Forensic Science International: Digital Investigation 35 (2020) 301075

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

A survey exploring open source Intelligence for smarter password cracking

Aikaterini Kanta [a, b], Iwen Coisel [a], Mark Scanlon [b, *]

[a] *European Commission Joint Research Centre (DG JRC), Via Enrico Fermi 2749, 21027, Ispra, VA, Italy*
[b] *Forensics and Security Research Group, School of Computer Science, University College Dublin, Ireland*

ARTICLE INFO

Article history:
Received 29 June 2020
Received in revised form
10 September 2020
Accepted 19 September 2020
Available online xxx

Keywords:
Open source intelligence
Password security
Context-based password cracking
Digital investigation

ABSTRACT

From the end of the last century to date, consumers are increasingly living their lives online. In today's world, the average person spends a significant proportion of their time connecting with people online through multiple platforms. This online activity results in people freely sharing an increasing amount of personal information – as well as having to manage how they share that information. For law enforcement, this corresponds to a slew of new sources of digital evidence valuable for digital forensic investigation.

A combination of consumer level encryption becoming default on personal computing and mobile devices and the need to access information stored with third parties has resulted in a need for robust password cracking techniques to progress lawful investigation. However, current password cracking techniques are expensive, time-consuming processes that are not guaranteed to be successful in the time-frames common for investigations. In this paper, the potential for Open Source Intelligence (OSINT) being leveraged for more efficient password cracking is explored. A comprehensive survey of the literature on password strength, password cracking, and OSINT is outlined, and the law enforcement challenges surrounding these topics are discussed. Additionally, an analysis on password structure as well as demographic factors influencing password selection is presented. Finally, the potential impact of OSINT to password cracking by law enforcement is discussed.

1. Introduction

Our society is in constant evolution. The advent of the Internet is often considered as a key turn of our civilisation same as controlling fire. While this is open to debate, what is not is that such technological advance opens the door to major changes of our digital world leading to both great opportunities and new challenges. This evolution is often referred to as the digital transformation of our modern society. There are barely any dimensions of our lives that are not affected by this change.

Law enforcement agencies (LEAs) are thereby impacted by the rise of a modern digital world. Their community is already benefiting from the development of new solutions to store, exchange and ease the access to information and tools. These new solutions can act as facilitators and enablers transforming the more traditional procedures they apply when conducting an investigation to prevent or react after a crime.

In parallel to those new opportunities, this digital transformation also creates new challenges for law enforcement by providing new opportunities and means to criminals. Crimes are now sometimes committed fully online, e.g., botnet exploitation and ransomware. The digital world can be the channel to sell and exchange illegal material, e.g., trading platform for drugs and weapons, or exchange of child sexual abuse materials. Whatever the crime, the common challenge for law enforcement is that data at rest or in transit is protected by encryption (Du et al., 2020). Recovering the data in clear is often the key to properly pursue an on-going investigation or prosecute the criminals.

How do we deal with encryption? Direct attacks aimed at breaking the encryption method itself are generally not possible, as robust and standards methods are nowadays available to everyone. Nevertheless, existing solutions are often password based, especially in the data at rest scenarios (the encryption method used in data in transit can be totally transparent to the user). Passwords are the weakest point of the whole security chain as human-chosen

* Corresponding author.
E-mail addresses: aikaterini.kanta@ucdconnect.ie (A. Kanta), iwen.coisel@ec.europa.eu (I. Coisel), mark.scanlon@ucd.ie (M. Scanlon).

https://doi.org/10.1016/j.fsidi.2020.301075

password are known to be somewhat weak in average (Taneski et al., 2019). Password cracking techniques are traditionally designed to produce generic candidates mimicking the most common passwords or patterns. This approach is typically sufficient to assess the average level of security of a system during penetration testing. A single hit, meaning the password of any user, might be sufficient to harm a system.

Law enforcement are in a different scenario as they focus on a single user or groups of users. While generic password cracking techniques can remain successful, they can benefit from a more targeted approach when dealing with encrypted material. Humans have the tendency to generate easy to remember passwords (Kuo et al., 2006). One common method involves using personal information in the password such as Jeremy Hammond, a wanted hacker, who used the name of his cat in his password.[1] There however stand two challenges that to our knowledge are unsolved:

- How can state-of-the-art password cracking tools benefit from a targeted approach?
- How can the targeted approach aid Law Enforcement in their fight against digital crime?

The contributions of this paper are threefold. Section 2 will describe more precisely how the digital transformation has impacted the investigation processes of law enforcement and their current available techniques to deal with encrypted material. Secondly, a look into current password cracking techniques and an analysis on password insights can be found in Section 3. Thirdly, Section 4 is dedicated to the merge between those two worlds, LEA and OSINT. A survey and comparison of existing OSINT tools is presented focusing mostly on those relevant for the collection of contextual information about a target. Lastly, we express our opinion about what could concretely improve investigation techniques and potential challenges we face to reach such point.

There are already a number of survey papers on the topic of password cracking, with analysis on password cracking methods and evaluation of strength estimators (Hu, 2017) and suggestions on countermeasures (Han et al., 2014). Where our literature review innovates, is on the incorporation of password tendencies of users and the inclusion of the OSINT element, where we present its use by LEA now and its potential usefulness as an additional element in a contextualisation attempt on password cracking. To this end, we have identified further research directions on how to leverage freely available information for a targeted approach.

2. Law enforcement practices

2.1. Digital and forensic investigation

Since the dawn of the digital era, physical evidence collected on a crime scene are not the only tools at the disposal of a law enforcement investigator. A variety of digital evidence such as those collected on the physical scene: hard drives, computers, smart devices provide information such as location off of GPS and tower cell data, interests and hobbies of a suspect, information on close contacts, etc and can give the investigator useful assistance. Nowadays, crimes, such as financial scams, human trafficking and child pornography distribution can be organised and perpetrated exclusively online. For this reason, many protocols and procedures on how to deal with digital evidence have been proposed by researchers, that cover all steps of the investigative process in both cyber and traditional investigations. According to Du et al. (2017), the typical stages of a digital investigation are:

1. Identification - The first stage is about identifying the details of a incident or crime and the relevant evidence that might need to be examined. For example, in a house search, all digital devices that belong to the suspect have to be identified for collection in the next steps.
2. Preservation - This stage is about preserving the crime scene and the evidence by taking photos, keeping a chain of custody on the evidence, etc. This is an important step in the investigation from the beginning to the end when/if the evidence have to be presented in a court of law.
3. Collection - In this stage of the investigation the digital evidence that is deemed relevant is collected from the crime scene. This is usually done by imaging the electronic devices by using special forensic equipment and software in order to not alter their content in any way.
4. Analysis - This is the stage where the investigator has to interpret, analyse and organise the evidence they have acquired and “build their case”.
5. Reporting/Presentation - The last stage refers to the presentation of the findings of an investigation to a court of law or other authority. An important detail to be taken into account is that the results presented at this stage would have to be reproducible by other investigators in order to be accepted.

In addition to the typical stages of a digital investigation mentioned above, The Association of Chief Police Officers (ACPO) has provided a Good Practice Guides for Digital Evidence which includes the known widely ACPO Principles that every practitioner must follow when handling digital evidence (Williams, 2012). The last update to this guide is from 2012.

2.2. Challenges in digital forensics

Despite the many established processes and procedures on dealing with digital evidence and performing digital forensics, there are many challenges in the field that hinder the effort of digital forensics specialists to acquire and process digital evidence in a timely manner. There are quite a few efforts over the years to identify, categorise and analyse the current challenges facing the digital forensics community, as well as look at the trends for the future. Al Fahdi et al. (Al Fahdi et al., 2013) conducted a survey of digital forensic practitioners who overwhelmingly predicted an increase in complexity for investigations in the future. Another survey of practitioners, showcased that the challenges spread across the spectrum; from technical (higher support for cloud forensics) to legal (privacy laws) and educational challenges (Harichandran et al., 2016). A taxonomy of current challenges in the field is presented by Karie and Venter (2015), while Lillis et al. (2016) aim to define the future areas of research in digital forensics. In general, the different categories of challenges are split into three main categories, technical challenges, challenges regarding the law and challenges regarding resources.

