Activity Report 2015

Team DECENTRALISE

DÉCENTRALISÉ

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions).

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Security and Confidentiality

Table of contents

Team DECENTRALISE

Creation of the Team: 2014 October 01, end of the Team: 2015 December 31

Keywords:

Computer Science and Digital Science:

1.2.8. - Network security
1.2.9. - Social Networks
4.3.3. - Cryptographic protocols
4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

6.3.2. - Network protocols
6.3.3. - Network services
6.3.4. - Social Networks
9.8. - Privacy

1. Members

Research Scientist

Christian Grothoff [Team leader, Inria, Advanced Research position]

Engineers

Marcello Stanisci [Inria, from May 2015]
Gabor Toth [Inria, from Nov 2015]

PhD Students

Florian Dold [Inria, from Nov 2015]
Alvaro Garcia Recuero [Inria]

Post-Doctoral Fellow

Jeffrey Paul Burdges [Inria, from Jun 2015]

Administrative Assistant

Cecile Bouton [Inria]

Others

Sebanjila Bukasa [Inria, Intern, from Mar 2015 until Aug 2015]
Nicolas Fournier [Inria, Intern, from Jun 2015 until Aug 2015]
Julien Morvan [Inria, Intern, from Jul 2015 until Aug 2015]

2. Overall Objectives

2.1. Overall Objectives

The objective of our team is to develop an alternative vision of an open secure global network, designed to protect individual citizens and liberal societies. In many ways, securing global networks is the grand challenge of information security, as in this context virtually all security issues get combined and conspire against the system designer: An open network allows the adversary to participate — security solutions thus cannot focus on just keeping the adversary out, and a secure network naturally requires secure software and secure hardware to operate. Finally, a "network" is only useful if it has applications, so we also need to secure the applications, which implies giving the user's tools to protect themselves against social engineering attacks and malware.

3. Research Program

3.1. Decentralisation as the way forward

The goal of the proposed research and development effort is to build the GNUnet, a fully decentralized Internet that respects user's freedoms, giving users free networking software that protects their privacy and makes it difficult for authoritarian institutions to control their lives, and to enable social groups to effectively organize dissent. Like the Internet, the GNUnet is not supposed to be a monolithic application, but instead a layered extensible architecture which enables continuous improvement.

Clear separation into layers should also facilitate testing and verification of the various components. Nevertheless, existing formal verification techniques do not scale to typical subsystems encountered in practice. Thus, we plan to use statistical model checking and static analysis to improve software security using methods that are applicable to real-world systems.

GNUnet is being realised as an overlay network; while it would ideally eventually supplant the Internet, replacing IP will take decades. By building GNUnet as an overlay network, we can use the existing global communication infrastructure to bootstrap a new network. This way, we can perform large-scale deployments and thereby engage researchers and developers worldwide at the cost of a software layer that deals with the intricacies of the modern Internet.

GNUnet currently use the R^5N Byzantine fault-tolerant and censorship-resistant distributed hash table as a key-value store. One of the special properties of R^5N is that, unlike most other DHT designs, it does not assume that any peer can talk to any other peer. Thus, R^5N is suitable for deployment in (ad-hoc) wireless networks, in friend-to-friend networks, or in environments where firewalls limit connectivity. Using R^5N to discover paths, GNUnet's MESH service constructs end-to-end encrypted channels between peers to enable any pair of peers to freely communicate.

These two building blocks are critical for the performance of many applications that we plan to build, and we would like to investigate various ideas for improving their performance. Specifically, we would like to compare R^5N with the X-Vine DHT (including in the presence of adversaries in the network), investigate a strategy for key randomization (learning from techniques used by botnets) and evaluate performance implications of different resource allocation strategies and incentive mechanisms for overlay tunnels.

An important aspect of organizing social movements is the ability to get a message quickly to a large number of people. For example, a user might need to transmit a video of atrocious actions by the authorities, or a call to assemble for a protest. Transmitting such information to a large number of interested parties without powerful central servers requires enlisting other peers to help multiply the traffic.

