IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier 10.1109/ACCESS.20xx.DOI*

# Defining Social Engineering in Cybersecurity

**ZUOGUANG WANG[1,2], LIMIN SUN[1,2], AND HONGSONG ZHU[1,2]**
[1]School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[2]Beijing Key Laboratory of IOT information security, Institute of Information Engineering, CAS, Beijing, China

Corresponding author: Zuoguang Wang (e-mail: wangzuoguang@iie.ac.cn).

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802804, and in part by the Joint Fund of the National Natural Science Foundation of China under Grant U1766215.

**ABSTRACT** Social engineering has posed a serious security threat to infrastructure, user, data and operations of cyberspace. Nevertheless, there are many conceptual deficiencies (such as inconsistent conceptual intensions, a vague conceptual boundary, confusing instances, overgeneralization and abuse) of the term making serious negative impacts on the understanding, analysis and defense of social engineering attacks. In this paper, an in-depth literature survey is conducted, the original meaning of social engineering in cybersecurity is traced, the conceptual evolution and technical development are analysed systematically, and the conceptual problems are discussed. Based on above work, this paper attempts to address these conceptual deficiencies by proposing a more compatible and precise definition of social engineering in cybersecurity (SEiCS). This definition eliminates the conceptual inconsistencies, covers the mainstream conceptual connotations, clarifies the conceptual boundary, mitigates the overgeneralization and abuse, etc. Five analysis tables (i.e., the comparative analysis of the SEiCS definition vs. mainstream conceptual intensions in the conceptual evolution, the comparative analysis of the SEiCS definition vs. typical definitions in the literature, the analysis of confusing "social engineering cases", the analysis of popular social engineering attack scenarios, and the analysis of social-engineering-based attacks) are provided to illustrate the performance of the proposed definition.

**INDEX TERMS** Definition, Social Engineering, Cyberspace, Security, Term and Conception, History and Origin, Literature Review, Conceptual Evolution and Analysis, Huaman factors, Attack.

## I. INTRODUCTION

As a quite popular attack method in the hacker community, social engineering has led to serious, pervasive and persistent security threats.

- Social engineering attacks have become an increasingly serious security threat. According to a global survey of 853 IT professionals conducted in the United States, United Kingdom, Canada, Australia, New Zealand, and Germany in 2011, social engineering attacks are costly especially in large organizations. 48% of large companies and 32% of companies of all sizes have experienced 25 or more social engineering attacks in the past two years. 30% of large companies cite a per incident cost of over $100,000 [1]. According to reports from *ISACA's State of Cybersecurity*, social engineering is the top cyberthreat for organizations from 2016 to 2018 [2, 3]. Social engineering attacks were experienced by 85% of organizations in 2018, an increase of 16% over one year. The average annual cost of social engineering attacks for organizations in 2018 has exceeded $1.4 million, an increase of 8% compared to the previous year [4].
- The universality of social engineering threat stems from the inevitability of human vulnerabilities in cyber security. There is not a computer system that doesn't rely on humans on earth, no matter how well the security measures are designed and implemented. These human elements involved are not only vulnerable, but vulnerable to the extent that it shadows most other security measures [5]. This means that this security weakness is universal, and independent of platform, software, network or age of equipment [6]. People could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, however the network infrastructure could still remain vulnerable to old-fashioned manipulation [7]. As a case in point, some of the classified material Edward Snow-

den, a former U.S. National Security Agency contractor, leaked to the media were accessed using login credentials and passwords obtained from 20 - 25 colleagues at the NSA regional operations center in Hawaii through persuading them these login credentials and passwords were needed for him to do his job as a computer systems administrator [8]. Although it is often said that the only secure computer is an unplugged one, the fact is that you could persuade someone to plug it in and switch it on, which means that even powered down computers are vulnerable [6].
- Social engineering has existed in many forms throughout history and will continue to exist [9]. Social engineering tries to fool decision makers, which is similar to stratagems used thousands of years ago [10]. To eliminate social engineering breaches is practically impossible [11], even the security awareness training is not likely to reduce this vulnerability to zero [12]. The persistent cybersecurity threat caused by social engineering is rooted in the human vulnerabilities exploited, rather than the security flaws of the computer system. Computer vulnerabilities may be patched to perfect. The human vulnerabilities existed universal will accompany with us throughout our lives until we die, and it will only "go away when the human race does [13]".