2.2.1. Technical challenges

Due to the rapid growth of digital crimes in conjunction with the number of seized devices in these crimes and ever-increasing data storage of these devices, each investigation might acquire a significant number of devices and data that need to be analysed (Quick and Choo, 2014), with additional complexity due to device encryption. In fact, according to Safaei et al. (2017), each person will use more than 9 devices in their day-to-day lives by 2025. This creates a backlog of cases even up to four years that leads to LEAs

[1] https://abcnews.go.com/Technology/fbi-wanted-hacker-jeremy-hammond-cats-password/story?id=26884738.

not being able to process the evidence in a timely manner and might even lead to cases being dropped (Scanlon, 2016). One more reason that adds to the backlog is the increasing use of Internet of Things (IoT) devices that we use in our everyday lives as well as the ever increasing use of cloud services (Lillis et al., 2016) as detailed below.

IoT Forensics. A consequence of the digitisation of our society is the ever growing constellation of IoT and smart devices surrounding each individual. Such growth raises privacy and security issues as threats and vulnerabilities, e.g., Denial of Service (DoS) attacks, spoofing, eavesdropping, etc, have already been identified in those devices (Nawir et al., 2016). From another point of view, those devices and the data they collect and process constitute a gold mine of information for law enforcement (Sayakkara et al., 2019). In a 2019 survey of digital forensic practitioners, it was found that many of them already encounter IoT devices in their work but feel undertrained to examine them (Wu et al., 2019). To this end, specific procedures for forensic investigations on IoT devices must be defined to take advantage of such data without contributing negatively to the already existing backlog.

Cloud Forensics. As more and more companies move to the cloud, due to its lower cost and ease of troubleshooting, the advantages of performing digital forensics on the cloud are also more apparent. Cloud forensics is defined by Ruan et al. (2011) as ‘the application of digital forensics in cloud computing as a subset of network forensics’. Therefore, it is important for digital forensic investigators to be able to apply the same techniques and procedures they use in digital devices to their cloud counterparts. To this end, Ruan et al. (2013) have conducted a survey with digital forensics expert participants in order to analyse the current issues and challenges faced by this industry when it comes to cloud forensics procedures, tools and investigations as well as to identify future opportunities for research and development. Some of the challenges the participants claimed posed a hindrance to the investigation include evidence segregation and lack of access to physical data. Furthermore, Manral et al. (2019) have summarised and grouped the digital forensic challenges in the cloud according to the step of the investigation process the investigators encounter them on. Some of these challenges that are specific to cloud forensics include dealing with jurisdiction issues and being familiar with different cloud architectures.

2.2.2. Legal challenges

When it comes to a digital investigation, a challenge for law enforcement is making sure they can guarantee the admissibility of digital evidence into a court of law. This means that, the proper procedures of the digital investigation process must be carried out successfully every step of the investigation, like ensuring the proper collection of evidence and keeping the chain of custody. It is a challenge for law enforcement to properly evaluate and report on digital evidence in a way that establishes their validity and admissibility. This challenge is directly tied to the correct following of the digital investigation process as described in section 2.1. Anti-forensics, is another hindrance to properly evaluating and reporting on digital evidence. Anti-forensics is defined by Liu and Brown (2006) as the “application of the scientific method to digital media in order to invalidate factual information for judicial review”. and has the goal of making the collection of digital evidence by investigators more complex and/or invalidating their findings. It is employed by criminals as a way to mitigate the results of LEA finding evidence that can incriminate them.

2.2.3. Resource challenges

When it comes to personnel challenges, police officers that have to perform digital forensics are most of the time not adequately trained on how to use the forensics analysis equipment and handle the evidence according to the established procedures (Bowcott, 2018). According to the UK’s House of Commons Justice Committee (House of Commons Justice Committee, 2018), the reason for this is the unavailability of funding. In addition to this, in many cases there is not enough available personnel to actually work on forensics analysis cases.

3. Password analysis

As far as a digital investigation is concerned, more often than not, a law enforcement officer will find themselves in a situation where gaining access into a digital device or computer system will be of the utmost importance for the course of an investigation. Password-based schemes are typically protecting access to those devices as they remain nowadays the most used authentication method and are unlikely to vanish in the coming years (Bonneau et al., 2012). Significant effort is put in place to on one side strengthen those mechanisms and enforce users in choosing safe passwords, and on the other side, improve the password cracking techniques to gain access, often illegally, to systems. There is a common belief that hackers are always a step ahead over defenders and sometimes defenders will suffer penalising (Maqbool et al., 2020). Nevertheless, both approaches can be beneficial to law enforcement and contribute to the success of an investigation. This section provides an overview of this field of research.

3.1. Passwords tendencies

A password is a sequence of alphanumerical and/or special characters used to validate that a user has the right to access a computer system, an application, or an online service. The average number of passwords users needs to remember is in constant evolution and diverge a lot, from 27 in one online survey,[2] to 191 in another.[3] Unfortunately, users find it difficult to recall and manage their passwords for all the accounts they maintain and this results in inherent security issues (Bonneau et al., 2012; Zimmermann and Gerber, 2020; Stobert and Biddle, 2013).

A typical consequence of this increasing number of passwords to memorise is that user either select easy-to-remember but weak passwords (Florencio and Herley, 2007) or reuse their potentially complex password (Stobert and Biddle, 2014; Wash et al., 2016), sometimes applying small modifications or simply following a predefined construction process (Haque et al., 2014). A study shows that 80% of users kept their current passwords when it was possible, while 16% changes the current password to one of the passwords they were using on another site and only 4% changes it to something completely new (Bang et al., 2012). One of the biggest security problem arising from password-reuse occurs when considering data breaches. Following the European Union’s General Data Protection Regulation (GDPR),[4] users are notified when a service they are using is compromised and they are strongly encouraged to update their credentials. However, even when the user does so, the other accounts of the user that are protected by the same passwords are still at risk. It was reported that in the first nine months of 2019 alone, almost 8 billion records were leaked in various data breaches (Turner, 2020) potentially opening doors to many other services, some of them being critical for the user or the

[2] https://www.buzzfeednews.com/article/josephbernstein/survey-says-people-have-way-too-many-passwords-to-remember.

[3] https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html.

[4] https://gdpr-info.eu.

society.

As revealed in an American survey with users from different background and ages (Ur et al., 2016), users have generally a biased understanding of password security. As highlighted in this study, participants have overestimated the security increase obtained by adding digits in the password, and underestimated the predictability of using keyboard patterns and common phrases. In a survey by Ur et al. (2015), participants not only overestimated the added security of appending passwords with symbols or digits at the end, but also chose to reuse passwords or elements of passwords frequently. Another common phenomenon is the integration of personal information in the password chosen by users.

In a study by Liu et al. (2014), where more than 20 million pieces of data from Chinese users were analysed, it was found that professionals used passwords with an average length of from 8 to 11 digits, while students tended to use shorter passwords. Concerning the complexity of passwords, they concluded that more than 50% of the users have passwords with only digits and less than 30% have a combination with special characters. The analysis also revealed that more than 12% of the professional users include birthday and mobile phone numbers in the password and moreover a 11,5% used its user name and e-mail to create the password. In another study of Chinese passwords (Han et al., 2017), the use of Pinyin in a pure form or in combination with dates and numbers accounted of 26% of the total, which seems to suggest that the use of English characters is widespread. It was also pointed out, that in the case of pure Pinyin passwords they were constructed with only 2–4 Chinese characters.

In a case study of passwords in North Macedonia, where a dataset of passwords from recent high school graduates was analysed, it was found that the passwords contained therein were found to be weaker than the baseline, already weak datasets they were compared against (Cvetkovski and Esposito, 2019). The authors stipulate that this is a result of a direct link between password security habits and general literacy.

Usually, users create passwords that contain familiar models, including the expression of feelings, names, dates, and places. This was demonstrated by Veras et al. (2014) where their semantic approach significantly improved the number of recovered passwords compared to state-of-the-art approaches. Veras et al. (2012), focused on the semantic meaning of numbers and especially dates in passwords, finding that 4.5% of all passwords in the Rock You dataset were dates. In Kuo et al. (2006), the authors created a survey and asked users to input either regular passwords or mnemonic passwords that were constructed by phrases and sentences. They found that the majority of the mnemonic passwords contained external information while only 13% of the participants in the control group did the same.

In the case of Chinese users, and as far as contextual information is considered, Zeng et al. (2019) performed a sentiment analysis on three different datasets and found that sentiments (and in their majority positive ones) were chosen more often than other contextual information such as places and names.

