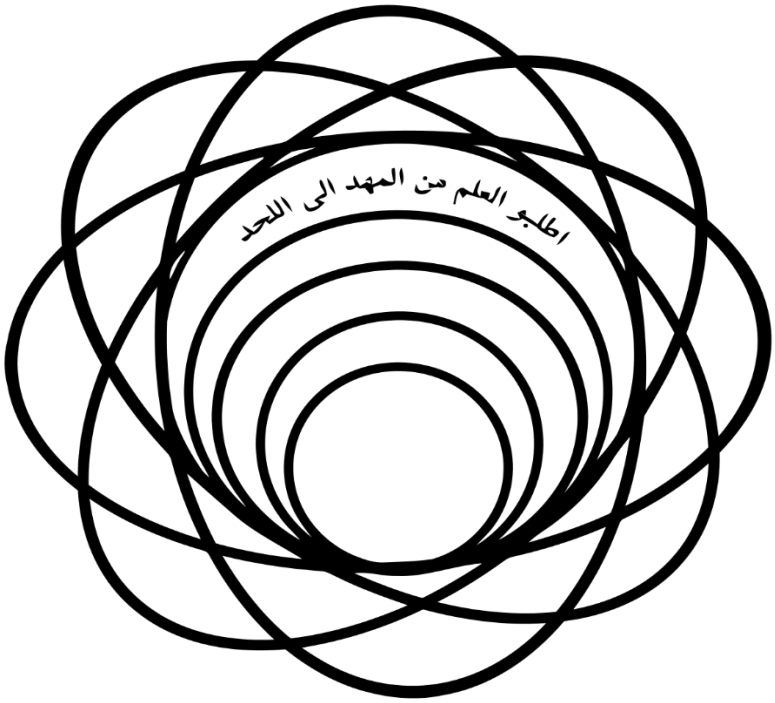

Shamsipour Technical and Vocational College

Eric Mangasar

Email : ttlking3@icloud.com

Social Engineering Attacks

Abstract

Social engineering has began as a serious warning in virtual communities and is an effective income to attack information systems. The services used by today's knowledge workers make the ground for sophisticated social engineering attacks. The rising trend towards BYOD (bring your own device) policies and the use of online communication and teamwork tools in private and business environments worsen the problem. In globally acting companies, teams are no longer physically co-located, but staffed just-in-time. The drop in personal interaction combined with a excess of tools used for communication (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 and RSA have shown that targeted spear-phishing attacks are an effective, evolutionary step of social engineering attacks. Mutual with zero-day-exploits, they become a risky weapon that is often used by advanced determined threats. This paper provides a taxonomy of well-known social engineering attacks as well as a complete overview of advanced social engineering attacks on the knowledge worker.

1. Introduction

The Internet has become the main communication and information exchange medium. In our everyday life, communication has become dispersed over a variety of online communication channels. In adding to e-mail and IM communication, Web 2.0 services such as Twitter, Facebook, and other social networking sites have become a part of our regular routine in private and business communication. Companies guess their employees to be highly mobile and flexible regarding their workspace and there is an increasing tendency towards expecting employees and knowledge workers to use their own devices for work, both in the office and somewhere else. This increase in flexibility and, equally, reduction in face-to-face communication and shared office space means that increasing quantities of data need to be made available to co-workers done online channels. The development of dispersed data access and cloud services has carried about a standard shift in file sharing as well as communication, which today is mostly showed over a third party, be it a social network or any other type of platform. In this world of universal communication, people freely publish information in online communication and teamwork tools, such as cloud services and social networks, with very little believed of security and privacy. They share highly complex documents and information in cloud services with other virtual users around the world. Most of the time,users reflect their communication partners as trusted, even though the only identification is an e-mail address or a virtual profile. In recent years, security vulnerabilities in online communication and data sharing channels have often been distorted to leak sensitive information. Such vulnerabilities can be fixed and the security of the channels can be wired. However, even security-enhancing methods are weak when users are operated by social engineers. The term

knowledge worker was coined by Peter Drucker more than 50 years ago and still describes the basic features of a worker whose main capital is knowledge.The most powerful tool an attacker can use to access this knowledge is Social Engineering: operating a person into giving information to the social engineer. It is larger to most other forms of hacking in that it can opening even the most secure systems, as the users themselves are the most vulnerable part of the system. Research has shown that social engineering is easy to mechanize in many cases and can therefore be performed on a large gauge. Social engineering has become an developing threat in virtual communities. International corporations and news agencies have fall over victim to sophisticated targeted attacks on their information systems. Google's internal system was cooperated in 2009, the RSA security token system was broken in 2011, Facebook was cooperated in 2013, as was the New York Times. Many PayPal costumers have received phishing e-mails and many have given the attackers private information such as credit card numbers. These recent attacks on high-value resources 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 alertness for software security issues and privacy-improving methods has increased as thoughtful incidents have been reported in the media. For example, the alertness for social engineering attacks over e-mail, which is without hesitation the most frequently used communication channel on the Internet and is flooded by scammers and social engineers every day, has increased among users. However, the alertness for social engineering in cloud services and social networks is still comparatively low.

