ENCRYPTED MOBILE PHONES

Milana Pisarić, PhD[1]
Faculty of Law, University of Novi Sad, Serbia

Abstract: The secure phone industry has become increasingly important in mobile computing. Various security mechanisms have been developed and put in place to counter the threats to which a smartphone user is exposed - one of them is encryption. There are many software and hardware solutions that enable encryption. On top of that are encrypted phones i.e. customized smartphones that are said to be more secure than mass-market phones. All of these products have been produced and used for legitimate reasons. However, criminals also use them as well. Encryption systems based on software and hardware represent the obstacle in criminal investigation, depriving authorities the possibility to gain electronic evidence while conducting search of phone or surveillance of electronic communications (Going dark problem). Also, in several past years the law enforcement agencies throughout the world encountered encrypted phones while investigating serious crime activities. That resulted in proactive approach which is presented and analyzed in this article.

Keywords: criminal procedure, digital evidence, mobile phone, encryption

INTRODUCTION

The increase in usage of smart phones and mobile applications for routine needs gave rise to privacy-related risks. Since a smartphone user is exposed to various threats, mobile device security is of particular concern, aiming to provide the protection against different types of attacks. Security countermeasures in different layers are being developed and applied, and encryption is only one of them. There are many software and hardware solutions enabling encryption, which may be applied to data in transit or to data at rest (in different levels: file, folder, partition or disk; at different location at same time), by different actors (hardware/software manufacturer, servise provider or a user) (Pisarić, 2020). The manufacturers have been integrating full-disk encryption into devices as a factory default, so accessing stored data is increasingly challenging - the only way to access encrypted device is to get around the encryption, rather than to break it (Pisarić, 2021). Beside that, many communication

1 mpisaric@pf.uns.ac.rs

applications (particularly instant messaging applications) rely more and more on end-to-end (E2E) encryption, as a manner to protect privacy of their users' communications.

On top of that, there are encrypted mobile phones, customized for encrypted communication that are said to be more secure than regular, mass-market phones, since they encrypt all communications, and block unauthorized tracking systems. In 2014 a company called Silent Circle launched the Blackphone (and Blackphone 2 in 2015) - a secure mobile handset, promising users to be able to make encrypted calls and send encrypted messages that could not be eavesdropped (Silent Circle, 2021). Other companies replicated the Blackphone's features afterwards. This industry have become a lively one[2], and the market is mainly driven by customers' inclination towards better security and reliable transmission of data. These ultra-secure smartphones (also calles encrophones, cryptophones etc.) are typically Android devices with a customized operating system, preloaded with applications for secure messaging, and they are designed in such a way that the stored data are encrypted as well. Some of them even have the microphone and camera removed, and other special security features.

Although encrypted phones were originally designed for military usage and have been commercially produced and used for legitimate reasons, a handful of them have been recognized as being used also by criminals. Since reports had shown the increased criminal abuse of cryptophones across many criminal threat areas[3], and since these devices are specifically designed and modified with features that frustrated the usual methods by which investigative bodies intercept communications and identify the communicators, the law enforcement agencies (LEA) have engaged in several actions in order to overcome such an investigative obstacle. The LEA managed so far to shutter a number of secure phone companies, but criminals continue to use encrypted phones to communicate, moving from one provider to another.

ENNETCOM

Ennetcom sold customized PGP BlackBerrys. Namely, the devices could only send and receive PGP encrypted email messages with other devices connected to the same Ennetcom network - they could not be used on conventional cellular telephone networks, nor could take pictures, the microphones had either been removed or disabled, and there was even a possible for Ennetcom to remotely "wipe" or erase the contents of any of their devices at any time. Rather, they operated through a system run by Ennetcom, that was generating anonymous email addresses by which the users of these devices could communicate in complete anonymity, while the devices could only operate through a BlackBerry Enterprise Server – i.e. a software package that permits IT administrators, within an organization, to control virtually all functions of BlackBerry devices connected to the network. According to Dutch Public Prosecution Service (2019, May 10), the company sold nearly 19,000 encrypted cell phones at 1500 euros each in a few years.