Existing designs for peer-to-peer multicast have focused on minimizing latency and bandwidth consumption. Our vision for secure multicast builds on these designs, but adds confidentiality and Byzantine fault-tolerance as additional requirements. Furthermore, we envision a stateful multicast channel where certain data is efficiently replayed to peers that join late. The resulting building block should then facilitate one-to-many communication to enable secure messaging at scale.

3.2. Secure electronic payments

Online payment systems are an important building block as they can be used to sustain community efforts (such as software development, research or editorial work) and are necessary for commercial success. The most well-known contender in this context is the decentralized Bitcoin currency. However, Bitcoin has the disadvantage that payments are not anonymous, that the money supply is not controlled, and that its operation requires vast amounts of computational power, which is hardly environmentally friendly.

We are creating Taler, a startup offering untraceable payments to provide support for payments on the Internet, but also of course within the future GNUnet. The basic goal is that the person sending money remains anonymous, whereas the receiver is easily identified. Furthermore, the money supply is tied to traditional currencies via peers that operate as banks. As a result, the system provides anonymity for buyers, while allowing states to tax income. Taler supports a controlled money supply, and requires vastly less computational resources compared to Bitcoin.

A key technology for Taler is onion routing, as this will enable users to hide their IP address during transactions. Initially, Taler will use the Tor network to provide an anonymous 1:1 communication channel. Today, the Tor project is the most well-known and widely deployed onion routing system. However, in the medium term, we would like to investigate an alternative design. In the Tor project, eight trusted directory servers provide the foundation for the security of the entire network. The directory servers are used to allow peers to enumerate the set of all active Tor routers. Using that list of all routers, peers choose routers *at random* to construct the circuits that are fundamental for onion routing. An adversary that is able to compromise five of the directory servers can thus completely violate all security guarantees of the Tor network.

We are not saying that this is a terrible design per-se and would certainly not claim that users should avoid Tor for this reason. However, given recent revelations about the nature of real-world advanced persistent threats, it is prudent to develop a system that does not have this weakness. Hence, we propose to construct an onion routing system in GNUnet that uses a form of Byzantine fault-tolerant random peer sampling instead of directory servers for the selection of random peers.

4. Application Domains

4.1. Identity management and naming

The GNU Name System (GNS) is a fully decentralized and censorship-resistant public key infrastructure. Names in GNS are personal, as each user is in full control of his ".gnu" zone. Users can delegate subdomains to the namespaces of other users, and resolve each other's names using a privacy-preserving, censorship-resistant secure network lookup mechanism. GNS is interoperable with DNS, and can be used as an alternative to the X.509 PKI or the Web-of-Trust.

Using GNS for identity management, we will build the foundation for fully decentralized social networking. Key design goals include never storing (or transmitting) unencrypted data at third parties, and the use of a messaging protocol for semantic extensibility, that is, to allow smooth migration of data to new revisions of the protocol.

4.2. Social networking applications

Peer-to-peer messaging applications need to support protocol evolution. As next generation applications are being deployed, existing clients must continue to be able to interact with newer versions. Furthermore, legacy information must continue to be available after software updates.

We want to realize our vision of a protocol that uses object-oriented techniques to provide semantic extensibility at the protocol layer, thus ensuring that all applications that are created using this infrastructure benefit.

Secure multiparty compuation-based voting can be used to realize secure polls or even elections within social groups. Ultimately, the system might result in an integrated application that also includes file-sharing, conversation, payment and news distribution.

4.3. News distribution and collaborative editing

We want to create a new application that allows users to distribute news using collaborative filtering. News would be gossipped among peers based on the rating assigned to news items by the various users. Furthermore, ratings would influence the timeline of news items displayed for each user, reflecting the user's preferences. A reputation system would enable established contributors to have their articles start with a higher a-priori ranking, allowing them to instantly rise above the noise generated by advertising. New contributors can use a proof-of-work calculation to increase the visibility of their work. The payment system can be used to reward contributors.

When peers compare scores, preserving the privacy of the individual rankings is important as users might not want to expose their political views, and as malicious participants might be able to game the process if they are able to determine the ranking of another peer. We thus propose to use the SMC scalar product (together with an efficient set intersection mechanism to deal with sparcity) for these joint computations.