The main assistances of this article are the following:

• We discuss social engineering with respects to knowledge workers.

• We provide a taxonomy of social engineering attacks.

• We give an overview of current attack vectors for social engineering attacks.

• We confer real-world events of successful social engineering attacks.

The goal of this paper is to deliver a full and complete overview of social engineering attacks on the knowledge worker, to monitor the state of the art of research in this field, and to provide a full taxonomy to categorize social engineering attacks and amount their impact. Our paper significantly extends the state of the art by including novel, non-traditional attacks such as APTs. Our taxonomy extends and combines already existing work in this field, e.g., by Ivaturi et al. and Foozy et al. Also, our taxonomy systemizes operators, channels, types and attack vectors as well. The remainder of this paper is organized as follows: Section 2 contains a brief overview to social engineering. In Section 3, we provide a full classification of social engineering attacks. In Section 4, we describe advanced social engineering attacks in online social networks, cloud services and mobile applications. Before final our work in Section 6, we discuss recent real-world social engineering attacks in Section 5.

2. Background

This section discusses the state of the art of social engineering and computer-supported cooperative work (CSCW). Attacks are separated into four different categories: physical, technical, social and socio-technical approaches.

2.1. Social Engineering (SE)

Social engineering is the art of getting users to cooperation information systems. In its place of technical attacks on systems, social engineers target humans with access to information, operating them into exposing confidential information or even into carrying out their malicious attacks

through influence and persuading. Technical protection events are usually ineffective in contradiction of this kind of attack. In adding to that, people generally believe that they are good at noticing such attacks. Research, however, shows that people perform unwell on detecting lies and dishonesty. The infamous attacks of Kevin Mitnick showed how shocking sophisticated social engineering attacks are for the information security of both companies and governmental organizations. When social engineering is deliberated in the information and computer security field, it is usually by way of examples and stories (such as Mitnick's). However, at a more important level, important findings have been made in social psychology on the values of persuasion. Mainly the work of Cialdini, an expert in the field of influence, is frequently cited in contributions to social engineering research. Though Cialdini's examples focus on persuasion in marketing, the important principles are critical for anyone seeking to understand how deception works.

2.2. Types of Social Engineering Attacks

Social engineering attacks are multilayered and include physical, social and technical features, which are used in different stages of the actual attack. This subset aims to explain the different approaches attackers use.

2.2.1. Physical approaches

As the name suggests, physical approaches are those where the attacker performs some form of physical action in order to fold information on a future victim. This can range from personal information (such as social security number, date of birth) to valid identifications for a computer system. An often-used method is dumpster plunging, i.e., searching through an organization's

garbage. A dumpster can be a valuable source of information for attackers, who may find personal data about employees, guides, memos and even print-outs of complex information, such as user credentials. If an attacker can advance access to a targeted organization's offices - e.g., in open-plan workspaces - they may find information such as passwords written on Post-it notes. Less sophisticated physical attacks include theft or pressure to get information.

2.2.2. Social approaches

The most important feature of successful social engineering attacks are social approaches. Hereby attackers trust on socio-psychological techniques such as Cialdini's values of influence to operate their victims. Examples of influence methods include the use of (purported) expert. One common social vector that is not clearly addressed by Cialdini is curiosity, which is, e.g., used in spear-phishing and tempting attacks. In order to rise the chances of success of such attacks, the committers often try to develop a relationship with their future victims.According to, the most predominant type of social attacks is done by phone.

2.2.3. Reverse social engineering

In its place of contacting a potential victim directly, an attacker can effort to make them believe that he/she is a dependable entity. The goal is to make possible victims approach him, e.g., to ask for help. This secondary approach is known as "reverse social engineering" and contains of three major parts: sabotage, advertising and support. The first step in this is damaging the company's computer system. This can range anywhere from disconnecting someone from the company's network to sophisticated operation of the victim's software applications. The attackers then promote that they can fix the problem. When the victim asks for help, the social engineer will

resolve the problem they created earlier while, e.g., asking the victim for their password (”so I can fix the problem”) or forceful them to install certain software.

