Saal: Project 2501 | 17:15 | 00:30 | Day: 2 | Track: Other | nA

Title: **Encrypted Email for Planet Earth**

Subtitle: Failures, Challenges, and the Future

Speaker: **harryhalpin, meskio**

Short: *After the Snowden revelations, demand for encrypted end-to-end communication has skyrocketed, even amongst ordinary users. However, today we still have do not have widespread deployment of OpenPGP, and post-email messaging protocols such as OpenWhisper still have less than a million users. How can we combat the fundamental problems afflicting encrypted messaging, from e-mail to beyond, so that it becomes a fundamental right for all people to have end-to-end encrypted messaging? This event brings together software projects working in this space to reflect on their future, debate their differences, and possibly develop a common strategy for the future.*

Long: After the Snowden revelations, demand for encrypted end-to-end communication has skyrocketed, even amongst ordinary users. As also shown by the catastrophic fate of Lavabit, running a high-security communications provider is fraught with danger, both political and technical. Yet today we see services that essentially sell security "snake oil" taking off with users, while real end-to-end encryption is barely used by activists, much less ordinary people. We still have do not have widespread deployment of OpenPGP, and post-email messaging protocols such as OpenWhisper still have less than a million users. Fundamental standards such as OpenPGP existing for over thirty years, but software such as Enigmail is still claimed to be virtually unusable. What is the source of this massive failure, and how can it be fixed? How can we combat the fundamental problems afflicting encrypted messaging, from e-mail to beyond, so that it becomes a fundamental right for all people to have end-to-end encrypted messaging? This roundtable will bring together software projects working in this space to reflect on their future, debate their differences, and possibly develop a common strategy for the future. Questions to be addressed are: 1. Are standards the solution or the problem? The IETF has recently re-opened the OpenPGP mailing list, and there is discussion around the Darkmail (DIME) protocols brewing. However, even the OpenPGP Working Group is not tackling the hard problems of metadata protection. Another strategy is to ditch e-mail entirely and go with new protocols such as TextSecure, but these protocols are still not federated and are thus centralized with particular applications. Decentralized blockchain-based messaging alternatives have also not taken off. 2. Why is the software still unusable by ordinary users? Two years onwards, we still do not have a better interface than Thunderbird, which has been abandoned by Mozilla. Mailpile is still in beta. Pixelated is still under development. Furthermore, how do we communicate to users if their messages are secure or not? 3. What research problems remain open? Currently, e-mail leaks metadata through the header, as well as through timing information and network traffic. Keyservers remain broken in terms of authentication and also reveal the social graph while key revocation and signing is difficult. Academic work on mix networking and privacy-enhancing technologies desperately needs to 4. How can we reach critical mass? Some companies such as OpenWhisper are now working with major providers such as WhatsApp. Others such as LEAP are working so that anyone can run their own provider. Start-ups such as Peer.io and Protonmail are pursuing centralized strategies, and even Gmail and Yahoo! are working on end-to-end encryption. Governments such as Brazil and Germany are pushing for nationalized or public-private partnerships for encrypted email, while business models in the 'privacy market' are still unclear at best and seem to be unable to take into account distributed systems. The goal of this even is to bring together key voices in this space so we combat the fundamental problems afflicting encrypted messaging, from e-mail to beyond, so that it becomes a fundamental right for all people to have end-to-end encrypted messaging.