5. New Software and Platforms

5.1. GNUnet

GNUnet
KEYWORD: Privacy
FUNCTIONAL DESCRIPTION

GNUnet is a framework for secure peer-to-peer networking that does not use any centralized or otherwise trusted services. Our high-level goal is to provide a strong free software foundation for a global network that provides security and in particular respects privacy.

GNUnet started with an idea for anonymous censorship-resistant file-sharing, but has grown to incorporate other applications as well as many generic building blocks for secure networking applications. In particular, GNUnet now includes the GNU Name System, a privacy-preserving, decentralized public key infrastructure.

- Participants: Hans Grothoff, Florian Dold, Jeffrey Paul Burdges and Gabor Toth
- Partner: The GNU Project
- Contact: Hans Grothoff
- URL: https://gnunet.org/

5.2. MHD

GNU libmicrohttpd
KEYWORDS: Embedded - Web 2.0
FUNCTIONAL DESCRIPTION

GNU libmicrohttpd is a small C library that is supposed to make it easy to run an HTTP server as part of another application.

- Author: Hans Grothoff
- Contact: Hans Grothoff
- URL: http://www.gnu.org/software/libmicrohttpd/

5.3. Taler

GNU Taler
KEYWORD: Privacy
FUNCTIONAL DESCRIPTION

Taler is a new electronic payment system.

- Partner: The GNU Project
- Contact: Hans Grothoff
- URL: http://taler.net/

6. New Results

6.1. Asyncronous Messaging

There are now a variety of end-to-end encrypted messaging platforms targeted at personal correspondences. Amongst these, only Pond and Ricochet provide meaningful resistance to traffic analysis by explicitly protecting the message metadata, although several can optionally operate over Tor to protect the user's location. Ricochet's design around Tor hidden services does not permit offline operation. Pond depends upon a centralized server.

In addition, there are messengers designed for academic research, like Vuvuzela, Dissent, and DP5. These employ information theoretically secure channels like dining cryptographers networks (DC-nets) and private information retrieval schemes (PIR) because they admit extremely simply proofs of security. As DC-nets and PIR schemes scale quadratically, these messaging research projects are effectively limited to a fixed maximum number of users, so they cannot realistically provide an alternative to modern email.

Instead, we have begun exploring the prospects of using mid-latency store-and-forward mixnets for asynchronous messaging. In fact, these are the amongst oldest anonymity systems, dating back to David Chaum, but they were normally restricted to anonymous email projects. At present, we remain in the early design phase, but our design scales linearly while providing many interesting properties desired by modern messengers.

We obtain provable security by basing our system on the Sphinx mixnet packet format, which is provably secure in the universal composability framework [7]. At first blush, Sphinx appears to be an overly restrictive format, but the restrictions are worth obtaining this degree of provable security along with a mixnet's scalability. After consideration, we have devised methods for adding entropy, and optimizing the location of entropy in Sphinx packet headers, without the need to use a larger and slower elliptic curve.

In Sphinx, there is a facility for single-use reply blocks (SURBs), as in other mixnets initially designed for anonymous remailers whose forward and backward messages look alike. We can store an SURB in the packet header, which enters use when the packet passes a fixed cross-over node, thereby allowing both sender and receiver remain anonymous to one another. We can orchestrate the usage of SURBs, and an authentication scheme using tokens, to provide optimal messaging propoerties that:

- Protect the identities of senders and recipients from each other and mixnet nodes, including the mailbox servers,
- Protect the identities of recipient's mailbox servers from even their contact to prevent denial of services attack,
- All redudancy through the usage of multiple mailbox servers.

We shall employ the Axolotl ratchet for long-term forward secrecy in messages, like Pond and Signal do. We can slightly improve upon the Axolotl ratchet by judiciously introducing side key material into the ratchet state. These side keys could be symmetric keys that take a different route through the mixnet, or travel outside the mixnet, thereby allowing the ratchet state to evolve based upon multiple concurrent paths. Side keys could also employ post-quantum public key cryptography, thus providing forward-secrecy against future attackers equipped with quantum computers.