2.2.4. Technical approaches

Technical attacks are mostly carried out over the Internet. Granger notes that the Internet is particularly interesting for social engineers to produce passwords, as users often use the same (simple) passwords for different accounts. Most people are also not conscious that they are freely provided that attackers (or anyone who will search for it) with sufficiently of personal information. Attackers often use search engines to fold personal information about future victims. There are also tools that can fold and collective information from different Web resources. One of the most popular tools of this kind is Maltego1. Social networking sites are becoming valued sources of information as well (see Section 4 for more details).

2.2.5. Socio-technical approaches

Positive social engineering attacks often syndicate several or all of the different approaches deliberated above. However, socio-technical approaches have created the most powerful weapons of social engineers. One example is the so-called baiting attack: Attackers leave malware-infected storage media in a location where it is probable to be found by future victims. Such “road apples” could, e.g., be a USB drive comprising a Trojan horse. Attackers furthermore exploit the interest of people by adding enticing labels to these road apples (storage media), such as “confidential” or “staff lay-off 2014”. Another common grouping of technical and social approaches is phishing. Phishing is usually complete via e-mail or instant messaging and is intended at a large user group in a rather unselective way, similar to spam. Social engineering, in contrast,1Maltego is an open

source intellect and forensics application. It allows the mining and collecting of information as well as the representation of this information in a expressive way. http://www. paterva.com/maltego/

is typically directed at individuals or small groups of people. Scammers hopefulness that by sending messages to a massive number of users, they will fool enough people to make their phishing attack profitable. Herley and Florencio argue that classical phishing is not lucrative, which might clarify why phishing attacks are moving towards more sophisticated “spear-phishing” attacks. Spear-phishing attacks are highly targeted messages carried out after original data-mining. Jagatic et al.used social networking sites to mine data on students and to then send them a message that looked like it had been sent by one of their friends. By using such “social data”, the writers were able to rise the success rate of phishing from 16 to 72 percent. Hence, spear-phishing is considered a grouping of technological approaches and social engineering.

2.3. Computer-supported collaboration

Businesses and employees use a extensive range of technologies to enable, automate and progress daily tasks. We also see cooperative business structures emerging: Computer-supported teamwork tools for file sharing or cooperative workspaces, internal or external communication, blogs, wikis, etc., help connect staff within the company and to customers, allow extensive and prompt information exchange about the entire business domain, and launch a constant communication channel to the customers and partners of the company. Considering the extensive range of different communication channels created by these computer-supported teamwork tools, social engineering attacks have a huge attack potential. However, in the business context, we differentiate between

office communication and external communication. This enables us to make guesses about a victim's ability to detect a social engineering attack.

2.3.1. Office communication

Modern communication tools have changed communication flows amongst staff members extremely, making the high-speed exchange of information probable. There are sophisticated technologies that protect the security of data transfer. However, the mainstream of these countermeasures cover technical attacks, while social engineering attacks remain unthinking. In enterprise situations, face-to face communication is often swapped by e-mails or instant messages, making a novel attack surface for social engineers. Clearly, social engineering attacks coming from inner accounts or e-mails with forged internal addresses are more likely to slip through the defenses of a possible victim. For example, Parsons et al. showed a roleplay scenario experimentation in which 117 participants were tested on their capability to differentiate between phishing emails and benign e-mails. Their results specified that people with a higher alertness level are able to identify expressively more phishing e-mails. Valuable personal information expanded through social engineering attacks could have direct significances, such as the exploit of a bank account, or indirect significances, such as status loss; it could also be used to improve the effectiveness of further social engineering attacks.

Overall, we face miscellaneous social engineering attacks - once an attack is successful, the outer adversary can use the information to convert an insider and make even more successful social engineering attacks.

2.3.2. External communication

As with intra-office communication, there is a tendency towards the use of e-mail services, cloud, blogs, etc., for outer communication, creating the same tests as in inner communication. However, as the organizational edge becomes progressively blurred, it is difficult to choose which information may be published or approved on to an outer communication partner. For example, marketing blogs are useful for promotion purposes, but also carry the risk of undesirable information leakage. Another example is the publication of information, e.g., about staff members, on LinkedIn, where a possible opponent can find out how many people are employed over a number of years and infer the financial status of the separate company from this data. The strongest potential risk of outer communication lies in the broad range of probable communication channels. Additionally, new tendencies increase the number of channels, such as Bring Your Own Device (BYOD) and the knowledge of "technology gets personal", which is used by Thomson to explain the impression of using mobile devices to work with business information in insecure situations, such as caf´es or public transportation systems. He mentions to mobile technology as the "window into the enterprises". Of course, security systems are installed on maximum of these devices; however, these systems offer no protection from social engineering attacks.

