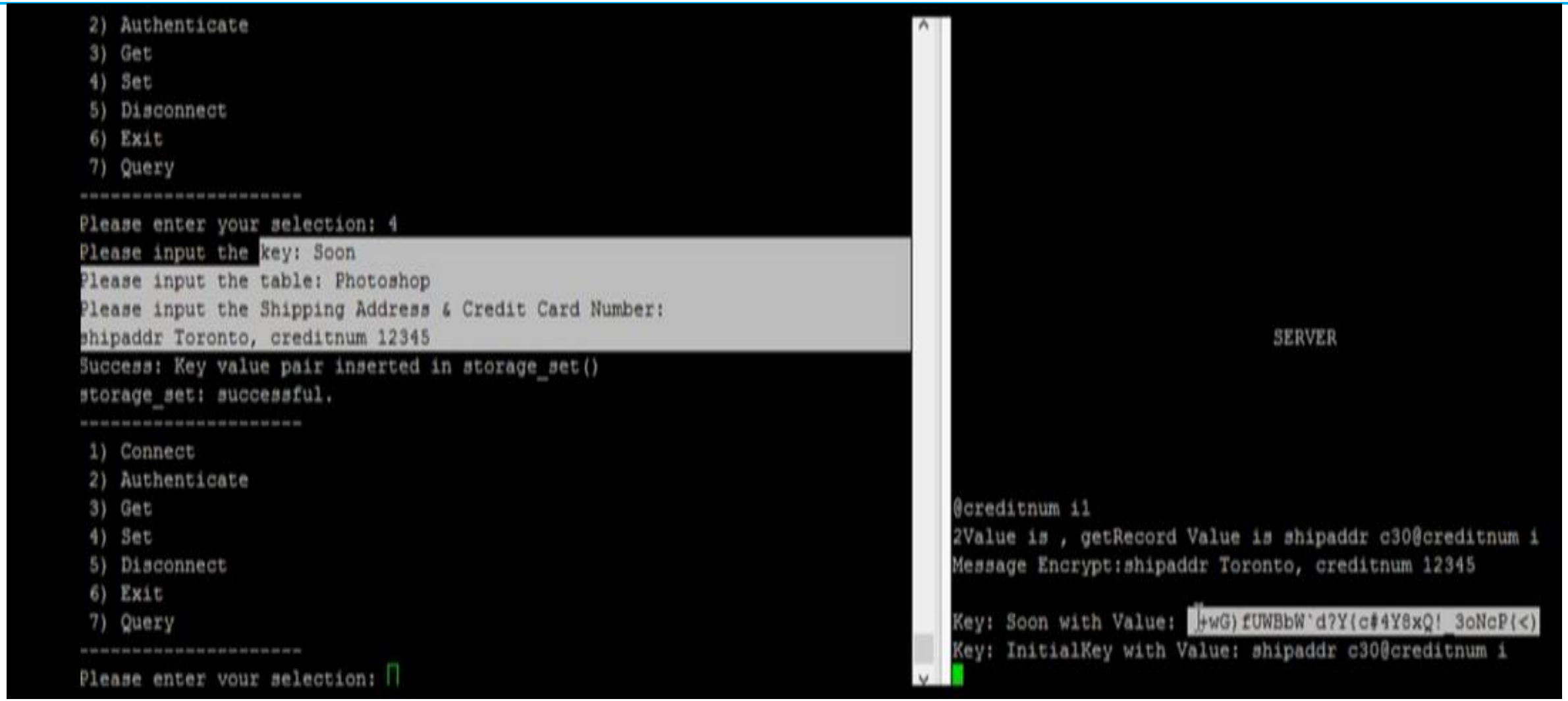

Figure 3a: Demonstration of Server Encrypting Information into Database

Code Available: https://code.google.com/p/ece297orange/

Data Security

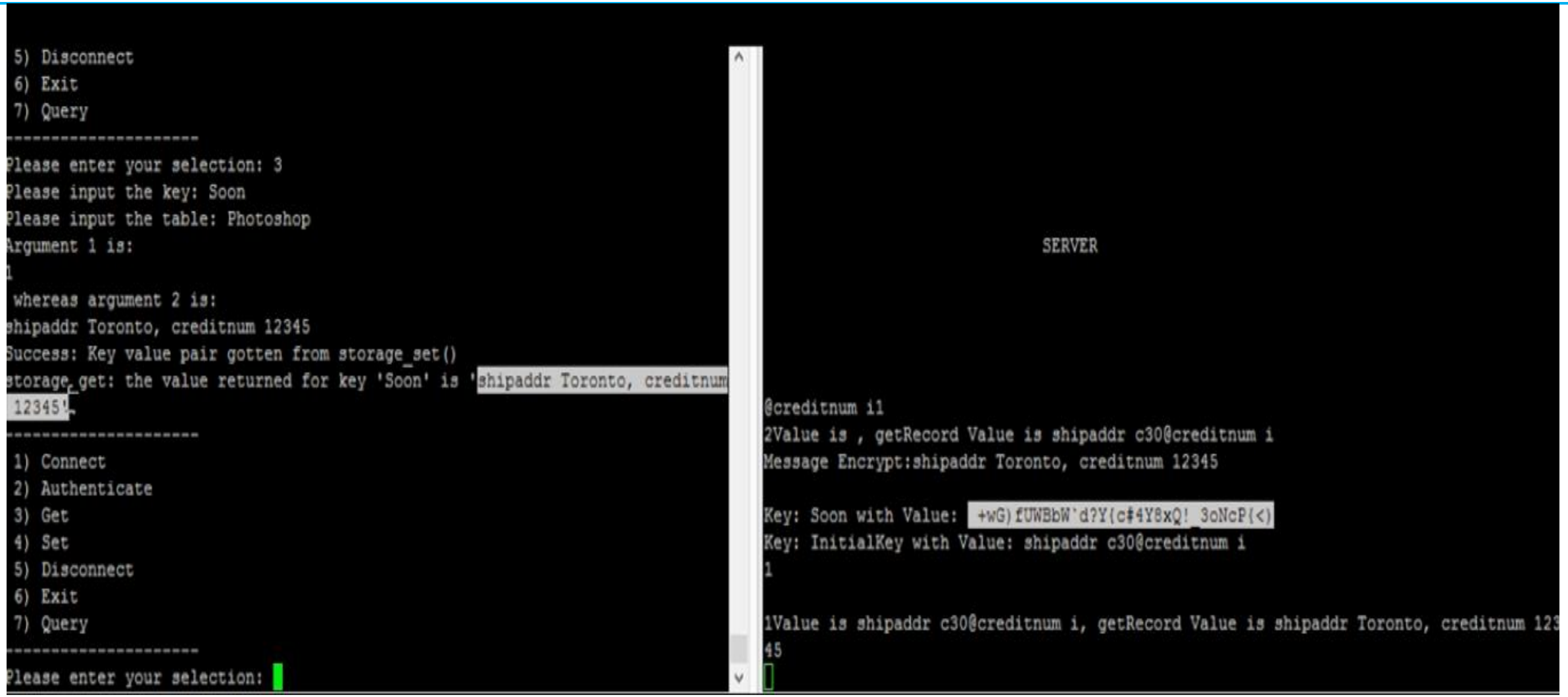

Figure 3b: Demonstration of Server Encrypting Information into Database

Code Available: https://code.google.com/p/ece297orange/

Data Security

Solitaire Encryption Trade-offs: Security VS Efficiency

Time to Decrypt
(microseconds)

