CONTEMPORARY CYBER-SECURITY TRENDS AND RELATED ETHICAL DILEMMAS (PART 1)

VESSELIN BONTCHEV
vesselin.bontchev@nlcv.bas.bg

DIMITRINA POLIMIROVA
dimitrina.polimirova@nlcv.bas.bg

National Laboratory of Computer Virology, BAS

Abstract

The paper is a review of the various ethical dilemmas created by the contemporary trends in cyber security. No attempt is made to provide the ethical resolution of each dilemma – only the various arguments for and against are described.

Keywords: ethics, ethical dilemmas, cyber security.

1. Introduction

Information technology is a relatively very new and very fast developing area. Some parts of it, like information security, are not very well understood, except by a few experts. Yet they present various problems that pose serious ethical dilemmas. Since the area is so new, the society has not had the centuries to come up with good and widely accepted solutions to these dilemmas.

While we are experts in cyber security, we definitely do not consider ourselves as being experts in ethics. Therefore, in this paper we shall contend ourselves with outlining some of the most important ethical dilemmas related to cyber security, with the various arguments for and against the possible answers to them – without, however, stating which is the "correct" answer from an ethical point of view. We are leaving this decision to the reader.

2. Ethical dilemmas

In this section we shall outline the main ethical dilemmas posed by the various contemporary trends in cyber-security.

2.1. Ransomware

Ransomware (from the words "ransom" and "software") is a malicious program that encrypts the data of the user without their consent and demands the payment of a ransom (usually, in some hard-to-trace virtual currency like Bitcoin) for its decryption. Historically,

the first program of this kind was created by Dr. Joseph Poppe in 1989 but this kind of malicious programs became really widespread once electronic currencies like Bitcoin were created and after the ransomware program known as CryptoLocker was released in 2013 and started grossing several millions of US dollars per day in ransoms. Currently, the creation and distribution of ransomware is a blooming criminal enterprise, costing the world economy billions of US dollars every year.

Currently, thousands of known ransomware programs exist. About half of them contain various cryptographic flaws, which makes it possible to break the encryption and to decrypt the encrypted files of the user without having to pay the ransom. However, none of the really widespread programs of this kind fall in this category. For them, only the author of the program is able to decrypt the data of the victim – and they are willing to do so only after the demanded ransom (which can vary between $300 and $30,000) is paid.

2.1.1. Paying the ransom or not

As mentioned in the previous section, in the vast majority of cases the victim has a simple choice – pay the ransom, or consider the encrypted data lost. There are various reasons why paying the ransom is not advisable on technical, legal, or even ethical grounds.

First, there is no guarantee that the data will be decrypted even if the ransom is paid. While the criminals behind the ransomware operation have interest in keeping a reputation of decrypting the data after payment (otherwise the victims simply will not pay), one should not forget that they are criminals that generally cannot be trusted. In addition, the decryption tool is often provided as a program (instead of simply as a decryption key) – and executing a program coming from an untrustworthy source on one's computer is always dangerous. Furthermore, in some cases either the ransomware itself or the decryptor is buggy and corrupts the files beyond repair. Finally, the criminal organization could have been already shut down by the authorities, meaning that there is nobody available to provide a decryption tool. According to some statistics, in about 20% of the cases paying the ransom does not result in decrypting the encrypted data.

Second, in some cases when the criminals realize that the victim is desperate and has a lot of money, they make additional demands of more money to be paid to them, in order to decrypt the data.

Third, in some countries there might not be a legal way for a company to expense the payment of a ransom. Bulgaria is one such country.

Fourth, by paying the ransom, the victim is essentially financing a criminal organization. Even leaving aside the legal aspects of this situation, it would be ethically questionable to provide funds to people who are likely to use them to further develop their malicious software and to conduct additional distribution campaigns, resulting in even more victims being hit.

