

Joe Hurley
Encrypting Jabber-based Instant Messaging
Practice Week at NST
3791 Telemedicine and E-Health Systems
24/4/2007

Introduction

In the Snow Agent System (SAS), sensitive data is searched by agents in a peer to peer fashion. The data that is being searched is sensitive and needs to be secured. Data privacy is an extremely important issue in all communication systems. Fortunately, SAS can benefit from the previous work that has been done in this field.

Project Background

The Jabber instant messaging system is the backbone of SAS. The agents that form the system communicate between each other using XMPP, the Jabber protocol for instant messages. This allows the system to conform to the strict guidelines for the health network set by Norwegian legislation. There are also strict guidelines about privacy of patient data. To meet this requirement, a solution is necessary that ensures that only the intended recipient can view the data.

Possible Solution

Clearly, an end-to-end encryption scheme is needed. The data needs to be encrypted before leaving the source agent, and it can only be possible for the receiving agent to decrypt the message. The needs of the system point towards a public key infrastructure as the best solution. Luckily there is support for such a scheme defined in the extensions to XMPP, XEP-0027 [1]. The protocol requires a tag labeling the message as encrypted, and the body of the message is then encrypted removing the possibility of privacy becoming compromised during transmission.

Implementation

To completely conform to XEP-0027, the message body must be in openPGP format. This is important for interoperability among the many different clients that wish to support encrypted instant messaging. However, since SAS uses one agent definition, it would be sufficient to model the message format after XEP-0027 and choose a preferred PKI encryption solution to encrypt the message body not necessarily supporting openPGP. An S/MIME message format, for instance, could be used. Any other option could also be used as long as the receiver knows how to interpret the encrypted body of the message.

The problems related to any PKI is key management and trust. A scheme must be introduced to manage keys and authenticate users. Privacy is easily compromised when the assumptions of any encryption scheme are not met. For the proposed solution, private keys must remain private, and all authenticated agents must be authentic agents. If this is met, the only remaining obstacle is key distribution, and due to the nature of SAS, this might be less of a headache than in traditional PKIs.

Public keys of receiving agents need to be available to all agents that collect data. The keys can be published to the Jabber server, or the receiving agents can support key requests using XEP-0189 [1]. Supporting this protocol will remove the need for a separate key management system, but it also makes authentication more difficult.

Alternative Solutions

Another end-to-end solution is proposed in XEP-0116 Encrypted Session Negotiation [1]. This uses a similar PKI encryption scheme. Rather than simply encrypting the message body, the message session is first negotiated between clients and then the whole session is encrypted. Assuming the agents are not having long conversations between themselves, this solution offers no improvements to the previously mentioned solution. It also requires more bandwidth to negotiate the sessions before actually sending the encrypted messages. Less secure solutions also exist.

Conclusion

The nice thing about the suggested solution is that it requires no modification to the jabber server. The messages are still routed like unencrypted messages. The agents will require support for some encryption scheme and some key management scheme, but these are hopefully only minor. It is up to the developer to choose which encryption algorithms to use. Benefits of well known formats are constantly debated, and one may have requirements that best fit SAS [2, 3]. OpenPGP seems like the best option, but the important thing is that all agents agree on the encrypted message format.

References

- [1] XMPP Extensions <http://www.xmpp.org/extensions/>
- [2] "A certified mail system (CMS) for the Internet" Computer Communications Volume 27, Issue 13, 15 August 2004, Pages 1229-1235
- [3] "Improving Message Security With a Self-Assembling PKI" Callas, Jon. 02 July 2003