

Enterprise Strength Security on a JXTA P2P Network

Bill Yeager
Sun Microsystems
William.Yeager@sun.com

Abstract

When one begins to think about security and P2P networks, and in particular, ad-hoc P2P networks with no real centralization, one must take a leap from the accepted, in place, on-the-Internet, security practices into the unknown. There are potentially billions of peer nodes, some related, and some not, all possibly vulnerable to attack in a multitude of ways: Impersonation attacks and thus identity theft by unauthorized or falsely authorized parties; Invasion of privacy and all that that carries with it; Loss of data integrity; And repudiation of previous transactions, "Hey, no way, I did not say that!" We imagine the equivalent of anti-matter, a complete negation of the fundamental principles of security, or the anti-secure net. Those among us with a strong interest in the secure net, and making P2P not only an accepted but preferred way of both doing business in the Enterprise as well as protecting the personal privacy of the innocent users of P2P software require a toolbox with sockets, and a socket wrench that is capable of applying the torque that is appropriate to each scenario we wish to secure.

It is easy enough for each peer node to be its own certificate authority, create its own root and service certificates, distribute the root certificate out-of-band or in some cases in-band, different sockets for different scenarios, and then use transport layer security to insure two way authorization and privacy. Then again, one cannot help think about Philip Zimmermann, PGP, and "webs-of-trust." This is surely another socket that can be used by small communities of peers to assure that the public keys that they distribute can be trusted with some degree of certainty based on the reputation of the signers.

If we imagine small groups of peers on a purely ad-hoc P2P network, for example, a family, then either mom or dad might be the certificate authority, place their root certificate on each family member's system by infra-red, eyeball-to-eyeball communication, and yes, if a certificate is signed by the CA, you trust it or else. One more socket for our toolbox.

Finally, without actually using a recognized CA, one can apply even more torque to tighten the security on a P2P network. Select one or more well protected and trusted systems, and give to them certificate-granting authority. These systems are unlike standard CA's in the sense that they are peers in the P2P Network, albeit, special peers. Each peer using these CA's boots with the appropriate root certificates, and acquires a root certificate from one of the CA's using a Certificate Signing Request. Furthermore, to acquire a certificate the peer must be authorized perhaps by using an LDAP directory with a recognized protected password. Here, the CA can also use a secure connection to a corporate LDAP service to authorize requesting peers.

In the end, each of the above scenarios, each socket in our mythical toolbox, is a not so mythical. This is how Project JXTA approaches security, and what we will discuss in this keynote presentation.

Bio

Bill Yeager has a career in software engineering, and computer science that spans nearly 40 years. His last 28 years have been spent at Stanford University, 19 years, and Sun Microsystems, 9 years. At Stanford among his many accomplishments, he is best known for having invented the multiple protocol Ethernet router in 1982 that was licensed by Cisco systems in 1987; co-invented the Intermediate Mail Access Protocol that later became IMAP; And, having written a serial line ftp program, ttyp, that was later rewritten at Columbia University, and renamed Kermit.

At Sun Bill invented, architected, and with a small team, developed the Sun Internet Message Server (SIMS) software for which he has filed four patents, and received three; Invented, and programmed the iPlanet

Wireless Server; Led Sun's WAP Forum team; Architected a security model for Java Mobile Phones that is incorporated in MIDP 2.0; And, was the CTO of Sun's JXTA team, there inventing and writing the code for the JXTA Security Model. Bill has filed 26 patents on his JXTA work. Bill is now at Sun Labs. In his current project, "The Virsona," personal privacy is fundamental, Virsona's are JXTA peers, and his is initial objective is to tweak the JXTA security model to support enterprise strength security.

Finally, Bill is the co-chair of the recently formed Internet Research Task Force Research Group on P2P.