Social Engineering Attacks on the Knowledge Worker

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl
SBA Research
Favoritenstraße 16
1040 Vienna, Austria
{kkrombholz,hhobel,mhuber,eweippl}@sba-research.org

ABSTRACT

Social engineering has become an emerging threat in virtual communities and is an effective means to attack information systems. Today's knowledge workers make use of a number of services that leverage sophisticated social engineering attacks. Moreover, there is a trend towards *BYOD* (bring your own device) policies and the usage of online communication and collaboration tools in private and business environments. In globally acting companies, teams are no longer geographically co-located but staffed just-in-time. The decrease in personal interaction combined with the plethora of tools used (E-Mail, IM, Skype, Dropbox, LinkedIn, Lync, etc.) create new attack vectors for social engineering attacks. Recent attacks on companies such as the New York Times, RSA, or Apple have shown that targeted spear-phishing attacks are an effective evolution of social engineering attacks. When combined with zero-day-exploits they become a dangerous weapon, often used by advanced persistent threats. This paper provides a taxonomy of well-known social engineering attacks as well as a comprehensive overview of advanced social engineering attacks on the knowledge worker.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; D.4.6 [**Security and Protection**]: Information flow controls; H.2.7 [**d Protection**]: Information flow controls

General Terms

Privacy, Security, Social Engineering

Keywords

security, privacy, social engineering, attack scenarios, knowledge worker, bring your own device

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
SIN '13 , November 26-28, 2013, Aksaray, Turkey
Copyright 2013 ACM 978-1-4503-2498-4/00/10 ...$15.00

1. INTRODUCTION

The Internet has emerged as the major medium for communication and information exchange purposes. In our everyday life, communication has become distributed over a variety of online communication channels. In recent years, Web 2.0 services such as Twitter, Facebook, and other social networking sites, have become a part of our daily routine. Online communication channels have gained popularity not only for private communication purposes but also for business communication. Employees are expected to be highly mobile and flexible concerning their workspace [9]. Some companies have started to encourage their employees and knowledge workers to bring their own devices to work and to fulfill their tasks from any place that is not necessarily the office provided by the employer. We have observed a paradigm shift in file sharing as well as in communication. Data access has become decentralized and cloud services enable the user to access their data from anywhere at any time. Communication is mostly conducted over a third party which may be a social network or any other type of platform. The term knowledge worker has been coined by Peter Drucker more than 50 years ago and still describes the basic characteristics of a worker who's main capital is knowledge [15]. Social engineering is the most powerful tool for an attacker to access this knowledge. However, people freely publish information in online communication and collaboration tools, such as cloud services and on social networks with very little thought of security and privacy. In cloud services, highly sensitive documents and information is shared with other virtual users around the globe. Most of the time, users consider their interaction partners as trusted, even though the only identifying evidence is an E-Mail address or any other type of virtual profile. In recent years, security vulnerabilities in online communication and data sharing channels have often been misused to leak sensitive information. However, even security enhancing methods are powerless against users getting manipulated by social engineers. *Social Engineering* in general is the ability to obtain information by manipulating a person into simply giving information to the social engineer. It is used by malicious attackers to obtain secret information. Social engineering is one of the most powerful tools a hacker can utilize as even the most secure systems can be affected. The users themselves remain as the most vulnerable part of the system with respect to social engineering. Scientists have shown that social engineering is in many cases easy to automate and therefore can be performed large scale. Social engineering has become an emerging threat in virtual communities. The awareness for software security is-

sues and privacy enhancing methods has increased as serious incidents were reported in the media. E-Mail which is by no doubt the most frequently used communication channel on the Internet is daily flooded by scammers and social engineers, although the awareness for social engineering attacks over E-Mail has been raised among the users. However, the awareness for social engineering in cloud services and social networks is still comparatively low. Multinational cooperations and news agencies fell victims to sophisticated targeted attacks on their information systems. Google's internal system was compromised in 2009 [2], RSA security token system was broken in 2011 [1], Facebook was compromised in 2013 [3], as well as the New York Times [32]. Many *PayPal* costumers received phishing E-Mails [37] and many provided private information such as their credit card numbers to the attacker. These recent attacks on high-value assets are commonly referred to as Advanced Persistent Threats (APTs). APTs often rely on a common initial attack vector: social engineering such as spear-phishing and water-holing.

