NextLeap Review meeting
Publication, Contribution, Dissemination

Vincent Puig, IRI
November 8th, 2017

D6.1 Public Web site

NEXT
generation
techno-social and
Legal
Encryption
Access and
Privacy

In the wake of the Snowden revelations, public trust in the Internet has eroded.

NEXTLEAP aims to create, validate, and deploy communication and computation protocols that can serve as pillars for a secure, trust-worthy, annotable and privacy-respecting Internet that ensures citizens fundamental rights. For this purpose NEXTLEAP will develop an interdisciplinary internet science of decentralisation that provides the basis on which these protocols will be built.

Why and how does it matter?

Francesca Musiani

Georges Danezis

Carmela Troncoso

Meet the NEXTLEAP team

NEXTLEAP combines expertise from across different disciplines in order to develop a set comprehensive answers to questions surrounding privacy and society. Our team is spread across Europe and includes specialists in computer science, formal protocol verification, sociology, social philosophy, cryptography and engineering.

Launch

The political Significance of Cryptography

Although historically cryptography has been restricted to government and industrial use, there has recently, after revelations of mass surveillance by Snowden, been increased interest in securing the everyday communications of citizens: Applications such WhatsApp, Telegram, Silence, Crypto.cat, Signal, and even PGP all claim to use end-to-end encrypted messaging to secure the content of communication. There has been discussion in France after the Bataclan attacks of banning end-to-end encryption, and in recent weeks, political parties have declared their desire to keep end-to-end encryption legal but have a backdoor or passwords available to the government. Rumors of hacking now dominate the news, and are claimed even influence elections. Given that cryptography has moved from an obscure branch of mathematical number theory to a real-world problem, the NEXTLEAP project is drawing together an interdisciplinary group of cryptographers, activists, and philosophers to discuss the political significance of cryptography.

- Keynote by bernard stiegler
- Panel with cryptographers and activists
- Presentations by nextleap researchers

Seminars

We are open source

Repositories of various deliverables worked on by NEXTLEAP are available as open source materials. Feel free to download, replicate, share, remix and provide us some feedbacks.

Consult our github repository

Projects

Autocrypt

As part of bringing privacy-preserving end-to-end encryption to decentralized messaging, researchers and implementers in NEXTLEAP have co-founded and are participating in the new Autocrypt effort. It aims to leverage the email ecosystem, the largest federated identity and messaging network, and bring encryption to a wider audience than other failed efforts in the last 15 years.

Claimchain

In order to be decentralized, secure messaging requires an ability to discover key material and guarantee its integrity. Typically, today this is done via a single centralized and unstandardised service provider. In order to create an interoperable standard around secure messaging, key discovery needs to be decentralized. Blockchain-based approaches have been suggested in

Highlights

The Internet, Private Actors and Security Challenges
Paris / 09.10.2017

« Nothing to hide » documentary screenings
Paris / 06.09.2017

Simpler secure group messaging?
Web / 20.07.2017

EuroUSec 2017 - 2nd European Workshop on Usable Security
Paris, UPMC, Paris 6, Sorbonne Universités / 29.04.2017

IEEE Security and Privacy on the Blockchain Workshop
Paris / 29.04.2017

Rightscon
Brussels / 29-31.03.2017

CryptoAction Symposium
Amsterdam / 27-28.03.2017

Internet Freedom Festival
Valencia / 06-10.03.2017

F2F Meeting
Madrid / 03.03.2017

Sciences à coeur
Paris / 01.12.2016

Crypto-design
Amsterdam / 25.11.2016

ELEVATE Festival
Graz / 22.10.2016

coming highlights

Current issues in SDO decision-making for the Internet 15.11.2017

Security, Privacy and Applied Cryptographic Engineering (SPACE 2017) 13-17.03.2017

Les Entretiens du Noveau Monde Industriel (ENMI 2017) 19-20.12.2017

past highlights

The Internet, Private Actors and Security Challenges 09.10.2017

« Nothing to hide » documentary screenings 06.09.2017

Availability, Reliability, and Security (ARES) 29-30.08.2017

International Association for Computing and Philosophy Conference 26-28.06.2017

Simpler secure group messaging? 20.07.2017

Privacy-Enhancing Technologies Symposium 18-21.07.2017

EuroUSec 2017 - 2nd European Workshop on Usable Security 29.04.2017

IEEE Security and Privacy on the Blockchain Workshop 29.04.2017

Rightscon 29-31.03.2017

CryptoAction Symposium 27-28.03.2017

Internet Freedom Festival 06-10.03.2017

F2F Meeting 03.03.2017

Computers, Privacy, and Data Protection Conference 26-28.01.2017

Sciences à coeur 01.12.2016

Crypto-design 25.11.2016

ELEVATE Festival 22.10.2016

The Internet Rules, But How? 05.10.2016

CAPSSI Community Workshop 28.09.2016

Internet Science 2016 12-14.09.2016

highlights

The Internet, Private Actors and Security Challenges Paris / 09.10.2017

International workshop ANR / UTIC

In the first of three conferences to be held over the next year, Didier Bigo (CERI-Sciences Po), Laurent Bonelli (ISP-Paris-10 Nanterre) and Sebastien-Yves Laurent (CMRP-Bordeaux) from the ANR project UTIC are bringing together representatives of major online service providers for a high-level experts roundtable. Participants will look at the ways in which technology firms engage with policy-makers and law enforcement agencies to address today's major security challenges: How did their relationship with intelligence and law enforcement agencies evolve amidst heated post-Snowden debates on surveillance and privacy? What are the main legal hurdles faced by online service providers to protect the rights of their users, and what changes in legislation are called for? How do these companies adapt their business practices to help address today's security challenges? By looking at these important issues at the intersection of policy, law and technology, the roundtable will analyse public-private relationships in the fields of surveillance and security, offering an opportunity for a much-needed discussion between key international stakeholders and researchers. To facilitate the discussion, the roundtable will be divided in two parts during which representatives of leading Internet companies will share their insights in interaction with researchers. The audience will have an opportunity to join the discussion during Q&A sessions.

CERI-56 rue Jacob, 75006 Paris / Salle de conférences

Program

Registration

« Nothing to hide » documentary screenings Paris / 06.09.2017

The documentary « Nothing to Hide », dedicated to electronic surveillance and its acceptance in society, will be released this Wednesday (September 6th) at the cinéma Saint-André-des-Arts in Paris (14 screenings at 1 pm). The documentary will also be screened at the Cinéma le Rio (Clermont-Ferrand, Sept 13-27) and September 24 and 28 at the cinema Le Régent (Saint-Gaudens).

On September 30, the film will be released on the Internet (Creative Commons Non Commercial).

Trailer (allocine.fr)

Simpler secure group messaging? Web / 20.07.2017

New article : Simpler secure group messaging?

NEXTLEAP publications in conferences, journals and other venues.