In the course of investigation against Danny Manupassa, a man who allegedly ran a company, the Dutch police discovered that the keys for the PGP encryption system were generated and stored on

2 According to report Ultra-Secure Smartphone Market (2018) in 2016 the global ultra-secure smartphone market was valued at $818 million and is projected to reach $4,934 million by 2025, growing at a CAGR of 22.3% from 2018 to 2025. The key players operating in the global ultra-secure smartphone market are ESD Crytophone, BlackBerry Limited, DarkMatter, Inc., Sirin Labs, Turing Robotic Industries, Boeing, Silent Circle, LLC, and Atos SE.

3 For example, see National Crime Agency (2018)

Ennetcom's server, rather than by the device – that was the lead for the farther course of investigation, according to Ontario Superior Court of Justice (2016). Although PGP encryption, by itself, is unbreakable, it doesn't offer any security if private keys are not secure as well - so, the fact the keys for the PGP encryption system were generated by the company's server, rather by the customers' devices, meant that the complete key management system would be found during the search of the server.

Although the majority of Ennetcom customers were in the Netherlands, the company's servers were in Canada, so on 8 April 2016, the Dutch authorities asked Canada to assist in a criminal investigation. On April 18th 2016 a Canadian judge authorized a search of Ennetcom's server, and in April 2016 police arrested Manupassa, seized company's servers based in the Netherlands and Canada and pulled them offline. Data was made available to the Dutch police on September 19th 2016. By taking down the servers, the police discovered a total of 7TB of data on the central server of Ennetcom in Canada and accessed to the contents of 3.6 million messages stored on that server[4], which data were processed and analyzed using Hansken, a forensic search engine developed at the Netherlands Forensic Institute.

It is not clear how the servers were identified, but the main question is how the LEA managed to decrypt the PGP-encrypted messages transmitted using the servers, not having the physical access to the devices themselves, and whether they obtained them correctly. Also, many issues on legality, reliability and accuracy of Hansken's use were raised in the course of criminal procedure. Nevertheless, on 19 April 2018 the criminal court in Amsterdam ruled that evidence collected from Ennetcom's servers are lawfully obtained and the use of Hansken is permitted. As a result, Manupassa was convicted to 18 years imprisonment for money laundering and attempted murder (Court of Amsterdam, 2018).

PHANTOM SECURE

Beginning at least as early 2008, the Canadian company Phantom Security Communications had been operating a worldwide encrypted telecommunication network, selling electronic communication devices and encryption service. The company achieved a revenue of $80 million over its ten years of activity and sold up to 20 000 devices (FBI News (2019, March 16). The company provided encrypted network, selling encrypted devices and service to its clients - at a cost of approximately $2,000-$3,000 per six-month subscription. Phantom Secure was operating mainly on the adjusted Blackberry handsets – they removed all of the typical functionality: the hardware and software tools responsible for external communications (a microphone, GPS navigation, camera, internet access and messaging applications) were removed and then PGP software and Advanced Encryption Standard (AES) were installed on top of an e-mail program, which was directing data through encrypted servers located in Panama and Hong Kong. In order to conceal the location of its keys and mail services, the company cloaked them in multiple layers of virtual proxy networks. Only existing clients could recommend new ones, and the company did not request, track or record the users' real names or other identifying information, but instead communicated with them via usernames, nicknames or email handles. After initiating service, the clients would create anonymous mail handle and the company owned domain would be assigned to him, so the email address was created. Phantom Secure devices communicated exclusively on the Phantom Secure network with other Phantom Secure devices, within which the smaller networks were created. On the request of a customer, all information stored on a device (or devices within a close network) could be remotely wiped.

4 Although Ennetcom's servers were reported to have been configured such that messages are wiped/overwritten after 48 hours.