Passwords based on meaningful common words, personal information, and patterns are considered as more memorable (Alomari et al., 2019). Also, culture and country of origin seems to play an important role in password selection (AlSabah et al., 2018). Furthermore, it seems that users are willing to accept more difficult authentication methods in the case of financial and e-mail accounts, but not for infrequently used web accounts (Alomari and Thorpe, 2019). They are also more likely to accept more strict password policies on a PC, than a smartphone or tablet and choose safer passwords (Von Zezschwitz et al., 2014). Finally, a study that compared a dynamic personalised password policy (DPPP) that takes into account a user's personality traits when prompting a user to form a secure password, with commonly used password policies, showed that the first resulted in passwords that are more resistant to guessing attacks (Guo et al., 2020).

3.2. Password strength

Well aware of the weakness of human-chosen passwords, attackers aim at guessing passwords to gain access to services or data (Carnavalet and Mannan, 2015). One way to better protect a service is therefore to make sure that the password chosen by the user would resist the efforts of a potential attacker. Password metrics are therefore needed in this context providing a measure of the strength of the password. Such a score can be the result of the combination of length, complexity, and unpredictability of the used password or trying to evaluate the number of guesses an attacker should perform before retrieving the password (Cybersecurity and Infrastructure Security Agency (CISA), 2009). These metrics have a large variance as it was shown that checking the same password in different meters can give highly inconsistent strength outcomes (Carnavalet and Mannan, 2015).

Many popular web services use password-strength meters to give feedback to users while they create new passwords, which might affect user behaviour during password creation. Stringent meters forced users to spent longer time creating and changing their password until they satisfy the requirements, but they also found the password meter annoying and in some cases did not pay attention in satisfying the meter (Ur et al., 2012). On top of this, this procedure causes great difficulties to users in creating and remembering their passwords (Kuo et al., 2006). Weak passwords can be remembered but strong passwords are more likely to be written down (Gołofit, 2007; Renaud and De Angeli, 2009). There is therefore an inherent weakness in knowledge-based authentication methods. In a study by Brown et al. (Brown et al. (2004), 15% of all passwords for email access were assigned to the users and they had not generated them themselves. Finally, Komanduri et al. (2011) concluded that increases in entropy of passwords often correlate with decreases in usability, suggesting a trade-off between these two aspects.

Various techniques regarding the creation of passwords with strengthening in mind have been proposed. The simplest ways usually proposed by IT administrators are inelastic rules for the length of the password and the type of the characters to be used, as well as a specific tolerance to the number of times credentials can be inputted incorrectly before the system locks the user out.

More sophisticated methods, such as the creation of mnemonic phrase-based passwords is another proposed way, where users take usually the first letter of each word of a favourable and memorable phrase and create a new password. It was found that the majority of users based these mnemonic passwords on phrases that can be found on the Internet, which could create problems concerning the strength of the produced password and especially if such a mnemonic dictionary is included in password cracking tools (Kuo et al., 2006).

Another alternative possibility is the use of graphical passwords (Thorpe and Van Oorschot, 2004; Birget et al., 2003). It is easier for users to remember pictures than complex text passwords. Graphical passwords can be utilised as a second step of verification, after the text password, in order to strengthen the verification process. It was found that users are more likely to remember graphical passwords and for longer (Tullis et al., 2011).

Similar is the use of a token, but it is considered inconvenient and costly (O'Gorman, 2003). The combination with bio-metrics is another aspect. It is more suited for getting access to local machines and requires a high cost to implement in other activities. Furthermore, it should be noted that the use of password as a back-up or recovery option will not easily be diminished (Siddique et al., 2017). Finally, it was found that password security training can bridge the gap between the IT administrators and the end users (Charoen et al., 2008).

IT designers have created many password meters (Shay et al., 2015) and many of them can be found in the Internet as free tools to check a given password's strength such as Passwordmeter,[5] My1login[6] and LastPass,[7] with Kaspersky[8] pointing out to never to enter your real password.

Concerning the password strength meters which are included in certain web pages, they are unable to assess precisely the number of guesses one needs to retrieve a password (Galbally et al., 2014), as this would demand a lot of resources and time. Yang et al. (2015), pointed out that commercial meters need to be improved due to the inconsistent and inaccurate feedback they provide compared to other meters. Entropy, which is traditionally used for measuring the strength of a password is proving inadequate when intelligence based attacks are concerned (Mazurek et al., 2013).In the case of graphical passwords, Heidt and Aviv (2016) points out that most strength meters incorrectly assume a linear relationship between pattern features and puts forth a new meter that takes into account the guessability of the pattern.

The community in this field remains active and new password strength meters have been recently designed, each of them following a different approach. Galbally et al. (2014) used a very large publicly available dataset of passwords to propose a flexible probabilistic framework, that can be adjusted to different environments or password policies and able to objectively measure the strength of a given password. A multi-modal strength metric was proposed by Galbally et al. (2017) based on the implementation of two new probabilistic Markov chain methods merged with an attack-based module and a heuristic-based module. Guo and Zhang (2018), proposed a lightweight password-strength estimation method (LPSE), which performed better than other existing LPSEs, in terms of response and storage space providing at the same time an excellent identification of the strength of the password. The complexity of the subject lead (Kelley et al., 2012), to propose their technique for evaluating password strength against a variety of password-guessing algorithms. Their algorithm can be trained to increase awareness of password strength. One of the most widely accepted password meters is zxcvbn, which is used by Dropbox (Wheeler, 2016). This strength meter has been used to evaluate the strength of password from a dataset of 3.9 billion leaked passwords.The meter ranks password between five classes, from 0 to 4, taking into consideration many criteria, one of them being the length as it can be seen in Fig. 1. As can be seen in this graph, the majority of the stronger passwords which are in class 4 are longer than those of the other classes.

Furthermore, in aiming to quantify the amount of personal information in a user's password, Li et al. (2017) put forth Coverage, a metric that can be integrated to existing password meters.

Finally, strength meters are weaker in predicting non-english passwords. This, as was stated in the previous section is the result of a lack of datasets/studies on non-english users/passwords. Doucek et al. (2020), have tried to address this issue, by adjusting zxcvbn to the Czech language. They have shown that by incorporating a Czech dictionary the strength estimation has improved, and this modification can be adapted to other languages as long as appropriate dictionaries exist/can be generated.

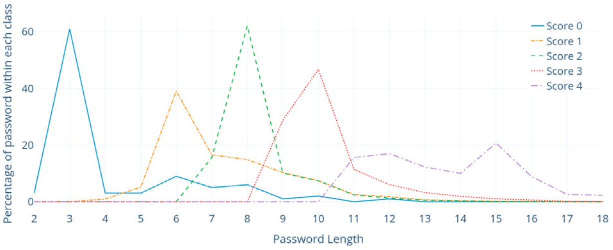

Fig. 1. Password Length Distribution within zxcvbn score Classes.

3.3. Password cracking techniques

Retrieving a password is not the only solution to penetrate a system as many other threats can be exploited by an adversary (Hassan, 2019). However, taking into consideration that the majority of users follow common patterns in password creation, the chances to retrieve a password are high (Lehto and Neittaanmäki, 2018). If the purpose is to retrieve a single successful password out of the set of users instead of a targeted one, the success ratio is even bigger. A wide range of tools is available to perform such password cracking process, which is useful not only in terms of a lawful investigation but also for penetration testing and account recovery purposes.

The most straightforward approach to recover a password is naturally to try all the possible combinations, also known as exhaustive search or brute-force attack. This resource-intensive approach quickly reaches its limits when the password sought is long and/or using a rich alphabet, i.e., alphanumerical with special symbols (Raza et al., 2012).

Hellman tables (Hellman, 1980), a time-memory trade-off allowing to retrieve efficiently the input of a one-way function, can be used to retrieved password in a very efficient manner. Many improvements of Hellman tables have been proposed since then (Biryukov et al., 2005; Saran and Doganaksoy, 2009; Thing and Ying, 2009; Wang et al., 2013) and especially Rainbow tables in 2003 (Oechslin, 2003), in terms of shortening the time span, increasing searching efficiency, success rate, space utilisation, etc. A countermeasure to this technique is relatively well spread nowadays consisting in concatenating a random value, known as a *salt*, to the password before computing the stored value. The precomputed table cannot be adapted to such value except by integrating it during its generation, making such task impossible due to the number of potential salts.

Dictionary attacks consist in testing password candidates from a given wordlist, the dictionary. Each entry can be tested after some modifications have been applied to them, known as mangling rules, such as adding numbers, capitalising a letter, etc. The purpose of those rules is to mimic user tendencies as highlighted in the previous section. Those rules can be manually designed or automatically learnt from previously cracked passwords (Aggarwal et al., 2018).