However, the decision not to pay the ransom is by far not obvious and clear-cut. For instance, the victim might have a legal and ethical obligation to maintain the integrity and availability of the data that was encrypted. Some examples would include medical records (which, if unavailable, can result in physical harm and suffering of human beings), financial or legal documents (the loss of which could result in serious financial or legal harm to third parties), and so on.

Clearly, there is no win-win solution here. The victim will be forced to weigh the different options and come up with a decision which minimizes the harm caused to others, even if it feels unpleasant. Some additional discussion of these issues can be found in [Jareth, 2019].

2.1.2. Outsourcing the ransom payment

The fact that ransomware attacks have become a widespread problem, combined with the reluctance (or, in some cases, the legal impossibility) of companies to pay the ransom, has lead to the creation of a new kind of businesses. Those are companies that advertise their services as being able to decrypt the data encrypted by a ransomware – for a fee, of course. Such claims are always suspicious, given that the widespread ransomware strains use sound cryptographic methods for encrypting the data – methods, which the current cryptanalytic science is unable to break. And, indeed, in practically all cases it turns out that such companies simply pay themselves the ransom to the criminals, in exchange for a decryption tool, and then decrypt the data of the victim, charging it both for the paid ransom and for the "service" rendered [Dudley, Kao, 2019].

At a first glance, such operations are clearly unethical. The victim contacted the company precisely because it didn't want to pay the ransom to the criminals – yet this is precisely what the company ends up doing. However, the situation is not always so black-and-

white. As mentioned in the previous section, the victim might not be willing to pay the ransom not on ethical grounds but because it has no legal way of expensing it. By offering to pay it on their behalf, the "decryption" company is rendering a useful service. Furthermore, in most cases this company already has considerable experience negotiating with criminals. It might be able to negotiate for a significantly lower ransom amount, to make sure that a decryption tool is indeed provided and it indeed works correctly (and to assume the business and financial risk if it does not). Again, this is a useful service. In fact, insurance companies that provide insurance against ransomware attacks often insist that the insured victim goes through the process of paying the ransom via such an intermediary, because it is more expedient and is often cheaper [Dudley, 2019].

Whether to use the services of such a company is again an ethical dilemma that the victim will have to resolve, based on the particular situation, ethical principles, and so on.

2.2. Surveillance

The past couple of decades saw the rise of the so-called "surveillance capitalism". It involves massive tracking of people's on-line behavior and monetization of the collected data for advertisement and other purposes. While in many cases it makes excellent business sense, it also leads to serious invasions of privacy. Therefore, developments in this area pose important ethical dilemmas.

2.2.1. Advertisements and tracking

Nowadays, users are offered a great multitude of on-line services for free. These include social networks (e.g., Facebook, Twitter, etc.) for social interaction, webmail (e.g., GMail, Yahoo Mail, etc.) for communication, on-line data storage (e.g., Dropbox, Google Drive, OneDrive, etc.), office automation (e.g., Google Docs, Slides, Sheets, and Callendar), and so on. While the user does not pay any money for these services, their upkeep is certainly not free – in fact, their costs are in the billions of US dollars. So, who pays for them?

The reality is that all these services collect data about the on-line behavior of their users and often display advertisements to their users. Even when the services do not display ads to the user directly, the collected data is sold to advertisement companies for better targeting of the people with advertisements elsewhere. According to some studies, targeted advertisements bring twice as much profit as the untargeted ones [Loechner, 2010], [Marotta, Abhishek, Acquisti, 2019]. As the saying goes "if you are not paying for it, then you are the product".

In one particularly shocking case, the advertiser had figured out that a young woman was pregnant just from her on-line behavior and had started showing her relevant advertisements even before her own father knew of this [Hill, 2012].

One the one hand, this constant tracking of every move and interest of the user is a serious invasion of privacy. On the other hand, the user is provided with excellent services for free – services, which would otherwise cost a lot of money and wouldn't be accessible to many low-income people. This poses an ethical dilemma to the software developers – is it ethical to develop such software or not?