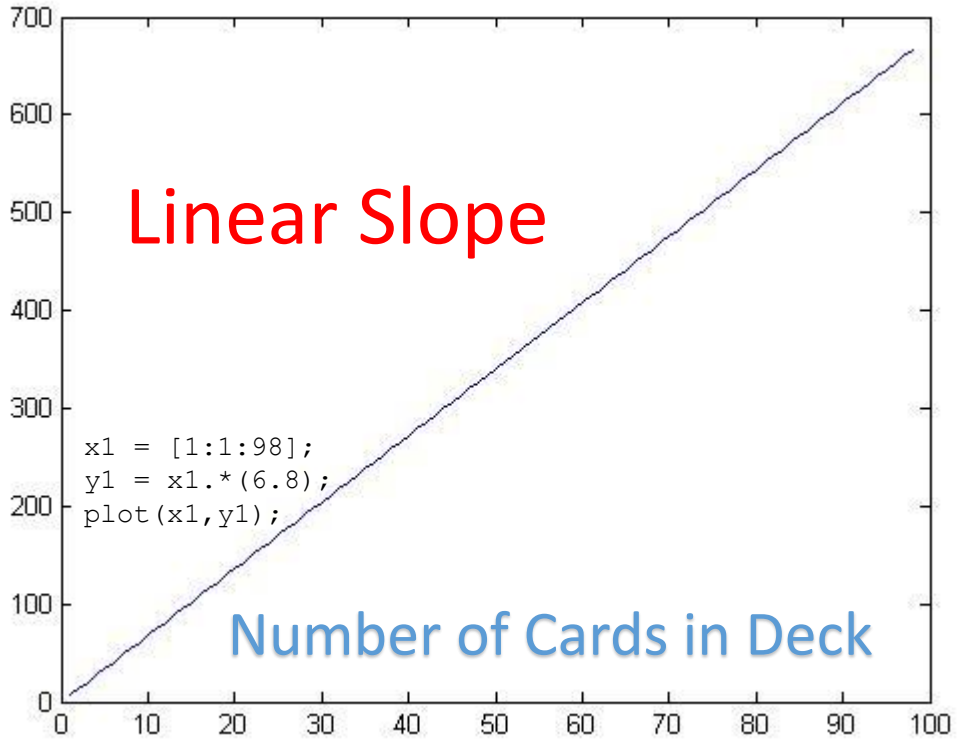

Figure 4: Time to Decrypt N number of cards

Time to Decrypt All Permutations
(microseconds)

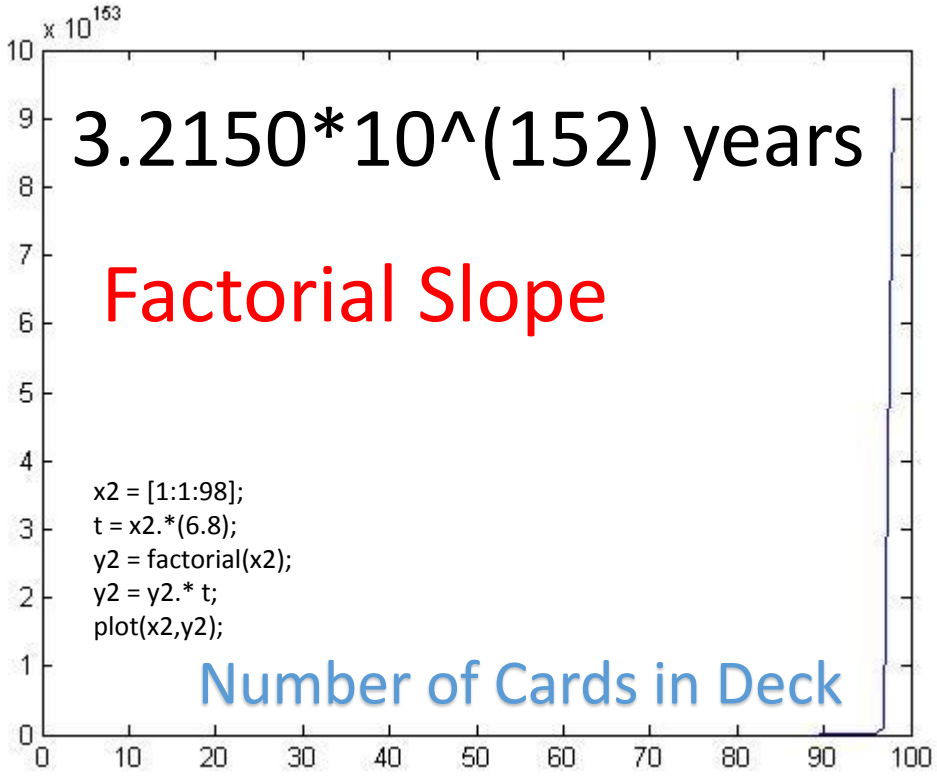

Figure 5: Time to Decrypt All Permutations

Transaction Security

Multiple clients require **concurrency:**

Possible methods:

- Select
- Fork
- Threads

Choose: **Threads**

Transaction Security

Malicious Editing:

- **Possible exploit:** Client can edit token
  - Trick server → perform invalid transactions

- **Fix:** Encrypt the version number

Transaction Security

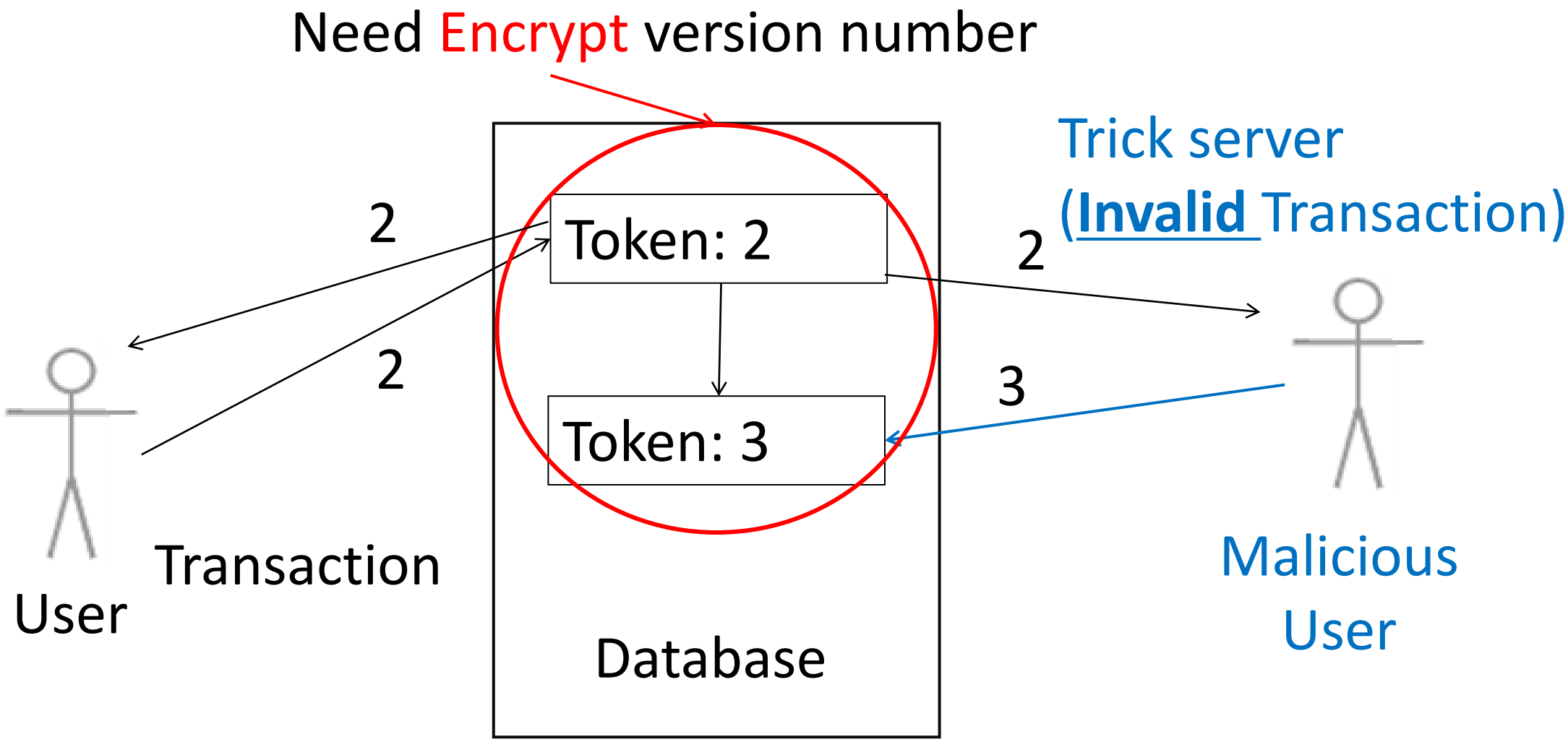

Figure 6: Invalid Transaction By Malicious User

Transaction Security

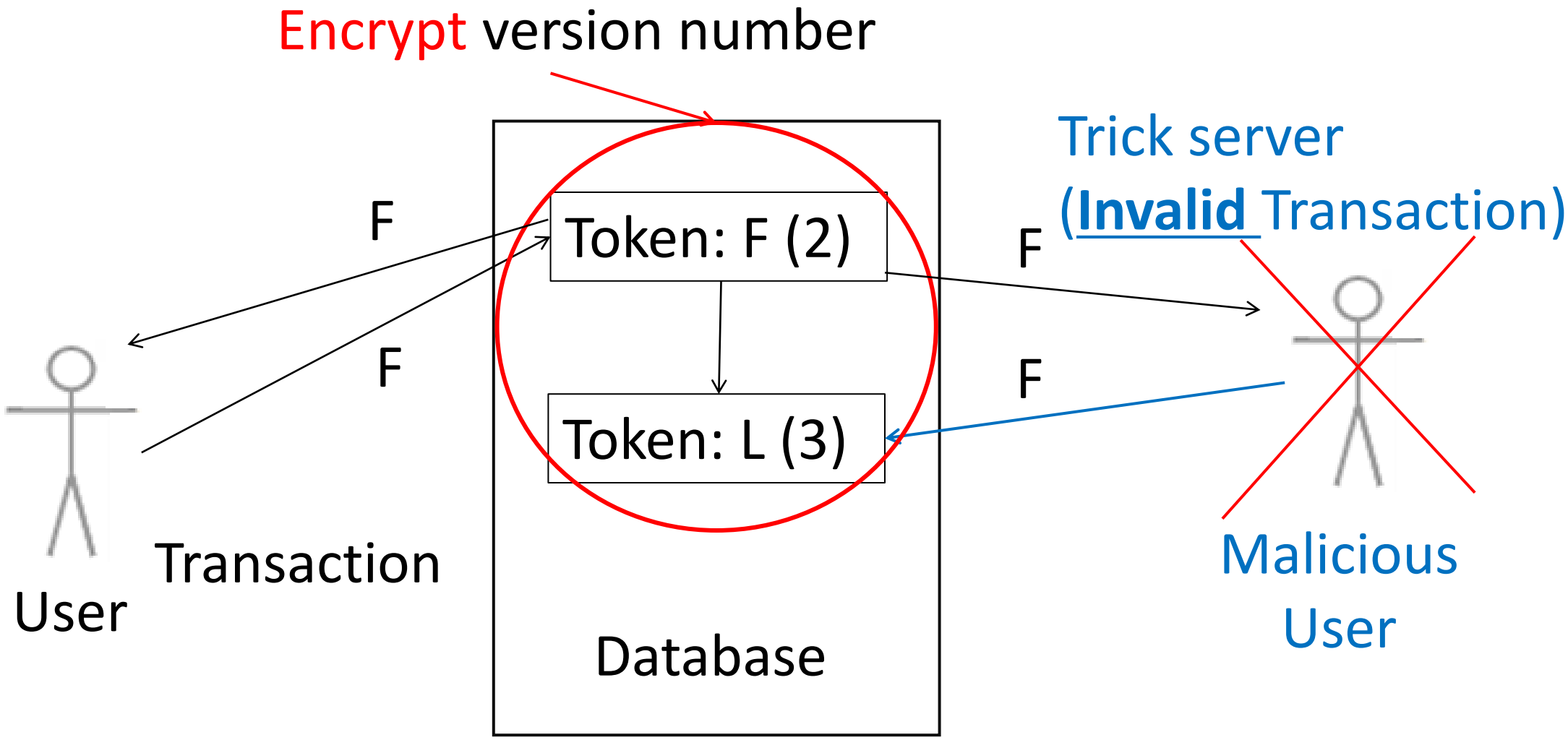

Figure 7: Transaction Security Added Server

Trade-offs: Security VS Efficiency

- Encrypting takes extra processing time
- Performance evaluation → negligible
- **Weakness:** Guess/Brute force methods

Performance Report

Effect of Two Security Features

Measuring methods

- Average end-to-end (set) [with one client
  with multiple clients
- Transaction abort rate with multiple clients