However, there are some basic problems related to the social engineering concept (according to the analysis in Section II). These conceptual deficiencies impede the understanding of social engineering incidents, the analysis and of social engineering threats, the research of social engineering security, security awareness training and the defense of social engineering attacks.

- The conceptual intension (connotation) of social engineering is not consistent.
- The conceptual boundary is vague. Some attack methods that obviously do not belong to social engineering (signal hijacking, Denial of Service [14, 15], web search [16], adware [17], etc.) have been regarded as social engineering instances, and some forms of attack have turned into borderline cases (watering hole [18], cross site request forgery [19], cross site scripting [20], etc.) hard to tell whether they belong to social engineering category.
- Concepts from extensional perspective (e.g. [21, 17]) have considered social engineering as an umbrella term, which leads to the term's overgeneralization and abuse.
- With the conceptual evolution, various kinds of social engineering concepts have been described, and some conceptual intensions are contradictory. Shoulder surfing and dumpster diving are considered as social engineering instances in quite a few studies, while some exclude them from the category. Some studies consider that any social engineering involves exploiting someone's trust, while some have argued that trust is not necessary. Although some studies considered social engineering as a type of non-technical attack, many different views exist. As the conceptual evolution, a more confusing trend reflected on the concept.

This paper makes the following contributions.

- This paper systematically analyses the conceptual evolution of social engineering based on an in-depth literature survey.
  In addition, the origin of social engineering in cybersecurity is investigated, the problems related to the concept are analysed, and the development of social engineering technology is discussed.
- Based on the evolution analysis, this paper proposes a new definition of social engineering in cybersecurity (SEiCS) that is more compatible and precise. This definition eliminates the conceptual inconsistencies, covers the mainstream conceptual connotations, clarifies the conceptual boundary, etc. Five analysis tables of the social engineering intension and extension are conducted to show the performance of SEiCS.

Organization: Section II is the analysis and discussion of social engineering conceptual evolution. Section III is the methodology of definition. Section IV proposes a new definition of social engineering in cybersecurity. Section V is the performance analysis. Section VI concludes the study.

## II. THE ANALYSIS AND DISCUSSION OF SOCIAL ENGINEERING'S CONCEPTUAL EVOLUTION

For the purpose of providing sufficient materials for defining social engineering in cybersecurity, this section systematically analyses the conceptual evolution process from approximately 1974 to now based on an in-depth literature review.

To cover the related materials as much as possible, the literature survey methodology mainly consists of 3 stages and 3 strategies. We first find the relevant literature using Google Scholar (which includes databases such as Elsevier, ACM, IEEE, Springer and numerous other publishers), and then we recursively examine the cited literature from the references (an indirect and recursive strategy). Second, we retrieve more of the related materials from Google Scholar and the Google search engine (direct strategy). The queries used include *"social engineering term OR concept OR define OR definition OR introduction OR evolution OR develop" "'social engineering is'", "social engineer attack OR computer OR security" "social engineering attack OR skill OR technique OR classification OR taxonomy OR classify" "SE attack" "phishing first", etc.* Finally, we use the advanced options of Google Scholar and Google to retrieve hard-to-find materials (direct fine-grained strategy), especially for the investigation of the origin of social engineering in cybersecurity. For instance, when we retrieved related literature before 1987 in Google Scholar, few valid materials were found. Therefore, we turned to Google where query model such as *"Keywords 80..86"* and *"Keywords 84"* were used to trace the origin of social engineering in cybersecurity year by year, although this search strategy requires lots of manual work. It should be