Similarly to such automated generation of rules, modern approaches to password guessing rely on a machine-learning approach exploiting the enormous quantity of real human-chosen passwords from leaked database. Probabilistic Context-Free Grammars (PCFG) is one example of such modern approach, initially released in 2009 (Weir et al., 2009) and recently updated to make it one of the most successful techniques. This approach is based on dictionary attack principles (Houshmand et al., 2015), and focuses on the calculation of the probability of each grammar (Jelinek et al., 1992). They are based on Markov chains and many password guessing tools are making use of them. PCFGs models are

[5] http://www.passwordmeter.com/.
[6] https://www.my1login.com/resources/password-strength-test/.
[7] https://lastpass.com/howsecure.php.
[8] https://password.kaspersky.com/.

variants of context-free grammars, extending them similarly to how hidden Markov models extend regular grammars (Jeong, 2014). OMEN (Dürmuth et al., 2015), is a Markov model-based password cracker that outputs password candidates in decreasing probability, thus speeding up the password guessing process. PRINCE[9]makes use of one input wordlist by creating "chains of combined words". PassGan (Hitaj et al., 2019) is Generative Adversarial Network (GAN) tool, that uses machine learning algorithms to replace human-generated password rules.

These techniques have a good success ratio when they are used to recover passwords from average users as they are designed or trained to reproduce the average human behaviour. When considering a single targeted user, additional information might or should be considered to increase the success ratio. A simple example is that chances of a dictionary attack relying on a English wordlist may be low if the target is not an English speaker.

4. Evolution of Open Source Intelligence

As highlighted in Section 3, much work has been done into looking at password habits of users, and it is shown that personal information such as interests and personal details are often included in passwords. When looking to access a specific suspects device, law enforcement might have better results when taking a more targeted password cracking approach. To this end, Open Source Intelligence (OSINT) could be a good source of information.

The US Intelligence Community Directive 301 (of National Intelligence, 2006) defines Open Source Information as "publicly available information that anyone can lawfully obtain by request, purchase, or observation," and Open Source Intelligence as "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement".

OSINT techniques appeared before World War II (Kott, 2018; Mercado, 2001, 2009) and was at the time known as overt intelligence. The main source was enemy press as well as press in countries that remained neutral (Kott, 2018). While it can be argued that this sort of information gathering rarely yielded great revelations, it provided a coherent image of the public opinion as well as the living conditions (Kott, 2018).

Nowadays, OSINT has evolved remarkably to include a plethora of online sources available to anyone such as the Internet (social networks, online encyclopedia, `whois` domain records, etc.), traditional media (newspapers, television, radio), academic publications (journals and conference proceedings), grey literature (technical reports, diplomatic message), geospatial information (Google Maps and Street view), publicly available data (government reports, budgets), etc (Hassan and Hijazi, 2018; Thompson, 2010).

One of the most useful traits of OSINT is the volume and the availability of information (Bradbury, 2011). According to Roser et al. (2019), the number of Internet users increased from 413 million in 2000 to more than 3.4 billion in 2016. As a consequence, millions of data are produced every second and the Internet is more than doubling its size in amount of data every two years (Turner et al., 2014). This is an information gold mine but it is also a tremendous task to sort through such a volume of data and transform the collected pieces into something valuable. According to Burke (2007), intelligence can be viewed as the end product that stems from the analysis and filtering of data to generate something of value for a specific purpose.

Furthermore, a downside of its availability is that it is not easy to evaluate the quality of the information, especially when it stems from the Internet (Gibson, 2004). This issue is not something new, or in fact singular to OSINT, as intelligence agencies have long resorted to keyword sampling and other filtering techniques to sort through exorbitant amounts of information (Hulnick, 2002).

On the other hand, Miller (2018) poses the question of whether or not information that is readily available on the Internet can be called intelligence. The argument against classifying OSINT as intelligence is that it is not acquired by clandestine means, nor does it need special handling like covertly acquired information.

4.1. *Types/classifications of OSINT*

4.1.1. *HUMINT + social engineering*

The NATO Glossary of Terms and Definitions defines HUMINT as "Intelligence derived from information collected by human operators and primarily provided by human sources" (NATO, 2003). HUMINT in literature is usually encountered in cases of an individual conducting espionage but can also be information that is acquired through diplomatic dialogue or liaison exploitation (Sano, 2015).

Social Engineering is similar to HUMINT but focused on social interactions. In Mouton et al. (2014), the authors gather existing definitions of social engineering and propose a more structured definition as: "the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity". Hatfield (2018) provides an evolution of this concept starting from its first appearance in a political context in the 19th century to its eventual migration to the field of cybersecurity. According to Krombholz et al. (2015), social engineering can include physical attacks (dumpster diving), social attacks (baiting, use of alleged authority), reverse social engineering (where the attacker tricks the victim into contacting them), technical attacks (usually carried out over the Internet), or a combination thereof. Of course, due to the increasing use of social media, it is natural that social engineering attacks increasingly focus on targeting users on social media.

4.1.2. *SOCMINT*

Social Media Intelligence is one of the newest members of the INT family, made necessary by the rapid development and increasing usage of social media since the beginning of the 21st century. SOCMINT differs from other traditional forms of intelligence because it can be viewed as a starting point for political, economical and social knowledge production (Donohue, 2015). Due to the ever-evolving nature of crime, it renders older models of intelligence less robust in this new digital era. It is up to police agencies to keep up with the times and be proactive in their fight against crime.

SOCMINT becomes more useful when it is applied to groups or individuals for establishing behavioural patterns (Ivan et al., 2015). Social media nowadays is used not only for communicating with people, but from things like organising social protests (Khondker, 2011) to spreading extremist propaganda (Nizzoli et al., 2019). For this reason, SOCMINT can be utilised to predict and identify online threats (Agarwal and Sureka, 2015; Nizzoli et al., 2019), as well as for gaining insight into group relations and online interactions (Jaeger and Cavelty, 2019).

4.1.3. *Crowdsourcing*

The term crowdsourcing was first coined in Howe (2006). Crowdsourcing is different to outsourcing because it is using the efforts of a virtual crowd to perform specific tasks (Buettner, 2015). When it comes to criminal investigations, crowdsourcing can be

[9] https://github.com/hashcat/princeprocessor.

described not as harnessing crowd resources, but as collecting investigative leads by the public to aid an investigation. There are plenty of advantages to crowdsourcing like the lower cost and the speed, because the network of people involved in the investigation is larger and varied (amateurs and professionals). Furthermore, crowdsourcing is flexible, as it is not hindered by time zones, public holidays, bureaucracy, and can be scaled easily from a local to a global scale (Xu et al., 2016). Users from all over the world can participate in crowdsourcing activities, such as CCTV monitoring or footage analysis, from their computers from their home or office. A study of four such cases from the UK is presented by Trottier (2014).

4.2. How can OSINT be useful for law enforcement/OSINT in a L.E. Context

Collecting available information and leverage it to generate useful leads was performed by law enforcement already before the digital era. During a typical crime investigation, they use and act on knowledge they acquire though traditional sources, such as victim and witnesses accounts and physical evidence in order to solve a crime. Such collection of evidences can nowadays be enriched by online sources thanks to existing OSINT techniques. Furthermore, the monetary and manpower costs of those tools during an investigation are both minimal.

4.2.1. Social and media monitoring

Social Network Analysis (SNA) is used by law enforcement agencies to identify the relations between different entities of a criminal network (Berlusconi et al., 2016). SNA is effective for collecting evidence, analysing interactions and online activities, deriving information about criminal activity as well as the patterns and ties of the involved actors. Van der Hulst (Van der Hulst, 2009) gives an analysis of SNA as an investigation and intelligence tool and a protocol draft for handling network data.

This typical procedure may sometimes miss crucial evidence that are solely located online justifying why such analysis is nowadays considering online sources and more specifically social networks. Integrating social media sources into the investigation can help police officers make more educated decisions. These sources also complement the evidence they have already acquired through traditional means. Social media can be a point of convergence for data and information, and this is also precisely what makes them useful in an OSINT investigation (Marwick and Boyd, 2011). The integration of social media to a law enforcer's toolkit is usually done as part of an ongoing investigation or as a preventative measure, to be obtained through continuous monitoring and data mining of known malicious online domains. Of course social media monitoring has to be performed alongside OSINT investigation in order to enrich the level of understanding of a particular target as well as to help verify the validity of information (Bartlett et al., 2013).