Performance Report

Measuring Data Security Feature's Effect

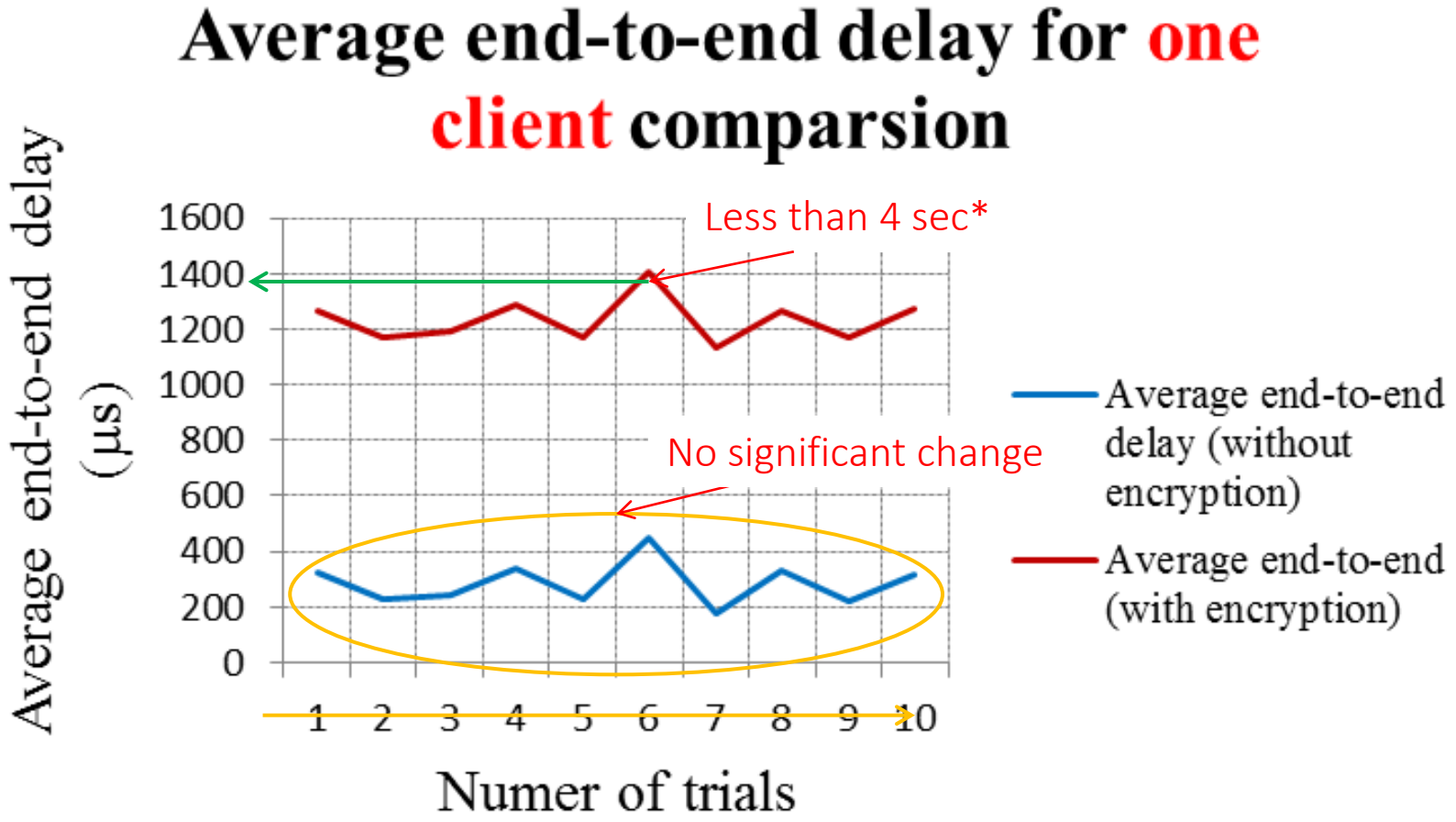

Figure 8: Set Average End-to-End Delay for One Client (With and Without Solitaire)

*based on experiential data done by Soon Chee, Jan. 25th, time to reset shipping address

