Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Thursday, May 11th, 2023 - 16:15, SQUARE 11-2091 (Arena)

## Evolution of E2EE Messaging on the Internet - From PGP to WhatsApp and Beyond

# Rolf Oppliger

End-to-end encrypted (E2EE) messaging is one of the eldest problems in communication security - at least as far as the Internet is concerned. The first solutions for asynchronous messaging in terms of electronic mail date back to the 1990s (e.g., PGP and S/MIME), whereas the first solutions for synchronous or instant messaging appeared in the 2000s (e.g., OTR). Generalizing these techniques and appliyng them to the centralized architecture of todays Internet messaging services led to the development of the Signal protocol that is omnipresent and marks the state of the art in the field. Most interestingly, its double ratchet mechanism provides what is known as forward secrecy and post-compromise security. In addition to Signal itself, the protocol is also used in many other widely deployed messengers, including Facebook Messenger, WhatsApp, and Wire. In its basic form, it targets the two-party setting, and does not provide an obvious solution for group communications. Such a solution is currently being developed within the IETF Messaging Layer Security (MLS) Working Group. The goal is to design a Signal-like protocol that meets the security and scalability requirements of potentially very large groups.

Rolf Oppliger works for the Swiss National Cyber Security Centre (NCSC) and eSECURITY Technologies, teaches at the University of Zurich, and is series editor and author on information security and privacy for Artech House. Since his Ph.D. (University of Bern, 1993) and Venia Legendi (University of Zurich, 1999) in computer science, he has been working and teaching in computer and network security. His main interests are related to applied and real-world cryptography, i.e., how to use cryptographic techniques to secure existing Internet applications or enable new applications in a hopefully secure way.

**From insight to impact.**