SOCMINT can be performed in real-time to monitor and intervene in a situation (Ivan et al., 2015). Social media with location tagging features such as Snapchat and Instagram, and most notably Twitter with its hashtag function, can provide a valid image of the real time developments on a certain topic or the current situation in a specific location. Similar approach is the processing of close-circuit television (CCTV) footage, either during criminal investigation or for monitoring purposes (Norris and Armstrong, 1999). According to Trottier (2015), the monitoring of public or semi-public spaces through private or public means enables LEA to take hold of information that would otherwise be considered fleeting and morph it into intelligence. The same can be said for online monitoring of open sources and social media accounts where users interact the same way they would do face to face, with the difference that the information that is exchanged is not ephemeral as speech but forever stored on the Internet.

Those capabilities provide almost real-time information that can be determinant during an investigation allowing sometimes an instant reaction (Staniforth, 2016). Digital traces left online by criminals can lead to location information or evidences about criminal activities (Seigfried-Spellar and Leshney, 2016).

4.2.2. Crowdsourcing contributions

Aside from obtaining publicly available information, law enforcement have also identified the advantage of leveraging the collective knowledge of the public in a crime investigation. A good example of the effect of crowdsourcing in a criminal investigation is in the case of the Boston Marathon bombing in April 2013. Citizens engaged in their own investigation of the case in real time, on Twitter and online forums like Reddit (Nhan et al., 2017). Often, the news of a breakthrough would reach Twitter before news agencies reported it. Citizens, amateurs and professionals pooled their resources, studied photos and videos from the scene of the bombing and performed forensic analysis on the evidence they collected (Ungerleider, 2017). While their endeavour did not correctly pinpoint the culprits, it was a useful assistance to law enforcement personnel who used the leads and efforts of the public to successfully identify and catch the perpetrators (Cunningham, 2018).

There are initiatives targeting the power of crowdsourcing for aiding in an investigation. Most notably, Europol's "Trace and Object"[10] initiative to help combat child abuse, asks individuals to examine objects in the background of images with sexually explicit material involving minors, with the aim of identifying the origin of the object. Another such initiative is TraffickCam,[11] which asks users to upload images of hotels they have stayed at in order to create a database of hotel rooms. This database can then be used by an investigator who can compare images recovered through an investigation to those in the database with the aim of finding the location of the crime.

Of course turning to the public for leads in a crime investigation means that you might be faced with a huge number of responses. For the first year of the Trace an Object initiative, Europol reported 21,000 leads sent by citizens for 119 objects, resulting in the identification of 79 objects in total and in 32 cases, in the identification of the country of production (EUROPOL, 2018). This overwhelming amount of leads though means that LEA need to implement procedures for handling, filtering and evaluating this information. One such case is of the Netherlands National Police and their use of an AI Agent messaging processing tool about the messages they receive through the Interpol Channel (Testerink et al., 2019).

4.2.3. Digital forensic intelligence

The application of knowledge gathered from OSINT can be incorporated with the information already gathered in a traditional investigation, where one source aids the other. Quick and Choo (2018) proposed a framework called DFINT + OSINT, which aims to use OSINT in conjunction with previously used Digital forensic intelligence with the aim of finding even more useful information about crimes based on already collected data. The authors developed a tool called DRbSi (Data Reduction by Selective imaging), which reduces the amount of data that need to be looked at, and an Entity extractor that processes data types found in the DRbSi subsets and merges them into a single source.

[10] https://www.europol.europa.eu/stopchildabuse.

[11] https://traffickcam.com/.

Table 1
OSINT tools.

Function	Example Tools	Notable Usage
Automation Suites		
Maltego	https://www.paterva.com/	Entity transformations
theHarvester	https://github.com/laramies/theHarvester	OSINT gathering from multiple sources
Spiderfoot	spiderfoot.net	Scanning and monitoring open data sources
Twitter		
Twitter ID	gettwitterid.com/, tweeterid.com/	Unique numerical identifier
GPS enabled tweets/geocoding	geosocialfootprint.com/	Estimate of likely location based on social check-ins and geocoding
Sleeping Patterns	Sleeping time.org/	Sleeping Patterns of specific user
Record of profile changes	spoonbill.io/	Profile changes of specific users
Trending topics by location	Trends map.com/, tweetarchivist.com/	Tracking and analytics of users and topics
Sentiment analysis on hashtags	Social bearing.com/	Analytics on twitter usage including sentiment analysis and hashtag use
Visualisation of a twitter community	burrrd.com/	Insights including top connected users and top topics
Facebook		
Find Facebook ID	findmyfbid.in/, lookup-id.com/	Unique numerical identifier
Facebook Search	facebook.com/help/821153694683665	Facebook's inherent search tool
Who Posted What	whopostedwhat.com/	Search by date, location or Facebook UID. Works on Instagram too
Email		
Email Format	email-format.com/	Find the email format of a company
Email Permutator	Metric sparrow.com/toolkit/email-permutator/	Permutations of possible email addresses
H8mail	github.com/khast3x/h8mail	Password hunting tool that matches email addresses to leaked passwords
Reverse Email Lookup	Thats them.com/reverse-email-lookup	Returns useful information associated with an email address
We Leak Info	Weleak info.com/	Data breach search engine (search by email, username, password, hash, etc)

4.2.4. *OSINT tools: a non-exhaustive list*

There are many tools in existence that digital investigators make use of to complement their investigations. In addition to paid tools, there is a variety of online OSINT tools that quickly gather and cluster information in ways that could be useful to an investigation. There is a massive amount of tools available, many of which are duplicates or not working anymore. Two useful lists of tools are the Awesome OSINT List[12] and the OSINT Framework.[13] These lists contain tools that can be useful in an investigation but also tools for marketing insights, etc. In Table 1, an indicative list of tools that can be useful to an investigator when looking at the online presence of a suspect is presented. As can be seen in this table, these tools can provide useful insights for the online presence of a suspect, such as the users they most interact with, the topics they most care about and even their sleeping patterns.

4.2.5. *Legal and ethical considerations*

However, the potential intrusive nature of OSINT, and more especially SOCMINT, should not be ignored. Guidelines needs to be established on how law enforcement officials can collect information with respect to the privacy and confidentiality of citizens (Ivan et al., 2015). Oftentimes, the information a police officer might be looking for can be found online but behind a safety net of privacy settings. There are cases where this digital limit has been circumvent through a friend of the potential suspect who had access to this information and offered it to the police (Morrison, 2020).

It is furthermore of the utmost importance that law enforcement check the validity of the information they have acquired, to ensure they are accurate before they act on it (Cook et al., 2013). For OSINT investigations, a methodology should be adopted, in a similar manner as for traditional and digital investigations, i.e., audit trail, chain of custody, etc. Additionally, the processing and storage of personal data should be done with respect to the laws of the country the investigation is conducted in.

5. Concluding remarks

The review presented in this paper aims to highlight current areas of challenge for law enforcement in digital investigations as well as point out, how using information that is already publicly available can help move these investigations along. When looking at current challenges in regards to the access of password protected systems during a digital investigation, the challenge of encryption poses the biggest hindrance to investigators. If a password cannot be retrieved in a timely manner, it can affect the swift resolution of an investigation or even allow for more crimes to be perpetrated.

Current analysis of password habits of users shows that demographics, e.g., age, profession, etc., plays an important role in password selection. The same stands true for personal information that users include in their passwords. Furthermore, where the password is for an account deemed more important/sensitive, e.g., online banking or government websites, the difficulty of the password chosen by the user is likely greater. Finally, the few studies that are specific to users of certain non-English speaking countries suggest that an approach tailored to a specific language will yield better results - even if it is only an inclusion of a simple dictionary of that language in the cracking process.

The combination of these factors suggest that this is an area where knowing targeted information about a specific user or a subset of users might be beneficial in helping with more “educated” guesses and smarter dictionary attacks. Keywords that have to do with important dates, family names, hobbies and interests are suggested to have a higher possibility of being parts of the password than regular dictionary words. By making use of this contextual information, we can build a personalised dictionary for a suspect(s) and tailor the cracking process to them. In the course of an investigation, using smart list in conjunction with current password cracking tools can aid police investigators in cracking the password faster.

