Ethique et STIC

Walid Dabbous
DIANA@ZRR.inria.fr
Café-in, 25 février 2016

Plan

- Le projet “BlueBear”
  - BitTorrent, Skype, Tor, Twitter
- Ethique et recherche
- Les “IRBs”
- Le COERLE

BlueBear

BlueBear

BitTorrent™

BlueBear

BitTorrent™

Tor

BlueBear

BitTorrent™

Tor

skype™

BlueBear

BitTorrent™

Tor

skype™

facebook

D’abord BitTorrent

- Intéressés initialement par l’aspect *performance*
- Découverte concernant la vie privée:
  - Identification des adresses IP de 148M utilisateurs
  - Et de 70% des « fournisseurs » de contenus
- Il est possible d’aller *très loin* dans la surveillance du réseau avec un seul ordinateur
- Tor ne protège pas dans ce cas

D’abord BitTorrent

clubic.com

Les chercheurs seraient alors parvenus à collecter en une centaine de jours pas moins de 148 millions d'adresses IP ayant échangé deux milliards de fichiers. La méthode de l'Inria serait, selon eux, beaucoup plus efficace que celle actuellement mise en place par TMG, la société chargée par les ayant-droits de la collecte d'IP pour Hadopi. De même, la technique permettrait d'être exécutée simplement depuis un simple ordinateur de bureau.

Autre constat évoqué par l'Inria, seulement une minorité d'internautes mettent en ligne du contenu via BitTorrent. A la loupe, les 1.000 « fournisseurs » les plus importants représentent 60 % du contenu téléchargé. On voit donc bien vers qui seront tournés les regards de l'Hadopi...

- Il est possible d’aller *très loin* dans la surveillance du réseau avec un seul ordinateur
- Tor ne protège pas dans ce cas

Puis Skype

- Lier une adresse IP à une identité sociale
- Localiser et de suivre la mobilité des 500M utilisateurs de Skype
- Et de ceux de leurs amis (via Facebook)
- Connaître leurs téléchargements (BitTorrent)
- Il est donc possible d'aller *très très loin* avec une infrastructure bon marché (50$ par semaine sur EC2 d'Amazon).

Plus de « Transparence »

- Flux d'information dans les réseaux sociaux:
  - Graphe de Twitter : +500M nœuds, + 24 Md liens
- Mesures de performance à l'accès du réseau
  - Information sur les pratiques de l'opérateur
- Web Tracking
  - Analyse marketing et relance commerciale
- Bcp d'autres thèmes du domaine des réseaux
- Et dans tout le « numérique »

Est-ce « Ethique »?

- Approche « responsable »
  - Pas de divulgation d'information nominative
  - Des tendances et des indicateurs généraux
- Auto discipline des chercheurs
- Toléré dans la communauté Réseaux
- Rejet d'articles par les comités de programme de la communauté S&P

===== Recommendation =====

On the one hand, we should accept it: this is well-explained research about a timely and pervasive Internet-wide privacy issue. The attack is real and this paper convinces us that the attack is real. I could easily see this paper winning best paper award at Oakland, getting broad press attention, etc.

On the other hand, the methodology in the paper raises serious ethical issues.

…..

I don't want to pin the blame solely on the authors of this paper. The community as a whole needs to figure out the right balance between encouraging papers like these (press attention and best paper awards are surely incentives to keep at it) versus making authors actually get approval from their IRB. In this case, I believe the institution in question doesn't have an IRB per se since it is in Europe. Whose responsibility is it to make sure authors go to their ethics committees, or more broadly to make sure research institutions *have* ethics committees that understand computer security issues and they consistently use them?

Recherche à risque

- Atteinte à la vie privée des internautes
  - Suivi de 10.000 utilisateurs Skype sans consentement pendant 15 jours
- Violation des conditions d'utilisation du logiciel
- Utilisation malveillante des résultats de la recherche
- Risque de fuite d'informations sensibles
- Partage de contenus protégés

Exemple des 148M adresses IP

L'anonymat du réseau BitTorrent mis en cause

Le Monde.fr | 08.05.2010 à 10h07

Une équipe de chercheurs de l'Inria a démontré qu'en utilisant plusieurs vulnérabilités du système d'échange de fichiers BitTorrent, il était possible d'obtenir des informations sur l'identité d'internautes

