Formal Security Analysis and Improvement of a hash-based NFC M-coupon Protocol

Ali Alshehri and Steve Schneider
Agenda

• Introduction. ✓

• Approach
  – CasperFDR (example)
  – More about the underline theory (CSP)

• Apply to the Hash-based NFC M-coupon protocols by Hsiang et al.
  – Capturing the requirements:
    • In CasperFDR
    • From the CSP aspect
  – Analysis (Attack & solutions)
Introduction

- **NFC** (Near Field Communication).
- **NFC mobile coupon protocols.**
  - The Hash-based M-coupon protocol.
- **Formal security analysis.**
  - CasperFDR
Agenda

• Introduction. ✓
• Approach ✓
  – CasperFDR (example)
  – More about the underline theory (CSP)
• Apply to a Hash-based NFC M-coupon protocols by Hsiang et al.
  – Capturing the requirements:
    • In CasperFDR
    • From the CSP aspect
  – Analysis (Attack & solutions)
CasperFDR

- **CSP (Communicating Sequential Processes):**
  is a formal language for describing patterns of interaction in concurrent systems.
- **FDR (Failures Divergences Refinement):** CSP refinement checker.

Ali Alshehri 2013
Example

I need a secure communication with Bob

This is Bob for sure! (authentication).

$K_{AB}$ is secret with Bob

Hello Alice!

I believe $K_{AB}$ is secret with Alice

Ali Alshehri 2013
# Free variables

A,B: Agent  
na : Nonce  
PK : Agent -> PublicKey  
SK : Agent -> SecretKey  
InverseKeys = (kab,kab), (PK, SK)  
kab : SessionKey

# Processes

INITIATOR(A,B,na, kab) knows PK  
RESPONDER(B,A) knows PK, SK[B]

# Protocol description

1. A → B : {A,na,kab}{PK(B)}  
2. B → A : {na}{kab}

# Specification

Secret[B, kab, [A]]  
Agreement[B,A,[na,kab]]

# Actual variables

Alice, Bob, Mallory : Agent  
Na, Nb, Nc : Nonce  
kab,Km : SessionKey  
InverseKeys = (kab,kab), (Km,Km)

# Functions

symbolic PK, SK

# System

INITIATOR(Alice,Bob,Na,Kab)  
RESPONDER(Bob,Alice)

# Intruder Information

Intruder = Mallory  
IntruderKnowledge = {Alice, Bob, Mallory, Na, Km, PK, SK[Mallory]}

Ali Alshehri 2013
Top level trace:
Bob believes Km is a secret shared with Alice
The intruder knows Km

System level:
Casper> 1. I_Alice -> Bob : {Alice, Nm, Km}{PK(Bob)}
2. Bob -> I_Alice : {Nm}{Km}
The intruder knows Km
Intruder

Bob

Alice

{Alice, N_m, K_{MB}}_{PK_B}

{N_m}K_{MB}

Alice

Hi Bob
I am Alice!

ZZZZ

Alice DOES NOT agree
K_{MB} is secret with Bob

Hi Alice

Bob agree
K_{MB} is secret with Alice

Alice

Bob

Ali Alshehri 2013
CasperFDR (black-box User)

High level protocol modeling

High level Interpretation of analysis

Ali Alshehri 2013
The CSP theory aspect

New events – Independent processes

Ali Alshehri 2013
The CSP theory aspect

Dolev-Yao model threat

Ali Alshehri 2013
The CSP theory aspect

Alice \hspace{1cm} Intruder \hspace{1cm} Bob

M1: \{A, N_m, K_{MB}\} \!^{PK_B}$\hspace{2cm}$Claim\_Secret.$

$Knows.K_{MB} \hspace{2cm} \rightarrow Bob.Alice.K_{MB}$

Ali Alshehri 2013
Agenda

• Introduction. ✓
• Approach ✓
  – CasperFDR (example)
  – More about the underline theory (CSP)
• Apply to a Hash-based NFC M-coupon protocols by Hsiang et al. ✓
  – Capturing the requirements:
    • In CasperFDR
    • From the CSP aspect
  – Analysis (Attack & solutions)
Hash-based M-coupon protocol

Security Requirements:
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

Ali Alshehri 2013
Hash-based M-coupon protocol

Security Requirements:
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:
StrongSecret (C, X, Offer, [I])

Ali Alshehri 2013
Hash-based M-coupon protocol

Security Requirements:
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:
NonInjectiveAgreement (I,C,[X,Offer])

Ali Alshehri 2013
Hash-based M-coupon protocol

Security Requirements:
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:
NonInjectiveAgreement (I,C,[X,Offer, ID(u)])
Hash-based M-coupon protocol

Security Requirements:
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:
NonInjectiveAgreement (I,C,[X,Offer,ID(u),ID(i)]))
Hash-based M-coupon protocol

Security Requirements:
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:
Agreement (I,C,[X,Offer])
## Analysis

### Hash-based Confidentiality

<table>
<thead>
<tr>
<th></th>
<th>Hash-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>✓</td>
</tr>
<tr>
<td>Forgery Protection</td>
<td>✓</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>✗</td>
</tr>
<tr>
<td>No Multiple Cash in</td>
<td>✗</td>
</tr>
<tr>
<td>Not Transferable</td>
<td>✗</td>
</tr>
</tbody>
</table>

### Equation

- \( M = \{ ID(u), V, C \} \)
- \( V = ID(u) \oplus h[ID(i)] \)
- \( C = h[h[ID(i)] \oplus X \oplus \text{Offer}] \)
- \( h[ID(i)] = ID(u) \oplus V \)
- \( V' = ID(\text{intruder}) \oplus h[ID(i)] \)
- \( M' = \{ ID(\text{intruder}), V', C \} \)
Solution

<table>
<thead>
<tr>
<th></th>
<th>Hash-based</th>
<th>Enhanced Hash-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Forgery Protection</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>No Multiple Cash in</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>Not Transferable</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>User Authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Hash-based**

\[ M = \{ ID(u), V, C \} \]

\[ V = ID(u) \oplus h[ID(i)] \]

\[ C = h[ h[ID(i)] \oplus X \oplus Offer ] \]

**Enhanced Hash-based**

\[ M = \{ ID(u), V, C \} \]

\[ V = ID(u) \oplus h[ID(i)] \]

\[ C = h[ h[ID(i)] \oplus X \oplus Offer \oplus ID(u) ] \]

Ali Alshehri 2013
A general framework

Data Integrity
NonInjectiveAgreement
(Issuer,Cashier,[ALL DATA])

Not Transferable
NonInjectiveAgreement
(Issuer,Cashier,[M-coupon , User ID])

Forgery Protection
NonInjectiveAgreement
(Issuer,Cashier,[M-coupon])

No Multiple Cash-in
Agreement
(Issuer,Cashier,[M-coupon])

Confidentiality
StrongSecret
(Cashier, SECRET, [Issuer])

User Authentication
Agreement
(User,Cashier,[CREDOENTIAL])

Cashier←→ Issuer

Cashier←→ User

Ali Alshehri 2013
Conclusion

• Hash-based M-coupon protocol.
• Deep formal analysis.
• Other solutions suggested (footfall, premium)
Thank you

• Questions?

Ali Alshehri
a.a.alshehri@surrey.ac.uk

Ali Alshehri 2013