When it comes to the creation of such smart list, the degree of contextualisation is another matter to be taken into account. Depending on the target and the trade-off between success and time efficiency, different levels of contextualisation, i.e., of inclusion of targeted information, in the process of creation of the custom dictionary are worthy of exploration.

An efficient targeted contextual-based approach requires an automation of the information extraction process. For the majority of Internet users, there are publicly available information on the Internet that can serve for this contextual-based approach, but collecting, analysing and extracting only the useful information is

[12] https://github.com/jivoi/awesome-osint.
[13] https://osintframework.com/.

the challenge ahead of us. Word embedding or other natural language processing approaches could be the answer to this automation challenge.

The next question that needs to be answered is: is OSINT the way to go? In this paper we have presented an indicative list of OSINT tools that are available with many capabilities that can return useful information on a suspect. An approach where digital evidence gathered by police can be enhanced by OSINT sources, and the two of them can be mutually assisting could result in more fruitful and faster investigations.

5.1. Future directions

There are many steps and challenges to address to provide law enforcement with a tool creating smarter and individualised dictionaries. The lack of testing data in this particular field is one of them (Kanta et al., 2020). A preliminary step could therefore be to focus on a community of individuals gathered around the same topic such as a hobby allowing to collect and process public data to validate if a context-based approach is increasing the success rate. This approach allows the design of a first generation of OSINT-based tools for password cracking that could be beneficial to law enforcement.

The community-based approach can be the stepping stone of the challenge of integrating information about a target in the password cracking process. A goal of building custom dictionaries that centre around community topics will facilitate the evaluation process because it does not require handling of personally identifiable information. Therefore, the impact of context in a digital investigation will be evaluated and it’s potential usefulness will be determined.

In terms of gathering this information using OSINT and other publicly available sources, there are many avenues to be explored. For the community-based approach, the creation of dictionaries that target specific topics would be the next step in our research. Looking at a community of users that share a common trait, we believe that a dictionary that is build around that trait would be able to recover more passwords than a generic English dictionary. When it comes to creating these custom dictionaries, a Wikipedia article or a forum dedicated to the topic can be the starting point the dictionary is built around. Furthermore, as the process evolves, additional sources can be added to enrich the dictionary, from online forums, social media and other forms of OSINT.

As mentioned above, the level of contextualisation and the process will be automatised as much as can be possible with the ultimate goal being the creation of a custom dictionary by the digital investigator as part of the investigative process.

References

Agarwal, S., Sureka, A., 2015. Applying Social Media Intelligence for Predicting and Identifying On-Line Radicalization and Civil Unrest Oriented Threats arXiv preprint arXiv:151106858.

Aggarwal, S., Houshmand, S., Weir, M., 2018. New technologies in password cracking techniques. In: Cyber Security: Power and Technology. Springer, pp. 179–198.

Alomari, R., Thorpe, J., 2019. On password behaviours and attitudes in different populations. J. Inf. Secur.Appl. 45, 79–89.

Al Fahdi, M., Clarke, N.L., Furnell, S.M., 2013. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In: Information Security for South Africa. IEEE, pp. 1–8.

Alomari, R., Martin, M.V., MacDonald, S., Maraj, A., Liscano, R., Bellman, C., 2019. Inside out-a study of users' perceptions of password memorability and recall. J. Inf. Secur.Appl. 47, 223–234.

AlSabah, M., Oligeri, G., Riley, R., 2018. Your culture is in your password: an analysis of a demographically-diverse password dataset. Comput. Secur. 77, 427–441.

Bang, Y., Lee, D.J., Bae, Y.S., Ahn, J.H., 2012. Improving information security management: an analysis of ID–password usage and a new login vulnerability measure. Int. J. Inf. Manag. 32 (5), 409–418.

Bartlett, J., Miller, C., Crump, J., Middleton, L., 2013. Policing in an Information Age. Demos London.

Berlusconi, G., Calderoni, F., Parolini, N., Verani, M., Piccardi, C., 2016. Link prediction in criminal networks: a tool for criminal intelligence analysis. PloS One 11 (4), 1–21.

Birget, J.C., Hong, D., Memon, N.D., 2003. Robust discretization, with an application to graphical passwords. IACR Cryptology ePrint Archive 2003, 168.

Biryukov, A., Mukhopadhyay, S., Sarkar, P., 2005. Improved time-memory trade-offs with multiple data. In: International Workshop on Selected Areas in Cryptography. Springer, pp. 110–127.

Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F., 2012. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy. IEEE, pp. 553–567.

Bowcott, O., 2018. Police mishandling digital evidence, forensic experts warn. https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn.

Bradbury, D., 2011. In plain view: open source intelligence. Comput. Fraud Secur. 2011 (4), 5–9.

Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K., 2004. Generating and remembering passwords. Appl. Cognit. Psychol.: Off. J.Soc.Appl. Res.Mem. Cognit. 18 (6), 641–651.

Buettner, R., 2015. A systematic literature review of crowdsourcing research from a human resource management perspective. In: 2015 48th Hawaii International Conference on System Sciences. IEEE, pp. 4609–4618.

Burke, C., 2007. Freeing Knowledge, Telling Secrets: Open Sourceintelligence and Development. No. 13 in Research Paper Series: Centre for East-West Cultural & Economic Studies. Bond University.

Carnavalet, X.D.C.D., Mannan, M., 2015. A large-scale evaluation of high-impact password strength meters. ACM Trans. Inf. Syst. Secur. 18 (1), 1–32.

Charoen, D., Raman, M., Olfman, L., 2008. Improving end user behaviour in password utilization: an action research initiative. Syst. Pract. Action Res. 21 (1), 55–72.

Cook, T., Hibbitt, S., Hill, M., 2013. Blackstone's Crime Investigator's Handbook. Oxford University Press.

Cunningham, M., 2018. Law enforcement social media investigations. Accessed: 2019-10-08. https://crimecenter.com/leverage-manage-crowdsourced-leads/.

Cvetkovski, A., Esposito, F., 2019. The password literacy in north Macedonia: a case study. In: Proceedings of the Third Central European Cybersecurity Conference, pp. 1–6.

Cybersecurity and Infrastructure Security Agency (CISA), 2009. Security tip (st04-002): choosing and protecting passwords. https://www.us-cert.gov/ncas/tips/ST04-002.

Donohue, L.K., 2015. The dawn of social intelligence (SOCINT). Drake Law Rev. 63, 1061.

Doucek, P., Pavlíček, L., Sedláček, J., Nedomová, L., 2020. Adaptation of password strength estimators to a non-English environment—the Czech experience. Comput. Secur. 101757.

Du, X., Hargraves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N-A., Scanlon, M, 2020. SoK: Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. Association for Computing Machinery, 46.

Du, X., Le-Khac, N.A., Scanlon, M., 2017. Evaluation of digital forensic process models with respect to digital forensics as a service. In: Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017). ACPI, Dublin, Ireland, pp. 573–581.

Dürmuth, M., Angelstorf, F., Castelluccia, C., Perito, D., Chaabane, A., 2015. Omen: faster password guessing using an ordered markov enumerator. In: International Symposium on Engineering Secure Software and Systems. Springer, pp. 119–132.

EUROPOL, 2018. With your help we are 21,000 steps closer to saving a child from sexual abuse. https://www.europol.europa.eu/newsroom/news/your-help-we-are-21-000-steps-closer-to-saving-child-sexual-abuse.

Florencio, D., Herley, C., 2007. A large-scale study of web password habits. In: Proceedings of the 16th International Conference on World Wide Web, pp. 657–666.

Galbally, J., Coisel, I., Sanchez, I., 2014. A probabilistic framework for improved password strength metrics. In: 2014 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–6.

Galbally, J., Coisel, I., Sanchez, I., 2017. A new multimodal approach for password strength estimation—Part II: experimental evaluation. IEEE Trans. Inf. Forensics Secur. 12 (12), 2845–2860.

Gibson, S., 2004. Open source intelligence. The RUSI Journal 149 (1), 16–22. https://doi.org/10.1080/03071840408522977.

Gołofit, K., 2007. Click passwords under investigation. In: European Symposium on Research in Computer Security. Springer, pp. 343–358.

Guo, Y., Zhang, Z., 2018. Lpse: lightweight password-strength estimation for password meters. Comput. Secur. 73, 507–518.

Guo, Y., Zhang, Z., Guo, Y., Guo, X., 2020. Nudging personalized password policies by understanding users' personality. Comput. Secur. 101801.

Han, A.L.F., Wong, D.F., Chao, L.S., 2014. Password Cracking and Countermeasures in Computer Security: A Survey arXiv preprint arXiv:14117803.

