Nachrichtenverschlüsselung im Alltag

Die Enthüllungen des Whistleblowers Edward Snowden haben eines deutlich gemacht: Unsere Kommunikation ist nicht so privat und geheim, wie wir es als normal und selbstverständlich erachten. Mit einfachen Mitteln ist es bereits möglich, das Abhören von Nachrichten zu erschweren. Wie genau, zeigt dieser Vortrag auf.

Der Vortrag wird die Grundlagen der Nachrichtenverschlüsselung allgemein aufzeigen und die Frage stellen, ob Verschlüsselung angesichts der aktuellen Umstände noch sinnvoll ist. Es werden zwei Verschlüsslungsmethoden aus den Bereichen *Instant Messaging* (IM) und *E-Mail* näher vorgestellt, die in der Praxis recht häufig anzutreffen sind.

Am Beispiel von *Off-the-Record*-(OTR)-Messaging wird gezeigt, wie einfach eine Integration in den IM-Alltag stattfinden kann. Dabei werden die Funktionsweise, Vorteile und Nachteile der Methode, sowie Alternativen zu OTR aufgezeigt.

Ein weiterer wichtiger Kommunikationskanal im Alltag sind E-Mails. Die PGP-Mailverschlüsselung ist Methode, Nachrichten so zu verschlüsseln, dass vertrauliche Informationen nur vom gewünschten Adressaten gelesen werden können. Hier wird ergänzend zur Funktionsweise und Signierung auch auf Key-Signing-Partys und Dateiverschlüsselung eingegangen.

Der Vortrag richtet sich an Einsteiger und wird praxisnah OTR- sowie PGP-Verschlüsselung erklären, so dass die Teilnehmer für das Thema der sicheren Kommunikation sensibilisiert werden.

Websites zum Thema OTR:

- `https://otr.cypherpunks.ca/`
- *Off-the-Record Communication, or, Why Not To Use PGP* (`https://otr.cypherpunks.ca/otr-wpes.pdf`)

Websites zum Thema PGP:

- `http://www.pgpi.org/doc/pgpintro/`
- `http://en.wikipedia.org/wiki/Pretty_Good_Privacy`