Le cas Skype

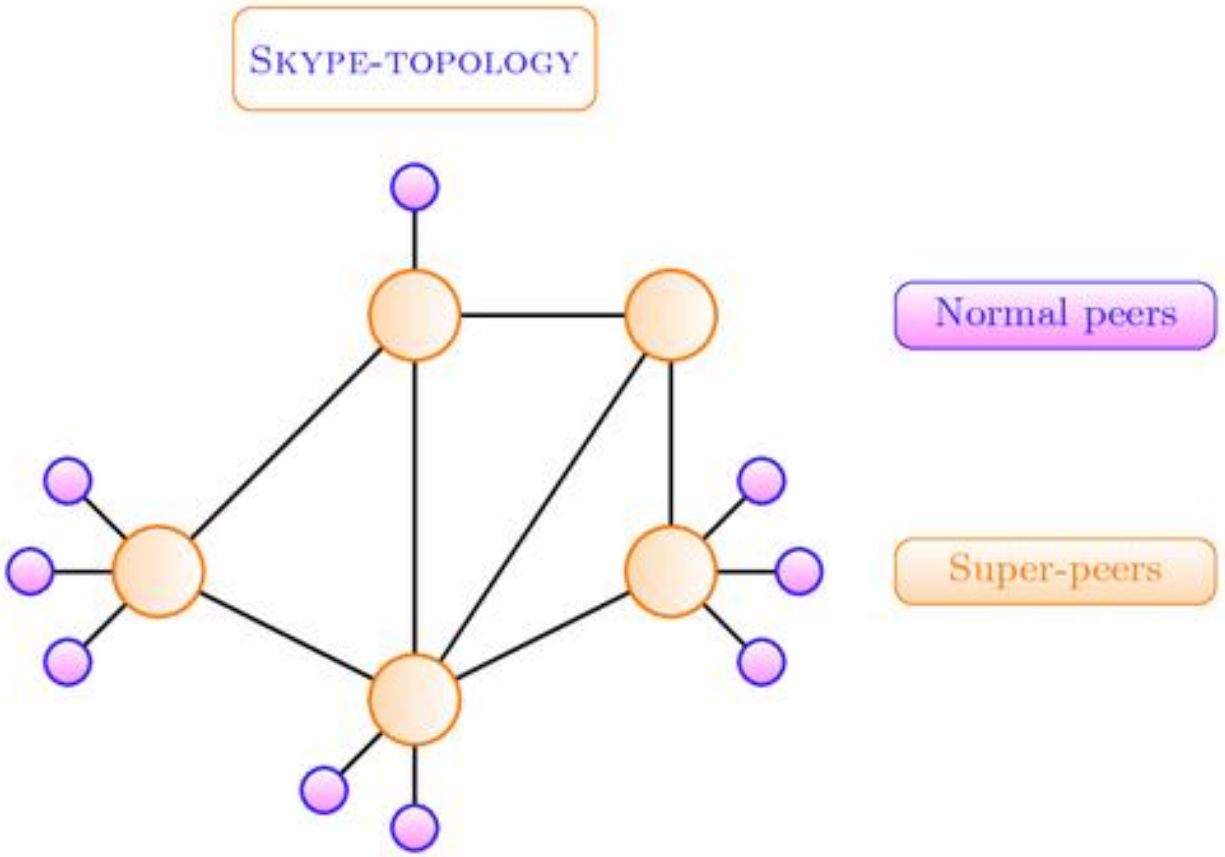
- Etude autorisée par le COERELE (février 2011)
- Contournement des clauses génériques des conditions d'utilisation du logiciel
- Skype puis Microsoft ont été informés des résultats de l'étude dès 2010
- Réponse de Microsoft quelques jours avant IMC en novembre 2011 à Berlin … demandant les « slides ».

ars technica

Skype replaces P2P supernodes with Linux boxes hosted by Microsoft (updated)

Microsoft has replaced P2P Skype supernodes with thousands of Linux boxes.

by **Dan Goodin** - May 1, 2012 7:23pm CEST



Par Guillaume Belfiore
le vendredi 22 janvier 2016

Skype masque par défaut les adresses IP pour éviter les attaques par DDoS

Skype annonce une mise à jour de son application de VoIP qui masque désormais par défaut les adresses IP des utilisateurs.