Performance Report

Real-life Case

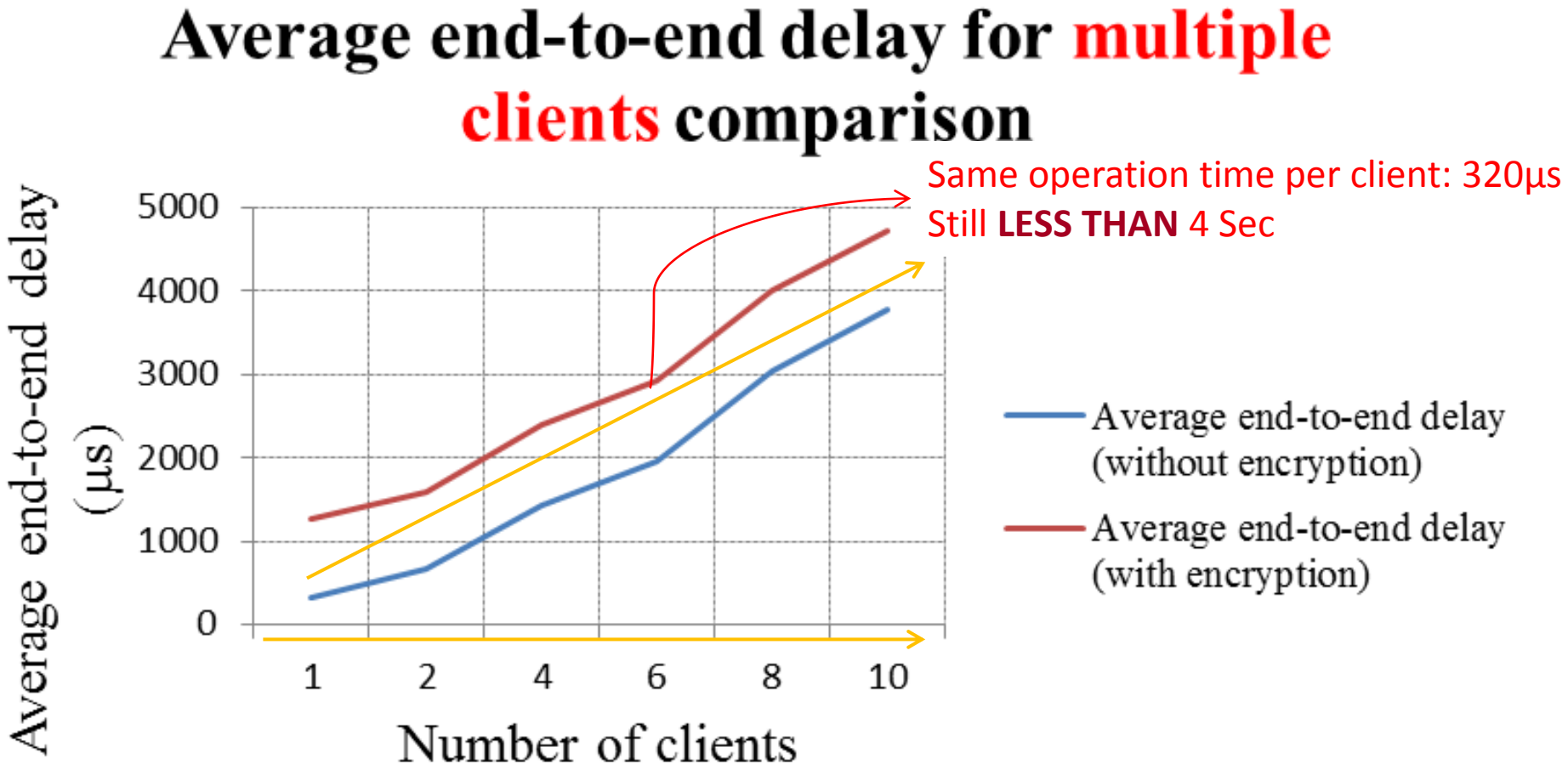

Figure 9: Set Average End-to-End Delay for Multiple Clients (With and Without Solitaire)