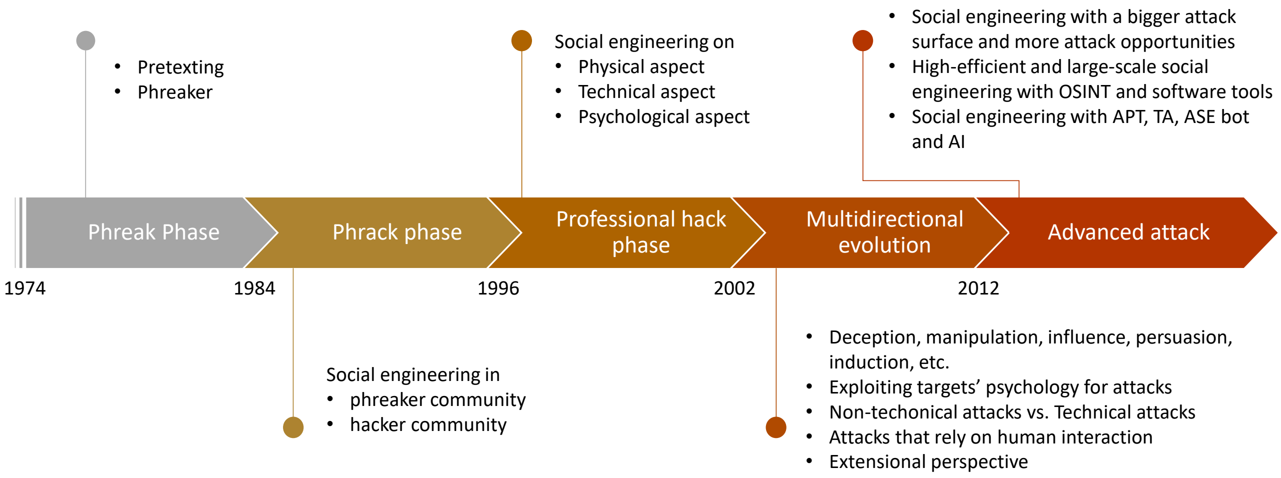
Pretexting
Phreaker
Social engineering on
Physical aspect
Technical aspect
Psychological aspect
Social engineering with a bigger attack surface and more attack opportunities
High-efficient and large-scale social engineering with OSINT and software tools
Social engineering with APT, TA, ASE bot and AI
Phreak Phase
Phrack phase
Professional hack phase
Multidirectional evolution
Advanced attack
1974
1984
1996
2002
2012
Social engineering in
phreaker community
hacker community
Deception, manipulation, influence, persuasion, induction, etc.
Exploiting targets' psychology for attacks
Non-techonical attacks vs. Technical attacks
Attacks that rely on human interaction
Extensional perspective

**FIGURE 1.** The Conceptual Evolution of Social Engineering in Cybersecurity.

noted that this paper concerns the social engineering concept, and specific topics such as phishing have been investigated but they are not the focus. All retrieved materials are added to Zotero, which automatically identifies duplicate items.

Based on the differences and characteristics of the conceptual evolution in different time periods, the evolution process is divided into five phases (Figure 1), and every evolution phase has been analysed and discussed in detail. These five phases are: Phreak phase (*1974* - 1983), Phrack phase (1984 - 1995), Professional hack phase (1996 - 2001), Multidirectional evolution phase (2002 - 2011), and Advanced social engineering attack phase (since 2012).

## A. SOCIAL ENGINEERING IN THE PHREAK PHASE

### 1) The spread of the term social engineering

In the context of cybersecurity, the earliest literature this paper found where the term **social engineering** appeared is an article titled *More on Trashing* [22] published in September 1984 volume 1 of *2600: The Hacker's Quarterly*, one of the earliest hacker magazines issued 1984 first and is still issuing now. This article showed that garbage of Telco company contains much valuable information and discussed some specific methods to gather information by trashing. "Numerous things of interest can be found in Bell trash ... binders and notebooks with the Bell logo on them, ... supplies of Bell letterhead ... Cosmos printouts abound in any CO trash ... telephone directories list employees of Bell, got to try **social engineering** on." "Maintenance reports, trunk outages reports, line reports, network control analysis (NCA), TSPS documents, and lists of abbreviations used by the phone company can be found." [22]

