A Secure Key Server for OpenPGP

With the TUM Secure E-Mail project, we have the goal to improve security and confidentiality of e-mail communication at TUM. The vision is to equip all students, researchers and administrative staff with digital S/MIME and OpenPGP certificates to enable to authenticated, integrity protected and confidential communication between internal and external communication partners.

OpenPGP uses so called key servers to distribute OpenPGP information between users. Today’s key servers are not designed to provide security when retrieving data from a key server or authenticity since anyone can publish any information on these key servers. These issues have a large impact on the usability and practicability of OpenPGP for secure e-mail communication.

The goal of this thesis is to develop the design for a secure key server architecture to be used with OpenPGP in the TUM Secure E-Mail project. Such a secure key server has to ensure that users are authenticated when publishing information and must ensure authenticity of information published. In addition it should allow the user to control which information is published with his information.

- Analyze requirements and processes
- Create and propose an architecture for key server
- Implement and test your idea with a strong focus on usability and security

- Passion and a good portion of curiosity
- You are aware OpenPGP exists
- You did some coding before and you liked it
- You like to create and realize software architectures

Matthias Wachs  (wachs@net.in.tum.de)
http://go.tum.de/080020