Il y a quelques années, en novembre 2010, des chercheurs français de l'Inria et de l'institut polytechnique de New York, avaient partagé leurs découvertes sur une vulnérabilité affectant l'application de Skype. Ils ont été en mesure de géolocaliser 10 000 utilisateurs du logiciel via leurs adresses IP. Les chercheurs ont ensuite développé un outil permettant d'effectuer de courts appels masqués vers ces utilisateurs tout en désactivant les notifications et sans apparaître dans le journal des communications.

Cette faille est restée ouverte... jusqu'à aujourd'hui. Si Microsoft a récemment permis de masquer son adresse IP,

Que font les collègues?

- Les Comités de protection des personnes (CPP), loi du 9 août 2004
  - Equivalent français des *ethical research committees*
  - Recherche biomédicale sur l'être humain
- Avis favorables d'un CPP et de l'ANSM avant de commencer une recherche biomédicale
- Pas d'équivalent en France sur le numérique

Institutional Review Board

- Aux US, les institutions disposent d'un IRB
- Mandatés pour valider, superviser et évaluer la recherche impliquant des « sujets humains »
- Enregistrés auprès de l'OHRP
  - Office for Human Research Protections
  - Mis en place par le Department of Health and Human Services, http://www.hhs.gov/ohrp/
- Recherches médicales et « non médicales »
  - comportement humain
  - sécurité informatique
  - aux mesures et expérimentations sur des réseaux informatiques concernent des sujets humains)

Un rôle et une juridiction clairs

A. JURISDICTION OF THE INSTITUTIONAL REVIEW BOARD

The IRB is an administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated. The IRB has the authority to approve, require modifications in, or disapprove all research activities that fall within its jurisdiction as specified by both the federal regulations and local institutional policy. Research that has been reviewed and approved by an IRB may be subject to review and disapproval by officials of the institution. However, those officials may not approve research if it has been disapproved by the **IRB** [Federal Policy §___.112].

http://www.hhs.gov/ohrp/archive/irb/irb_chapter1.htm

Des textes fédéraux

Code of Federal Regulations

TITLE 45
PUBLIC WELFARE

Department of Health and Human Services

PART 46
PROTECTION OF HUMAN SUBJECTS

* * *

http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html

Encadrement des IRBs

- Les IRBs doivent s'assurer que les recherches sont menées :
  - En respectant le 45CFR46
  - En tenant compte des trois principes éthiques mentionnés dans le « Belmont Report »
    - le respect de la personne (*acknowledge autonomy and protect those with diminished autonomy*)
    - la bienfaisance (*do not harm and maximize possible benefits and minimize possible harms*)
    - la justice (*Share Benefits and Burdens Equitably*)

Trois principes éthiques

- Les personnes sujettes à une recherche devraient être libres d'y participer ou pas. Elles doivent donc être informées *en détail* de la nature de leur participation.
- Les *risques* associés à la participation devraient être *moins importants* que les avantages attendus de l'étude. Les chercheurs doivent être attentifs à la suppression, ou du moins la gestion de façon appropriée, des risques de participation.
- Les risques et les avantages de l'étude doivent être distribués équitablement.

Consentement éclairé

- Avant toute collecte d'informations sensibles sur Internet
  - Il faut un « *informed consent* »
- L'usage de la tromperie (*deception*) porte atteinte au principe du respect de la personne
- Mais il est indispensable pour pouvoir mener certaines expériences
  - Phishing

Phishing

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

IRB-approved Phishing attack

Peter Finn, Markus Jakobsson, Indiana University Bloomington, 2007

When academic researchers plan phishing studies, they are faced with the reality that such studies must not only be conducted in an ethical manner, but they also must be reviewed and approved by their Institutional Review Board (IRB). This requirement can be daunting. To begin with, we see that the phishing researcher typically would have to request a waiver of aspects of the informed consent process and request the use of deception when performing an experiment. This is in order to be able to ensure the validity of the study by the use of experimental, fake, phishing attacks that the subject/victim can not distinguish from *real* phishing attacks. The ethical issues relating to waiving aspects of informed consent are controversial and there is little consensus among IRB members and ethicists. Such issues are particularly controversial in the domain of online research, especially phishing research, which is relatively new to IRBs and ethicists in general.

Que dit le 45CFR46 à ce sujet?