An article titled *Switching centres and Operators* in October 1984 at the same magazine *2600: The Hacker's Quarterly* also discussed social engineering. "There is also a directory assistance for deaf people who use Teletypewriters ... They tend to be nicer and will talk longer than your regular operators. Also, they (directory assistance operators) are more likely to be persuaded to give more information through the process of '**social engineering**'." "CN/A operators do exactly the opposite of what directory assistance operators are for. You give them the number, and they give you the name and address ... In my experiences, these (CN/A) operators know more than the DA operators do and they are more susceptible to '**social engineering**'." [23] Subsequently, the literature [24] considered that "One interesting thing to try is to pose as a phone company employee for **social engineering** purposes".

Thus, the concept of social engineering in 1984 referreds mainly to a process using pretext to persuade targets, e.g. operators in switching centres, to provide more information. In addition, the description of social engineering in the literature [23] used quotation marks, which implies that the term social engineering at this time might be a proper noun or has a special meaning.

### 2) The origin of the concept social engineering

According to the literature survey and analysis, the origin time of the concept social engineering is very likely earlier than 1984, i.e. the time of term spread.

Before the release of *2600: The Hacker's Quarterly* in 1984, *YIPL/TAP* as an earlier underground publication popular in the phreaker community, is not found discussed social engineering directly. According to literature [25], the bulletin board system (BBS) of Legion of Doom (LoD) was the first hacking BBS to deal with many subjects such as trashing and social engineering) in close detail, and the BBS of LoD is actually earlier than the establishment of LoD in 1984. Literature [26] showed that plover-NET as the original home of LoD attracted 500 eager users in 1983, and Lex Luthor as the founder of LoD was one-time co-sysop of plover-NET. Besides, there have been underground boards almost as long as there have been BBS in 1978. One of the first was 8BBS founded in 1980, in which social engineers like Roscoe and Susan Thunder are active at that time [27]. Thus, the concept of social engineering may be earlier than the emergence of BBS.

John Draper (Captain Crunch) described that social engineering is "going in and talking to people on the inside of the phone company making them believe that you're working the phone company" [28]. Hatfield [29] did a investigation, "In a 2017 interview for this article, Draper recalled that it was he who originally introduced the term into the phreaker community sometime in the mid-1970's as a way to describe these impersonation attacks. Draper was unaware of the term's political origin and does not recall having adapted it from any prior usage" [29]. Lapsley [30] noted that "the term social engineering in the phreak/hacker sense seems to have come into vogue in the mid-1980's", and "Bill Acker recalls it being used as early as 1974 or so. Prior to that the term was 'pretexting,' that is, calling someone on a pretext to get information or convince them to do something for you", a term FBI invented and used to assist in the investigations [30].

In light of the analysis and comparison above, it is reasonable to conclude that the social engineering concept originated at approximately 1974. Furthermore, the social engineering concept during the Phreak phase (1974 - 1983) is basically a pronoun of "pretexting".

To sum up, social engineering in the decade from 1974 to 1983 (the Phreak phase) can be described as an approach to obtain information or help from operators in the switching centres of telephone companies by means such as pretext, impersonation and persuasion.

### B. SOCIAL ENGINEERING IN THE PHRACK PHASE

Since the concept spread in the hacker BBS and magazine in 1984, social engineering manifests a duality just as the term Phrack means, i.e. a Phreak concept and a Hack concept.

On one hand, social engineering continues to serve as a concept of phone phreaker community, not only inherited the meanings of impersonation, pretext and persuasion, but also manifested the meaning of deception. Quittner [31] considered that social engineering is using conversation to exchange information under false pretenses, e.g. posing as a telecommunications employee to gain more knowledge and insight into the different phone network systems. Kluepfel [32] described social engineering as an exploitation towards employees in telephone industry through fraudulent impersonation of other employees or vendors. Social engineering was also regarded as bullshitting [33], trickery and deceit [34] to obtain information.