Measuring Transaction Security's Effect

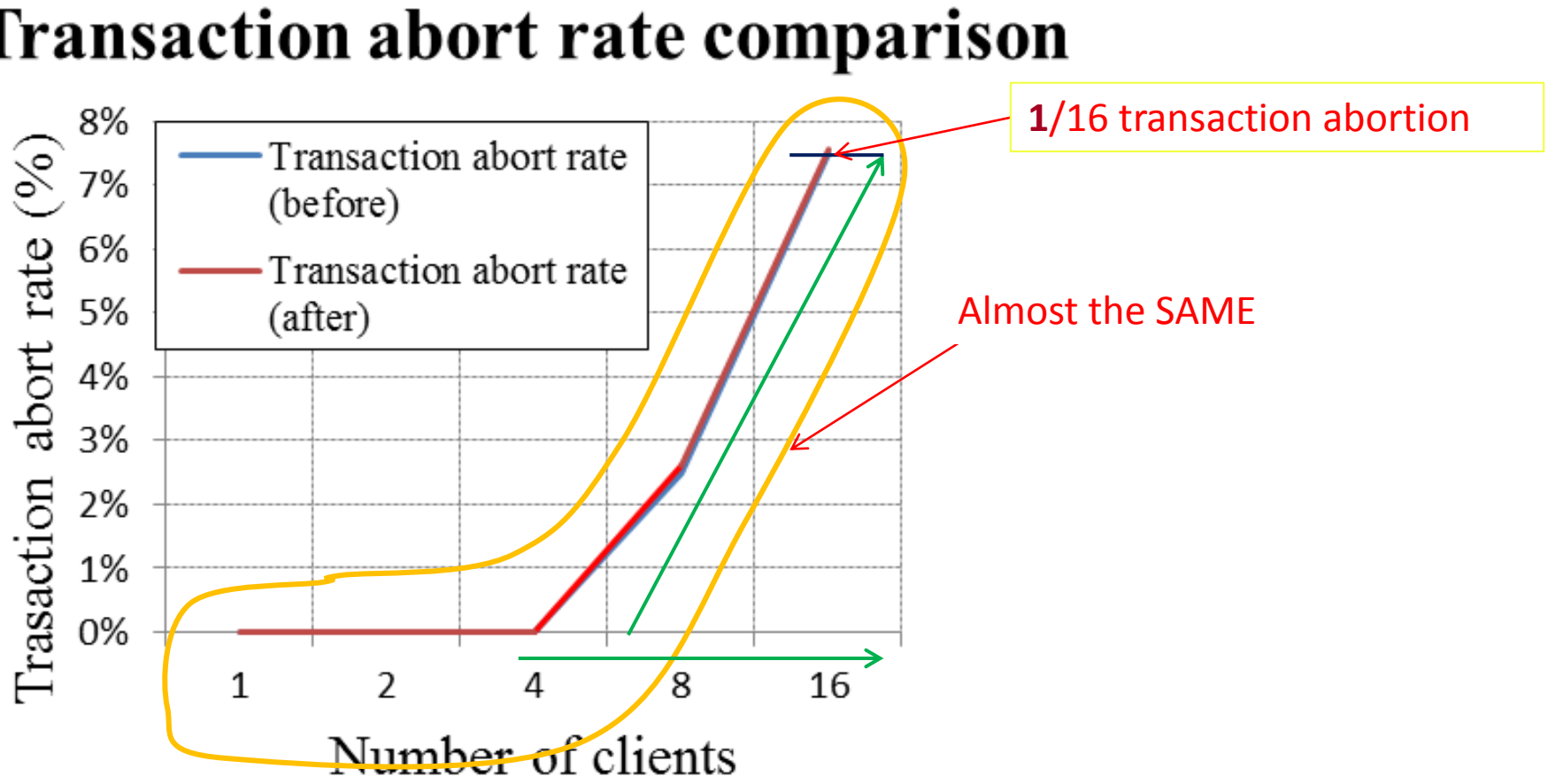

Figure 10: Transaction Abort Rate (With and Without Transaction Security Feature)

Performance Report

Security vs Efficiency

Although solitaire and transaction security method are included,

⟶ efficient processing time and minor transaction abortion

Conclusion : Security Vs Efficiency

- Credit Card Transactions
- Linear Time for Factorial Security
- Transaction Security
- < 4 seconds

http://www.bbc.com/news/technology-26954540

Take Away: How Important Is Security?

- BBC News: Flaw in OPENSSL [3]
- Change Your Passwords Everywhere!
- *"Catastrophic is the right word. On the scale of one to 10, this is an 11" (Bruce Schneier)*

[3] L. Kelion. (2014, Apr 9). *Heardbleed Bug: Tech firms urge password reset.* [Online]. Available: http://www.bbc.com/news/technology-26954540