In the course of investigation against Vincent Ramos, the company's CEO, multiple FBI undercover agents met him in 2017, posing as members of a transnational drug trafficking organization who were seeking secure communications and data deletion services. They purchased 10 devices with accompanying services at a cost of $20,000 for six months and renewed the service for additional $25,000 afterwards. On May 2018 Ramos was arrested, and authorities shut down the Phantom Secure network, and took over more than 180 web domains it used. The Australian, Canadian, and American LEA executed 30 search warrants across offices associated with Phantom as well as the homes of criminal users of the phones. Ramos and his associates were charged for RICO (Racketeer Influenced and Corrupt Organizations) conspiracy and conspiracy to distribute controlled substances, and in May 2019 he was sentenced to nine years in prison for leading a criminal enterprise that facilitated the transnational importation and distribution of narcotics through the sale of encrypted communication devices and services (Department of Justice, 2019, May 28).[5]

ENCROCHAT

Encrochat, a company based in the Netherlands, offered custom-built phones that sent E2E encrypted messages to one another. The EncroChat phones are essentially modified Android devices in which a special, encrypted operating system, EncroChat OS, is installed (phones were dual boot[6]), as well as encrypted messaging programs which route messages through the company's servers. These devices were presented as guaranteeing perfect anonymity and perfect discretion both of the encrypted interface (being hidden so as not to be detectable) and the terminal itself (the camera, microphone, GPS and USB port were disabled). The devices provided special facilities such as automatic deletion of messages on the terminals, specific PIN code intended for the immediate deletion of all data on the device (a panic wipe feature), deletion of all data in the event of consecutive entries of a wrong password, remote wiping from a distance by the reseller/helpdesk. EncroChat phones did not allow voice calls but only text or picture messages, and instead of using mobile networks, it used a Wi-Fi signal. The devices were sold at international scale at cost of around 1,000 EUR, while the EncroChat service with 24/7 support was priced at 1,500 EUR per six months. In early 2020, EncroChat was one of the largest providers of encrypted digital communication (around 60,000 users) with a very high share of users presumably engaged in criminal activity (Europol, 2020, July 2).

The French authorities started investigating EncroChat phones in 2017, after they began finding them in operations against organized crime groups, and discovered that the network was using servers in France. In April 2020 the joint investigation team (JIT) with LEA of the Netherlands was created. In the Netherlands, under the code name Lemont, and in France, under the code name Emma 95, investigators were following the communications of thousands of criminals, with authorization of magistrates. The interception of EncroChat messages ended on 13 June 2020, when the company sent a warning to all its users with the advice to immediately throw away the phones, and decided to shut itself down entirely. The investigation has so far led to the arrest of 60 suspects, the seizure of drugs and dismantling of synthetic drugs labs, the seizure of dozens of (automatic) fire weapons, expensive watches and 25 cars, including vehicles with hidden compartments, and almost EUR 20 million in cash. The JIT has also passed information to law enforcement in other countries, including in the UK, Sweden and Norway (Eurojust (2020, July 2).

5 Ramos's co-defendants remain international fugitives.

6 There are two operating systems side-by-side: the devices run on the OTR (Off-The-Record) operating system, but users could alternatively start the Android operating system.

The phrase used in official reports stating that the police "had access to an encrypted data stream" could be read as suggesting that EncroChat's encryption had been broken, but that's not what happened. The method used to access the EncroChat systems is still unknown to the public. Supposedly, the police hacked into devices – they managed to install software on the servers that provided the phones with updates, or delivered malware to the phones in another form - either way, infecting devices allowed them to see the unencrypted messages. That let the investigators to go beyond the encryption technique, to infiltrate the network, which made it possible to intercept, share and analyse millions of messages that were exchanged between users – meaning, they read users' messages written and stored on the device before they were encrypted and sent (Pisarić, 2021). French police said that they had legal authority to deploy this mass hack, while there is a legal mechanism that allows the capture of computer data by such a technical tool without the consent of the interested parties, to access, in any places, computer data, to record it, to keep it and to transmit it. What is not clear is whether the hack/ malware/'technical device allowed the authorities to read messages as they were sent (but before they were encrypted) or once they had been received (and after being de-encrypted).