3. Social Engineering Taxonomy

In this section, we suggest a taxonomy for the classification of social engineering attacks. Figure 1 illuminates the structure of our taxonomy and the attack scenarios, which we define in detail in this section. To classify social engineering attacks, we first current three core categories: Channel, Operator, and Type.

Attacks can be completed via the following channels:

• E-mail is the maximum common channel for phishing and reverse social engineering attacks.

• Instant messaging applications are achievement popularity amongst social engineers as tools for phishing and reverse social engineering attacks. They can also be used easily for identity theft to exploit a dependable relationship.

• Telephone, Voice over IP are mutual attack channels for social engineers to make their victim deliver complex information.

• Social networks offer a diversity of chances for social engineering attacks. Given their possible to create fake identities and their complex informations haring model, they make it easy for attackers to hide their identity and harvest complex information.

• Cloud services can be used to improvement situational alertness of a teamwork scenario. Attackers may place a file or software in a shared directory to make the victim hand information over.

• Websites are most usually used to perform waterholing attacks. Additionally, they can be used in grouping with e-mails to perform phishing attacks (e.g., sending an e-mail to a potential customer of a bank that covers a link to a malicious website that looks just like the bank's original website).

We also classify the attack by operative. The originator (operator) of a social engineering attack can be:

• Human: If the attack is showed directly by a person. The number of targets is limited owing to the lower capacity compared to an attack showed by software.

• Software: Certain types of attacks can be automatic with software. Examples include the Social Engineering Toolkit (SET), which can be used to craft spearphishing e-mails. A number of writers have discussed automatic social engineering based on online social networks, such as Boshmaf et al, Huber et al. and Krombholz et al. The main benefit of automatic attacks is that the number of

possible targets that can be reached within a short period of time is significantly higher than with purely human attacks.

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

• Physical as defined in Section 2.2.1

• Technical as defined in Section 2.2.4

• Social as defined in Section 2.2.2

• Socio-technical as defined in Section 2.2.5

Concerning social engineering, we control the following attack scenarios: Attackers perform social engineering attacks over a variety of different channels. They are mostly showed by humans as well as by software and additionally categorized as physical, technical, social or socio-technical. The limits of the individual types of attack are highly inflatable and have, in most cases, not yet been technically exhausted.

• Phishing is the attempt to obtain sensitive information or to make somebody act in a wanted way

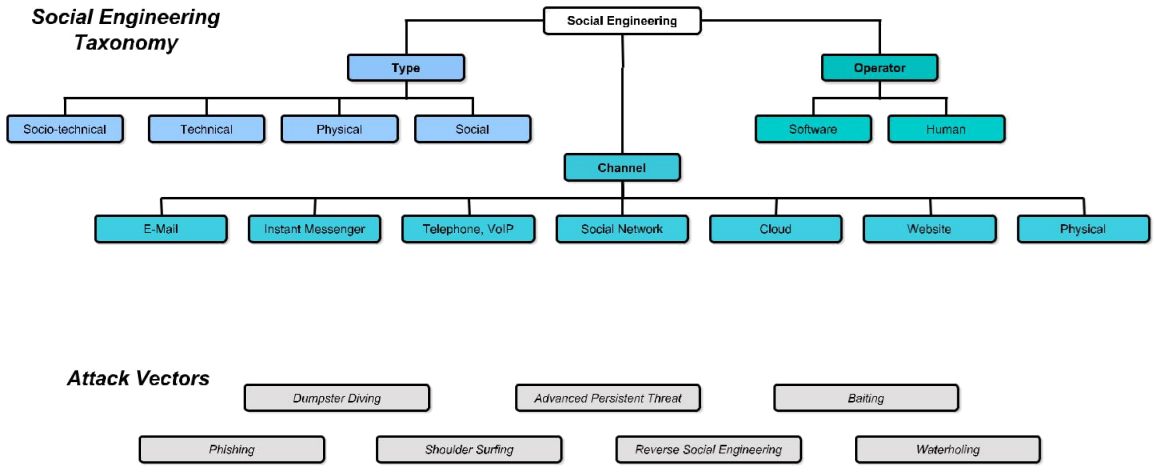

Figure 1: Impression of our classification of attack features and attack scenarios.

by masquerading as a dependable entity in an electronic communication medium. They are typically targeted at large groups of people. Phishing attacks can be achieved over almost any channel, from physical attendance of the attacker to websites, social networks or even cloud services. Attacks targeted at specific people or companies are referred to as spearphishing. Spear-phishing needs the attacker to first gather information on the planned victims, but the success rate is higher than in conservative phishing. If a phishing attack is intended at high-profile targets in enterprises, the attack is referred to as whaling.