The main contributions of this paper are the following:

- We discuss social engineering with regards to knowledge workers.
- We provide a taxonomy of social engineering attacks.
- We give an overview of current attack vectors for social engineering attacks.

The goal of this paper is to provide an overview of social engineering attacks on the knowledge worker, and to monitor the state-of-the-art in research in this field. Furthermore, we provide a comprehensive taxonomy to categorize social engineering attacks and to measure the impact. The remainder of this paper is structured as follows: Section 2 provides a brief introduction to social engineering. Furthermore, in Section 3, we provide a detailed classification of social engineering attacks. In Section 4 we describe advanced social engineering attacks in online social networks, cloud services and mobile applications. Section 5 concludes our work.

2. BACKGROUND

This section discusses state-of-the-art work in the field of social engineering and computer-supported collaborative work (*CSCW*). We divide the attacks in four different categories, namely physical, technical, social and socio-technical approaches.

2.1 Social Engineering (SE)

Social Engineering is the art of exploiting users to compromise information systems. The focus of these attacks is on people instead of technical attacks on information systems. Social engineers try to manipulate their victims into divulging confidential information or performing their malicious objectives by using influence and persuasion. This form of attack thus often renders technical protection measures ineffective. People, in general, think that they are good at detecting these attacks. Research, however, indicates that people perform poorly on detecting lies and deception [34, 26]. The infamous attacks of Kevin Mitnick showed how devastating sophisticated social engineering attacks are for the information security of both companies and governmental organizations. In the area of information and computer security, social engineering is mostly discussed with examples and stories (such as Mitnick's). However, the field of social psychology entails important findings on the principles of persuasion. Especially the work of Cialdini [14], who is an expert in the field of persuasion, is frequently cited within contributions to social engineering research. Although Cialdini exemplifies persuasion on the basis of marketing, his principles are crucial to understand how deception works.

2.2 Types of Social Engineering Attacks

Social engineering attacks are multifaceted and include: physical, social, and technical aspects which are used in different stages of the actual attack. This subsection aims to explain the different approaches attackers use.

2.2.1 Physical approaches

With physical attacks, as the name implies, the attacker performs some form of physical action in order to gather information on a future victim, which can range from personal information (such as e.g. social security number, date of birth) to valid credentials for a computer system. A common technique is searching through the trash of an organization, which is also known as *dumpster diving* [16]. An organization's dumpster can provide valuable information for attackers such as personal data about employees, manuals, memos, and even print-outs of sensitive information such as user credentials. An attacker can also try to have a look at the office environment for information such as passwords written down on Post-it notes. Less sophisticated attacks of this kind involve *theft* or *extortion* to obtain information.

2.2.2 Social approaches

Obviously, social attacks are the most emergent facet of social engineering which use socio-psychological techniques such as Cialdini's principles of persuasion. According to [16] the most prevalent type of these social attacks is conducted by phone. To increase the chances of these attacks, the perpetrators try to develop a relationship with their future victims beforehand.

2.2.3 Reverse social engineering

Instead of contacting the victim, attackers can try to make the victims ask for help from them. This indirect approach is known as *"reverse social engineering"* [16, 28] and consists of three major parts: sabotage, advertising, and assisting [30]. At first the attackers sabotage the company's computer system, this can reach from disconnecting someone from the company's network up to sophisticated manipulations of the victim's software applications. The attackers then advertise that they can fix the problem. Finally when the victim asks for help the social engineers resolve the problem they created earlier and while doing so ask the victims to comply with their requests (e.g. "Password is needed to fix the problem", "software installation required" etc.).

2.2.4 Technical approaches

Technical facets of attacks are mainly carried out over the Internet. Granger [16] notes that the Internet is especially interesting for social engineers to harvest passwords, due to

the fact that users often use the same (simple) passwords for different accounts. Furthermore, most people are not aware that they give away a lot of personal information for free, which is useful to the attackers. Web search-engines are used by attackers to gather personal information about future victims. There are also tools available to gather and aggregate information from different web resources with Maltego[1] being one of the most popular of such tools. Social Networking Sites are becoming valuable sources for information as well, this issue is explained in more detail in Section 4.