We have also found another forward-secure ratchet inspired by Axolotl that integrates well with the Sphinx packet format. We believe this allows mixnet messages to be protected by long-term ratchets and posses a modicum of protection even against attackers with quantum-computers. At best, long-term ratchets themselves are only pseudonymous, not actually anonymous, so using the integrated ratchets requires considerable care.

6.2. Efficient Privacy-Preserving Scalar Product

We have designed, implemented and evaluated two variants of new privacy-preserving scalar product protocols. The first variant is based on an original idea of Ioannidis et al. [8] and was refined by Amirbekyan et al. [6]. Our first design improves on this by supporting signed values. A second design uses discrete logarithms over Elliptic curves instead of a homomorphic cipher, resulting in a substantially more efficient computation as long as the final result is numerically small.

In both protocols, Alice learns the scalar product $\sum a_i b_i$ of her private vector $\overrightarrow{a}$ with Bob's private vector $\overrightarrow{b}$. The protocol is privacy-preserving in that Alice cannot discern details about $\overrightarrow{b}$ other than what she can learn from $\overrightarrow{a}$ and the scalar product $\sum a_i b_i$, and Bob does not learn anything.

Table 1 summarizes our experimental results.

Table 1. Preliminary performance data for the SP algorithms, wall-clock time running on a single-core of an i7.

Length	RSA-2048	ECC-2^{20}	ECC-2^{28}
25	14 s	2 s	29 s
50	21 s	2 s	29 s
100	39 s	2 s	29 s
200	77 s	3 s	30 s
400	149 s	OOR	31 s
800	304 s	OOR	33 s
800	3846 kb	OOR	70 kb

6.3. GNS support for Tor

We have worked with the Tor community to understand how best to support integration of the GNU Name System with Tor via specialized Tor exit nodes. There are two components to this work:

At present, there are somewhat fragile configuration options to Tor that should allow Tor users to locate the specialized exit nodes, although a small patch to Tor itself would improve upon these.

There are security reasons why Tor should not interact with locally configured name resolution services. OnioNS created a method to make Tor use local services for some domain name lookups, but doing so is somewhat heavy [9]. If we're creating a GNS patch to Tor anyways, then we'll likely extend it to optimize this process.

7. Partnerships and Cooperations

7.1. Regional Initiatives

We obtained ARED funding (40% of a PhD) from the region (starting 11-2015). The focus of the proposed research is how to preserve a free and independent quality press in the age of online distribution. We propose to tackle this challenge from two sides: First, we will broaden the online revenue stream by enabling convenient anonymous payments that preserve the reader's privacy and are more efficient and secure than traditional payment systems. Thus, the resulting system will allow for a larger fraction of the payment to arrive at the newspaper, and for a higher conversion of visitors to purchases. Second, we will consider an alternative means for distributing news, which integrates the typical Web-processes of third parties linking to, commenting on, translating and regurgitating stories while also enabling fair compensation of those involved in the creative process. A key challenge here will be to semi-automate the editorial process, leaving it to readers and decentralized, privacy-preserving algorithms to filter worthwile news. The ideal outcome will be a news distribution system that provides censorship resistance, financial compensation for quality (online) journalism and privacy for readers.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Invited talks

- 19th Workshop on Elliptic Curve Cryptography, on “Cryptography in GNUnet: Protocols for a Future Internet for Libre Societies”

8.1.2. Scientific expertise

- IETF 93, on “Special Use Domain Names of P2P Systems”
- IETF 93, on “Knocking down the HACIENDA with TCP Stealth”
- Invited expert for the high-level conference on “Protecting on-line privacy by enhancing IT security and EU IT autonomy” organized by the Civil Liberties Justice and Home Affairs Committee (LIBE) and the Science and Technology Options Assessment Panel (STOA) of the European Parliament, in association with the Luxemburg Presidency of the European Council

8.2. Teaching - Supervision - Juries

8.2.1. Supervision

PhD : Matthias Wachs, “A Secure Communication Infrastructure for Decentralized Networking Applications”, TU Munich, 2015, Christian Grothoff (advisor)