• Dumpster diving is the exercise of sifting through the garbage of private people or companies to find rejected items that include sensitive information that can be used to cooperation a system or a specific user account.

• Assume surfing refers to using direct remark techniques to get information, such as looking over someone's assume at their screen or keyboard.

• Reverse social engineering is an attack where regularly trust is recognized between the attacker and the victim. The attackers create a condition in which the victim requires help and then present themselves as someone the victim will reflect someone who can both answer their problem and is allowed to receive advantaged information. Of course, the attackers try to choose an separate who they believe has information that will help them.

• Waterholing defines a targeted attack where the attackers cooperation a website that is probable to be of interest to the chosen victim. The attackers then wait at the waterhole for their victim.

• Progressive Persistent Threat refers to long-term, regularly Internet-based espionage attacks showed by an attacker who has the abilities and intent to comprise a system obstinately.

• Baiting is an attack during which a malware-infected storing medium is left in a location where it is probable to be found by the targeted victims.

Table 1 frameworks the relationship between our proposed social engineering taxonomy and present attack scenarios. We classified existing social engineering attack scenarios based on our taxonomy. We can, for example, detect that a number of social engineering attacks completely rely on a physical attack channel, such as assume surfing, dumpster diving and baiting. To protect against this class of attacks, physical security needs to be enhanced. The table additionally highlights that the mainstream of today's social engineering attacks rely on a grouping of social and technical methods. Hence, to effectively protect against socio-technical attacks, user alertness for social engineering attacks needs to be enhanced and their devices protected on a technical level.

4. State-of-the-Art Attacks

This section delivers an impression of state-of-the-art social engineering attacks. These attacks frequently use personal information from online social networks or other cloud services and can be completed in an automatic fashion.

4.1. Online Social Networks (OSNs)

While the more old-style forms of social engineering use information calm through dumpster diving or phone calls, OSNs cover a wealth of personal information that can be distorted as an initial source for social engineering attacks. Huber et al. were amongst the first researchers to argue that OSNs enable automatic social engineering (ASE) attacks because information harvested from OSNs is easy to process.

		Phishing	Shoulder ngSur	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Threat	Baiting
Channel	E-mail	X			X		X	
	Instant Messenger	X			X			
	Telephone, VoIP	X			X			
	Social Network	X			X			
	Cloud	X						
	Website	X				X	X	
	Physical	X	X	X	X			X
Operator	Human	X	X	X	X			X
	Software	X		X	X	X	X	
Type	Physical		X	X				X
	Technical					X	X	
	Social				X			
	Socio-technical	X			X	X	X	X

that information on employees of a assumed target company can be calm in an automatic fashion and possibly misused for automatic social engineering. Reverse social engineering describes a specific social engineering technique where an attacker lures the victim into starting the conversion as described in 2.2.3. Irani et al.argue that OSNs enable reverse social engineering attacks and define three possible attack vectors. The writers evaluated their proposed attack vectors on three different OSNs: recommendation-based inverse social engineering on Facebook, demographic-

based inverse social engineering on Badoo and visitor-tracking-based inverse social engineering on Friendster. Their results show that inverse social engineering attacks are possible in practice and can be automatic by exploiting the features of current online social networks. While social spam is usually sent via an OSN's primary communication channel, attackers who harvest information can also send old-style e-mail messages to deliver spam because users provide their email addresses on their profiles. If spam is delivered via traditional e-mail instead of OSN platforms, these hateful messages cannot be detected by the OSN's provider. Balduzzi et al showed that OSNs can be distorted for automatic user profiling, to validate large sets of e-mail addresses and to collect extra personal information corresponding to these sets.

Social phishing and context-aware spam Phishing is a widely-spread danger on the Internet and contains of an attacker attempting to lure victims into entering complex information like passwords or credit card numbers into a faked website that is controlled by the attacker. It has been shown that social phishing, where "social" information specific to the victim is used, can be particularly effective equated to regular phishing. Jagatic et al found that when phishing e-mails mimicked a target's friend, the achievement rate improved from 16% to 72%. The social graph is, therefore, not only of value for the social network operator, but also for attackers. This is the case particularly if it covers additional information like a valid e-mail address or recent communication between the victim and a friend whom the attacker can mimic. With automatic data extraction from social networks, a vast quantity of further usable data becomes available to spammers. Prior talks within the social network, such as private messages, comments or wall posts, could be used to control the language normally used for message exchange between the victim and his friends, as a phishing target might find it very doubtful to receive a message in English from a friend with whom they generally communicate in French. Context-aware spam misappropriations personal information

