Inria, CNRS, Institut de recherche et d'innovation, University College London, IMDEA, Merlinux

NEXTLEAP

NeXt generation Techno-social and Legal Encryption Access and Privacy

http://nextleap.eu /

1 OBJECTIVES

In the wake of the Snowden revelations, public trust in the Internet as eroded. Yet as put by Snowden "We need to encode our values not just in writing but in the structure of the Internet, and it's something that I hope, I invite everyone … around the world, to join and participate in." The primary motivation of NEXTLEAP is to create an interdisciplinary **internet science of decentralisation** in order to study, create, validate, and deploy **core protocols** that can form the foundation for a secure, trust-worthy, and privacy-respecting Internet based on fundamental rights. In detail:

1) The creation of an integrated socio-technical science of decentralised and rights-preserving architecture that takes as foundational provable security, privacy by design, federated identity, anonymity, and decentralised governance based on a number of detailed sociological analyses of real-world case-studies.

2) A fundamental re-thinking of the ethical and philosophical foundations of the Internet ground principles of collective intelligence, digital hermeneutics, and net-rights - crowd-sourced with annotations - to be published in book and online, with events to attract diverse stake-holders to deploy the protocols.

3) The modular specification of decentralised protocols implemented as open-source software modules for a) federated identity with a privacy-preserving address-book b) secure messaging for both synchronous (chat) and asynchronous (e-mail) messaging c) privacy-preserving analytics based on private information retrieval.

There are many open technical questions NEXTLEAP will strive to answer. For example, **Can decentralisation help privacy and anonymity?** While intuitively many people claim that decentralisation helps privacy, actually recent research shows that de-anonymisation and surveillance is actually easier on decentralised networks. **How can we build scalable, high-performing, and secure decentralised architectures based on verified protocols?** Decentralisation typically has impact on the performance of the system with respect to centralised solution. Necessary security properties need to be proven in many protocols, and then also hold as part of a larger heterogeneous system, is often hard for users and developers to understand.

The foundation of these technical questions is rooted in philosophy and real-world usage of the Internet that is best studied via sociology and STS-based approaches. To continue, **what motivations and values can be used to predict successful use of decentralised systems by communities of users?** While it appears citizens are often unhappy with losing control of their data to companies that own centralised platforms, very few users do move to

alternatives and what precisely the social success or failure of a system is unclear. **Is there a decentralised philosophy at the core of the Internet that makes sense of the success of existing protocols?** It is claimed that values around collective intelligence, open innovation, privacy, and decentralisation are built into Internet protocols, but the precise philosophical grounding of these principles – and any new kinds of "internet rights" they entail - is often vague. Furthermore, we need to verify and determine if protocols have the properties needed to guarantee these rights.

2 PROTOCOLS

The core of modern Internet systems are based on a few protocols that can be re-designed. An **address-book** ("friends", social graph, contacts, etc.) is the fundamental building block for any messaging protocol. Such an addressbook can be based on a sharable identifier ranging from *user@example.org* to a hash of a public key (Bitcoin) to a telephone number. Currently, identities and their addressbooks typically are centralised and, if decentralised, not accessed in a privacy-preserving manner. Can we achieve a break-through to allow users to keep track of their contacts without losing their rights or becoming part of a centralised silo?

How can a person send **secure messages** to others, regardless of what system they are using? These messages need to be end-to-end encrypted, resistant to 'metadata' analysis, and may have a number of properties such as forward secrecy and future secrecy. While currently a number of secure next generation protocols exist such as Signal's Axolotl are emerging, existing secure messaging systems are incompatible and so lead to silos between systems such as CryptoCat, Signal, and Telegram. Existing interoperable protocols like SMTP (e-mail) are by default non-encrypted and leak metadata. Can we unify a protocol that starts with e-mail and goes all the way to secure messaging?

Lastly, much of the drive towards centralisation in Internet-based systems is also driven by practical needs to harness the collective 'wisdom of the crowds', improve their system, and to 'know your user.' However, even those that run the system are typically not interested in the personal data of individual users, but only in answering questions about groups. Can we create **privacy-preserving analytics** that can harness the power of machine-learning for good while respecting the rights of their users?

3 METHODOLOGY

Each of the core protocols will be based on sociological case-studies of users and software projects, including other CAPS projects. The values in the protocols will emerge both from a systematization of the philosophy of the Internet (based on the work of French philosopher Bernard Stiegler) as well as a crowd-sourced discussion of net rights. For each protocol, there will be a specification that will be both formally verified for security properties as well as an analysis in terms of privacy and scalability. These protocols will be implemented in running code and deployed with real users, and submitted to open standards bodies such as the IETF and W3C. They can then serve as the building blocks for other CAPS projects and wider software development. Intensive education and outreach

to policy-makers, developers, academics and the general public will raise awareness of the values of decentralisation, security, and privacy – and a new kind of Internet.

Contact (Co-coordinator): harry.halpin@inria.fr