- Harry Halpin. The Responsibility of Open Standards in the Era of Mass Surveillance , Workshop on Hot Topics in Privacy-Enhancing Technologies (HotPETS 2016).
- Jamie Hayes, Carmela Troncoso, and George Danezis. TASP: Towards Anonymity Sets that Persist. In Workshop on Privacy and the Electronic Society (WPES 2016)
- D. Fiore, A. Mitrokotsa, L. Nizzardo, E. Pagnin. Multi-Key Homomorphic Authenticators. ASIACRYPT 2016.
- D. Fiore and A. Nitulescu. On the (In)security of SNARKs in the Presence of Oracles, TCC 2016-B.
- Marios Isaakidis, Harry Halpin, and George Danezis: UnlimitID: Privacy-Preserving Federated Identity Management using Algebraic MACs. In Workshop on Privacy and the Electronic Society (WPES 2016)
- Ksenia Ermoshina, Francesca Musiani: Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. Association of Internet Researchers (AoIR) Conference.
- Mélanie Dulong de Rosnay, Francesca Musiani, "Towards a (De)centralization-Based Typology of Peer Production", TripleC: communication, capitalism & critique , vol. 14, n. 1, 2016, p. 189-207.
- Dmitry Epstein, Christian Katzenbach, Francesca Musiani (coord.), 2016, Internet Policy Review, vol. 5, issue 3, Doing internet governance: practices, controversies, infrastructures, and institutions.
- Kelsey Cairns, Harry Halpin, and Graham Steel: Security Analysis of the W3C Web Cryptography API. In Proceedings of Security Standardization Research Conference (SSR 2016).
- Ksenia Ermoshina, Francesca Musiani, Harry Halpin: End-to-End Encrypted Messaging Protocols: An Overview In Proceedings of Internet Science Conference (INSCI 2016): 244-254.
- Elijah Sparrow, Harry Halpin, Kali Kalineko, and Ruben Pollan: LEAP: A Next-Generation Client VPN and Encrypted Email Provider. In Proceedings of International Conference on Cryptology and Network Security (CANS 2016).
- Carmela Troncoso, Marios Isaakidis, George Danezis, Harry Halpin. Systematizing Decentralization and Privacy: Lessons from 15 years of research and deployments.Proceedings of Privacy-Enhancing Technologies 2017 (PoPETS 2017).

NEXTLEAP Videos and other resources.

Harry Halpin: Presentation at IMMWorld

November 22nd 2017: Harry Halpin presented on "The Next Revolution in Security Standardization: Beyond the Crisis of Cyberwar, Mass Surveillance, and DRM" at Internet and Mbile World. Bucharest, Romania. **View Video**

Marios Isaakides: Presentation at PETS

July 20th 2017: Marios Isaakidis presented on "Systematizing Decentralization and Privacy" at the 17th Privacy Enhancing Technologies Symposium. Minneapolis, United States. **View Video**

Ksenia Ermoshina: Interview for GnuPG

June 10th 2017: Ksenia Ermoshina was interivewed about NEXTLEAP, activism, and GnuPG. **View Video**

Holger Krekel and Bogdan Kulynych: Presentation at 33c3

December 28th 2017: Bogdan Kulynych presented ClaimChain as "Decentralized PKI system based on blockchains". **View Video**. Also, Holger Krekel presented "Autocrypt: Email-encryption for everyone". **Video Video**. Holger Krekel took part in a panel on opportunistic email encryption with Volker Birk (pEp) and Neal Walfield (GPG). Hamburg, Germany. **Video Video**

Ksenia Ermoshina: Presentation at EuroUSEC

April 29, 2017: Ksenia Ermoshina presented a paper entitled "Can Jonny build a protocol? Coordinating developer and user intentions for privacyenhanced secure messaging protocols" at the European Usability and Security Workshop (EuroUSec 2017), Paris, France. **Download Slides**

Harry Halpin: Presentation at HotPETS

July 22nd 2016: Harry Halpin presented a paper entitled "The Responsibility of Open Standards in the Era of Surveillance" at the 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016), Darmstadt, Germany. **View Video**

Holger Krekel: Presentation at 32c3

December 27th, 2015: Holger Krekel presented a talk entitled "Hacking EU funding for a decentralizing FOSS project: Understanding and adapting EU legal guidelines from a FOSS perspective" at the 32nd Chaos Communication Congress in Hamburg, Germany. **View Video**

Harry Halpin: Presentation at ENMI 2015

December 14th, 2015: Project coordinator Harry Halpin presents the NEXTLEAP Project at ENMI 2015 in Centre Pompidou, Paris, France. **View Video**

Project Presentation Slides

NEXTLEAP Project presentation slides. **Download Slides**

Project Factsheet

NEXTLEAP's official project factsheet. **Download Slides**

NEXTLEAP

EC H2020 CAPS Project on developing decentralized and secure protocols.

Paris, France https://nextleap.eu

Search repositories... Type: All Language: All

verified-claimchain

OCaml Updated 12 hours ago

nextleap-website

NEXTLEAP Project Website

HTML Updated 12 hours ago

claimchain-simulations

Forked from claimchain/claimchain-simulations

Simulations for ClaimChain decentralized PKI

Top languages

Python Ruby JavaScript

HTML Makefile

People 1 >

misaakidis
Marios Isaakidis

D6.2 Dissemination Plan

D6.2 Dissemination Plan

Goals

- Provide stakeholders (other CAPS projects, standard bodies, human rights activists…) with details on the projet scope, intention and expected results
- Bring Nextleap partners external audience and maximize impact of the project results.

Means

- Partner's social networks and professional contacts
- Academic papers and public events
- Interaction with other CAPS projets and Internet Science events

Materials

- Website, social media presence, flyers

D6.2 Dissemination Plan

KPI

- Awareness of key audiences
- High-quality academic conferences
- Interdisciplinary events
- Enlarge the audience (public events, popular events)
- Local, National, European and International levels
- Stimulate new opportunities

Policy

- Communication in English (additional languages encouraged for local impact)
- Carreful use of disclosure of confidential information (for security analysis)
- Acknowledge support of European Commission
- Preference for Open Access publication

Strategy

- Communicate on Nextleap purpose and results
- Impact on European innovation
- Key terms and vocabulary

D6.2 Dissemination strategy

Key messaging

- Interdisciplinarity (sociology, philosophy, cryptography/privacy research based on the emerging field of Internet Science
- Cybersecurity based on fundamental rights of end-users (privacy, security)
- Sovereignty and empowerment of citizens restoring trust
- Privacy-preserving data-mining
- Decentralized protocols
- Open-source libraries
- Open standards (IETF, W3C)

Results

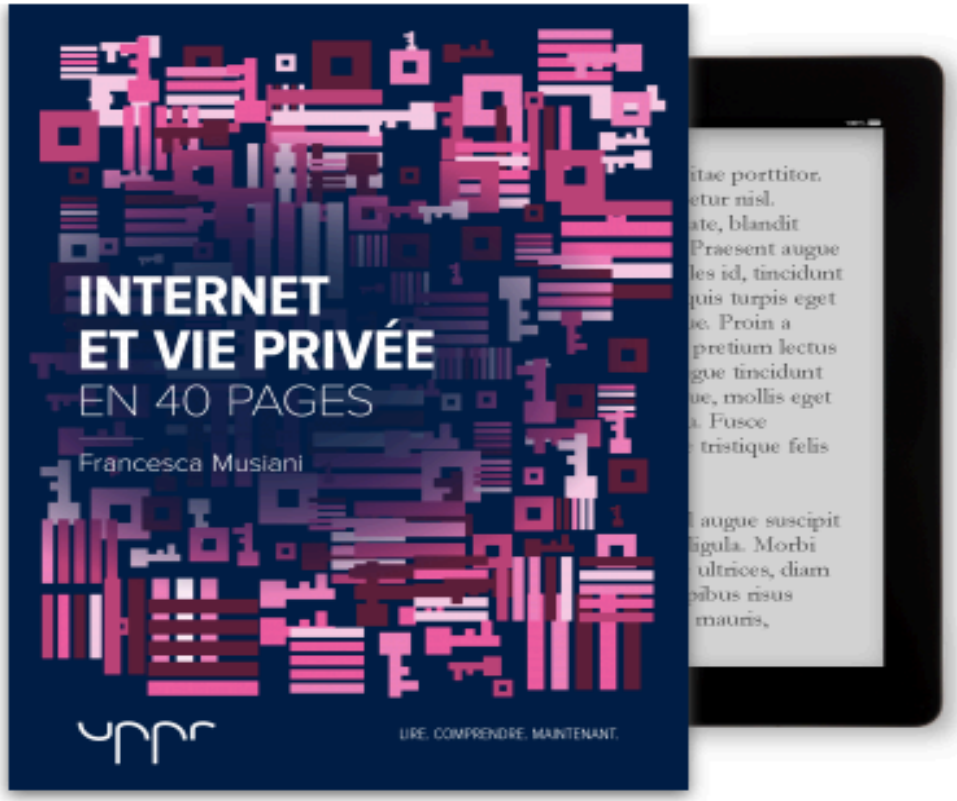
- Interdisciplinary understanding of decentralization
- Formally verified protocols for federated identity and encrypted messages
- Interaction with users
- Global discussion on NetRights
- Big picture book