extracted from OSNs to rise the appearance of validity of old-style spam messages. Brown et al. identified three context-aware spam attacks: relationship-based attacks, unshared-attribute attacks, and shared-attribute attacks. Relationship-based attacks exclusively exploit relationship information, making this the spam equal of social phishing. The two other attacks exploit extra information from social networks, information that is either shared or not shared between the spam target and the tricked friend. An example of an unshared attack are birthday cards that seem to create from the target's friend. Shared attributes, e.g., photos in which both the spam target and her spoofed friend are tagged, can be exploited for context-aware spam. Huber et al found that the lost support for communication security can be exploited to mechanically extract personal information from online social networks. Moreover, the writers showed that the extracted information could be distorted to target a large number of users with context-aware spam.

Fake profiles

At the time of writing, the only necessity for the creation of a social networking account is a usable e-mail address, which makes it rather easy for attackers to create fake accounts. A study by Sophos published in 2007 with casually chosen Facebook users showed that approximately 41% of social networking users accepted friendship requirements from a fake profile. Ryan and Mauch additional showed that fake profiles can be distorted to infiltrate social networks: they set up a profile for a fictional American cyber danger analyst, called "Robin Sage", and were able to gain access to complex information in the armed and information security community. Bilge et al.outlined two sophisticated fake profile attacks that could be used to infiltrate the trusted circles of social networking users: profile duplicating attacks, where attackers replica existing user profiles and attempt to "reinvite" their friends, and cross-profile duplicating attacks, where attackers create a

duplicated profile on an online social network where the target user does not yet have a profile and then contact the targets' friends. If a user, for example, has a Facebook account but no LinkedIn account, an attacker could replica the Facebook profile to create a LinkedIn profile and then contact the target's Facebook friends who are also on LinkedIn. Bilge et al. showed that their attacks can be fully automatic and are feasible in exercise. If an attacker is able to create fake accounts on a large scale, Sybil attacks on OSNs are possible. OSN earners therefore use various protection mechanisms to limit the creation of large amounts of fake accounts. Boshmaf et al. however found that OSNs can be infiltrated on a large scale. They assessed how vulnerable OSNs are to a important infiltration by socialbots - computer programs that control OSN accounts and mimic real users. The writers created a Socialbot Network (SbN): a group of adaptive socialbots that are scored in a command-and-control fashion on Facebook. The writers used 102 fake profiles to send friendship requests to 5,053 casually selected Facebook users. 19.3% of these users accepted the friendship requirements. Next, the SbN tried to infiltrate the circle of friends of the users who had accepted their fake friendship requests. Within 8 weeks, the SbN was able to extra infiltrate the network and improvement access to personal information. A recent survey by Alvisi et al. delivers an overview of Sybil defenses for online social networks and suggests community detection algorithms.

4.2. Cloud services

Cloud services deliver a new channel through which social engineers can behavior attacks on the knowledge worker. Knowledge workers regularly cooperate with others who do not work at the same location. Sharing information on a cloud service has consequently become popular. In this scenario, an attacker exploits this state and uses the cloud as a channel for the social engineering attack. Recent publications defined a variety of probable attacks in the cloud, e.g., an attacker placing a hateful file into another user's cloud as defined by Gruschka et al. and then using social engineering to make them perform the malicious file. A malicious piece of software can also be used to extract personal information from the victim's account, which is then used to perform more targeted attacks. Mulazzani et al. provide countermeasures to decrease the risk by stopping the attacker from placing malicious files on Dropbox, one of the presently most usually used cloud services. The level of trust between users of a shared directory or file is not permanently as high as wanted. Social engineers can exploit this fact by using a fake identity or a cooperated user account to invitation the victim to share specific information with the attacker in the cloud. Affording to Roberts et al. one of the biggest weaknesses of cloud services is that the users - companies and separate users - lose control over their data when they store and access it remotely. On old-style servers that are owned by a company itself, it can limit access and define customized access policies. In cloud services, the accountability for that is shifted to a third party. Therefore, if a cloud service is to be used for the exchange of complex information, a certain level of trust must be recognized not only between cooperating users, but also between the cloud hosting company and the user. The most usually observed attacks on cloud services are spear-phishing and APTs.

