Le cours d'image numérique rend-t-il

NOS ORDINATEURS DANGEREUX ?

le droit à l'image est-il plus fort que
le droit à la liberté d'expression ?

Conférence & débat

auditoire 103-B3
19.mars.12h30

ESA.STLUC.LIÈGE
CVG.MASTER 1
IMAGES NUMÉRIQUES
EXERCICE 2

Objectif

Créer une campagne de sensibilisation
aux traces numériques que l'on laisse
derrière soi, volontairement ou non.

Cible

Les étudiants de St Luc qui
passeront dans l'année à venir.

Techniques

Selon votre propre choix

Publication

Le résultat de nos travaux
sera exposé durant au moins an
sur un mur de l'école,
choisi par vous ensemble.

Sources

Aram Bartholl : ***Forgot your password? (2013)***
Durant l'été 2012 le réseau social LinkedIn.com
a connu une vulnérabilité suite à une attaque.
Ce qui a permis aux attaquant d'entrer dans
le système et de copier les données relatives
aux utilisateurs. Plusieurs mois plus tard,
les mots de passe les plus faibles (4.7 millions)
ont été décryptés et publiés sur Internet.
Aram publie en 2013 une série de 8 livres
contenant l'entièreté de ces passwords.
https://arambartholl.com/forgot-your-password/

Julian Oliver : ***Newstweek (2011)***
Il s'agit d'un boîtier anodin qui une fois branché
à n'importe quel prise électrique, diffuse un réseau
«Free WIFI spot». Les sites d'informations tel que
Le Monde, CNN, BBC et d'autres vu au travers
de «cet innocent Free Wifi» se retrouvent modifier
en arrivant sur l'écran du lecteur. Cela sans que
ce lecteur ne puisse s'en rendre compte.
http://newstweek.com/overview

Julian Oliver : ***With PRISM : The Beacon Frame (2014)***
Un Prisme de verre diffuse sur un écran
des informations obtenue par l'interception
de communication de téléphones portables.
Julian donne forme à une technologie utilisée
par les services de surveillance du gouvernement
américain.
Nous avons tous entendu parler de ces surveillances
massives, dévoilées par Edward Snowden, mais nulle
d'entre nous ne sait à quoi cette technologie ressemble.
https://criticalengineering.org/projects/prism-the-beacon-frame/

Julian Oliver : *Men In Grey (2009-2014)*

Il s'agit d'une intervention urbaine.
Deux hommes en costume gris, attaché-case
à la main se rendent comme tout le monde
à pied au boulot. Néanmoins, leur mallette
renferme un dispositif capable d'intercepter,
sur les réseaux wifi environnant, tout contenu
transmis et non-sécurisé. Tout l'intérêt tient
du fait qu'en plus de ce dispositif astucieux,
les valises sont munient d'un écran sur une face extérieur.
Laissant les passants circonspects de voir que
le message qu'ils viennent de recevoir via un
service peu fiable, se retrouve là. Affiché devant
eux et aux yeux de tous. Que représente un message
privé dévoilé, pour dénoncer des failles dans
la sécurité de tous?

https://criticalengineering.org/projects/men-in-grey/

Kyle mcDonald : *Exhausting a Crowd (2015)*

Le public de cette vidéo de 12h, issue de cameras
de surveillances placées sur Piccadilly Circus à Londre,
est invité à décrire les actions de personnes à même l'image.
Cette pièce est inspirée par le classique de 60 pages
de littérature expérimental de George Perec,
«Tentative d'épuisement d'un lieu parisien»,
écrit sur un banc en trois jours en 1974.

http://www.exhaustingacrowd.com

Kyle mcDonald : *People Staring at Computers (2011)*

Une intervention photographic. Un logiciel
fait-maison installé sur plusieurs ordinateur
de démonstration dans un Apple Store New-Yorkais,
prend des images chaque minute et les téléverses
en ligne. De plus ces photos sont exposées sur
le lieu de capture en plein-écran,
sur tous les ordinateurs.

https://vimeo.com/groups/openframeworks/videos/25958231

Extrait du MANIFEST de Julian Oliver

Il est vital que l'art basé sur la technologie reste un cadre
dans lequel nous pouvons développer un discourt critique à propos
d'aspects allant de la technique au culturelle en passant par
le politique du monde dans lequel nous vivons.
Parfois cela requière que nous ne soyons pas limité par des peurs
exagérées ou par des définitions légals.
Aussi que nous agissions de façon proportionnée et avec conscience
dans nos efforts pour comprendre la puissance des luttes et
les tentions que notre environement technico-médiatique implique.
Parfois cela demande des risques, des risques sans l'intention
de blesser mais seulement pout engendrer un élargissement
du spectre de la critique.

