Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

Open Projects 2016

For further inquiries contact:
Matthias Wachs, matthias.wachs@tum.de

State of the Art of Key Backup and Disaster Recovery for Cryptographic Keys

Using digital certificates and related security approaches is challenging in organizations. Here one of the key requirements can be to have the possibility to recover cryprographic user key in case of a desaster within strict organizational requirements.

This work focuses on elaborating the current state of the art of key escrow mechanisms, cryptographic approaches (e.g. Publicly Verifiable Secret Sharing) and techniques and to develop suitable processes for key backup and recovery.

Secure Email with today's Applications – An Evaluation and User Study

End-to-End Security is advertised as the golden bullet to realize secure email communication. Technologies like OpenPGP and SMIME are available for several decades. But often email applications lack basic support to faciliate the user in using this technologies in every day life.

This project analyzes the state of the art how technologies as OpenPGP and S/MIME to secure email communication are supported in email applications. As a result the work can present a user study how users expect such tools to integrate with applications and how big the gap to the state of the art is.

~~Email in the Wild - Analyzing Email Security on the Internet~~

~~Several approaches like DANE, DKIM, SPF exist to improve email security and to counteract unsolicited email. But it is unclear how well established these approaches are and if they are used correctly in a secure manner.~~

~~The goal of this project is to analyze how widely such approaches are used and if how operators employ them to improve email security.~~

Secure, Resilient and Privacy Preserving Key Distribution for Secure E-Mail

Key distribution and lookup with communication partners is one of the most challenging tasks when it comes to secure communication. With end-to-end secured email approaches like S/MIME and OpenPGP, often public directory services like HKP key servers or LDAP servers are used. Those systems have inherent problems with respect to authenticity of information and secure and privacy preserving data exchange.

This work has the goal to employ the GNU Name System (GNS) , a fully decentralized, secure and privacy preserving name system to publish, distribute and retrieve user certificates in a secure and privacy preserving manner. Those certificates can be used for secure email and many more applications. The vision is to couple GNS with the work on the Certificate Management Service (CMS) and to integrate CMS with GNS.

~~A Workbench to analyze X.509 in Applications~~

~~X.509 is a widely used standard for certificates on the Internet and used with TLS, S/MIME and many more. While several libraries exist to integrate X.509 in applications, applications still have to take care and enforce the correct use of such certificates including verification and validation. This is a challenging and error-prone task where many developers and applications fail.~~

~~The goal of this project is to analyze X.509 certificate validation, elaborate corner stones and realize a workbench to create and test this validation process. This workbench will provide functionality to analyze the use of X.509 in applications based on the analyzed validation process and corner stones.~~

~~Privacy Implications of mDNS~~

~~The Multicast Domain Name System (mDNS) is a zero-configuration service to advertise and discover services in a local network. mDNS is supported by all major operating systems. By announcing services and capabilities within the network, mDNS can have implications on the users' privacy since these announcements often contain sensitive information.~~

~~The goal of this project is to analyze what information is advertised with mDNS in the network and how this information be used to create user profiles.~~

~~Privacy Implications of Mobile Push Services~~

~~Some platforms for mobile devices use certificate-based authentication to identify and authorize a particular device when accessing services. This approach has major implications on the users' privacy since these certificates are visible in the traffic and therefore allow to track users and create user profiles.~~

~~This project has the goal to investigate the implications of certificate-based authentication on the Internet and its implication on users' and their privacy.~~

Technische Universität München
Fakultät für Mustertechnik
Lehrstuhl für Musterverfahren