4.3. Mobile applications

The improved use of mobile applications in both business and private frameworks makes them an progressively popular channel for social engineering attacks. In business communication, mobile messaging and e-mail applications are of high attention to social engineers. BYOD policies recognized by companies often include the use of mobile phones and tablets. More and more employees use their smartphones to check their company e-mails or to read documents that are stored in the cloud. However, many smartphone users use highly vulnerable smartphone applications that can be distorted to behavior social engineering attacks. Schrittwieser et al.presented two different attack scenarios that can serve as a starting point for such an attack.

In their work, they established how sender ID spoofing can be done on general mobile messaging applications such as WhatsApp. A social engineer can use this to send a message to a victim while imagining to be one of his friends. The writers also highlighted how vulnerabilities can be exploited to hijack user accounts, which can then be used to perform social engineering. Considering that many smartphone applications are highly vulnerable and can leak complex information, we can achieve that such mobile devices offer a variety of attack vectors for social engineering and other attacks on user privacy. Moreover, some smartphone applications request permissions to access complex data on the user's device. If an attacker were to create such an application, they would gain the information and could use it as a starting point for a social engineering attack. Chin et al.discussed how inter-application information exchange can be sniffed on smartphones and then be distorted to violate application policies and permissions. In some cases, such as defined by Potharaju et al. the attacker simply plagiarizes a general smartphone application and deploys it in order to perform an attack.

5. Real-world Examples

In this section, we define how targeted attacks against the knowledge worker are performed in real-world scenarios. Two methods were generally used in recent social engineering attacks, namely spear-phishing and waterholing attacks. We converse these two methods in detail and in the environment of recent real-world attacks.

5.1. Spear-Phishing

Many companies organize highly sophisticated end-point security controls to protect their networks. Nevertheless, targeted attacks such as spear-phishing are an growing threat for knowledge workers because of their targeted accuracy. In practice, the first step within an attack scenario is that the attacker seeks widely available information on the company's Internet site and public profiles on social networks to obtain exact information on the targeted victim. Then the attacker concepts an e-mail using the gathered information to gain the victim's trust. In general, such e-mails are only sent to a carefully selected small group of people. In most cases, they cover attachments with malicious software to deliver a remote control tool to the attacker. Zero-day exploits are a good way of installing a backdoor via an existing vulnerability. The remote control functionality is then used to harvest complex information and to get into inner company networks. In this section, we converse three real-world spear-phishing attacks and their influence on knowledge workers.

RSA, 2011. As defined in, RSA suffered from an attack by an advanced determined threat.

A small number of employees received an e-mail with "2011 Recruitment Plan" in the subject line. Even though most of them found this e-mail in their garbage mail folder, the e-mail was ready well enough to convince the receiver of its dependability. A number of employees thus directly opened the e-mail from the garbage mail folder. The e-mail had a spreadsheet attached. Affording to, the

spreadsheet contained a zero-day exploit that installed a backdoor via an Adobe Flash vulnerability. The attacker chose to use a Poison Ivy2 variant to gain remote control of the target's device which initially was not detected. After the initial social engineering phase was completed, the attackers cooperated further machineries in the local network. The attackers then successfully cooperated a number of strategic accounts and were able to steal complex information on RSA's SecurID system. Finally RSA had to swap millions of SecurID tokens due to this successful social engineering attack.

New York Times, 2013. The New York Times was hit by a alike attack as RSA. Chinese hackers completed a 4month targeted attack, infiltrating The New York Times computer systems and harvesting the employees' user credentials. Reports advise that there is evidence of political reasons behind the attack. The attackers broke into e-mail accounts, tried to cloak the source of traffic to the The New York Times and to route traffic caused by the attacks through university computers located in the United States. Again, the primary attack vector had been a spear-phishing attack which sent fake FedEx notifications. The New York Times hired computer security specialists to analyze the attack and prevent a determined threat. They found that some of the methods used to break into the company's substructure were associated with the Chinese military. Furthermore, the malware that was installed to gain access to the computers within the company's network followed the pattern of earlier reported Chinese attacks. Perlroth also reported that the same university computers in the United States had been earlier used by hackers from the Chinese armed. With this attack, the hackers stole the passwords of all employees at The New York Times and were thus able to access the personal devices of 53 people. However, affording to The New York Times, no customer data was stolen. The characteristics of the attack clearly show a political motive for this APT. China's Ministry of National Defense stated that hacking is clearly banned

under Chinese law and denied being the originator of the attack. Affording to Perlroth China is using such attacks to control its public image in the West and therefore approved attackers to injure organizations that might harm the reputations of Chinese authorities. They furthermore reported that hackers allocated by Chinese authorities had stolen complex information from more than 30 Western journalists.