D6.2 Dissemination Targets

- **Citizens**
  - Workshops by partners:
- ENMI, Pharmakon, Plaine Commune, Digital Studies (IRI)
- Nextleap seminars
  - Attended conferences (OuiShare, CCC Congress, LibrePlanet, OKCon, Re:publica, Internet Freedom Festival)
  - Magna carta of the Web
  - F. Musiani Book (uppr editions)
  - Web we want book (IRI, Web foundation, Fyp)
  - NextLeap book (D3.2)
- **CAPS and other projets**
  - Liaison with MAZI, Netcommons, D-CENT, P2P Value
  - Socratic, PQCrypto, CACE, ERCC, HEAT, Ecrypt-CSA, HINT, MATTHEW, SAFECrypto, SEPIA, ENONYMITY

Internet et vie privée en 40 pages

De Francesca Musiani



Explosion du volume des données, développement de l'Internet des objets et de l'intelligence artificielle, naissance d'une 'gouvernance algorithmique', valorisation (et détournements) des données personnelles à des fins commerciales et publicitaires, usages mobiles de l'Internet, une surveillance numérique (et pour le numérique) toujours plus intrusive et opaque… Les récents bouleversements de la société et de l'économie numériques s'accompagnent de transformations dans l'exposition et la protection de la vie privée – transformations qui sont à la fois techniques, économiques, sociales et culturelles.

La toile que nous voulons

Le web néguentropique

Collection du Nouveau Monde Industriel

Depuis son origine, et sous la pression d'un secteur économique désormais hégémonique, le web a évolué en un sens qui l'a profondément dénaturé, au point d'en faire un instrument d'hypercontrôle et d'imposition d'une gouvernance purement computationnelle de toutes choses. Privilégiant à outrance l'automatisation mise au service de modèles économiques devenus la plupart du temps ravageurs pour les structures sociales, cette évolution a affaibli toujours plus gravement les conditions d'une pratique réflexive, délibérative — outre les aspects révélés par Edward Snowden.

Cet ouvrage présente les principaux aspects théoriques et pratiques d'une refondation indispensable du web, dans lequel et par lequel aujourd'hui nous vivons. L'automatisation du web ne peut être bénéfique que si elle permet d'organiser des plateformes coopératives et des processus délibératifs, notamment à travers la conception d'un nouveau type de réseaux sociaux.

La toile que nous voulons balaye les aspects et enjeux économiques, politiques, militaires et épistémologiques de cette rénovation nécessaire, et avance des hypothèses pour l'élaboration d'un avenir meilleur.

FYP éditions

cap·digital Paris Region

WORLD WIDE WEB FOUNDATION

iri Institut de recherche et d'innovation

21 €

ISBN 978-2-36405-152-2

9 782364 051478

Couverture : Clément Lacocq

Sous la direction de **Bernard Stiegler**

La toile que nous voulons

fyp éditions

Sous la direction de **Bernard Stiegler**

Paul Jorion

Evgeny Morozov

Julian Assange

Dominique Cardon

Le web néguentropique

François Bon
Thomas Berns
Bruno Teboul
Ariel Kyrou
Yuk Hui
Harry Halpin
Pierre Guehenneux
David Berry
Cristian S. Calude
Guiseppe Longo

La toile que nous voulons

iri Institut de recherch et d'innovation

FYP éditions

D6.2 Dissemination Targets

D6.2 Dissemination Targets

- **Standardization**
- W3C WG : Web cryptography, Web Authentication, Social Web, DRM
- IETF WG: OpenPGP, Public Notary Transparency, Oauth, CryptoForum, Human Rights Condiderations for Protocols
- **Industry conferences**
- RSA, ISSE, Mozilla, OSCon, FOSDem, OpenPGP, LEAP, Signal, Tor
- **Internet Governance**
- F. Musiani (CNIL, CSA, ARCEP), B. Stiegler (CNNum, ARCEP)
- Liaison with : EuroDIG, CPDP, Digital Enlightment Forum, IGF, ISOC, ICANN, OECD ITAC, RightsCon
- **Academia**
- INRIA EuroSP2017
- Publications, Courses

D6.2 Dissemination Materials

Logo
- Project announcement

Web site (D6.1)
- Dissemination actions
- Seminars and videos

Social Networks
- Events

Leaflets
- Events
- + Project info

Home 99+ Notifications Messages Search Twitter Tweet

NEXTLEAP
@nextleap2020 Follows you

Tweets 298 | Following 117 | Followers 204 | Likes 137 | Lists 1

Following

NEXTLEAP @nextleap2020
Ça commence ⬤ #cryptopartycamp ⬤ nextleap.eu /events/cryptoc…

1

NEXTLEAP Retweeted

Transmedia Ready @TransmediaReady · Oct 27
@MONACOHUB @mel0delphe
all weekend it's real life game w/ #cryptopartycamp & @nextleap2020 @IRILive @StoryHacking ;-)bit.ly/2hK4j1r

2 1

NEXTLEAP @nextleap2020 · Oct 26
Ça commence ⬤ #cryptopartycamp ⬤ nextleap.eu/events/cryptoc…

NEXT GENERATION TECHNO-SOCIAL AND LEGAL ENCRYPTION ACCESS AND PRIVACY

WORKSHOP
10:00 AM - 16:00 May 5th
Centre Pompidou - Salle Triangle

LAUNCH EVENT
17:00-21:00 May 5th
Centre Pompidou - Petite Salle

NEXTLEAP

DEVELOPING AN INTERNET SCIENCE OF DECENTRALISATION

In the wake of the Snowden revelations, public trust in the Internet has eroded.

The primary motivation of NEXTLEAP is to create, validate, and deploy communication and computation protocols that can serve as pillars for a secure, trust-worthy, annotable and privacy-respecting Internet that ensures citizens fundamental rights.

For this purpose, NEXTLEAP will develop an interdisciplinary internet science of decentralisation that provides the basis on which these protocols will be built.

OBJECTIVES

Are you a concerned citizens or partipant in a CAPS project that is concerned about privacy and security?

Workshop
10:00 AM - 16:00 May 5th
Centre Pompidou - Salle Triangle
NEXTLEAP will be hosting an all day training and use-case elicitation work so we can help your code maintain privacy and be compliant with Data Protection.

Launch event
17:00-21:00 May 5th
Centre Pompidou - Petite Salle
The second part of the day will be the launch event of the project on the significance of next generation, secure, privacy-enhanced Internet systems. Among other speakers, Bernard Stiegler, Phil Rogaway, and more will participate in a roundtable discussion.