- le 45CFR46 116(d) autorise l'utilisation de la tromperie et permet d'accorder une modification ou même une dispense de l'obligation de fournir un consentement éclairé dans certaines circonstances :
  - La recherche ne comporte qu'un *risque minimal* pour les sujets;
  - La dispense ou la modification ne portera pas atteinte aux droits et au bien-être des sujets;
  - la recherche ne peut être entreprise sans la dispense ou la modification, et
  - *le cas échéant*, fournir aux sujets des informations pertinentes supplémentaires *après* la participation.

Médical = non Médical?

- IRBs introduits dans un cadre bioéthique
  - Un grand soin à l'information des « patients »
- Sur Internet, une expérience n'attaque pas directement l'intégrité physique d'une personne
  - l'information des personnes est moins primordiale
- Par contre, la fuite d'informations sensibles peut être préjudiciable
  - le contrôle, l'exploitation, et la sécurisation des données sont eux très importants

Le COERLE

- La direction de l'Inria était très impliquée dans le suivi des travaux (Planète, Madynes)
- Claude Kirchner nous accompagnait à la demande de Gérard.
- Absence d'IRB pour l'Inria, donc on était en zone « grise » (*maintenant en ZRR*)
- Hadopi, CNIL, FSD, ANSSI, SACEM, etc..
- Il nous fallait une « couverture »

Missions du COERLE

- Conseiller le Président d'Inria sur les problématiques éthiques ou légales :
  - en vue d'autoriser ou non des *recherches* ou *expérimentations* ;
  - en vue d'autoriser ou non la diffusion des *résultats* ou de *logiciels* ;
  - en matière d'intégrité scientifique et en particulier en ce qui concerne les questions de *plagiat*.

Saisine du COERLE

- DCR, DS ou membre de la DG
- Via le CPPI dans le cas de dossiers ERC ou ANR
- Relais locaux: un(e) juriste et un(e) scientifique
- Le REP est « tenu informé »
- Dossier :
  - Une lettre présentant le sujet et les risques perçus par son auteur
  - Le formulaire, dûment complété par le REP concernée, en ligne sur l'intranet du COERLE
  - La description du protocole

Le formulaire

INRIA
Comité Opérationnel d'Évaluation des Risques Enjeux Légaux et Éthiques
Demande d'Autorisation pour une Recherche impliquant des Sujets Humains

Nom du porteur du projet de recherche (PP) _____ **No Tél.** _____
(permanent membre d'un projet INRIA)
Nom du co-porteur du projet de recherche (co-PP) _____ **No Tél.** _____

E-Mail du PP _____ **E-Mail du Co-PP** _____

Nom et adresse du contact pour recevoir les documents d'approbation _____

_____

Nom de l'étudiant chercheur _____ **No. Tél.** _____

E-Mail de l'étudiant chercheur _____ @ _____

Cocher la case s'il s'agit d'une recherche médicale ☐ ou non médicale ☐

Avis et recommandations du COERLE

- Expérimentation:
  - Autoriser sans modification
  - Autoriser avec modification
  - Interdire
- Distribution de logiciel
  - Autoriser sans contrainte particulière
  - Autoriser une diffusion partielle ou conditionnelle
  - Interdire

Où en est la communauté?

Workshop on Ethics in Networked Systems Research

Co-located with ACM SIGCOMM'15

Friday August 21st 2015

London, UK

Statement from the SIGCOMM 2015 Program Committee: The SIGCOMM 2015 PC appreciated the technical contributions made in this paper, but found the paper controversial because some of the experiments the authors conducted raise ethical concerns. The controversy arose in large part because the networking research community does not yet have widely accepted guidelines or rules for the ethics of experiments that measure online censorship. In accordance with the published submission guidelines for SIGCOMM 2015, had the authors not engaged with their Institutional Review Boards (IRBs) or had their IRBs determined that their research was unethical, the PC would have rejected the paper without review. But the authors did engage with their IRBs, which did not flag the research as unethical. The PC hopes that discussion of the ethical concerns these experiments raise will advance the development of ethical guidelines in this area. It is the PC's view that future guidelines should include as a core principle that researchers should not engage in experiments that subject users to an appreciable risk of substantial harm absent informed consent. The PC endorses neither the use of the experimental techniques this paper describes nor the experiments the authors conducted.

Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests

Take home message

- La procédure est bien rôdée
- La réponse du COERLE est relativement rapide
- Y a plus qu'à contacter Gérard, Alain ou le/la remplaçant(e) de Sabine