2.2.5 Socio-technical approaches

Successful social engineering attacks often use the different facets, discussed so far, in combination. However, socio-technical approaches have led to the most powerful weapons of social engineers. Examples include so called *baiting*, hereby attackers leave malware-infected storage media in a location where it is likely to be found by future victims. Those *"road apples"* could for example be USB sticks containing a Trojan horse [39]. Attackers are furthermore exploiting the curiosity of people by adding tempting labels to these road apples (storage media) e.g. "confidential" or "personal layoff 2009". Another common combination of technical and social approaches is phishing. Phishing typically involves E-Mail or instant messaging and in comparison with social engineering aims, similar to Spam, at a large user group. Social engineering on the other hand is typically directed at single persons or small groups of people. Scammers hope that by the vast number of messages they send to users, enough people will get fooled and make their phishing attack profitable. Herley and Florencio [18] argue that classical phishing is not lucrative, which might explain why phishing attacks are moving towards more sophisticated "spear"-phishing attacks. Spear-Phishing attacks are highly targeted messages following initial data-mining. Jagatic et al. [24] used social networking sites to mine data on students which then received a message that looked like being send from a friend of the victim. The authors showed that they could increase the phishing success rate from 16 per cent to 72 using this "social data". Hence, spear-phishing can be seen as a marriage of social engineering and technology.

2.3 Computer-supported collaboration

In business execution we rely on a broad range of technologies used to facilitate, automate and enhance our daily tasks. In addition to these technologies, we have to consider that collaborative business structures are emerging supported by the usage of computer-supported collaboration tools in the fields of file sharing or collaborative workspaces, internal or external communication, blogs, wikis, etc. These tools are aimed at interlinking the staff and customers, and leading to widespread and instant information exchange about the whole business domain and establishing a constant communication channel to the customers and partners of the company.

Considering the multifarious communication channels that emerge with computer-supported collaboration tools, social engineering attacks have a broad range of attack potential. However, in business context we can differ between office communication and external communication enabling us to make predictions about the victim's ability to detect a social engineering attack.

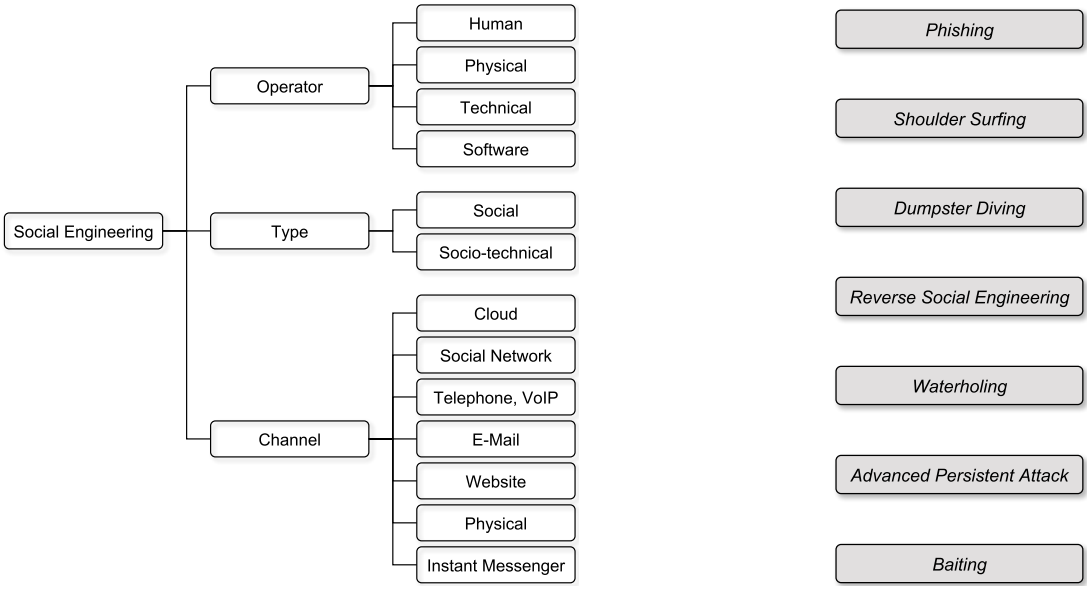
2.3.1 Office communication

The usage of communication tools changed the communication flows between the staff members enormously, facilitating high-speed exchange of information. The security of data transfer is already well-covered by sophisticated technologies. However, as the staff do not longer communicate face-to-face but rather hiding behind their email addresses and pseudonyms, we have to consider several implications for social engineering. Obviously, social engineering attacks that are started from internal accounts or emails with forged internal addresses are more likely to slip through the screening of a potential victim. For instance, Parsons et al. [31] conduced a role play scenario experiment where 117 participants were tested about their ability to judge about phishing emails and real emails. Their results indicates that people with a higher awareness level identify significantly more phishing emails. Valuable personal information that is retrieved from social engineering attacks could have direct consequences, such as the exploit of a bank account, or indirect consequences, such as reputation loss, [40] as well as it could be used for further social engineering attacks enhanced with the retrieved information of the previous attacks. Concluding, we face multifarious social engineering attacks and once an attack was successful the external adversary can use the information to become an insider and can then perform more successful social engineering attacks.

