



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

What is Facebook Connect?

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).

The screenshot shows a blue header with the Facebook logo and the text "Connect with Facebook". Below this is a paragraph of text explaining the connection. A diagram illustrates the data flow: a blue arrow labeled "Bring your friends and info" points from the Facebook icon to the "Run Around" site icon, and a black arrow labeled "Publish content to your Wall" points from the "Run Around" site icon to the Facebook icon. Below the diagram are two input fields: "Email:" and "Password:". At the bottom, there is a grey bar with a "Sign up for Facebook" link, a blue "Connect" button, and a grey "Cancel" button.

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.

Run Around

Bring your friends and info

facebook

Publish content to your Wall

Email:

Password:

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

Sign up for Facebook

Connect Cancel

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

What is Facebook Connect?

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

f 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](#) in your use of The Run Around. By using The Run Around, you also agree to the The Run Around [Terms of Service](#).

Sign up for Facebook

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).

The screenshot shows a blue header with the Facebook logo and the text "Connect with Facebook". Below this is a paragraph explaining the connection: "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." A diagram illustrates the data flow: a box for "Run Around" (with a profile picture) has an arrow pointing to a "facebook" box labeled "Bring your friends and info", and a return arrow labeled "Publish content to your Wall". Below the diagram are input fields for "Email:" and "Password:". A small disclaimer text reads: "By proceeding, you are allowing The Run Around to access your information and you are agreeing to the Facebook Terms of Use in your use of The Run Around. By using The Run Around, you also agree to the The Run Around Terms of Service." At the bottom, there is a grey bar with a "Sign up for Facebook" link, a blue "Connect" button, and a "Cancel" button.

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?



Facebook Connect Authentication Protocol Security

Question

Is Facebook Connect Authentication Protocol secure?

Steps to Answer the Question

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)

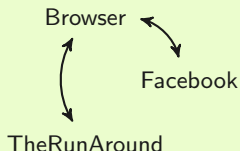
Facebook Connect Authentication Protocol Security

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



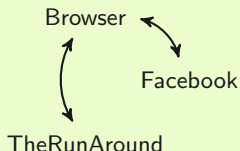
Facebook Connect Authentication Protocol Security

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



2. we have defined a protocol formalization in **Alice-Bob notation**

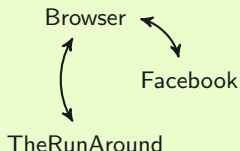
Facebook Connect Authentication Protocol Security

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



2. we have defined a protocol formalization in **Alice-Bob notation**
3. we have translated the protocol in Alice-Bob notation into **HLPSTL**

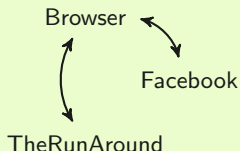
Facebook Connect Authentication Protocol Security

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



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**.

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.

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 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.

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 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.

Bibliography



A. Armando, D.A. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P.H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. *The AVISPA tool for the automated validation of internet security protocols and applications*. In K. Etessami and S.K. Rajamani, editors, Proc. CAV, volume 3576 of Lecture Notes in Computer Science, pages 281-285. Springer, 2005.



A. Armando, R. Carbone, L. Compagna, J. Cuéllar, and M.L. Tobarra. *Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for Google Apps*. In V. Shmatikov, editor, Proc. FMSE, pages 1-10. 2008.



AVISPA Project. *Deliverable D6.1: List of selected problems*. Technical report, <http://avispa-project.org>, 2005.