2.2.2. IoT data collection

The present trend is to install computer chips to all kinds of consumer devices and connect them to the internet. The internet-connected fridge from 1998 was the first step [Cook] but nowadays there are all sorts of devices connected to the internet – from such things like surveillance cameras and TV sets to ridiculous cases like light bulbs and thoothbrushes. These devices have an extensive view of the behavior of their users. As such, the data obtained from them is invaluable to advertisers [Seitz, 2016]. For instance, a recent study discovered that various smart TVs were sending the user's watching habits to Facebook, Netflix, Microsoft, and various advertising companies [Ren, Dubois, Choffnes, Mandalari, Roman, Haddadi, 2019].

Again, the developers of such devices are facing an ethical dilemma here. On the one hand, internet-connected devices are much more convenient and easier to control for the user (e.g., from a smart phone). Their price can also be lower, given the additional revenue from the sale of user data to the advertisers. Clearly, the users want them, because they sell very well – otherwise the market would have driven their producers out of business. On the other hand, they present a serious invasion of privacy. Also, since their security often leaves a lot to be desired, the can fall victim to hacking and facilitate other, physical crimes against their owners – like burglary, theft, and so on.

2.2.3. State surveillance of social media

During the Obama administration, the US government introduced a new field in their visa application forms, asking the applicants for all the user names that they have used in the popular social networks for the past five years. Filling that field was optional – but the Trump administration made it mandatory. Omitting, or filling incorrect information on a visa application form is a crime in itself.

Furthermore, under the Trump presidency, the US government started making extensive use of the information gathered from the social networks. This new, required field was also introduced in other official documents – like the documents filled by those seeking to obtain refugee status, a green card, or citizenship [Cimpanu, 2019]. In at least one case, a Harward student from Lebanon was denied entry into the USA because of things posted by *other people* in his social network and clearly outside of his control [Keane, 2019]. While this practice is currently in use mainly in the USA, we fully expect it to be widely adopted by most governments around the world.

Again, the implementation of such practices poses a clear ethical dilemma to those charged with implementing them. On the one hand, terrorist organizations make extensive use of social networks for recruiting new members and a government has the full right to screen off potential terrorists and deny them entry into the country. On the other hand, this is a clear invasion of privacy and it is repressive to punish people for what others might have posted on-line if it was something the government didn't like.

2.2.4. Employee traffic monitoring

Many employers these days monitor all the traffic of their employees' computers. There are several good reasons for this. The main one is the detection of malware, phishing, and other on-line threats, and stopping them before they had the chance to reach the employee's computer. Another reason is to ensure employee efficiency – that the people the company is paying to work for it aren't spending their business hours watching on-line movies or otherwise visiting sites that are not work-related.

Since nowadays most of the web traffic is encrypted via HTTPS, implementing such monitoring basically means that the company has to break the encryption by conducting a so-called man-in-the-middle attack. The incoming traffic decrypted, then re-encrypted and signed with a corporate certificate that the employee's browser is instructed to trust, instead of the certificate used by the site the employee is visiting.

Unfortunately, this again can lead to a serious invasion of privacy when the employee is reading personal e-mail or is performing other, permitted but private on-line actions. Again, this poses an ethical dilemma to the company – the weighting of security and efficiency against privacy of their employees.

2.2.5. Facial recognition

Nowadays the computer vision and facial recognition technology is extremely advanced – sufficiently advanced to be deployed *en masse* and used in real-time. Several cities around the world have deployed hundreds of thousands of security cameras in public spaces. The top use of this technology is in China [Bischoff, 2019], where some cities have several millions of such cameras deployed – but even in the Western world (e.g., in London) this technology is widely used [Thakkar].

The benefits of it are obvious – it can reduce crime (or at least increase the percentage of solved crimes). In some cases, when combined with machine learning, it is possible to detect in real-time that a crime is being committed and to automatically alert the authorities without human help.

On the other hand, it again poses significant challenges to privacy. While it can be argued that the face of a person who is in a public place is also public information, the application of this technology allows for total surveillance of every step of the people in the city. Again, it is an ethical dilemma for the local authorities (and for the developers of such systems) whether to opt for reduced crime or for increased privacy.