2.3.2 External communication

Similar that in respect to office communication, in external there is a trend towards the usage of email services, cloud, blogs, etc., and thus we have to face the same challenges than in internal communication. However, as the organizational border becomes more and more blurry, it is difficult to decide which information may be published to public or passed on to an external communication partner. For instance, marketing blogs are useful for advertisement purposes but also carry the risk of unwanted information leakage. Another example is the release of information like the information about staff members on XING, where a potential adversary can find out how many people are employed in a series of years, and thus infer the economic status of the respective company [7]. The most potential impact of external communication lies in the broad range of possible communication channels an external adversary can use. Furthermore, the possible channels are extended by new emerging trends, such as Bring Your Own Device (BYOD) [27], and the idea of "technology gets personal", which is used from Thomson [41] to explain the impact of using mobile devices to work with corporate information in insecure environments, such as cafes or public transport systems, and designates mobile technology as the "window into the enterprises". Of course, most of the systems have security systems installed; however, these systems do not protect the staff from social engineering attacks.

[1]Maltego is an open source intelligence and forensics application. It allows for the mining and gathering of information as well as the representation of this information in a meaningful way. `http://www.paterva.com/maltego/`



(a) Classification of attack characteristics.

(b) Social engineering attack scenarios.

Figure 1: Overview about our classification of attack characteristics and attack scenarios.

3. SOCIAL ENGINEERING TAXONOMY

In this Section, we propose a taxonomy to classify social engineering attacks. Figure 3 illustrates the structure of our taxonomy and attack scenarios that in this section we describe in detail. Table 1 provides an overview about the concrete classification of common attack scenarios according to our taxonomy.

To classify social engineering attacks, we first introduce three different main categories: **Type**, **Operator**, and **Channel**.

The channel over which an attack is performed can be as follows:

- **E-Mail** is the most common channel to perform phishing and reverse social engineering attacks.
- **Instant Messenger** are gaining popularity amongst social engineers to perform phishing and reverse social engineering attacks. The can be also used easily for identity theft to exploit a trustworthy relationship.
- **Telephone, Voice over IP** are common attack channels for social engineers to physically make the victim deliver sensitive information.
- **Social Networks** offer a variety of opportunities to social engineers to perform their attacks. With their potential to create fake identities and their complex information-sharing model they make it easy to for attackers to hide their identity and to harvest sensitive information.
- **Cloud** services can be used to create situational awareness of a situation within a collaboration scenario. The attackers may place a file or software in a shared directory to make the victim hand information over to them.
- **Website**s are most commonly used to perform waterholing attacks. Furthermore, they can be used in combination with E-Mails to perform a phishing attack (e.g.: sending an E-Mail to a (potential) customer of a bank that contains a link to a malicious website that looks just like the bank's original website.)
- **Physical** social engineering attacks are costly but very effective. This attack channel covers the scenario of the attackers physical presence during the attack is performed.

Moreover, we classify the attack according to it's originator. The originator of a social engineering attack can be:

- **Human** If the attack is directly conducted by a human. The number of targets is limited due to the capacities compared to an attack conducted by software.
- **Software** Some types of social engineering attacks are easy to automate as discussed by Boshmaf et al. [11], Huber et al. [21] and Krombholz et al. [25]. The main advantage of automated attacks is that the number of possible targets within a short period of time is incomparably high.

Furthermore, we categorize social engineering attacks into four types, namely:

- **Physical** as described in Section 2.2.1
- **Technical** as described in Section 2.2.4
- **Social** as described in Section 2.2.2
- **Socio-technical** as described in Section 2.2.5

Concerning social engineering, we determine the following attack scenarios: Attackers are performing social engineering attacks over a variety of different channels. They can mostly be conducted by humans as well as by software and furthermore be categorized as physical, technical, social or socio-technical. The boundaries concerning a different type of attack are highly expandable and in most cases not yet technically exhausted. Therefore, we consider the following attack scenarios as hard to match with the remaining categories.

