Formal analysis of Facebook Connect Single Sign-On authentication protocol

Caterina Urban
Prof. Marino Miculan

Dept. of Mathematics and Computer Science,
University of Udine,
Italy

SOFSEM 2011 Student Research Forum
Monday, 24th January 2011
Facebook Connect is a Single Sign-On service integrated in the Facebook Platform (until few months ago).
What is Facebook Connect?

Facebook Connect is a **Single Sign-On service** integrated in the Facebook Platform (until few months ago).

Facebook Connect **enables Facebook users** to connect their Facebook account with any third party partner Web site.

**Connect with Facebook**

Connect [The Run Around](#) with Facebook to interact with your friends on this site and to share on Facebook through your Wall and friends’ News Feeds. This site will also be able to automatically post recent activity back to Facebook.

Email: 
Password: 

By proceeding, you are allowing The Run Around to access your information and you are agreeing to the Facebook [Terms of Use](#). By using The Run Around, you also agree to the [Terms of Service](#).
What is Facebook Connect?

Facebook Connect is a Single Sign-On service integrated in the Facebook Platform (until few months ago).

Facebook Connect enables Facebook users to connect their Facebook account with any third party partner Web site.

Using Facebook Connect members will be able to use their Facebook identity across the Web, and at the same time...
What is Facebook Connect?

Facebook Connect is a Single Sign-On service integrated in the Facebook Platform (until few months ago).

Facebook Connect enables Facebook users to connect their Facebook account with any third party partner Web site.

Using Facebook Connect

+ members will be able to use their Facebook identity across the Web, and at the same time
+ third party Web sites can access to Facebook users data outside of Facebook itself.
Facebook Connect Authentication Protocol Security

Question

Is Facebook Connect Authentication Protocol secure?

Steps to Answer the Question

1. A detailed protocol description has not been officially provided (Facebook Connect is proprietary).
2. We have defined a protocol formalization in Alice-Bob notation.
3. We have translated the protocol in Alice-Bob notation into HLPSL.
4. We analyzed the HLPSL formalization using AVISPA.
### Question

Is Facebook Connect Authentication Protocol secure?

### Steps to Answer the Question

1. A detailed protocol description has not been officially provided (Facebook Connect is proprietary).
2. In order to understand the protocol, we have analyzed all incoming and outgoing HTTP traffic among parties: Browser, Facebook, TheRunAround.
3. We have defined a protocol formalization in Alice-Bob notation.
4. We have translated the protocol in Alice-Bob notation into HLPSL.
5. We analyzed the HLPSL formalization using AVISPA.
Question
Is Facebook Connect Authentication Protocol secure?

Steps to Answer the Question
1. a detailed protocol description has not been officially provided (Facebook Connect is proprietary)
Facebook Connect Authentication Protocol Security

**Question**

Is Facebook Connect Authentication Protocol secure?

**Steps to Answer the Question**

1. A detailed protocol description has not been officially provided (Facebook Connect is proprietary) ⇒ in order to understand the protocol, we have analyzed all incoming and outgoing HTTP traffic among parties

   ![Diagram](image)

   - Browser
   - Facebook
   - TheRunAround
Facebook Connect Authentication Protocol Security

**Question**
Is Facebook Connect Authentication Protocol secure?

**Steps to Answer the Question**

1. A detailed protocol description has not been officially provided (Facebook Connect is proprietary).
   
   In order to understand the protocol, we have analyzed all incoming and outgoing **HTTP traffic** among parties:

   ```
   Browser <-> Facebook <-> TheRunAround
   ```

2. We have defined a protocol formalization in **Alice-Bob notation**.
Question
Is Facebook Connect Authentication Protocol secure?

Steps to Answer the Question
1. a detailed protocol description has not been officially provided (Facebook Connect is proprietary) ⇒ in order to understand the protocol, we have analyzed all incoming and outgoing HTTP traffic among parties

   ![Diagram showing communication between Browser, Facebook, and TheRunAround]

2. we have defined a protocol formalization in Alice-Bob notation
3. we have translated the protocol in Alice-Bob notation into HLPSL
Facebook Connect Authentication Protocol Security

**Question**

Is Facebook Connect Authentication Protocol secure?

**Steps to Answer the Question**

1. A detailed protocol description has not been officially provided (Facebook Connect is proprietary)
   \[\Rightarrow\] in order to understand the protocol, we have analyzed all incoming and outgoing **HTTP traffic** among parties

   ![Diagram](Browser \rightarrow Facebook \rightarrow TheRunAround)

2. We have defined a protocol formalization in **Alice-Bob notation**
3. We have translated the protocol in Alice-Bob notation into **HLPSL**
4. We analyzed the HLPSL formalization using **AVISPA**.
Facebook Connect authentication protocol is subject to
+ a replay attack, and
+ a masquerade attack, which allows an intruder to be authenticated as a user to obtain illegitimately other resources.

Replay Attack - Fixes
+ mechanisms based on timestamps and nonces, or
+ SSL channels.

Masquerade Attack - Fixes
+ SSL channels, or
+ authentication of resource requests
⇒ we propose an authentication of resource requests by means of a Diffie-Hellman session key.
Facebook Connect Authentication Protocol Security
Analysis Results

## Weaknesses
Facebook Connect authentication protocol is subject to

+ a **replay attack**, and  
+ a **masquerade attack**, which allows an intruder to be authenticated as a user to obtain illegitimately other resources.

## Replay Attack - Fixes

+ mechanisms based on timestamps and nonces, or  
+ SSL channels.
Facebook Connect authentication protocol is subject to:

- a replay attack, and
- a masquerade attack, which allows an intruder to be authenticated as a user to obtain illegitimately other resources.

**Replay Attack - Fixes**

- mechanisms based on timestamps and nonces, or
- SSL channels.

**Masquerade Attack - Fixes**

- SSL channels, or
- authentication of resource requests
Facebook Connect Authentication Protocol Security Analysis Results

Weaknesses
Facebook Connect authentication protocol is subject to
+ a replay attack, and
+ a masquerade attack, which allows an intruder to be authenticated as a user to obtain illegally other resources.

Replay Attack - Fixes
+ mechanisms based on timestamps and nonces, or
+ SSL channels.

Masquerade Attack - Fixes
+ SSL channels, or
+ authentication of resource requests
  ⇒ we propose an authentication of resource requests by means of a Diffie-Hellman session key.
