Links

Ben Laurie blathering

« Federated Login Usability Studies
WTF Does Open Source Have To Do With Business Models? »

J-PAKE in C

Just for fun, I wrote a demo implementation of J-PAKE in C, using OpenSSL for the crypto, of course. I've pushed it into the OpenSSL CVS tree; you can find it in `demos/jpake`. For your convenience, there's also a copy here.

I've tried to write the code so the data structures reflect the way a real implementation would work, so there's a structure representing what each end of the connection knows (`JPakeUser`), one for the zero-knowledge proofs (`JPakeZKP`) and one for each step of the protocol (`JPakeStep1` and `JPakeStep2`). Normally there should be a third step, where each end proves knowledge of the shared key (for example, by Alice sending Bob H(H(K)) and Bob sending Alice H(K)), since differing secrets do not break any of the earlier steps, but because both ends are in the same code I just compare the resulting keys.

The code also implements the protocol steps in a modular way, except that communications happen by magic. This will get cleaned up when I implement J-PAKE as a proper OpenSSL library component.

The cryptographic implementation differs from the Java demo (which I used for inspiration) in a few ways. I think only one of them really matters: the calculation of the hash for the Schnorr signature used in the zero-knowledge proofs – the Java implementation simply concatenates a byte representation of the various parameters. This is a security flaw, as it can be subjected to a "moving goalposts" attack. That is, the attacker could use parameters that gave the same byte representation, but with different boundaries between the parameters. I avoid this attack by including a length before each parameter. Note that I do not claim this attack is feasible, but why gamble? It worked on PGP, after all.

The code and data structures are completely different, though. Also, because of the cryptographic difference, the two implementations would not interoperate.

Share This

This entry was posted on Sunday, October 19th, 2008 at 19:12 and is filed under Crypto, Open Source, Programming, Security. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

3 Comments »

1. This, of course, is more than I have done, but still, not a demo till it runs on two machines, with a toy browser and toy server. Not a demo till it can be seen.

   Comment by James A. Donald — 20 Oct 2008 @ 0:36

2. [...] I wrote last week that I had implemented a J-PAKE demo someone rather churlishly commented, "not a demo till it runs on two machines, with a toy [...]

   Pingback by Links » J-PAKE Again — 27 Oct 2008 @ 15:15

3. [...] (2008-06-28): a crude J-PAKE demo source code (.java). Update (2008-11-04): a more refined J-PAKE in C and OpenSSL module by Ben [...]

   Pingback by Light Blue Touchpaper » Blog Archive » J-PAKE: From Dining Cryptographers to Jugglers — 4 Nov 2008 @ 14:47

RSS feed for comments on this post. TrackBack URI

Leave a comment

Name

Mail (will not be published)

Website

Submit Comment

- **Blogroll**
  - Adriana Lukas
  - Ben Hyde
  - Bob Blakley
  - Cambridge Security Group
  - Groklaw
  - Kim Cameron
  - Lilian Edwards
  - Open Rights Group
  - Pamela Dingle
  - Pat Patterson
  - Randall Munroe
  - Stefan Brands
  - Steve Bellovin
  - Wendy Seltzer
- **Links**
  - Apache-SSL
  - Camilla's Genealogy
  - Flickr
  - My Homepage
  - The Bunker Secure Hosting
- Categories:
  - Arduino/Freeduino
  - Art/Music
  - Books
  - Brain Function
  - Civil Liberties
  - Climate
  - Digital Rights
  - Distributed stuff
  - Food
  - General
  - Identity Management
  - If You Really Loved Me

- September 2008
- August 2008
- July 2008
- June 2008
- May 2008
- April 2008
- March 2008
- February 2008
- January 2008
- December 2007
- November 2007
- October 2007
- September 2007
- August 2007
- July 2007
- June 2007
- May 2007
- April 2007
- March 2007
- February 2007
- January 2007
- December 2006
- November 2006
- October 2006
- September 2006
- August 2006
- July 2006
- June 2006
- May 2006
- April 2006
- March 2006
- February 2006
- January 2006
- December 2005
- November 2005
- October 2005
- September 2005
- December 2004

- Meta:
  - Log in
  - RSS
  - Comments RSS
  - Valid XHTML
  - XFN
  - WP

*Powered by **WordPress***