- **Phishing** refers to the act of attempting to acquire sensitive information or to make somebody act in the favor of the attacker by masquerading as a trustworthy entity in an electronic communication medium. Phishing attacks can be performed over almost any channel, from physical presence of the attacker to websites, social networks or even cloud services. Apart from traditional phishing attacks, attacks targeted at specific individuals or companies are referred to as *spearphishing*. Spear-phishing requires the attacker to gather information on the directed victims, hence the success rate is higher than without defining a target group. If a phishing attack is aimed at high profile targets of enterprises, the attack is referred to as *whaling*.

- **Dumpster Diving** is the practice of sifting through physical waste or waste data of private individuals or companies to find discarded items that include sensitive information that can be used to compromise a system or a specific user account.

- **Shoulder Surfing** refers to using direct observation techniques to get information, just as looking over someone's shoulder.

- **Reverse Social Engineering** describes an attack that usually involves the establishment of trust between the attacker and the victim. The attackers create a situation where they must help the target individual and then pose as some people who the victim will recognize as individuals who can both solve the victim's problem and receive privileged information. Of course, the attackers try to choose an individual that they believe has information to help them.

- **Waterholing** describes a targeted attack where the attackers compromise a website that is likely to be of interest to the chosen victim. The compromised website is left and the attackers are waiting on the "waterhole" like a predator for their victim to visit.

- **Advanced Persistent Attack** refers to long-term mostly Internet-based espionage attacks conducted by an attacker who has the capabilities and intent to comprise a system persistently.

- **Baiting** refers to an attack when a malware-infected storage media is left in a location where it is likely to be found by the targeted future victims.

Table 1: Classification of social engineering attacks according to our taxonomy.

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Attack	Baiting
Channel	E-Mail	✓			✓			
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓		✓

4. STATE-OF-THE-ART ATTACKS

This section provides an overview of state-of-the-art social engineering attacks. These attacks often use personal information from online social networks or other cloud services and can be performed in an automated fashion.

4.1 Online Social Networks (OSNs)

While social engineering traditionally relies on information collected through dumpster diving or phone calls, OSNs contain a plethora of personal information which could be misused as an initial source for social engineering attacks. Because information harvested from OSNs can be easily processed, we were among the first researchers to argue that OSNs enable automated social engineering (ASE) attacks [19]. Reverse social engineering (RSE) describes a particular social engineering technique whereas an attacker lures targets into initializing the conversion. Irani et al. [23] argue that OSNs enable RSE attacks and describes three potential attack vectors. In the following, the authors evaluated their proposed attack vectors on three different OSNs: recommendation-based RSE on Facebook, demographic-based RSE on Badoo, as well as visitor tracking-based RSE on Friendster. Their results show that RSE attacks are feasible in practice and can be automated by exploiting the features of current online social networks. In comparison with social spam, attackers can send traditional email messages to delivery spam, because users provide their email addresses as part of their profiles. Hence, if spam is delivered via traditional email instead of OSN platforms, these malicious messages cannot be detected by the OSNs providers. Balduzzi et al. [8], for example, showed that OSNs can be misused for automated user profiling. The authors found that OSNs

can be misused to validate large sets of email addresses and to collect additional personal information corresponding to these sets.

Social-phishing and Context-aware spam

Phishing is a common threat on the Internet where an attacker tries to lure victims into entering sensitive information like passwords or credit card numbers into a faked website under the control of the attacker. It has been shown that social phishing [24], which includes some kind of "social" information specific to the victim, can be extremely effective compared to regular phishing. Jagatic et al. [24] found that once phishing mails impersonated a target's friend the success rate of their campaign increased from 16% to 72%. The social graph is therefore not only of value for the social network operator, but for attackers as well. Especially if it contains additional information like a valid email address or recent communication between the victim and the impersonated friend. With automated data extraction from social networks, a vast amount of further usable data becomes available to spammers. Prior conversations within the social network like private messages, comments or wall posts could be used to deduce the language normally used for message exchange between the victim and the spam target. For example, a phishing target might find it very suspicious if someone sends a message in English if they normally communicate in French. Context-aware spam misuses personal information extracted from OSNs to increase the authenticity of traditional spam messages. Brown et al. [12] identified three context-aware spam attacks which might be misused: relationship-based attacks, unshared-attribute attacks, as well as shared-attribute attacks. Relationship-based attacks solely exploit relationship information, this attack thus represents the spam equivalent of social phishing. The two remaining attacks exploit additional information from social networks, which could either be shared or unshared amongst the spam target and the spoofed friend. An example for an unshared attack are birthday cards that seem to origin from the target's friend. Finally, attackers might exploit shared attributes for context-aware spam, such as photos where both the spam target and her spoofed friend are tagged. Huber et al. [20, 22] found that the missing support for communication security can be exploited to automatically extract personal information from online social networks. Moreover, the authors showed that the extracted information might be misused to target a large number of users with context-aware spam.