On the other hand, as an approach to obtain information related to computer and bypass the security obstacle, the merits of social engineering were gradually realized. Just as what described in literature [31, 35] that initial hacking was thought to be a day-to-night password brute force, yet social engineering shocked those who the first time hears about it for its off the beaten track. Besides, crackers in this phase were discovering that it is much easier and less risky to compromise people and procedures than to break into computer systems [36]. Social engineering is an attempt to exploit the help desks and other related support services normally associated with computer systems [37]. Social engineering is the act of talking to a lawful user of the system, pretending that you are also a legal user of the system, and in the course of the conversation, manipulating the discussion so that the user reveals passwords or other stuff necessary to break through the security barriers [35]. Social engineering is the term the hacker community associates with the process of using social interactions to obtain information about a "victim's" computer system [38]. What's more, social engineering provides hackers with efficient short cuts, and in many cases facilitates attacks that would not be possible through other means [38].

The target group of social engineering in this phase has expanded beyond operators in switching centres of telephone companies. With regard to the implementation methods of social engineering, literature [22, 39] showed that Dumpster Diving approach can find a great deal of valuable information. Thus, the first line of defense against social engineering is the company's rubbish [36]. Winkler [40] described the methods of reverse social engineering, in which a social engineer, e.g. first creates a network failure, and make victims believe that the attacker is a member of a legitimate organization such as a support service, then wait for the victim to actively interact with them and hand them information.

Thus, in the decade from 1984 to 1995, social engineering on one aspect manifests the connotation of Phreak that exploiting the employees of telephone companies by means such as pretext, impersonation, persuasion and deception to gain more knowledge and insight into the different phone network systems; on another aspect manifests the connotation of Hack that using social interactions to obtain information about targets' computer system by means such as deception, manipulating dialogs, reverse social engineering, and dumpster diving. The connotation of the social engineering concept was expanded in the aspects of targets group, implementation approaches and purposes of social engineering attacks.

### C. SOCIAL ENGINEERING IN THE PHASE OF PROFESSIONAL HACKER

The phase of 1996 to 2001 have seen tremendous growth in the information security domain [7]. During these six years, the evolution of social engineering mainly manifests in three aspects. (1) The implementation approaches of social engineering were more diverse in physical aspect. (2) With the development of network information technology, technical social engineering attack approaches such as email phishing and Trojan gradually out into the social engineering concept. (3) Special characteristics in aspect of social engineering psychology, such as social influence, persuasion and trust manipulation began to be discussed, and the significance that people serve as the weakest link of security chain has been gradually realized.

### 1) The physical aspect of social engineering

Granger [41] considered that social engineering attacks take place on two levels: the physical and the psychological. For social engineering attack in physical level, the hacker may pretend to be a maintenance worker or consultant who has access to the organization and walk in the workplace to conduct office trashing, finds passwords lying around, or stand there and watch an oblivious employee type in his password (i.e. shoulder surfing). Similarly, Jordan and Taylor [42] argued that perhaps most important of all is the ability of social engineering, which can be as simple as talking people into giving out their passwords by impersonating someone, stealing garbage in the hope of gaining illicit information (trashing) or looking over someone's shoulder as they use their password (shoulder surfing).

Higgins [43] considered physical penetration as the art of advanced social engineering, since "typically social engineering is conducted in a non-face to face interaction". Many physical penetration methods and attack scenarios were also discussed in literature [43], such as gaining access to an establishment under the cover of lunch rush at a large corporation or the 9 AM time rush of getting to work, wearing something that resembles a building badge to bypass guards, getting hired temporarily onto a contracted cleaning team for several days in order to get inside into the target organization, and planting a KeyGhost device that installs in line with the keyboard connector that captures everything that is typed on the keyboard.