See http://nextleap-launch.eventbrite.com for details and registration.

WHO IS CONCERNED

scientists
innovative research work that can bring closer disciplines from different "cultures of sciences"

civil society and local authorities
empowering grassroots initiatives

designers and developers
open/free software and hardware

policy makers and politicians
regulations for defending the digital rights of the local population

website: http://nextleap.eu
coordinator: Harry Halpin harry.halpin@inria.fr

This project has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation (H2020-ICT-2015, ICT-10-2015) under grant agreement n° 688722

D6.2 Dissemination KPI

	KPIs	Target	Action	Realized	%
Develop decentralized and privacy-preserving protocols	Number of Protocols produced	4	Devpt	under dvpt.	-
Bind social and technological	Number of case studies	30 (5 in depth)	Use cases organisation	30 surveys + 3 in-depth	50%
Net Rights awareness	Number of participants	10.000	Web platform	under dvpt.	-
Portability of decentralization	Domains using protocols	10	Outreach	under dvpt.	-
Scalability	Number of users	100.000	Outreach	under dvpt.	-
Innovation	Institutions adopting protocols	12	Outreach towards public and private	under dvpt.	-

D6.2 Dissemination KPI

Dissemination Type	Examples	Target	Realized	%
Blog posts	G. Danezis	30	6	15%
Seminars	Prosecco, Digital Studies	30	10	33%
Online outreach	Twitter followers, Facebook	10.000	105 (now 250), not including Website analytics	1% (now 2,5%)
Scientific conferences		8	13	160%
Industry & Standard conferences		3	12	400%
Policy conferences		5	10	200%
Research Journals		3	8	230%
Media Events		2	3	150%
Courses, vidéos, ressources		5	8	160%

D6.3 Dissemination Report

OpenPGP.conf

Cologne, September 8+9, 2016

NEXTLEAP and Automatic end-to-end encrypted emails

Holger Krekel

Email providers form the largest open federated network for social identification and messaging although there never was a shortage of doomsayers during this millennium. Providers and email technology developers can now play a pivotal role in both bringing about automatic end-to-end email encryption and bootstrapping and in anchoring other decentralized platforms. While there are some open research questions we are not alone in considering these goals within practical reach. Decentralization efforts also involve techno-social questions and perspectives such as how to empower communities to run their own privacy-preserving communication infrastructures. We sketch our planned open source and collaboration efforts regarding decentralized messaging. We place special emphasis on the role of providers who are to mediate public keys between users and on related social and technical accountability practises. Through this report and our prospective open source activities embedded within the EU-funded NEXTLEAP research project we wish to contribute to a privacy leap for email, more decentralized messaging and more community-operated infrastructures.

Holger Krekel is member of EU projekt NEXTLEAP.

Blockchains and the Web

A W3C Workshop on Distributed Ledgers on the Web

29–30 June 2016, MIT Media Lab, Cambridge, Massachusetts

Many projects and companies are looking at ways to use the Bitcoin blockchain or other public or private distributed ledgers, to record an immutable timestamped public record that can be independently verified by any stakeholder.

What does this mean for Web technologies, beyond payments? What emerging capabilities could blockchains enable for the Web, such as distributed identity management? Conversely, should features be added to the Web Platform and to browsers to enable blockchain use cases, such as a JavaScript blockchain API to write to blockchain nodes? With the proliferation of different approaches and technology stacks (like Bitcoin, Ethereum, and Hyperledger), is there a need for interchange formats, protocols, or APIs to share transaction data across services and stacks or between public and private networks? What will help Web developers to take

1 Important Dates

9 June 2016:
Deadline for submission of expressions of interest and position statements

12 June 2016:
Acceptance notification and registration instructions sent

15 June 2016:
Program announced

iGmena Summit 2016: Together for a free and open Internet

Update: see the iGmena Summit 2016 press release here!

Since its inception in 2012, iGmena has been on the forefront of developing and reinforcing knowledge as well as building capacity on Internet governance in the Middle East and North Africa (MENA). Over the course of four years, iGmena has successfully implemented a range of projects, including the Internet Policy Analyst program (IPA), the Internet Legislation Atlas (ILA), the Click Rights initiative, regular iGmena Hangouts with policy experts, iGmena alumni, and grassroots activists, and local roundtables throughout the MENA region. In order to accomplish this, the iGmena team has received tremendous support from a range of stakeholders since the start of the program, which culminated in iGmena Summit 2016 – held at Cogite Coworking Space in Tunis, Tunisia, from 30 September – 2 October 2016.

We invited these stakeholders, which includes our alumni, local partners, program contributors, and other regional collaborators, to the Summit in order to take stock of the work we have done so far, reflect on iGmena's achievements, and learn from their experience with the program so we can create a more effective and sustainable program. Over three days, more than 75 human & digital rights activists, journalists, technical experts, nongovernmental organizations, Internet governance professionals, and other stakeholders came together – many meeting for the first time in person – to share their work with the community, reflect on the achievements of the program, and formulate relevant steps and strategy for the next four years. This included sharing their perspective about the program openly with the community, discussing how

NEXTLEAP

Berkeley Center for New Media

HTNM: Technology, Space and Reason with Bernard Stiegler Revisited

Posted on 17 October, 2016 in **Event Related Posts**, **News**

D6.3 Large audience events

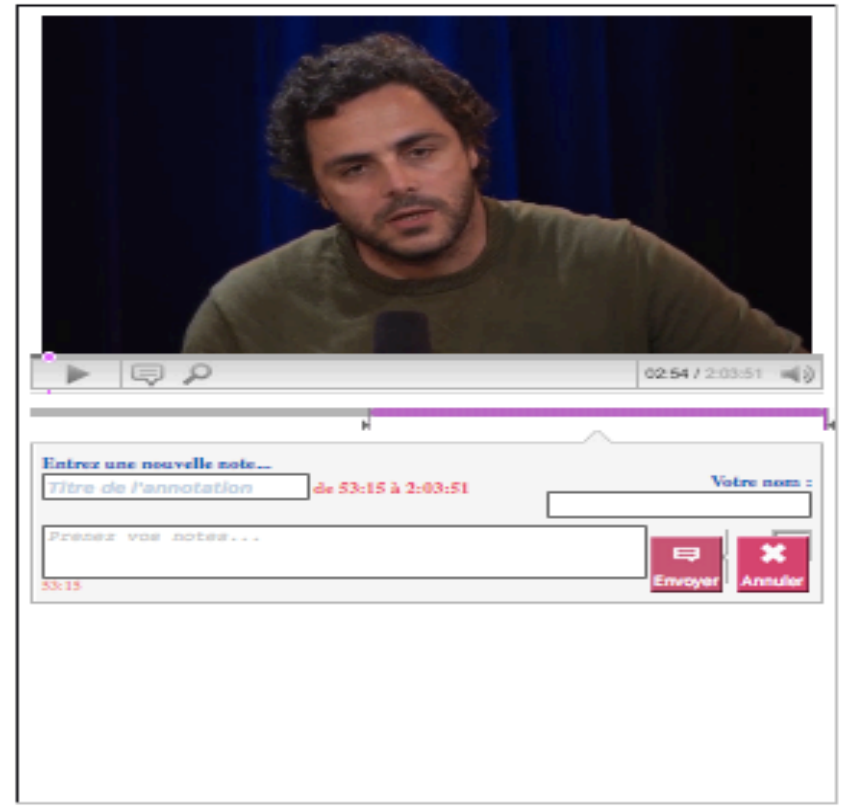
With EuroCrypt 2017

NEXTLEAP

18:30 Panel

This panel will discuss both the possibilities that applied cryptography can help preserve fundamental rights in an era of mass surveillance. We'll look at the political history of the field of cryptography, the subversion of cryptographic standards by the U.S. government, and the challenges facing cryptography due to quantum computing. Then we'll focus on the necessity of usable cryptographic and privacy-enhancing technologies given the lessons of Arab Spring in 2011 and the challenges facing Europe in the coming year. The panel will feature both activists and cryptographers in order to open a dialogue between them.