Han, G., Yu, Y., Li, X., Chen, K., Li, H., 2017. Characterizing the semantics of passwords: the role of Pinyin for Chinese Netizens. Comput. Stand. Interfac. 54, 20–28.

Haque, T., Wright, M., Scielzo, S., 2014. Hierarchy of users' web passwords: perceptions, practices and susceptibilities. Int. J. Hum. Comput. Stud. 72 (12), 860–874.

Harichandran, V.S., Breitinger, F., Baggili, I., Marrington, A., 2016. A cyber forensics needs analysis survey: revisiting the domain's needs a decade later. Comput. Secur. 57, 1–13.

Hassan, N.A., 2019. Digital Forensics Basics: A Practical Guide Using Windows OS. Apress.

Hassan, N.A., Hijazi, R., 2018. The Evolution of Open Source Intelligence. Apress, Berkeley, CA, ISBN 978-1-4842-3213-2, pp. 1–20. https://doi.org/10.1007/978-1-4842-3213-2_1.

Hatfield, J.M., 2018. Social engineering in cybersecurity: the evolution of a concept. Comput. Secur. 73, 102–113.

Heidt, S., Aviv, A.J., 2016. Refining graphical password strength meters for android phones. In: Poster Presented at the Twelfth Symposium on Useable Security and Privacy, vol. 16. SOUPS.

Hellman, M., 1980. A cryptanalytic time-memory trade-off. IEEE Trans. Inf. Theor. 26 (4), 401–406.

Hitaj, B., Gasti, P., Ateniese, G., Perez-Cruz, F., 2019. Passgan: a deep learning approach for password guessing. In: International Conference on Applied Cryptography and Network Security. Springer, pp. 217–237.

House of Commons Justice Committee, 2018. Disclosure of Evidence in Criminal Cases.

Houshmand, S., Aggarwal, S., Flood, R., 2015. Next gen PCFG password cracking. IEEE Trans. Inf. Forensics Secur. 10 (8), 1776–1791.

Howe, J., 2006. The rise of crowdsourcing. Wired 14.

Hu, G., 2017. On password strength: a survey and analysis. In: International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Springer, pp. 165–186.

Hulnick, A.S., 2002. The downside of open source intelligence. Int. J. Intell. Count. Intell. 15 (4), 565–579. https://doi.org/10.1080/08850600290101767.

Ivan, A.L., Iov, C.A., Lutai, R.C., Grad, M.N., 2015. Social media intelligence: opportunities and limitations. CES Working Papers 7 (2A), 505.

Jaeger, M.D., Cavelty, M.D., 2019. From madness to wisdom: intelligence and the digital crowd. Intell. Natl. Secur. 34 (3), 329–343. https://doi.org/10.1080/02684527.2019.1553375.

Jelinek, F., Lafferty, J.D., Mercer, R.L., 1992. Basic methods of probabilistic context free grammars. In: Speech Recognition and Understanding. Springer, pp. 345–360.

Jeong, H., 2014. Architectures for Computer Vision: from Algorithm to Chip with Verilog. John Wiley & Sons.

Kanta, A., Coisel, I., Scanlon, M., 2020. Smarter password guessing techniques leveraging contextual information and OSINT. In: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–2.

Karie, N.M., Venter, H.S., 2015. Taxonomy of challenges for digital forensics. J. Forensic Sci. 60 (4), 885–893.

Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Lopez, J., 2012. Guess again (and again and again): measuring password strength by simulating password-cracking algorithms. In: 2012 IEEE Symposium on Security and Privacy. IEEE, pp. 523–537.

Khondker, H.H., 2011. Role of the new media in the arab spring. Globalizations 8 (5), 675–679. https://doi.org/10.1080/14747731.2011.621287.

Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., Egelman, S., 2011. Of passwords and people: measuring the effect of password-composition policies. In: Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems, pp. 2595–2604.

Kott, M., 2018. British intelligence and Hitler's empire in the Soviet Union, 1941–1945. J. Baltic Stud. 49 (2), 268–271. https://doi.org/10.1080/01629778.2018.1469843.

Krombholz, K., Hobel, H., Huber, M., Weippl, E., 2015. Advanced social engineering attacks. J. Inf.Secur. Appl. 22, 113–122.

Kuo, C., Romanosky, S., Cranor, L.F., 2006. Human selection of mnemonic phrase-based passwords. In: Proceedings of the Second Symposium on Useable Privacy and Security, pp. 67–78.

Lehto, M., Neittaanmäki, P., 2018. Cyber Security: Power and Technology, vol. 93. Springer.

Li, Y., Wang, H., Sun, K., 2017. Personal information in passwords and its security implications. IEEE Trans. Inf. Forensics Secur. 12 (10), 2320–2333.

Lillis, D., Becker, B., O'Sullivan, T., Scanlon, M., 2016. Current challenges and future research areas for digital forensic investigation. In: The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016). ADFSL, Daytona Beach, FL, USA, pp. 9–20.

Liu, V., Brown, F., 2006. Bleeding-edge anti-forensics. In: Presentation at InfoSec World.

Liu, Z., Hong, Y., Pi, D., 2014. A large-scale study of web password habits of Chinese network users. J. Software 9 (2), 293–297.

Manral, B., Somani, G., Choo, K.K.R., Conti, M., Gaur, M.S., 2019. A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Computing Surveys (CSUR) 52 (6), 1–38.

Maqbool, Z., Aggarwal, P., Pammi, V.S.C., Dutt, V., 2020. Cyber security: effects of penalizing defenders in cyber-security games via experimentation and computational modeling. Front. Psychol. https://doi.org/10.3389/fpsyg.2020.00011 (in press).

Marwick, A.E., Boyd, D., 2011. I tweet honestly, i tweet passionately: Twitter users, context collapse, and the imagined audience. New Media Soc. 13 (1), 114–133. https://doi.org/10.1177/1461444810365313.

Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G., Shay, R., Ur, B., 2013. Measuring password guessability for an entire university. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 173–186.

Mercado, S.C., 2001. Fbis against the axis, 1941-1945. Stud. Intell. 11, 33–43.

Mercado, S.C., 2009. Sailing the sea of osint in the information age. Secret intelligence: A reader 78.

Miller, B.H., 2018. Open source intelligence (OSINT): an oxymoron? Int. J. Intell. Count. Intell. 31 (4), 702–719. https://doi.org/10.1080/08850607.2018.1492826.

Morrison, S., 2020. The police want your phone data. here's what they can get – and what they can't. https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-password-rights.

Mouton, F., Leenen, L., Malan, M.M., Venter, H., 2014. Towards an ontological model defining the social engineering domain. In: IFIP International Conference on Human Choice and Computers. Springer, pp. 266–279.

NATO, 2003. Nato Glossary of Terms and Definitions. NATO Standardisation Agency.

Nawir, M., Amir, A., Yaakob, N., Lynn, O.B., 2016. Internet of Things (IoT): Taxonomy of Security Attacks. In: 2016 3rd International Conference on Electronic Design (ICED). IEEE, pp. 321–326.

Nhan, J., Huey, L., Broll, R., 2017. Digilantism: an analysis of crowdsourcing and the boston marathon bombings. Br. J. Criminol. 57 (2), 341–361.

Nizzoli, L., Avvenuti, M., Cresci, S., Tesconi, M., 2019. Extremist Propaganda Tweet Classification with Deep Learning in Realistic Scenarios, pp. 203–204. https://doi.org/10.1145/3292522.3326050.

Norris, C., Armstrong, G., 1999. Cctv and the social structuring of surveillance. Crime Prevention Studies 10 (1), 157–178.

Oechslin, P., 2003. Making a faster cryptanalytic time-memory trade-off. In: Annual International Cryptology Conference. Springer, pp. 617–630.

of National Intelligence, D., 2006. Intelligence Community Directive.

O'Gorman, L., 2003. Comparing passwords, tokens, and biometrics for user authentication. Proc. IEEE 91 (12), 2021–2040.

Quick, D., Choo, K.K.R., 2014. Impacts of increasing volume of digital forensic data: a survey and future research challenges. Digit. Invest. 11 (4), 273–294.

Quick, D., Choo, K.K.R., 2018. Digital forensic intelligence: data subsets and Open Source Intelligence (DFINT+ OSINT): a timely and cohesive mix. Future Generat. Comput. Syst. 78, 558–567.