Fake profiles

At the time of writing the only requirement for the creation of a social networking account is a valid email address, fake accounts can therefore be relatively easy created by attackers. A study by Sophos in 2007 showed, based on randomly chosen Facebook users, that around 41% of social networking users accepted friendship requests from a fake profile they set up [38]. Ryan and Mauch [4] further showed that fake profiles can be misused to infiltrate social networks and gain access to sensitive information in the military and information security community. Bilge et al. [10] outlined two sophisticated fake profile attacks to infiltrate the trusted circles of social networking users. First, with profile cloning attacks, attackers clone existing user profiles and attempt "reinvite" their friends. Second, with cross-profile cloning attacks, attackers create a cloned profile on a online social network where the target users do not have a profile yet and contact the targets' friends. For example, if a user has a Facebook account but no LinkedIn account, an attacker clones the Facebook profile of the target to LinkedIn and contacts the target's Facebook friends who are also on LinkedIn. Bilge et al. showed that their attacks can be fully automated and are feasible in practice. If an attacker is able to create fake accounts on a large scale, sybil attacks on ONSs become possible. OSN provider therefore employ a number of protection mechanisms to limit the creation of large amounts of fake accounts. Boshmaf et al. [11] found that OSNs can be infiltrated on a large scale and evaluated how vulnerable OSNs are to a large-scale infiltration by socialbots: computer programs that control OSN accounts and mimic real users. The authors created a *Socialbot* Network (SbN): a group of adaptive socialbots that are orchestrated in a command-and-control fashion, on basis of Facebook. Hereby, the authors used 102 fake profiles to sent friendship requests to a random sample of 5,053 Facebook users. Overall friendship requests were accepted by 19.3% of all users. In the following the SbN tried to infiltrate the circle of friends of users who accepted their fake friend requests. Within 8 weeks SbN was able to further infiltrate social networking users and gain access to personal information. A recent survey by Alvisi et al. [6] provides an overview on sybil defenses based for online social networks and proposes community detection algorithms for sybil detection.

4.2 Cloud services

Cloud services provide a new channel for social engineers to conduct attacks on the knowledge worker. For knowledge workers, it is a very common scenario to collaborate with others that are distributed over multiple places and therefore to share information over a cloud service. In this scenario, an attacker can exploit this situation using the cloud as a channel to perform a social engineering attack. There is a variety of possible attacks in the cloud described in recently published scientific papers. One is that an attacker can place a malicious file into another user's cloud as described by Gruschka et al. [17] and to use social engineering to make her execute the malicious file. A malicious piece of software can be used to extract personal information from the victim's account. This information is then used by the attacker to perform more targeted attacks. Mulazzani et al. [29] provide countermeasures to reduce the risk by preventing the attacker from placing a malicious file on Dropbox, which is currently one of the most commonly used cloud services. Concerning social engineering, at this point it must be clarified that the level of trust between users of a shared directory or file is not always as high as desired. Social engineers can exploit this fact by using a fake identity or a compromised user account to invite the victim to share specific information with the attacker on the cloud. According to Roberts et al. [35] one of the biggest weaknesses is that the companies and individuals loose control over their data when using a cloud service to store and access their data. On traditional servers that are owned by the users themselves, the companies can restrict the access and define customized access policies. By using a cloud services, the responsibility is shifted to a third-party. Hence, when using cloud services for sensitive information exchange, a certain level of trust must be established not only between the collaborators but

also the cloud hosting company and the user. Most commonly observed attacks on cloud services are spear-phishing and APTs.