The Red October Cyber-espionage Network. Kaspersky Lab recently out a new research report on spearphishing attacks against diplomatic, governmental and research organizations. The mainstream of the organizations targeted were located in former USSR Republics in Eastern Europe and Central Asia. The attack was launched in 2007 and continued active until the beginning of 2013. Complex data was not only stolen from research institutes but also from nuclear and energy groups as well as aerospace organizations. Alike to the attacks against RSA and The New York Times, the attackers sent a spearphishing e-mail to a carefully selected group of people. For instance, the attackers promoted cheap diplomatic cars in spear-phishing messages, which included custom malware. Affording to Kaspersky, the malware construction consisted of malicious extensions, info-stealing modules and a backdoor Trojan that exploited Microsoft Office security vulnerabilities. The attackers also exfiltrated an enormous amount of sensitive data from the infiltrated networks. Stolen credentials were organized in lists and then used to guess passwords of extra systems. The Red October APT remained active for almost six years. The in-depth analysis exposed artifacts within the executables of the malware that show that the attackers were located in a Russian-speaking country.

5.2. Waterholing

Newly, waterholing attacks have been the main vector in attacks on multi-national organizations alongside spear-phishing. In its place of directly targeting employees with customized phishing messages, the attackers target websites that are probable to be visited by their victims. They infect specific websites with malware and expect that some of their target companies' employees will visit them.

Apple, Facebook, Twitter. In 2013, a zero-day vulnerability in Java was exploited to specifically infiltrate company networks via waterholing attacks. Apple and Facebook fell victim to this. The attackers first cooperated the development site "iPhoneDevSDK", which is a general forum for iOS application developers. The website was modified to exploit the Java vulnerability on devices which visited the website. A number of Apple's employees visited the infested website and their devices were cooperated. The infested machineries were connected to Apple's cooperate network and the attackers were thus able to infiltrate Apple's inner networks . Facebook's inner network was infiltrated by the same waterholing campaign . In both reported cases, it is expected that no confidential data was stolen. A alike breach was reported earlier; however, it was not confirmed that the main cause was related to Java's zero-day vulnerability. In this attack, the attackers exploited Twitter's network and were able to cooperation about 250,000 user accounts, theft user names, e-mail addresses, session tokens and encrypted passwords . At first, it was supposed that the attack was showed by Chinese attackers instructed by the country's government or military, but others disagree and trust that one of Twitter's employees visited the same infested website as Apple's and Facebook's employees . Reports on real-world examples focus to a large extent on the original attack vector of social engineering and do not cover the technical facets of these attacks. The first systematic analysis of targeted attacks at a large scale was showed by Le Blond et al.In adding to the social facets of targeted attacks, Le Blond et al.'s analysis conversed technical

facets based on malicious emails received by an NGO over a four-year period. The writers found that malicious office documents are the most general attack vectors, followed by malicious archives. The analysis also showed that attackers tend to use well-known in its place of zero-day vulnerabilities. The real-world instances of recent attacks performed by APTs underline that social engineering remains the most successful strategy to cooperation large-scale organizations. The instances also highlight that the predominant channels of social engineering are e-mail communication and websites. Recommendations to counter social engineering attacks focus mainly on security policies and staff training . Gragg points out that any education on social engineering must include psychology and persuading in order to understand and counter attacks. Srikwan recommends cartoons to impart users about social engineering and phishing. In the light of our conversed instances, user education might indeed help to counter spear-phishing attacks. Waterholing attacks, however, are hard to counter even with extra user alertness training and security policies. One possible approach to counter waterholing attacks could be to identify the most popular websites visited by employees to behavior an extra monitoring of these websites.

6. Conclusions

In this paper, we defined common attack scenarios for modern social engineering attacks on knowledge workers. BYOD-policies and dispersed teamwork as well as communication over third-party channels offers a variety of new attack vectors for advanced social engineering attacks. We believe that a complete understanding of the attack vectors is required to develop efficient countermeasures and protect knowledge workers from social engineering attacks. To enable this, we presented a complete taxonomy of attacks, classifying them by attack channel, operator, different types of social engineering and specific attack scenarios. We conversed real-world instances and advanced attack vectors used in general communication channels and the specific issues of computer-supported teamwork of knowledge workers in the business situation such as cloud services, social networks and mobile devices as part of BYOD policies.

References:

1. Google hack attack.
2. Microsoft hacked: Joins apple, facebook, twitter.
3. Wikipedia
4. Whittaker. Facebook, Apple hacks could affect anyone.
5. Whittaker. Facebook hit by ’sophisticated attack’; Java zero-day exploit to blame.