J’ai reçu une liste de question, aux quelles il semblerait qu’une réponse puisse apporter une passification des échanges et pourquoi pas une confiance renouvellée.

La liste exhaustive des scripts et programmes utilisés pour le TP dont vous avez fait mention et ceux que vous avez installés sur les machines.

Les scripts modifiés qui ont étés installés sur les machines (ceux qui tournaient directement sur les machines).

Les procédures et démarches que vous avez développés pour installer ces scripts sur les machines (avez-vous utilisez le mot de passe administrateur pour les installer).

Liste de logiciels n’ayant pas nécissité d’installation :

Automator :

Logicial Apple permettant de programer
des actions automatiques relative à l’interface maxOS.

Terminal & **BASH** :

Langage d’instruction permettant un controle fin
des actions réalisable par vos ordinateurs.

Liste des logiciels installé avec mot de passe administrateur :

SDK JAVA : *https://www.oracle.com/technetwork/java/javase/downloads*

Peut-être le logiciel le plus utilisé au monde.
C’est avant tout un cadre de travail, il est notamment
au centre du fonctionnement de tous les téléphones
et tablette Androïd. Autant vous dire que concidérer
ce logiciel comme malveillant serait totalement loufoque.

FFMPEG : *https://ffmpeg.org/*

Une solution complète et cross-plateform pour
enregistrer, convertir et streamer des fichier
audios et vidéos. C’est une sorte de Adobe Premiere
en mieux et sans interface graphique. De plus,
il est Open Source et ultra utilisé ce qui garanti
que toute intention malveillante ou faille de sécurité
serait déclarée, amandée et corrigée en moins
de quelque jours.

Liste des logiciel installé sans mot de passe adminitrateur :

Swift-Keylogger : *https://github.com/SkrewEverything/Swift-Keylogger*

Logiciel Open source dont je me permet de traduire
la description dont les premieres lignes en disent long
sur les intentions de ses auteurs.
C’est un simple et facile à utilisé logiciel
d’enregistrement de frappe clavier pour macOS.
Il n’est pas prévu pour être malicieux....
Si l’utilisation de ce logiciel cause la mort
de votre premier né ou de quiconque, Je ne suis
pas responsable (sans garantie,).
Pour les personnes comprenants la technique :
Il s’agit d’un projet éducatif.
Note : Ce keyLogger n’enregitre pas les champs
sécurisés comme les mots de passe
du à la configuration EnableSecureEventInput

Si vous ne souhaitez pas faire confiance aux auteurs
de ce logiciel ce que je peux comprendre.
Il vous faudra soit me faire confiance, car sachez que
j’ai moi même parcourut l’entièreté du code,
afin de m’assurer qu’aucun autre processus que celui
que l’on désirait puisse nuire à quiconque à notre insu.

Soit entrer vous même dans le code afin de vérifier par vous même, je vous y invite par le lien au début de cet article.

Liste de logiciel installé sur l'ordinateur de certains étudiant :

Wireshark : *http://www.wireshark.org*

Logiciel gratuit et Open source permetant l'analyse de paquets réseau. Il est utilisé pour visualiser, pour analyser d'éventuel problème de communication sur les réseaux, ainsi que pour l'enseignement du fonctionnement de ces derniers. Originellement appelé Ethereal, le projet a été renommé Wireshark en 2006 pour des raisons relatives aux droits des marques.

Arduino : *http://arduino.cc*

Logiciel de programation et plateforme de prototypage d'interfaces électroniques.
Également Open Source / Open Hardware. Ce logiciel et plusieurs de ses variantes sont massivements utilisées dans le monde de l'art, du spectacle, de la communication et de l'enseignement. Il permet de capter tous types de signaux électrique et d'actionner tout type d'engin électrique et ou électronique.

Liste de logiciel développé par nos soins, fonctionnant sans mot de passe administrateur :

Smile : *https://github.com/oogre/NOS-ORDINATEURS-DANGEREUX*

Logiciel développé en JAVA(processing) permettant d'enregistrer 20 secondes d'une camera webcam toutes les heures. Aucune donnée audio n'est enregistrée.

Onde :

Logiciel développé en JAVA(processing) permettant de convertir la taille des paquets de données circulant sur le réseau wifi, en modulation de fréquence d'un oscillateur audio. Le contenu des paquets n'est ni lu, ni enregistré par ce programme.

Cette liste n'est certainement pas exhaustive, mais néanmoins vous pouvez au travers de celle-ci, sentir l'orientation idéologique ainsi que l'attention que j'ai à pouvoir faire confiance aux différents logiciels que j'utilise et propose à mes étudiants. J'aimerai ajouter que je serai ravi de continuer à développer le sujet. Peut-être au travers d'un cours pour pouvoir rentrer plus en profondeur dans la méthodologie mise en place afin de mettre en oeuvre la réalisation de vos envies de recherches alliant nouveau média et art.