SKY GLOBAL

After the EncroChat network was infiltrated, users opted to switch to a new cryptophone supplier, and that was Sky Global. The company, founded in 2008 and operating from Canada and the US, installed sophisticated encryption software on a device (iPhone, Google Pixel, Blackberry or Nokia), which routed encrypted text messages through its servers in France and Canada, while using proxy servers to hide their location. On the modified devices the camera, GPS, and microphone were disabled, and the application itself was in a "stealth mode", hidden on the screen of the device. All messages were encrypted using 512-bit elliptical curve cryptography, while network connections were secured by 2,048-bit SSL encryption. The company stored the Sky ECC app in a secure container on the phone, to protect it from malware, such as keyloggers, while no encrypted messages were stored on its servers - the encrypted message sent to unreachable contact would be hold for up to 48 hours, and then it would be deleted. Also, there was the option of self-destructing messages, and if a user would enter a "panic" password, the contents of the device would be immediately deleted. These devices could be bought online or through "authorised partners" for between €900 and €2,000, depending on model, while the subscriptions cost between $1,200 and $2,000 for six months. Worldwide, in March 2021 approximately 170 000 individuals used the tool (mainly in Europe[7], North America, some Central and Latin American countries (mainly Colombia) and the Middle East), around 70,000 phones actively communicated on the SKY ECC network, with around three million messages exchanged each day (Eurojust (2021, March 2021).

After Sky ECC mobile phones had been recognised as being used in increasing number by criminal groups, the Belgian investigation into the tool started at the end of 2018. As of mid-February 2019 the judicial and law enforcement authorities in Belgium, France and the Netherlands were monitoring the criminal use of the Sky ECC communication service tool, which provided insights into hundreds of millions of messages exchanged between criminals. The investigation mirrored the French and Dutch infiltration of EncroChat, by conducting a two-stage attack on the network. In the first phase, the encrypted communications were intercepted and stored. Extensive investigative work, extensive international cooperation and the support of special expertise have been put into finding a way to decipher encrypted communications as much as possible. In a second phase, the content of the de-

7 Over 20 percent in Belgium and the Netherlands

crypted messages was read live for about 3 weeks. On 9 March 2021, a large number of arrests were made, as well as numerous house searches and seizures in Belgium and the Netherlands, several SKY ECC phones were seized from users who could be identified, and also over 1.2 million euros, 15 prohibited weapons, eight luxury vehicles, three money-counting machines, police uniforms and GPS beacons (Police Federal (2021, March 2021). Following the international police operation, a federal grand jury in the US has indicted Sky Global's CEO, Jean-François Eap, on 12 March 2021, along with former phone distributor Thomas Herman, for racketeering and knowingly facilitating the import and distribution of illegal drugs through the sale of encrypted communications devices (according to US District Court, Southern District California (2021, March 12).

Although the Belgian authorities claim they have successfully unlocked the encryption of Sky ECC, which enabled them to decrypt around a billion messages sent by users and to read tens of thousands of Sky messages in real-time (De Staandard (2021, March 10), the officials have not described how they were able to access Sky ECC message content. Have the police analysed unencrypted metadata, or had access to a limited number of decryption keys? The company claimed that Belgian authorities may have broken into counterfeit code to uncover a network— not Sky ECC, i.e. that someone created a fake phishing application, installed that onto unsecure devices, while the security features of authorized SKY ECC phones were eliminated in these devices, which were then sold falsely branded as SKY ECC through unauthorized channels. This statement raises questions: Which phones and networks were broken into? Did the police hacked, or even created, an insecure imposter device they can monitor, the one that make potential criminals believe they have the encrophone? It remains unclear.

ANOM

After the authorities take down one of these platforms, the users seek a replacement – so after the takedown of Sky ECC in March 2021, there was a migration toward ANoM. The only working application on these devices was the messaging application which came preinstalled, disguised as the calculator function, while the devices themselves were stripped of all other functionality. After entering a code, users could send encrypted text and voice messages, make secure voice calls, share photos, videos, animated GIFs, locations, drawings, and send files of any type. Also, phone owners also had the option to verify their contacts via a QR code, create distribution lists, and chat completely anonymously without even requiring a phone number, according to a listing from the now taken down anom.io website. By May 2021, the phones, which were procured from the black market, had increased to 11,800 in number, of which at least 9,000 were in active use, spanning over 300 criminal syndicates operating in more than 100 countries. Reportedly, the top five countries, where ANoM devices was used, were Germany, the Netherlands, Spain, Australia, and Serbia. The devices cost varied by location, but were generally sold, on six-month subscriptions available for $1,700 in the United States and Australia, and 1000-1500 EUR in Europe.