Moderator: Harry Halpin



Slim Amamou

Tunisian Blogger/Activist, former Secretary of State for Sport and Youth post-2011 revolution

Philip Rogaway

University of California, Davis, Author of "The Moral Character of Cryptographic Work"

Moti Yung

Snapchat, inventor of cryptovirology and kleptography

Daniel Bernstein

University Illinois/Eindhoven, designer of Curve25519

Tanja Lange

University Eindhoven, Project co-ordinator of PQCRYPTO (Post-Quantum Cryptography)

Fabrizio Sestini

Collective Awareness Platforms, European Commission DG CONNECT

EVENEMENT

Revoir la soirée «Quand ils sont venus chercher Assange»

— 10 juin 2016 à 18:35 (mis à jour le 21 juin 2016 à 16:08)

Dimanche, 20h30, en direct sur Mediapart. Soirée de soutien à Julian Assange

17 JUIN 2016 | PAR LA RÉDACTION DE MEDIAPART | BLOG : LE BLOG DE LA RÉDACTION DE MEDIAPART

Depuis le 19 juin 2012, le fondateur de WikiLeaks vit reclus dans les locaux de l'ambassade d'Équateur à Londres. Nous diffusons dimanche, à partir de 20h30, en accès libre et en direct, la soirée de soutien organisée par l'Institut de Recherche et d'Innovation et Ars Industrialis en partenariat avec le Centre Pompidou et Libération. Parmi les nombreux invités : Bernard Stiegler, Edgar Morin, Edwy Plenel ou encore Patti Smith et, bien entendu, Julian Assange.

32 COMMENTAIRES | 25 RECOMMANDÉS | A + A -

CRYPTODESIGN

CRYPTO DESIGN AWARDS

The Deep Web evokes images of an underworld, the locus of shadow economies where illicit trade takes place that cannot bear the light of day. The Deep Web is much more than an online black market teeming with illegal activity. In fact, the Deep Web contains an estimated 96% of all the content to be found circulating online. It is one of the remaining bastions of individual privacy against corporate and governmental snooping and data mining, a place where anyone can remain anonymous.

The iceberg metaphor affects popular understanding of the Deep Web, as the inaccessible dangers of the murky "underwater" world. This Crypto Design Challenge is a shout out to artists, designers, researchers and visionaries to create a new images and conceptualizations of the Deep Web and related topics.

On the 25th of November, we explore such new imagery with designers, artists and researchers at the *Crypto Design Awards* in Paradiso, Amsterdam. We exhibit the nominated submissions, and a professional jury will choose the winner of the Crypto Design Award (€1250). The audience can also vote on their favorites for the Audience Award of €750!

Confirmed speakers include: Ingrid Burrington (Networks of New York), Harry Halpin (W3C), Luna Maurer & Roel Wouters (Studio Moniker), Constant Dullaart, Stefan Schäfer, Hendrik-Jan Grievink (Next Nature Network), David Gauthier, Metahaven, Cryptokids (Waag Society), Tijmen Schep (SETUP Utrecht) and Marjolijn Ruyg. The moderator is Josephine Bosma.

SPEAKERS AND PERFORMERS

Ingrid Burrington - Taking Apart A Time Machine

Ingrid Burrington writes, makes maps, and tells jokes about places, politics, and the weird feelings people have about both. She's the author of *Networks of New York: An Illustrated Field Guide to Urban Internet Infrastructure.* Her writing has also appeared in *The Atlantic, Fusion, The Nation,* and *e-flux-journal.* She lives on a small island off the coast of America.

Décrypte et Glitch ta vi(ll)e

#CryptoPartyCamp

27-28-29 octobre 2017

Dans le cadre du festival ROUXTEUR en lien avec la biennale Nemo, nourri de parcours artistiques, immersifs et interactifs, à Maïns d'Oeuvres, St-Ouen, l'Institut de Recherche et d'Innovation du Centre Pompidou engagé dans le projet européen NextLeap propose un #CryptoPartyCamp, un mix entre l'UNconference, le Barcamp et la Cryptoparty.

Inscription gratuite

vendredi 27 octobre - Unconference - 14:00-19:00

samedi 28 octobre - Unconference - 15:00-23:00

dimanche 29 octobre - CryptoParty - 14:00-19:00

isabel chiara / @bethychiara / @TransmediaReady

A travers du hack, du glitch, du diy et du bricolage, montrons qu'il est possible de fournir à chacun des instruments pour aller vers des pratiques numériques autonomes et décentralisées.

RENCONTRER / DISCUTER, témoigner, demander, sous la forme de micro ateliers ouverts à tous, à vraiment tous : experts, artistes, citoyens, apprenants et bidouilleurs. L'aspect informel et libre est facilité par une équipe de trans-médiateurs.

Les objectifs des ateliers sont de penser et construire des outils et pratiques autour des problématiques de plateformatisation croissante de l'Internet, de disruption des mondes urbains, dans des visées d'auto-défense numérique citoyenne et d'auto-détermination de chacun dans son rapport aux technologies.

REFLECHIR / EXPERIMENTER, jusqu'au prototype éventuel autour de l'auto-défense numérique. Fabriquer des protos ou outils (par exemple, créer une boîte à outils sur un serveur avec un index et un glossaire qui s'adresse à tous).

INSPIRER / FAIRE, avec une réflexion citoyenne ouverte dans un but de capacitation, de production de savoirs, et d'éducation populaire. Exemple de sujets et thèmes d'ateliers (l'improvisation est aussi possible et recommandée ;-) :

- Les pratiques d'émancipation numérique, l'identité numérique ("privacy"),
- La maîtrise des données, notamment par les élèves dans les classes de collège et lycée,
- Les droits et protocoles de l'Internet, la décentralisation,
- Code, encodage, chiffrement, cryptage,
- Les nouvelles plateformes coopératives
- Vos sujets à vous ... (préparés ou improvisés)

19 ET 20 DÉCEMBRE 2017. CENTRE POM

Bêtise et intelligence artificielles

SESSION 1 : ARTIFICAL INTELLIGENCE, ARTIFICIAL STUPIDITY AND THE FUNCTION OF CALCULUS

TUESDAY, DECEMBER 19, 2017

MORNING

with

10H : BERNARD STIEGLER, PHILOSOPHY(IRI)

10H45 :DAVID BATES, HISTORY OF SCIENCE (BERKELEY)

11H30 : GIUSEPPE LONGO, MATHEMATICS AND BIOLOGY (ENS)

12H15 : LAURENCE DEVILLERS (LIMSI/CNRS).

SESSION 2 : DATA ARCHITECTURES AND THE PRODUCTION OF KNOWLEDGE

TUESDAY , DECEMBER 19, 2017

with

14:30 : ANDRÉ SPICER (UN. OF LONDON)

15H15 : BENJAMIN BRATTON (SAN DIEGO UNIVERSITY)

16:00 : CHRISTIAN FAURÉ (OCTO TECHNOLOGY)

17H : YUK HUI (LEUPHANA UN.)