PhD in progress : Bart Polot, “Practical Routing in Overlays”, 2011-, Christian Grothoff (advisor)

PhD in progress : Florian Dold, “Secure payment systems and applications”, 2015-, Christian Grothoff (encadrant), Jean-Louis Lanet (encadrant)

PhD in progress : Alvaro Garcia-Recuero, “Privacy for the Trolls”, 2014-, Christian Grothoff (encadrant)

8.2.2. Juries

- PhD : Michael Kiperberg, “Preventing Reverse Engineering of Native and Managed Programs”, University of JYVÄSKYLÄ, 2015, Pekka Neittaanmäki (supervisor), Nezer Zaidenberg (supervisor), Christian Grothoff (opponent)

8.3. Popularization

- ACTUX Meeting, on “Résistance des GNUs”
- Security in Times of Surveillance (TU Eindhoven), on “Knocking down the HACIENDA with TCP Stealth”
- Linux User Group (LUG) Camp, on “Résistance des GNUs”
- Studentenforum im Tönissteiner Kreis e.V., on “State Surveillance: Benefits and Risks”
- Invest in Cyber Convention, on
  “La protection de la vie privée et sécurité des objets connectés” (Panel)
- Post Snowden Cryptography, on “The GNUnet: 45 Subsystems in 45 Minutes”
- Organizing YBTI workshop at 32c3 in Hamburg (December 29th)

9. Bibliography

Publications of the year

Invited Conferences

[1] C. GROTHOFF. *Design Requirements for Civil Internetworking (Position paper)*, in "Protecting online privacy by enhancing IT security and strengthening EU IT capabilities", Brussels, Belgium, LIBE committee and the STOA panel together with the Luxembourg Presidency, December 2015, https://hal.inria.fr/hal-01244744

Scientific Books (or Scientific Book chapters)

[2] H. WOLF, J. JAROMIL, R. RADIUM, C. GROTHOFF. *Free Software Economics*, in "Cost of Freedom: A Collective Inquiry", Julien Taquet, 2015, pp. 131-136, https://hal.inria.fr/hal-01239072

Other Publications

[3] M. ERMERT, C. GROTHOFF. *Über Umwege ans Ziel*, August 2015, pp. 66-67, c't 19/2015, https://hal.inria.fr/hal-01239077

[4] C. GROTHOFF, Y. EUDES. *Comment fonctionne Skynet, le programme ultra-secret de la NSA créé pour tuer*, October 2015, Le Monde, https://hal.inria.fr/hal-01239089

[5] C. GROTHOFF, M. WACHS, M. ERMERT, J. APPELBAUM, L. COURTÈS. *Le programme MORECOWBELL de la NSA sonne le glas du DNS*, January 2015, Cet article décrit le programme « MORECOWBELL » de l'agence d'espionnage étasunienne NSA et montre les défauts du protocole DNS qu'il exploite. Un état de l'art des alternatives à DNS est ensuite donné, en évaluant l'efficiacité contre les attaques telles que celles perpétrées par la NSA, https://hal.inria.fr/hal-01114307

References in notes

[6] A. AMIRBEKYAN, V. ESTIVILL-CASTRO. *A new efficient privacy-preserving scalar product protocol*, in "Proceedings of the sixth Australasian conference on Data mining and analytics - Volume 70", Australian Computer Society, Inc., 2007, pp. 209–214

[7] G. DANEZIS, I. GOLDBERG. *Sphinx: A Compact and Provably Secure Mix Format*, in "Proceedings of the 30th IEEE Symposium on Security and Privacy (S&P 2009)", IEEE Computer Society, May 2009, pp. 269–282

[8] I. IOANNIDIS, A. GRAMA, M. ATALLAH. *A Secure Protocol for Computing Dot-Products in Clustered and Distributed Environments*, in "Proceedings of the 2002 International Conference on Parallel Processing", IEEE Computer Society, 2002, pp. 379–384

[9] J. VICTORS. *The Onion Name System: Tor-Powered Distributed DNS For Tor Hidden Services*, Utah State University, Logan, Utah, 2014, https://github.com/Jesse-V/OnioNS-literature/blob/master/thesis/thesis.pdf