Le nombre exacte de machines infectées et la procédure qui permet d'enlever les spyware et malware qui y ont été installés.

Avant de pouvoir répondre à cette question, il me faut expliciter ici devant vous que je me sens gravement insulté par ces mots, Infecté, spyware, malware... Il en va de ma réputation.
Ce ne sont pas des termes anodins lorsqu'ils sont associés à l'identité d'un artiste dont la pratique et la production tourne autour de la pacification des relations homme/machines.
Un malware est un logiciel conçu dans le but de faire des actions néfaste pour son propre plaisir ou pour en tirer des avantages.
Un spyware est un logiciel conçu pour soutirer discretement des informations à l'un pour les revendre à l'autre. Son but est donc l'enrichissement personnel.
Infecté s'applique dans le cadre d'un logiciel malveillant capable de se répandre au travers de différents moyens dans le but

d'atteindre une cible précise.
Je dois bien vous l'avouer mes compétances et envies ne vont pas jusque là. C'est donc un mot qui, si je l'acceptais, me catégoriserait aux yeux de ma communauté directement dans une catégorie de prétencieux.
En rompant indiscutablement le lien de confiance qui existe entre un artiste et son public, l'utilisation de ces mots met en périle l'avenir de ma pratique.
Que feriez-vous d'un soupson de plagia transformée en acusation publique?

Néanmoins, par soucis de transparence et pour apaiser les personnes les plus apeurées. Voici platement ce qui à été fait.

Le logiciel de capture de vidéo appelé SMILE a été installé sur 2 machines (les ***cvg-wrks-b3-210-70*** et ***cvg-wrks-b3-210-62***).
Hier une seul contenait encore le logiciel. Dans les deux cas, la procédure de démarrage automatique avait été désactivé depuis la mise en place de l'exposition le 18 janvier 2019.
Ils étaient donc désactivé depuis lors.

Le logiciel d'enregistrement de frappe au clavier appelé SWIFT-KEYLOGGER à été installé sur 2 machines (les : ***cvg-wrks-b3-210-55*** et ***cvg-wrks-b3-210-27***). Hier aucun de ces logiciel n'étaient encore actif, d'une part parce que la procédure de démarrrage automatique avait été supprimée, de l'autre parce que le logiciel lui même avait été supprimé. Il restait néanmoins, un archivage de donnée sur l'ordinateur cvg-wrks-b3-210-55 celle-ci correspondant aux dates que voici :

05-12-2018, 06-12-2018, 07-12-2018, 10-12-2018, 13-12-2018, 14-12-2018, 17-12-2018, 18-12-2018, 19-12-2018, 20-12-2018
09-01-2019, 18-01-2019
05-02-2019, 07-02-2019, 08-02-2019, 14-02-2019, 15-02-2019, 20-02-2019, 22-02-2019, 27-02-2019, 28-02-2019
01-03-2019, 14-03-2019

Je les ai copié sur ma machine et je les ai supprimé de l'ordinateur de l'école. Je ne connais pas leurs contenu. Cela ne m'intéresse pas.
Par contre nous allons décider ensemble de leur avenir.
Voulez-vous les voir et donc les rendre public ?
Ou décidez-vous de me faire confiance et je les supprime devant vous ?

Le nombre exacte de personne qui ont eu accès à ces outils et aux procédures qui permettent de les mettre en oeuvre et de récupérer les données.

17 étudiants sont inscrits à mon cours. Nous avons, en amont à cette production, eu une discussion autour des responsabilités et des enjeux de la thématique que nous abordions. Pour résumer, celle-ci nous engageait sur cette pensée : ***«Nous faisons cela ni pour nuire, ni pour plair, juste pour sentir la matérialité des logiciels et plus particulièrement ceux qui nous font peur.»***
Au vu de ma méthodologie d'enseignement qui consiste à accompagner la production de projets individuels basés sur une thématique commune, seul les auteures des projets incriminés par cette affaire on été informées sur les méthodes et logiciels, que certains ont vu comme espions. Et je me répete certainement, tous les étudiants ont été sensibilisés sur les enjeux risqués que nous avions.
La production des 2 projets mise en accusation, sont du chef de deux étudiantes qui, par se biai, on quelque part exploré, leurs propres peur du viol de leur intimité, du à de véritables logiciels malveillants.

Les emails de l'ESA ont-ils été utilisés pour tester les hacks emails présentés? Cette technologie a-t-elle été utilisée durant le TP?