2.2.6. License plate readers

The past few years saw an increased development and deployment, especially in the USA, of the so-called automated license plate readers (ALPRs). These are devices, usually mounted on street poles, road overpasses, or police cars, which automatically capture the license plates of the passing cars, together with location and a time stamp [EFF]. The information is stored in databases and can be accessed in order to determine whether a particular car has been at a particular location at a particular time.

Such devices have clear advantages in fighting various kinds of crime – locating stolen vehicles, tracing the movements of a suspect, detecting insurance fraud, and many others. On the other hand, their extensive use allows total surveillance of every move of the motorized population. The people have no choice in the matter, because the law requires that the license plate of a vehicle is clearly visible at all times.

What is even worse, in some cases the local governments have been found selling for proffit the collected data to private parties for the purpose of tracking people [Cox, 2019]. While such activities are undoubtedly legal, they seem at least ethically questionable to us.

In fact, it was discovered that such activities are being adopted by private businesses too – not just by the local governments. At least one US company was found to pay subcontractors to install ALPRs on their cars and collect data for the company – access to which is then sold to other private parties [Cox, 2019b].

Acknowledgments

The preparation of this paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICT in SES)", financed by the Ministry of Education and Science of the Republic of Bulgaria.

REFERENCES

Bischoff, P. (2019). *The world's most-surveilled cities*, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Cimpanu, C. (2019). *US to collect social media profiles from immigrants, asylum seekers, and refugees*, https://www.zdnet.com/article/us-to-collect-social-media-profiles-from-immigrants-asylum-seekers-and-refugees/

Cook, J. *A complete history of internet-connected fridges*, https://www.businessinsider.com/the-complete-history-of-internet-fridges-and-connected-refrigerators-2016-1?op=1

Cox, J. (2019). *DMVs Are Selling Your Data to Private Investigators*, https://www.vice.com/en_us/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars

Cox, J. (2019b). *This Company Built a Private Surveillance Network. We Tracked Someone With It*, https://www.vice.com/en_us/article/ne879z/i-tracked-someone-with-license-plate-readers-drn

Dudley, R. (2019). *How insurance companies are fueling a rise in ransomware attacks*, https://arstechnica.com/information-technology/2019/08/how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks/

Dudley, R., J. Kao. (2019). *The Trade Secret*, https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

EFF, *Street-Level Surveillance*, https://www.eff.org/pages/automated-license-plate-readers-alpr

Hill, K. (2012). *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Jareth (2019). *To pay or not to pay ransomware: A cost-benefit analysis of paying the ransom*, https://blog.emsisoft.com/en/33686/to-pay-or-not-to-pay-ransomware-a-cost-benefit-analysis-of-paying-the-ransom/

Keane, S. (2019). *Harvard student gets into US after entry denied over friends' social media posts*, https://www.cnet.com/news/harvard-student-gets-into-us-after-entry-denied-over-friends-social-media-posts/

Loechner, J. (2010). *Behaviorally Targeted Ads Yield Twice The Revenue and Twice the Converts*, https://www.mediapost.com/publications/article/125477/behaviorally-targeted-ads-yield-twice-the-revenue.html

Marotta, V., V. Abhishek, A. Acquisti. (2019). *Online Tracking and Publishers' Revenues: An Empirical Analysis*, https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf

Ren, J., D. Dubois, D. Choffnes, A. Mandalari, K. Roman, H. Haddadi. (2019). *Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach*, Proc. of the Internet Measurement Conference, 2019, https://moniotrlab.ccis.neu.edu/imc19/

Seitz, B. (2016). *The Importance of IoT Data Collection*, https://buddy.com/blog/importance-iot-data-collection/

Thakkar, D. *Facial Recognition for Biometric Mass Surveillance and Security,* https://www.bayometric.com/facial-recognition-biometric-mass-surveillance/