17H45 : RAND HINDI

D6.5 Education/contribution

NEXTLEAP D6.5 Seminars Objectives

- Developing Digital capabilities (Sen and human rights)
- Opening the black-box (understanding digital organology and its social and political impact)
- Individuation and capacitation (ind/group, attention ecology, contribution/participation)
- Categorization and knowledge (vs. skills) in decentralized context (commons, learning territories)
- Communication and Trust (personalization, usability)
- Certification and Truth (black-box, fake news)

NEXTLEAP D6.5 Online contribution objectives

- From Legal organology of Net Rights
- To digital hermeneutics of decentralized and encrypted systems

NEXTLEAP D6.5 Nextleap Seminar

NEXTLEAP Home Seminars Highlights About Results

Decrypting Algorithms (2017)

28.03 What is "good encryption"? A pragmatic turn from a tool-centered to a user-centered approach
Ksenia Ermoshina (CNRS), Francesca Musiani (CNRS), Mykola Kostynyan (Digital security trainer and expert, ISCproject)

19.04 Cryptography and Usability
Joseph Bonneau (Standford University), Nadim Kobeissi (INRIA), Ksenia Ermoshina (ISCC/CNRS)

18.05 Decentralized systems and new urban territories
Bernard Stiegler - IRI, Franck Cormerais - Bordeaux-Montaigne University, Etudes Digitales, Julien Rossi - UTC

28.06 Decentralized certification and blockchain systems
Christian Fauré (OCTO Technologies, Ars Industrialis), Adli Takkal Bataille (La voie du Bitcoin), Lyse Brillouet (Orange Labs), André Reinald (PeerStorage, former Mozilla)

What is "good encryption"? A pragmatic turn from a tool-centered to a user-centered approach

who

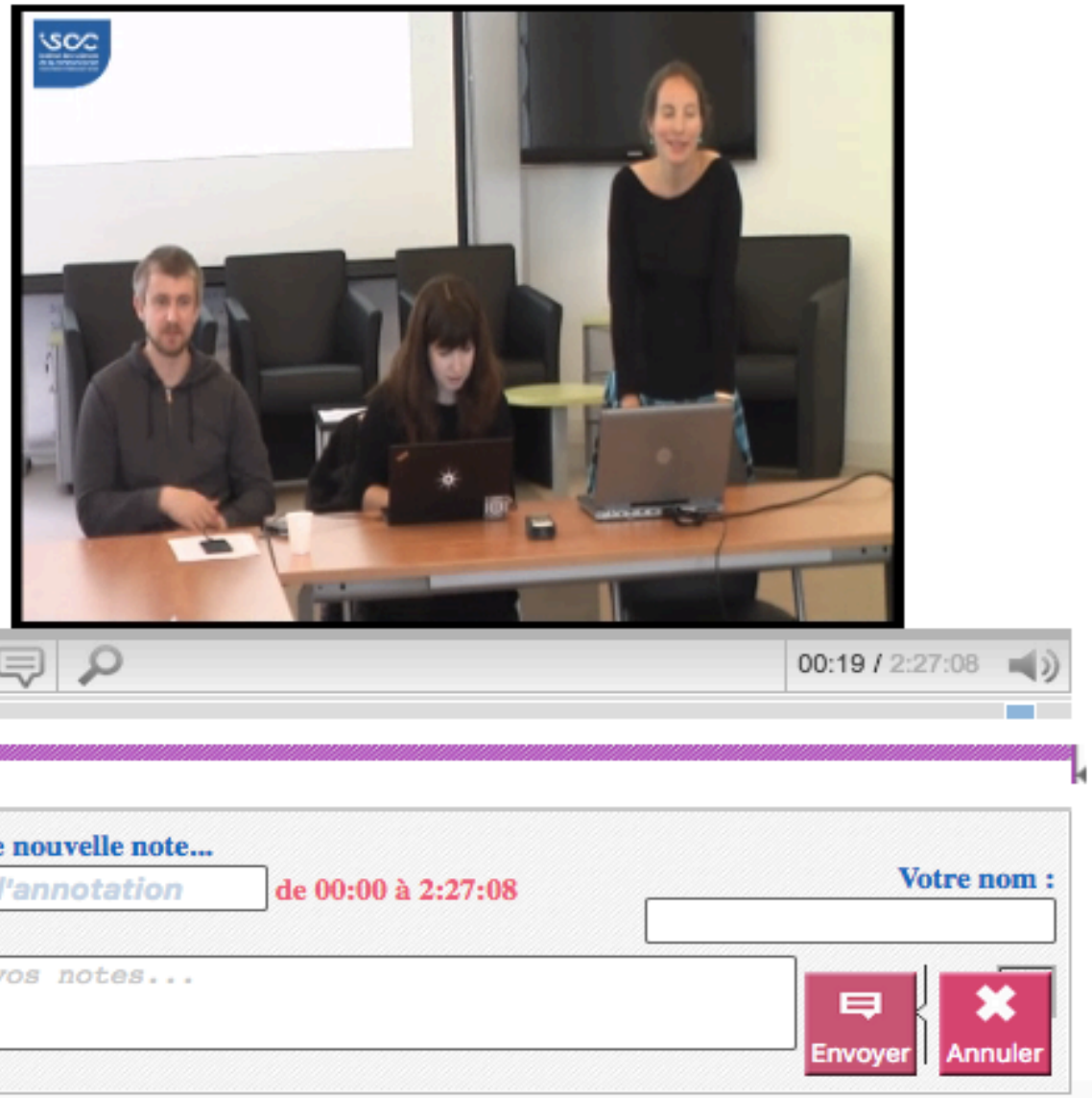
- Ksenia Ermoshina (CNRS)
- Francesca Musiani (CNRS)
- Mykola Kostynyan (Digital security trainer and expert, ISCproject)