4.3 Mobile applications

Mobile application are more and more serving a channel to perform social engineering attacks. In business communication, especially mobile messaging and E-Mail application that are used to exchange information by knowledge workers are of high interest for social engineers. *BYOD* policies established by companies often include the usage of mobile phones and tablets. More and more employees check their company E-Mails on their smartphones or read documents stored in a cloud. However, many smartphone users use highly vulnerable smartphone applications that can be misused to conduct social engineering attacks and to gather sensitive information. Schrittwieser et al. [36] presented two different attack scenarios that can serve as a starting point to perform such an attack. In their work [36] they demonstrated how sender ID spoofing is performed on popular mobile messaging applications such as *Whatsapp* [5]. Sender ID spoofing can be used by a social engineer to send a fake message by a pretended friend of the victim. Furthermore, they highlighted how vulnerabilities can be exploited to hijack user accounts that can then be used to perform social engineering. Taken the fact into consideration that many smartphone applications are highly vulnerable and leaking sensitive information, we determine that such mobile devices offer a variety of attack vectors for social engineering and other attacks on user privacy. Moreover, some smartphone applications require permissions to access sensitive data on the user's device. Assuming the attacker is a publisher of such an application, the information obtained through access on these data can also be used as a starting point for a social engineering attack. Chin et al. [13] discussed how inter-application information exchange can be sniffed on smartphones, and then be misused to violate application policies and permissions. In some cases, such as described by Potharaju et al. [33], the attacker simply plagiarizes a popular smartphone application and deploys it in order to perform an attack.

5. CONCLUSIONS

In this paper, we described common attack scenarios for modern social engineering attacks on knowledge workers. Bring your own device policies and distributed collaboration as well as communication over third-party channels offers a variety of new attack vectors to perform advanced social engineering attacks. In order to develop efficient countermeasures to prevent knowledge workers from social engineering attacks, we believe that a detailed understanding of the attack vectors is necessary. Therefore we introduced a comprehensive taxonomy to classify social engineering attacks with respect to the attack channel, the operator, different types of social engineering and specific attack scenarios. Furthermore, we discussed real-world examples and advanced attack vectors in popular communication channels and computer-supported collaboration used by knowledge workers in the business environment, such as cloud services, social networks and mobile devices as part of *BYOD* policies. In this work, we discussed not only complex advanced attack scenarios but also provided a comprehensive classification to support the development of countermeasures and further interdisciplinary research in the field.

6. ACKNOWLEDGEMENTS

This research was funded by the Austrian Science Fund (FWF): P 26289-N23 and COMET K1, FFG - Austrian Research Promotion Agency.

7. REFERENCES

[1] Anatomy of an attack. available online: http://httpblogs.rsa.com/anatomy-of-an-attack/, last accessed on 2013-07-17.

[2] Google hack attack was ultra sophisticated. available online: http://www.wired.com/threatlevel/2010/01/operation-aurora/, last accessed on 2013-07-17.

[3] Microsoft hacked: Joins apple, facebook, twitter – InformationWeek. available online: http://www.informationweek.com/security/Attackacks/microsoft-hacked-joins-apple-facebook-tw/240149323, last accessed on 2013-07-10.

[4] The robin sage experiment: Fake profile fools security pros. available at http://www.networkworld.com/news/2010/070810-the-robin-sage-experiment-fake.html?t51hb, last accessed on: 2013-07-14.

[5] Whatsapp. available online: http://www.whatsapp.com/, last accessed on 2013-07-18.

[6] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi. Sok: The evolution of sybil defense via social networks. *IEEE Symposium on Security and Privacy*, 2013.

[7] G. Bader, A. Anjomshoaa, and A. Tjoa. Privacy aspects of mashup architecture. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, pages 1141–1146, 2010.

[8] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel. Abusing social networks for automated user profiling. In *Recent Advances in Intrusion Detection*, pages 422–441. Springer, 2010.

[9] R. Ballagas, M. Rohs, J. G. Sheridan, and J. Borchers. Byod: Bring your own device. In *In Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp*, 2004.

[10] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web*, pages 551–560. ACM, 2009.

[11] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 93–102. ACM, 2011.

[12] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders. Social networks and context-aware spam. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, CSCW '08, pages 403–412, New York, NY, USA, 2008. ACM.

[13] E. Chin, A. P. Felt, K. Greenwood, and D. Wagner. Analyzing inter-application communication in android. In *Proceedings of the 9th international conference on Mobile systems, applications, and services*, MobiSys '11, pages 239–252, New York, NY, USA, 2011. ACM.

[14] R. Cialdini. *Influence: science and practice*. Allyn and Bacon, 2001.

[15] P. F. Drucker. *Landmarks of tomorrow: a report on the new "post-modern" world*. Harper, New York, 1st edition, 1959.