Est-ce que les clés usb utilisées pour la récupération des données proviennent des armoires des classes d'infographie ? (Plusieurs explications ont été données).

Fournir les clés usb et les données qui ont été récupérées à qui de droit pour évaluer ce qui à été récupéré.

De mon point de vue, cette question est hors-sujet, car aucun hack email, ni clef usb n'ont été utiliser lors de nos productions.

Y a-t-il d'autres endroits ou outils physiques qui ont été utilisés pour espionner les étudiants et/professeurs?

Si oui, quels sont-ils (liste exhaustive) et où sont les données récoltées?

Je perçois via cette question, qu'un lien de confiance, que je pensais exister naturellement entre gens passionés, collègues, à été rompu. Je me demande néanmoins, s'il n'a jamais existé? Car apès tout, avec combien de de gens, qui aujourd'hui portent plainte, a-ton seulement eu une discussion. Celle-ci j'en fais le pari, aurait-été la solution, avant d'annoncer publiquement avoir trouvé ***«le responsable de ce piratage»***.

Comment avez vous exploité les données recueillies durant ce TP ?

Les avez-vous diffusées en dehors de la classe de M1 ?

Sont-elles stockées de manière sécurisée ?

Et combien de copies de ces données existe-t-il?

Je vous propose un visionnage commenté d'une vidéo de présentation de nos productions.
Les données ne sont qu'un prétexte. À aucun moment il n'a s'agit de parler spécifiquement de quelqu'un en particulier.
Mais derière ses noms, ces visages, c'est chacun de nous que nous mettions en scène afin de questionner nos peur et nos rêves à propos des ordinateurs et des réseaux,

Aucune donnée compromettante n'a été publiée.
Toutes les données enregistrées avant ou après production des différents supports exposé, n'ont absolument aucune valeur à nos yeux, le sujet est ailleur. Les données collectées ont été misent en scène ou détruitent.

Les travaux résultant de ces « hacks » contiennent-ils des données sensibles ou des données qui permettent d'identifier les personnes hackées?

Si vous le voulez vous en assurer par vous mêmes, je vous propose de vous projeter cette vidéo qui fut présente sur youtube et puis retirée.

De mon intervention, certain attendaient aussi des solutions pour **sécuriser leurs ordinateurs**.

> Je n'en ai pas, hormis peut-être celle qui est de faire à intentionnellement confiance en les intentions des développeurs qui fabrique vos programmes.
> Ou faire confiance en les développeurs qui publie leur code afin de les soumettres aux vues de tous.
> Ou de fabriquer vos programmes vous même.

Pour ce qui est des ordinateurs publics, des réseaux publics et de toutes ces choses pour lequels on peut se passer d'apprentissage.

> **Ne leur racontez pas vos secrets**. Vérifiez aussi quels logiciels sont en cours de fonctionnement. Si vous avez un doute sur l'un d'eux, renseignez-vous sur le web. Si vous ne trouvez pas d'information à son sujet n'hésitez pas : **coupez-le!**

Sentez-vous responsable de se qui se trouve sur votre ordinateur privé.
Si quelque chose ne vous convient pas, vous n'êtes certainement pas le seul.
Quelqu'un d'autre a du se retoruver dans le même cas et à certainement développé une solution Open Source **digne de confiance**.

Toujours est-il que, je ne pense pas que l'intention des personnes, certainement ici présente, ayant porté plainte pour «viol de droit à l'image» ayent été jusqu'à vouloir nuire à quiconque.
Et pourtant, **j'affirme, que prit de panique et sur de simples accusations, mon nom et celui d'Olivier Evrard ont été sali.**
Les mots et les méthodes de communications employées ont été à charge de notre culpabilité, sans même avoir pris la peine de nous entendre, de nous confronter aux accusations.

Là où certains porte plainte pour **une vidéo au contenu insignifiant vue 30 fois sur youtube** et supprimée dans l'heure des premiers émois.
Notre accusation, même si elle se démonte à l'issue de cette réunion, est arrivée sur **le téléphone et la boite mail de peut-être 1500 personnes** qui nécéssitent de **pouvoir nous faire confiance**.

Il ne doit s'agire que de maladresse ou d'un manque d'habilité en ce qui concerne les interactions humain/humain. Loin de moi l'idée de contre attaquer. Il se trouve que pour ces mêmes erreurs ou maladresses **je vous dois des excuses**.

À refaire, LE point sur lequel je tâcherais d'améliorer cet exercice, est que vous serez tous officielement, peut-être même par SMS, invité à participer au vernissage de l'exposition.

Vincent Evrard,
assistant du professeur Olivier Evrard pour le cours d'Image Numérique en master 1 & 2 de communication visuel et graphique.