# Researchers establishing security standards for the internet

July 7 2009

Sean Smith, Max Pala, and Scott Rea are helping make computing security easier to implement. (Photo by Joseph Mehling '69)

(PhysOrg.com) -- Dartmouth researchers who were pioneers in Public Key Infrastructure (PKI) - a system that secures and authenticates computer communications - are now playing leading roles establishing Internet standards and guidelines for security.

Secure Internet activity requires being able to prove who you are. Security experts agree that the traditional approach of passwords is not always effective. PKI and public key cryptography solve these problems, and Dartmouth researchers are leading the way in helping organizations deploy PKI. A new system developed at Dartmouth called PRQP, which stands for PKI Resource Query Protocol, is now in the pipeline with the

Internet Engineering Task Force (IETF) to become the universal way to easily implement PKI-enhanced computing security.

"PKI labors under the misconception that it's difficult," says Scott Rea, senior PKI architect at Dartmouth. "PKI is most successful when it runs under the covers or in the background." And that's what it does on a lot of commercial websites that accept credit card numbers, ensuring security behind-the-scenes using PKI or "certificate authority" technology.

Dartmouth's Institute for Security, Technology, and Society (ISTS) has received funding from the Department of Homeland Security to explore ways to make PKI more user-friendly, for individuals and for businesses of all sizes. That's how PRQP was born.

"PRQP, very simply, provides a more distributed system for PKI; it works in a way to get trustworthy references in order to verify the PKI certificates of individuals or servers," says Massimiliano "Max" Pala, research fellow with ISTS and the Open Certificate Authority Lab director.

In other words, as PKI becomes ubiquitous, IT professionals need PQRP, which provides a standard way to operate PKI efficiently, and therefore ensures a consistent and robust measure of security.

And, according to Pala and Rea, adoption of PKI is growing, and there is a deliberate program to bring more and more organizations into the PKI fold. Consortiums have been established, grouped around common themes, so that all members within each group can trust each other's PKI certificates. For example, there are eight organizations now in the Higher Education group, or "bridge," which includes colleges and universities. It's called HEBCA, which stands for Higher Education Bridge Certificate Authority, and Rea serves as director of the HEBCA

Operating Authority and secretary of the HEBCA Policy Management Authority.

There are also bridges for federal employees and contractors, pharmaceutical companies and researchers, and one for defense and aerospace companies and contractors. All four existing bridge organizations have formed a "federation" to trust everyone within these networks, and there are varying levels of security, because PKI is customizable. Among all four bridges, approximately 15 million certificates have been issued (mainly to individuals, but servers and other network devices can also carry certificates). That figure is expected to double in the next 12-18 months. At Dartmouth alone there are 34,000 active certificates and about 1,500 server certificates issued from the Dartmouth PKI.

"It's rewarding to see the real-world impact that PKI researchers and practitioners like Scott and Max are having," says Sean Smith, associate professor of computer science and ISTS faculty affiliate. "It's also great to see the institutional support that Dartmouth gives to technological innovation - and in bringing this new technology to the higher ed community at large." Smith co-founded Dartmouth's PKI laboratory in 2000.

Research Director of ISTS Denise Anthony sees the role of Dartmouth as one of mentor or parent when it comes to PKI and PRQP. "Dartmouth faculty members and researchers led by Sean Smith have been at the forefront of PKI technology for more than 9 years," says Anthony. "Our students, grad students, and post-docs have learned about this emerging technology since it was born. And we continue to be involved as PKI and PQRP go global and become the standard way to deploy inter-operable computing security." Anthony is also an associate professor and chair of sociology at Dartmouth.

Dartmouth has a long history of pushing the computing envelope, from hosting the first demonstration of remote computing using standard phone lines in 1940 to convening the conference in 1956 that coined the term Artificial Intelligence to being the home of the birthplace of the BASIC computing language and the Dartmouth Time Sharing System. Dartmouth was also one of the first institutions of higher education to deploy a wireless network and converge computing, voice, and television on its data network.

Source: Dartmouth College