when

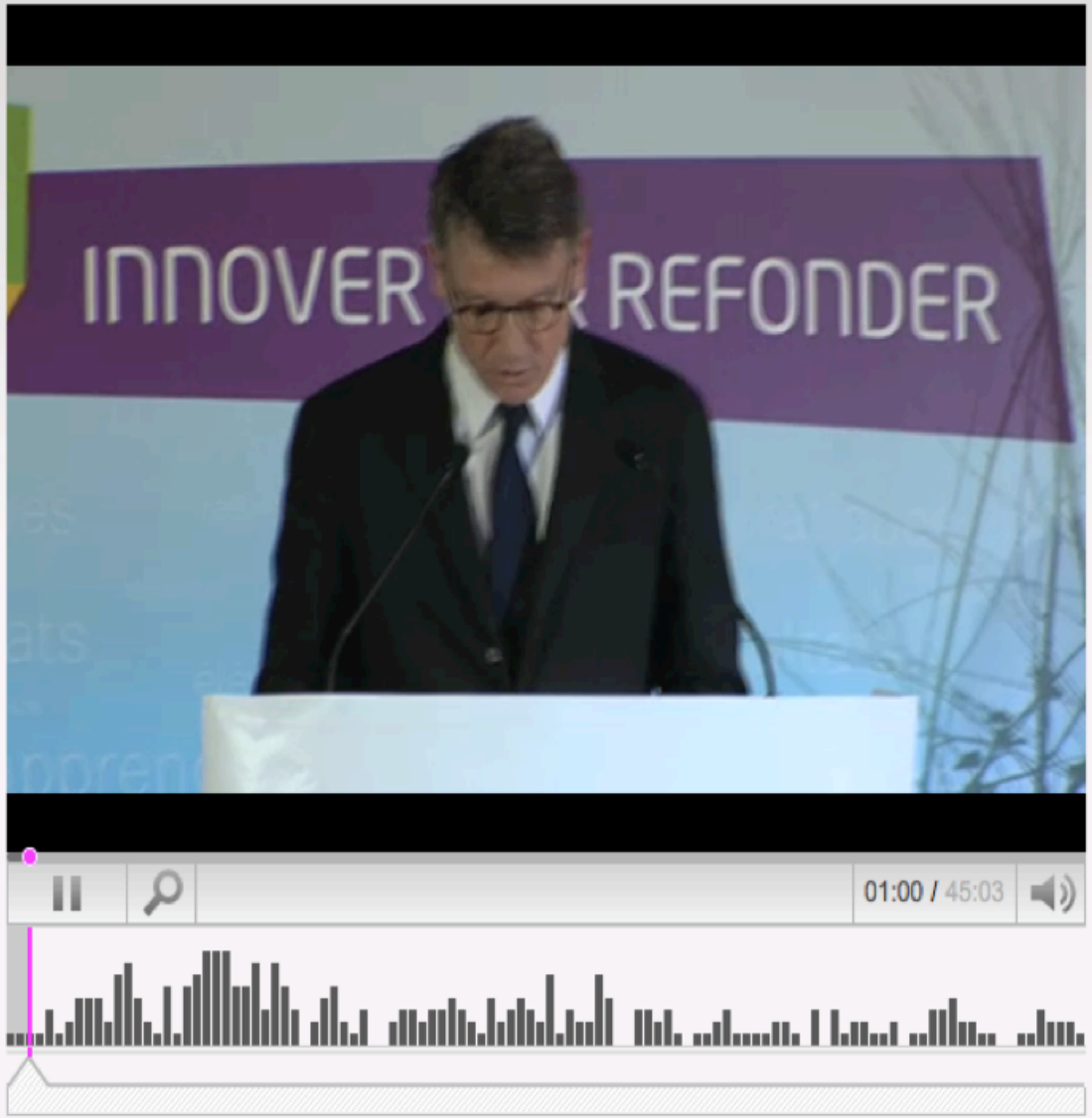
28.03.2017 14:00-17:00

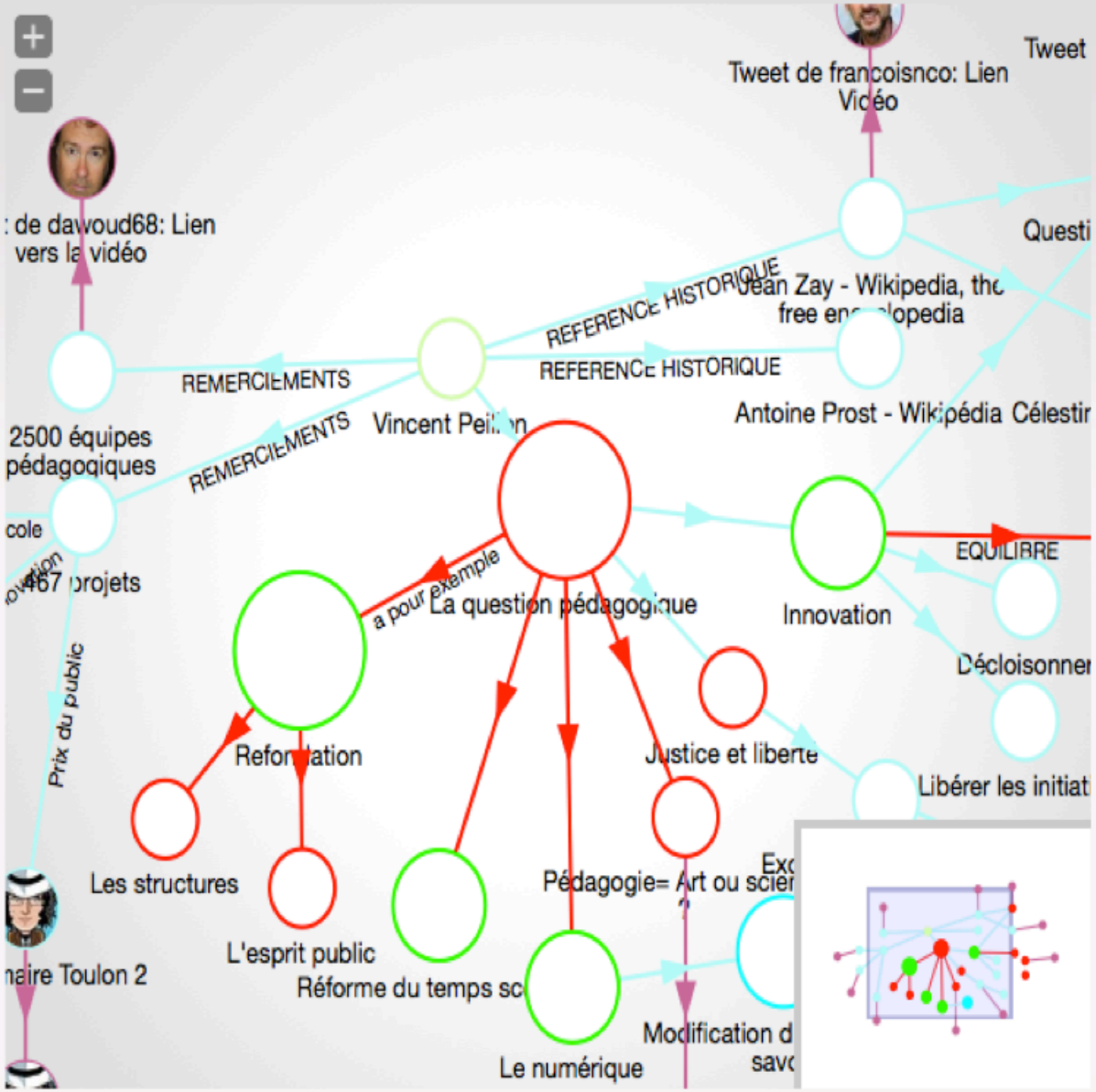
where

Institut des Sciences de la Communication
Salle de conférences (RdC)
20 rue Berbier-du-Mets
75013 Paris



Journées de l'Innovation 2013, Intervention du ministre de l'Éducation nationale et remise des prix de l'innovation





NEXTLEAP D6.5 Crowsourcing Net Rights issues

- Confronting Legal and Technical info, opinions, advises
- Selection of sources (open to contribution)
- Web annotation protocol
- Mind mapping and synthesis of exchanges
- KIALO controversies

NEXTLEAP D6.5 Crowsourcing Net Rights issues

- Internet access as a human right (code is law)
- Internet Rights and Principles (2010-2015) proposed 10 rights: Universality, Social justice, Accessibility, Expression, Privacy, Security, Diversity, Equality, Standards, Governance
- Internet Governance Forum (blockchains and platform reponsabilities)
- French Parliament report (2015, 100 recommendations)
- Italian Declaration of Internet Rights (2014-2015)
- Magna Carta for the Web (2015)

Net Rights

The goal of this project part is not to write a new legal contribution to net rights but to analyze how they may be re-interpreted and modified by decentralized and crypto-based systems. To achieve that aim, we will set up a contributive categorization on Net Rights and augment existing corpus with links to related technologies and experts point of views.

Our plan is thus to experiment with a contributive Forum over Net Rights and related Decentralized and crypto-based systems using text annotation, categorization protocols and contributive mindmapping. The first step is to collect previous contributions on Net Rights and related systems.

If you want to participare, here is a quick tutorial about hypothes.is.