[16] S. Granger. Social Engineering Fundamentals, Part I: Hacker Tactics. *SecurityFocus*, 2001.

[17] N. Gruschka and M. Jensen. Attack surfaces: A taxonomy for attacks on cloud services. In *IEEE CLOUD*, pages 276–279, 2010.

[18] C. Herley and D. Florencio. Phishing as a Tragedy of the Commons. *NSPW 2008, Lake Tahoe, CA*, 2008.

[19] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa. Towards automating social engineering using social networking sites. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, volume 3, pages 117–124. IEEE, 2009.

[20] M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, and E. Weippl. Social snapshots: digital forensics for online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*, 2011.

[21] M. Huber, M. Mulazzani, S. Schrittwieser, and E. Weippl. Cheap and automated socio-technical attacks based on social networking sites. In *3rd Workshop on Artificial Intelligence and Security (AISec'10)*, 10 2010.

[22] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch. Friend-in-the-middle attacks: Exploiting social networking sites for spam. *IEEE Internet Computing: Special Issue on Security and Privacy in Social Networks*, 5 2011.

[23] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu. Reverse social engineering attacks in online social networks. *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 55–74, 2011.

[24] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007.

[25] K. Krombholz, D. Merkl, and E. Weippl. Fake identities in social media: A case study on the sustainability of the facebook business model. *JoSSR*, 4(2):175–212, 2012.

[26] K. Marett, D. Biros, and M. Knode. Self-efficacy, Training Effectiveness, and Deception Detection: A Longitudinal Study of Lie Detection Training. *lecture notes in computer science*, 3073:187–200, 2004.

[27] K. Miller, J. Voas, and G. Hurlburt. Byod: Security and privacy considerations. *IT Professional*, 14(5):53–55, 2012.

[28] K. Mitnick and W. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.

[29] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. Weippl. Dark clouds on the horizon: using cloud storage as attack vector and online slack space. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 5–5, Berkeley, CA, USA, 2011. USENIX Association.

[30] R. Nelson. Methods of Hacking: Social Engineering. online, 2008. available at: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html, last accessed on 2013-07-04.

[31] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram. Phishing for the truth: A scenario-based experiment of usersâĂŹ behavioural response to emails. In L. Janczewski, H. Wolfe, and S. Shenoi, editors, *Security and Privacy Protection in Information Processing Systems*, volume 405 of *IFIP Advances in Information and Communication Technology*, pages 366–378. Springer Berlin Heidelberg, 2013.

[32] N. Perlroth. Chinese hackers infiltrate new york times computers, Jan. 2013. available at https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html, last accessed on: 2013-07-01.

[33] R. Potharaju, A. Newell, C. Nita-Rotaru, and X. Zhang. Plagiarizing smartphone applications: attack strategies and defense techniques. In *Proceedings of the 4th international conference on Engineering Secure Software and Systems*, ESSoS'12, pages 106–120, Berlin, Heidelberg, 2012. Springer-Verlag.

[34] T. Qin and J. Burgoon. An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. *Intelligence and Security Informatics, 2007 IEEE*, pages 152–159, 2007.

[35] J. C. Roberts, II and W. Al-Hamdani. Who can you trust in the cloud? a review of security issues within cloud computing. In *Proceedings of the 2011 Information Security Curriculum Development Conference*, InfoSecCD '11, pages 15–19, New York, NY, USA, 2011. ACM.

[36] S. Schrittwieser, P. Fruehwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. Weippl. Guess Who Is Texting You? Evaluating the Security of Smartphone Messaging Applications. In *Network and Distributed System Security Symposium (NDSS 2012)*, 2 2012.

[37] SocialEngineer. What is phishing – paypal phishing examples. available online: http://www.social-engineer.org/wiki/archives/Phishing/Phishing-PayPal.html, last accessed on 2013-07-04.

[38] Sophos. Sophos facebook id probe shows 41% of users happy to reveal all to potential identity thieves, 2007. available online: http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx, last accessed on 2013-07-13.

[39] S. Stasiukonis. Social Engineering, the USB Way. 2006. available at http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634, last accessed on: 2013-07-02.

[40] L. Tam, M. Glassman, and M. Vandenwauver. The psychology of password management: a tradeoff

between security and convenience. *Behav. Inf. Technol.*, 29(3):233–244, May 2010.

[41] H. Thompson. The human element of information security. *Security Privacy, IEEE*, 11(1):32–35, 2013.