Übungsgruppe: Qianli Wang und Nazar Sopiha

Aufgabe 9-1:

1. **Verhalten:**
   Beispiel: Ein großes Beispiel für alle. Im 18. Jahrhundert wurde das Panoptikum erfunden. Sein Hauptmerkmal war der Bau eines enormen Turms in der Mitte der Anstalt. Von dort konnte der, der die Anstalt leitete, jeden Insassen stets beobachten, auch wenn er nicht alle gleichzeitig und immer beobachten konnte. Das Entscheidende an dem Entwurf war, dass die Insassen nicht in das Panoptikum, in den Turm, hineinschauen konnten. Sie wussten also nie, ob und wann sie beobachtet wurden. An dieser Entdeckung begeisterte ihn, dass die Insassen würden annehmen müssen, dass sie zu jeder Zeit beobachtet würden, was sie endgültig zu Gehorsam und Wohlverhalten zwingen würde.
   Und das hat echt einen großen Einfluss, wie gedacht. Später wurde es auch von anderen Psychologen nachgewiesen. Falls die Überwachungsmöglichkeit existiert, verhält man sich anders, als ohne. Das schadet die Freiheit.
   (Quelle:https://www.ted.com/talks/glenn_greenwald_why_privacy_matters)

2. **Meinungen:**
   Beispiel: Bürger in China sollen ihre Meinungen z.B. zur Pressefreiheit, Redefreiheit verbergen, obwohl solche Meinungen nicht gegen Gesetze verstoßen, weil es sehr wahrscheinlich ist, wenn man solche Meinungen explizit auf Internet veröffentlicht, wird man bestraft oder sogar gefangen.

3. **Gefühl, Meinung:**
   Beispiel: Es gibt ein Beruf - der Psychologe. Man darf als Psychologe keine persönliche Geschichte von Kunden erzählen. Das ist eine Wissenschaft und diese Regelung ist nicht einfach so entstanden

b) Es ist sehr schwer, eine klare Linie zwischen Überwachung und Freiheit zu ziehen. Einerseits, wenn Freiheit, dann keine Überwachung. Andererseits, Überwachung kann zur Vermeidung großer Terrorakten führen und ohne ständige Überwachung kann man nicht deutlich sagen, wer ein Verbrecher ist und wer nicht. Für mich ist es besser, wenn meine Daten stark geschützt sind und niemand die angreifen kann, ich verstehe aber, dass es nicht so ist. Ich denke darüber sehr selten, also bewusst fühle ich keine Beschränkungen wegen Überwachung.

Aufgabe 9-2:

FLASH-COOCKIES

a) **Eher nein. Flash Cookies werden normalerweise nicht im Browser, sondern in Filesystem des verwendeten Betriebssystems gespeichert.**
   (**Quelle**:https://policies.google.com/technologies/managing?hl=en)

b) **Flash-Cookies werden von Adobe Flash entwickelt. Das ist ein Plattform, das von mehreren Webseiten benutzt wird. Technologien haben sich weiterentwickelt, Browser games u.s.w. und es gibt "non-executable data" (authentication information, game high scores or saved games, server-based session identifiers, site preferences, saved work, or temporary files), das für Browser nur als Belastung gilt, wenn es gerade auf der Webseite gespeichert wird, deswegen speichert Adobe Flash diese Information auf Hard Driver. Mit Flash Player können nur Inhalte, die von genau derselben Website-Domain stammen, auf Daten zugreifen, die im lokalen Speicher gespeichert sind**
(Quelle: https://en.wikipedia.org/wiki/Adobe_Flash_Player)

c) **Nein, nicht so dringend. Einerseit, es gibt schon manche Browser wie z.B. IE8 und Chrome, die den Benutzer Möglichkeiten anbieten alle browsing Daten zu löschen(Cookies, Flash Cookies, plug-in data, data stored on device by Adobe Flash Player...). Aber andererseits, privates Bedenken ist ein großes Problem. "Local shared objects can be used by web sites to collect information on how people navigate them, although users have taken steps to restrict data collection."**
(Quelle: https://en.wikipedia.org/wiki/Local_shared_object)

CSS&HISTORY

a) **The principle is that in CSS there are 4 pseudo-classes which are used to define style of links → a:link, a:visited {color: #00FF00}, a:active, a:hover. Hackers can get histories by using Javascript and CSS, called "Javascript/CSS history hack", by using in Dom defined methode: getComputedStyle(). By using CSS, the developers can define the style of visited hyperlinks. With Javascript, developers can get all CSS information of any elements so that the visited links can be easily recognized.**
(Quelle: https://developer.mozilla.org/en-US/docs/Web/API/Window/getComputedStyle, https://github.com/acgotaku/WebSecurity/blob/master/docs/content/XSS/CSS-history-hack.md)

b) **It depends on the compatibility of Browser(for each browser, the vendor prefixes can be different) and the limit of getComputedStyle() API**

c) **Every technology has its pros and cons. It is very useful to know what I have clicked and what I haven't. We can not implement those features without obtaining information about what's been clicked. Dom concept gives a lot of information about user action, but it is mostly used for handling and proper reactions. We think if this concept still works and even develops, it is well defined. We can't avoid misuse.**