Raza, M., Iqbal, M., Sharif, M., Haider, W., 2012. A survey of password attacks and comparative analysis on methods for secure authentication. World Appl. Sci. J. 19 (4), 439–444.

Renaud, K., De Angeli, A., 2009. Visual passwords: cure-all or snake-oil? Commun. ACM 52 (12), 135–140.

Roser, M., Ritchie, H., Ortiz-Ospina, Internet, E., 2019. Our world in data. https://ourworldindata.org/internet.

Ruan, K., Carthy, J., Kechadi, T., Crosbie, M., 2011. Cloud forensics: an overview. In: Proceedings of the 7th IFIP International Conference on Digital Forensics, pp. 16–25.

Ruan, K., Carthy, J., Kechadi, T., Baggili, I., 2013. Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit. Invest. 10 (1), 34–43.

Safaei, B., Monazzah, A.M.H., Bafroei, M.B., Ejlali, A., 2017. Reliability side-effects in internet of things application layer protocols. In: 2nd International Conference on System Reliability and Safety (ICSRS). IEEE, pp. 207–212.

Sano, J., 2015. The changing shape of humint. Intel. J. 21 (3), 77–80.

Saran, N., Doganaksoy, A., 2009. Choosing parameters to achieve a higher success rate for Hellman time memory trade off attack. In: 2009 International Conference on Availability, Reliability and Security. IEEE, pp. 504–509.

Sayakkara, A., Le-Khac, N-A., Scanlon, M., 2019. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. Digit. Invest. 29, 43–54.

Scanlon, M., 2016. Battling the digital forensic backlog through data deduplication. In: 2016 Sixth International Conference on Innovative Computing Technology (INTECH). IEEE, pp. 10–14.

Seigfried-Spellar, K.C., Leshney, S.C., 2016. The intersection between social media, crime, and digital forensics: #WhoDunIt?. In: Digital Forensics. Elsevier, pp. 59–67.

Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L., Melicher, W., Segreti, S.M., Ur, B., 2015. A spoonful of sugar? The impact of guidance and feedback on password-creation behavior. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 2903–2912.

Siddique, K., Akhtar, Z., Kim, Y., 2017. Biometrics vs passwords: a modern version of the tortoise and the hare. Comput. Fraud Secur. 2017 (1), 13–17.

Staniforth, A., 2016. Police Use of Open Source Intelligence: the Longer Arm of Law, ISBN 978-3-319-47670-4, pp. 21–31. https://doi.org/10.1007/978-3-319-47671-1_3.

Stobert, E., Biddle, R., 2013. Memory retrieval and graphical passwords. In: Proceedings of the Ninth Symposium on Useable Privacy and Security, pp. 1–14.

Stobert, E., Biddle, R., 2014. The password life cycle: user behaviour in managing passwords. In: 10th Symposium on Useable Privacy and Security (SOUPS 2014), pp. 243–255.

Taneski, V., Heričko, M., Brumen, B., 2019. Systematic overview of password security problems. Acta Polytechnica Hungarica 16 (3).

Testerink, B., Odekerken, D., Bex, F., 2019. AI-assisted message processing for The

Netherlands national police. In: Branting, L.K. (Ed.), Proceedings of the Workshop on Artificial Intelligence and the Administrative State Co-located with 17th International Conference on AI and Law (ICAIL 2019), Montreal, QC, Canada, June 17, 2019; Vol. 2471 of CEUR Workshop Proceedings. CEUR-WS.org, pp. 10−13. http://ceur-ws.org/Vol-2471/paper2.pdf.

Thing, V.L., Ying, H.M., 2009. A novel time-memory trade-off method for password recovery. Digit. Invest. 6, S114−S120.

Thompson, B., 2010. Giving a Voice to Open Source Stakeholders: A Survey of State, Local, and Tribal Law Enforcement: Congressional Report. DIANE Publishing Company, ISBN 9781437918694. https://books.google.it/books?id=3u3K86aXuo4C.

Thorpe, J., Van Oorschot, P.C., 2004. Towards secure design choices for implementing graphical passwords. In: 20th Annual Computer Security Applications Conference. IEEE, pp. 50−60.

Trottier, D., 2014. Crowdsourcing CCTV surveillance on the internet. Inf. Commun. Soc. 17 (5), 609−626. https://doi.org/10.1080/1369118X.2013.808359.

Trottier, D., 2015. Open source intelligence, social media and law enforcement: visions, constraints and critiques. Eur. J. Cult. Stud. 18 (4−5), 530−547. https://doi.org/10.1177/1367549415577396.

Tullis, T.S., Tedesco, D.P., McCaffrey, K.E., 2011. Can users remember their pictorial passwords six years later. In: CHI'11 Extended Abstracts on Human Factors in Computing Systems, pp. 1789−1794.

Turner, S., 2020. 2020 data breaches - the worst breaches of the year | identityforce. https://www.identityforce.com/blog/2020-data-breaches.

Turner, V., Gantz, J.F., Reinsel, D., Minton, S., 2014. The digital universe of opportunities: rich data and the increasing value of the internet of things. IDC Analyze the Future 16.

Ungerleider, N., 2017. How Reddit became A hub of the crowdsourced boston marathon bombing investigation. Accessed: 2019-10-08. https://www.fastcompany.com/3008466/how-reddit-became-hub-crowdsourced-boston-marathon-bombing-investigation.

Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L., et al., 2012. How does your password measure up? the effect of strength meters on password creation. In: Presented as Part of the 21st USENIX Security Symposium (USENIX Security 12), pp. 65−80.

Ur, B., Noma, F., Bees, J., Segreti, S.M., Shay, R., Bauer, L., Christin, N., Cranor, L.F., 2015. I added '!'at the end to make it secure": observing password creation in the lab. In: Eleventh Symposium on Useable Privacy and Security (SOUPS 2015), pp. 123−140.

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., 2016. Do users' perceptions of password security match reality?. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 3748−3760.

Van der Hulst, R.C., 2009. Introduction to social network analysis (SNA) as an investigative tool. Trends Organ. Crime 12 (2), 101−121.

Veras, R., Thorpe, J., Collins, C., 2012. Visualizing semantics in passwords: the role of dates. In: Proceedings of the Ninth International Symposium on Visualization for Cyber Security, pp. 88−95.

Veras, R., Collins, C., Thorpe, J., 2014. On semantic patterns of passwords and their security impact. In: Network and Distributed System Security (NDSS) Symposium.

Von Zezschwitz, E., De Luca, Hussmann, A., Honey, H., 2014. I shrunk the keys: influences of mobile devices on password composition and authentication performance. In: Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, pp. 461−470.

Wang, X.j, Liao, X.f, Huang, H.y., 2013. Improvement of rainbow table technology based on number cutting of reduction function. Comput. Eng. 7, 36.

Wash, R., Rader, E., Berman, R., Wellmer, Z., 2016. Understanding password choices: how frequently entered passwords are re-used across websites. In: Twelfth Symposium on Useable Privacy and Security (SOUPS 2016), pp. 175−188.

Weir, M., Aggarwal, S., De Medeiros, B., Glodek, B., 2009. Password cracking using probabilistic context-free grammars. In: 2009 30th IEEE Symposium on Security and Privacy. IEEE, pp. 391−405.

Wheeler, D.L., 2016. zxcvbn: low-budget password strength estimation. In: 25th USENIX Security Symposium (USENIX Security 16), pp. 157−173.

Williams, J., 2012. ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers of England, Wales & Northern Ireland.

Wu, T., Breitinger, F., Baggili, I., 2019. IoT ignorance is digital forensics research bliss: a survey to understand IoT forensics definitions, challenges and future research directions. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1−15.

Xu, Z., Liu, Y., Yen, N., Mei, L., Luo, X., Wei, X., Hu, C., 2016. Crowdsourcing based description of urban emergency events using social media big data. IEEE Trans. Cloud Comput. 8 (2), 387−397. https://doi.org/10.1109/TCC.2016.2517638.

Yang, S., Ji, S., Hu, X., Beyah, R., 2015. Effectiveness and soundness of commercial password strength meters. In: Network and Distributed System Security Symposium (NDSS).

Zeng, J., Duan, J., Wu, C., 2019. Empirical study on lexical sentiment in passwords from Chinese websites. Comput. Secur. 80, 200−210.

Zimmermann, V., Gerber, N., 2020. The password is dead, long live the password—a laboratory study on user perceptions of authentication schemes. Int. J. Hum. Comput. Stud. 133, 26−44.