However, this was a honeypot tactic, used in covert investigation by the authorities in Operational Task Force, under code name Operation Ironside (AFP), Operation Greenlight (Europol), and Operation Trojan Shield (FBI). Since 2019, the FBI in close coordination with the AFP, strategically developed and covertly operated this encrypted device company, in order to fill the vacuum left by Phantom Secure. The encrypted communications application was monitored in order to collect its users' messages - more than 20 million messages from over 11,800 devices used by suspected criminals. The FBI and the 16 other countries of the international coalition, supported by Europol and in coordination with the US Drug Enforcement Administration, then exploited the intelligence from messages obtained and

reviewed them over 18 months while ANoM's criminal users discussed their criminal activities. The operation resulted in more than 700 house searches, more than 800 arrests and the seizure of over 8 tons of cocaine, 22 tons of cannabis and cannabis resin, 2 tons of synthetic drugs (amphetamine and methamphetamine), 6 tons of synthetic drugs precursors, 250 firearms, 55 luxury vehicles and over $48 million in various worldwide currencies and cryptocurrencies in June 2021. Acting U.S. attorney in San Diego charged 17 foreign nationals with were charged for RICO conspiracy and criminal forfeiture.

The users believed their ANoM devices were secured by encryption. They were — but every message was also fed directly to law enforcement agents. Supposedly, the FBI recruited a confidential human source, who had previously sold phones from both Phantom Secure and Sky Global to criminal organizations and had invested a substantial amount of money into the development of a new hardened encrypted device to penetrate the crime networks and distribute the devices - the informant agreed to work for the FBI for the possibility of a reduced prison sentence (he developed a "master key" that allowed them to reroute the messages to a third country and decrypt them, and authorities also relied on the informant to get the devices into criminal networks). The informant started in October 2018 by offering the devices to three other distributors with connections to organized crime in Australia (according to US District Court, Southern District California 2021, May 28). The AFP gained lawful access to these encrypted messages using the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, i.e. executing a man-in-the-middle (MitM) scheme to decrypt and retrieve the messages as they were transmitted (according to US District Court, Southern District California (2021, May 17).

CONCLUSION

The market of super secure phones have flourished in past several years, and although companies state they are only offering a reliable and secure service for any organization or individual that want to secure their information, these devices and accompanying services are used, not only for legitimate, but for criminal purpose as well. Criminal networks have a huge demand for encrypted communication, and beyond regular messaging application that use E2E, they also have a great interest in the customized phones with special security features, which make it difficult for authorities to intercept communications. This has additionally deepened the Going dark problem, so government officials continue to demand that the use of strong encryption by communications networks be banned and only weak encryption - containing a backdoor, thus enabling exceptional access for police upon a court order - be allowed.

The authorities have been targeting companies providing these devices and platforms and its leaders for assisting a criminal organization by providing them with technology to "go dark," or evade law enforcement's detection of their crimes. In s several successful police operations, in which encrypted platforms have been dismantled, LEA have demonstrated that are able to disrupt even encrypted communications networks. The Phantom, Sky, and Encrochat operations showed that law enforcement may shutdown or even hack into encrypted phone companies. But the Anom case shows that law enforcement will also go one step further: they might run such a network themselves. This supports our point that the police doesn't need built-in backdoors to catch criminals. Providing LEA with backdoor access into platforms would be a dangerous precedent, putting all (even legitimate) users' information in jeopardy. Instead, there is yet another possibility.

Although encrophones form presented examples were marketed as bullet-proof to surveillance, they are not actually – since they were not resistant to the malware, which enabled the LEA to hack into end-point device in order to surveil communication before encryption, or after decryption. However, it remains to be seen whether the results of these operations will be admissible in court.