BITMESSAGE

a) **We propose a message transfer mechanism similar to Bitcoin's transaction and block transfer system but with a proof-of-work for each message. Users form a peer-to-peer network by each running a Bitmessage client and forward messages on a best-effort basis. In order to send a message through the**

network, a proof-of-work must be completed in the form of a partial hash collision. The difficulty of the proof-of-work should be proportional to the size of the message and should be set such that an average computer must expend an average of four minutes of work in order to send a typical message.

It takes a couple of minutes(in average 4 mins) to send a simple text email via bitmessage and a couple of seconds via Gmail (for example), so it is expected the data traffic to be increased more than 60 times. But it is only for private messaging. Not to consider corporate messages and spam. Because to send the same corporate message to n users via Bitmessage you need to establish n connections, whereas via email makes it as simple as to send a single email. So in those cases it rises dramatically and can not be even close predictable. If the whole world begins to use Bitmessage, the term of "Spam" will be restricted or even gone, because it will take too much effort.

"Include extra bits in Bitmessage addresses and require that those bits be included in a message, thus proving that the sender has the Bitmessage address. Including an extra two bytes of data in a Bitmessage address would make the address 9% longer but would make spamming a user require 65536 times as much computing power. Bots who crawl the web looking for Bitmessage addresses would thwart this option."

(Quelle: https://bitmessage.org/bitmessage.pdf)

b) **If we will add an extra node for the group of members, it will cost a lot to send the emails for the first time, but after this process has been carried out once, connecting to the destination stream a second time would be trivial as the sending node would now already have a list of nodes that are in the destination stream saved. So it will simplify the company communication and we should consider only the extra time for sending a message. So it won't be that enormous anymore, but still much bigger.**

c) **For a), normally it takes just a few seconds to send messages via email. In a few cases the message could take as long as 5 days to complete its trip from sender to recipient. It rarely takes more than 5 days as one of the SMTP servers will send the message back as undeliverable. The Email that contains the error message could take 5 days to get back.**
Our assessment is partially precise. We used simplified values without considering the extreme situations to understand the tendency and the possibilities of this technology (which we also learned only today). Besides, Bit Messaging is not very popular and common used, so there aren't enough statistics, tests and comparisons to estimate it more precisely.

Aufgabe 9-3

a) **Zuckerberg(2016): "It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too."**

Bewertung:

The purpose of security is to safeguard privacy. Facebook and its develop-team should have the responsibility to protect our data from obtaining by others improperly and if they can't then they don't deserve to serve us.

Als 2. wir nehmen die erste bekannte Aussage von Mark Zuckerberg(2003): "Issues about violating people's privacy don't seem to be surmountable"

Bewertung: Das ist die Aussage von Zuckerberg im Alter von 19 Jahren, damals hatte er noch gar kein Facebook entwickelt und hat das Problem der Privatsphäre so verstanden. Wie wir sehen können, mit der Zeit hat er seine Meinung geändert und jetzt versucht er und das ganze Facebook mit diesem Problem möglichst gut umzugehen. Oder mindestens versuchen, andere zu überzeugen, dass Facebook sich bemüht.

(Quelle1:https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html)
(Quelle2:https://www.cnbc.com/2019/10/24/19-year-old-mark-zuckerberg-on-privacy-issues-versus-today.html)

b) **Wünschenswerte Auswirkung:**

Weil Facebook so populär geworden ist, hat es offensichtlich viele nützliche Features für Benutzer, wie z.B. Marketplace oder Gruppen nach Interessen.

Ich vermute, dass (fast) alle positive Auswirkungen von Facebook wurden vorgesehen, denn diese Techniken wurden genau dafür gestalten.

Nicht wünschenswerte Auswirkung:

Die persönlichen Daten von Benutzern werden absichtlich ohne Genehmigungen gesammelt, um später die zu verwenden, wie z.B. im Jahr 2016 das Ergebnis der Präsidentenwahl beeinflusst wurde.
(Quelle: http://www.xinhuanet.com/2018-04/10/c_1122660023.htm)

Meiner Meinung nach ist es mittels Technikabschätzung vorher absehbar. Vorher gab es in Facebook keine strenge Beschränkung für Entwickler, dass Sie Genehmigung haben, auf die persönlichen Daten von Benutzern zugreifen zu können, was auf jeden Fall dazu führen kann, dass jemand mit der Absicht persönlichen Daten sammeln wird, um davon zu profitieren.