Documents

The following documents are starting points for a discussion and interpretation of a global framework of Net Rights. They embed the Web Annotation system proposed by hypothes.is. You can add page notes and annotations to the NextLeap group but don't forget to set the privacy setting to share them with the group.

- Web We Want
- The charter of human rights and principles for the internet
- Rapport du Conseil du Numérique
- Digital Charta

Science articles

- Degrees of Freedom, Dimensions of Power
- Internet Bill of Rights
- Caring about the plumbing

Categories

- Type of right (legal category)
- Title
- Source/inspiration
- Description
- Other References
- Interest for decentralized systems
- Interest for encryption
- Other technologies of interest
- Communities involved
- Lobbies
- Other comments
- Tags

16 februari 2017 19:24
Door David Korteweg

English
Geheime diensten

DUTCH HOUSE OF REPRESENTATIVES PASSES DRAGNET SURVEILLANCE BILL

On Tuesday February 14, 2017 the bill for the new Intelligence and Security Services Act was passed by the Dutch lower house. Despite being met with serious opposition from experts, regulators, civil society, political parties and citizens, the revised bill passed virtually unchanged from the proposal submitted to the lower house. It's beyond disappointing that a bill with such momentous consequences is rushed through the lower house with such relentless determination.

How we got to this point? Read up on the history of this bill.

Political expediency trumps sound legislation
Political expediency, rather than sound legislation that would actually protect citizens, seems to have persevered. After publishing the draft legislation online for consultation in July 2015, cabinet took their time to revise the poorly received draft legislation. However, when the revised bill was submitted to the lower house late last year, suddenly time was of the essence, and the legislative process needed to be hastily concluded before the elections in March.

Despite being pressed for time, various opposition parties fought tooth and nail to amend the flawed bill. Unfortunately, most amendments failed as coalition parties closed ranks around the Dutch Minister of the Interior. So what are the bill's biggest flaws?

From targeted to bulk data collection
Most importantly, the controversial new law will allow intelligence services to systematically conduct mass surveillance of the internet. The current legal framework allows security agencies to collect data in a targeted fashion. The new law will significantly broaden the agencies' powers to include bulk data collection. This development clears the way for the interception of the communication of innocent citizens.

This law seriously undermines a core value of our free society, namely that

Debates

need:expertise
Use this tag when you need an expert advice about a topic

need:discussion
Use this tag when you want to start a discussion about a topic

need:collective_action
Use this tag if you think that something could be done about that with a bit of collective action

need:reference

controversial

+glossary
Add the highlighted text to the collective glossary. Use this when you find terms that are important for the understanding of our issues. e.g. "thread model".

++
approval

--
disapproval

??
ask a question

==
add a reference/source

Categories

This is the list of tags we are going to focus on in this studies.

decentralization
encryption
net right
activism
industrial lobby
surveillance
political threat
technology

Starter

The charter of human rights and principles for the internet

Internet Rights and Principles Coalition

Open with hypothes.is

Research into Human Rights Protocol Considerations

Human Rights Protocol Considerations Research Group

Open with hypothes.is

Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique

Conseil National du Numérique

Open with hypothes.is

Digital Charta

Die Zeit

The Digital Charta is a German proposal of Net Rights. There is also an available english version

Open with hypothes.is

Web We Want

Tim Berners Lee

Open with hypothes.is

Article 19

Open with hypothes.is

STS

The Black Stack

Benjamin Bratton

This text is a shorter of Bratton's book "The Stack". This is an interesting starting point to understand net rights issues from

Degrees of Freedom, Dimensions of Power

Yochai Benkler

Internet Bill of Rights

Francesca Musiani

Open with hypothes.is

Debates

need:expertise
Use this tag when you need an expert advice about a topic
need:discussion
Use this tag when you want to start a discussion about a topic
need:collective_action
Use this tag if you think that something could be done about that with a bit of collective action
need:reference
controversial
+glossary
Add the highlighted text to the collective glossary. Use this when you find terms that are important for the understanding of our issues. *e.g.* "thread model".
++
approval
--
disapproval
??
ask a question
==
add a reference/source

Categories

This is the list of tags we are going to focus on in this studies.

decentralization
encryption
net right
activism
industrial lobby
surveillance
political threat
technology

TLS Client Authentication - BrowserAuth.net

cation About the Author TLS Client Authentication Traditionally, TLS Client Au

Iness21@hypothes.is - 4 months ago #
So basically with TLS the user Authentication is not possible ?

encryption

RFC 4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)

ertificates in the chain.) 4. TLS Extensions for ECC Two new TLS extensions are d

Iness21@hypothes.is - 4 months ago #
The Ellipitic Curves cryptography emplemented in TLS

Foundations of Computer Security - Lecture 53: Digital Signatures

oved and re-used.Can we define a mechanism for signing a document digitally thathas analogous characteristics?Lecture 53: 2Digital SignaturesD

Iness21@hypothes.is - 4 months

organize:howto [CryptoParty.]

taniki@hypothes.is - 5 months ago #
crypto-party_ressource
community organization

Basic Security Guide (Tech Solidarity)

taniki@hypothes.is - 5 months ago #
security guide ressource crypto-party

Socialize Uber

tch to Uber's competitor, Lyft. But this approach ignores the fact that Uber's abuses are baked into how "sharing" companies operate, a way of doing business that is shared by its competitors. More important, it misses a way to transform these companies that is right there in front of us: by socializing ownership among their workers. jQuery(document).r

taniki@hypothes.is - 5 months ago #
platform ownership

'Governance in the Real World Is So Fucked:' Lawrence Lessig Is Working on an MMO

taniki@hypothes.is - 5 months

Autocrypt - E-mail Encryption for Everyone — Autocrypt 0.4 documentation

urce of digital identification? Why a new approach to e-mail encryption? Encrypted e-mail has been around for decades, but has failed to see wide adoption outside of specialist communities, in large part because of difficulties with user experience and certification models. Autocrypt first aims to provide convenient encryption that is neither perfect nor as secure as traditional e-mail encryption, but is convenient enough for much wider adoption. The social Autocrypt approach

Iness21@hypothes.is - 5 months ago #
Call for expertise on Decentralization

on our github Autocrypt repo Upcoming events¶ Dec 2016: at 33c3, Hamburg, scheduled talk at the We Fix the Net session and probably a separate one. Jan 2017: a prospective lightning talk from dkg at RealWorldCrypto 2017 in New york Mar 2017: Autocrypt sessions at the Internet Freedom Festival with hackers and users, several Autocrypt-people there. April/May 2017: next Autocrypt unconf-hackathon planned roughly around DE/NL/CH

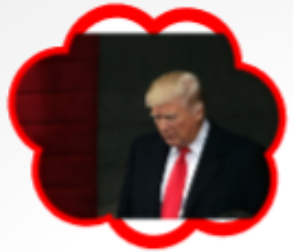
taniki@hypothes.is - 10 months ago #
related to autocrypt

RENKAN > Space

NetRights

Rechercher dans carte

<non authentifié>



Surveillance

Secrecy

Transparency

Data protection

Encryption

NextLeap Video

JPA

geopolitical

Pros

users show concern of where their data is located; high-risk users are more concerned of the client side attacks while low risk users care about the server side

the 'neutrality' of certain countries or the image of neutrality

Cons

Audience: problem with encrypting hard drives and devices because of the new US law
Mykola: HRD are using a technique of fake account showing a fake gmail or facebook when they cross border with Crimea

Everywhere she goes she can lend a laptop. Encryption by physical solidarity network.