These cases do not represent the end of encrypted phones – although it may have seemed that criminal groups would not revert to communication via encrypted phones in the near future, soon after one company's shut-down, users go to new provider. Encrophone market will not disappear overnight. While the status, impact and potential legal arguments that can be raised against the admissibility of cryptophone evidence remain uncertain and currently untested, criminal groups will certainly continue to operate and will be awaiting the next device that is able to offer security and anonymity.

REFERENCES

1. Court of Amsterdam (2018). Judgment in case No. 13/997097-16, April 19, 2018. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:2504

2. Department of Justice (2019, May 28). Chief Executive of Communications Company Sentenced to Prison for Providing Encryption Services and Devices to Criminal Organizations. https://www.justice.gov/usao-sdca/pr/chief-executive-communications-company-sentenced-prison-providing-encryption-services.

3. Eeckhaut, M (2021, March 10). Zware klap voor georganiseerde misdaad: gerecht hackt 'onkraakbare' misdaadtelefoons. De Staandard. https://www.standaard.be/cnt/dmf20210309_93750346

4. Eurojust (2020, July 2). Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. https://www.eurojust.europa.eu/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

5. Eurojust (2021, March 2021). New major interventions to block encrypted communications of criminal networks. https://www.eurojust.europa.eu/new-major-interventions-block-encrypted-communications-criminal-networks

6. Europol (2021, June 8). 800 Criminals arrested in biggest ever law enforcement operation against encrypted communication. https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

7. FBI News (2019, March 16). International Criminal Communication Service Dismantled.. https://www.fbi.gov/news/stories/phantom-secure-takedown-031618;

8. National Crime Agency (2018). National Strategic Assessment of Serious and Organised Crime. https://nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-andorganised-crime-2018/file

9. Ontario Superior Court of Justice (2016). Mutual Legal Assistance in Criminal Matters Act (Re), 2016 ONSC 5699 (CanLII). https://www.canlii.org/en/on/onsc/doc/2016/2016onsc5699/2016onsc5699.html?searchUrlHash=AAAAAQAIZW5uZXRjb20AAAAAAQ&resultIndex=1

10. Opnieuw aanhoudingen voor leveren crypto-gsm's aan onderwereld, (2019, May 10). https://www.om.nl/actueel/nieuwsberichten/@98954/opnieuw-aanhoudingen/

11. Pisarić, M. (2020). Encryption as an Obstacle for Crimimanl Investigation and Evidence Collection. Collected Papers of the Faculty of Law in Novi Sad, LIV (3), 1079–1100

12. Pisarić, M. (2021). Mobile phone encryption as an obstacle in criminal investigation – review of comparative solutions. Annals of the Faculty of Law in Belgrade, LXIX (2), 415-442

13. Police Federal (2021, March 2021). Des messages décryptés donnent un aperçu unique du fonctionnement des organisations criminelles. https://www.police.be/5998/fr/actualites/des-messages-decryptes-donnent-un-apercu-unique-du-fonctionnement-des-organisations

14. Silent Circle (2021). https://www.silentcircle.com/looking-for-blackphone/

15. Ultra-Secure Smartphone Market by Operating System (Android and iOS) and End User (Govenment Agencies, Aerospace & Defense, and Enterprises) - Global Opportunity Analysis and Industry Forecast, 2018-2025 (2018). https://www.alliedmarketresearch.com/ultra-secure-smartphone-market

16. US District Court, Southern District California (2021, March 12). Indictment in Case No. '21 CR822 GPC. https://cryptome.org/2021/03/sky-indictment.pdf

17. US District Court, Southern District California (2021, May 17). Application for a warrant by a telephone or other reliable electronic means in Case No. '21 MJ01948. https://storage.courtlistener.com/recap/gov.uscourts.casd.707623/gov.uscourts.casd.707623.1.0.pdf

18. US District Court, Southern District California (2021, May 28). Indictment in Case No. '21 CR1623 JLS. https://int.nyt.com/data/documenttools/anom-indictment/17316f82c405ed83/full.pdf