Granger [44] summarized some social engineering attack methods such as impersonation and persuasion, unauthorized physical access, shoulder surfing, dumpster diving, wandering through halls looking for open offices, attach a protocol analyzer to grab confidential data and/or remove equipment. Manske [45] discussed attack types of social engineering, such as dumpster diving, shoulder surfing, using fake business cards, making payoffs to targets (security staff, hotel staff, janitors, etc.) and impersonation. Three impersonation scenarios discussed are calling users and acting like technology support staff, pretending to be a phone company employee acting like a film crew doing a "movie", and posing as a student wanting to interview a business's technical staff.

### 2) The technical aspect of social engineering

The first phishing attack occurred in 1996 was designed to steal the username, passwords, credit card numbers and other personal information of America Online (AOL). Attackers sent fake emails and instant messages that appeared to come from AOL support. Many unsuspecting victims gave away their information and were subsequently billed for the activities and purchases that the hackers made on their compromised accounts [46]. Phishing attacks also lead the risk of internet fraud. Rusch [47] noted that social engineering originally was used by hackers to obtain codes or email passwords for access to long-distance telephone lines or computers, but later, social engineering attacks are being used to conduct internet fraud, e.g. acquiring credit card numbers and other financial data. Manske [45] also considered "forging electronic mail" is a popular and common social engineering attack. Harley [13] considered masquerading, dumpster diving and direct psychological manipulation as different types of social engineering, and further included spam, hoaxes, viruses and Trojan Horses into the context of social engineering deriving from "the recognition among some security practitioners of an increase in the range of threats based on psychological manipulation".

Thus far, phishing and Trojan Horse as the representative of technical attack approaches came into the social engineering concept. Manske [45] argued that social engineering in this period is extremely difficult to define and describe, and probably the best definition of social engineering is the practice of acquiring information through technical and non-technical means, since effective social engineering is open-ended and flexible.

### 3) The psychological aspect of social engineering

Social engineering in this phase were also described as "psychological subversion" to steal password [13]. Rusch [47] argued that the success of social engineering stems from the application of psychological techniques for interacting with and manipulating the victim to obtain the desired information, and social psychology needed to be paid more attention. Generally, social engineering can be defined as the process by which a hacker deceives others into disclosing valuable data that will benefit the hacker in some way [47]. Granger [41] considered that social engineering is generally the manipulation of the natural human tendency to trust. Social psychology contents such as routes to persuasion, the false consensus effect and influence techniques, in internet fraud were also discussed in literature [47].

Harl [6] described social engineering as the art and science of getting people to comply to your wishes from the perspective of psychology. Although it is not a way of mind control and getting people to perform tasks wildly outside of their normal behaviour, it is far from foolproof; social engineering concentrates on the weakest link of the computer security chain [6].

A phenomenon that draws the authors' attention is while social engineering in this phase caused severe damage [47], social engineering did not get into the public view still as an attack methods of professional hacker community. This is likely attribute to (1) victim organizations did not want to admit the attack since it would damage to the organization's reputation, (2) the low security awareness of public, (3) as well as the social engineering concept was not widespread in the mass media.

## D. THE MULTIDIRECTIONAL EVOLUTION OF SOCIAL ENGINEERING CONCEPT

Around 2002, the publication of works such as *The Art of Deception (2001, 2002, 2011)* [48] and *Social Engineering Fundamentals, Part I & II* [41, 44], provided the public with detailed examples and discussions about the concept of early-stage social engineering. People began to have an intuitive and specific understanding of the "core technology" of "the world's most notorious hacker", i.e. social engineering. The spread of the social engineering concept and the increased social engineering threat gradually attracted the public's attention.

Compared with the former phase, there was a significant increase in the number of works on social engineering in this phase. Henceforth, the concept of social engineering moved into a multidirectional evolution phase in which various kinds of conceptual descriptions emerged and some of them have been used until now. This paper collected the social engineering concepts in this phase and clustered them into different conceptual categories based on their conceptual attributes.

On one hand, inter-disciplines such as social psychology, social trust, language psychology and emotion & expression were explored. With the application of other disciplines' knowledge in social engineering, the development of computers & network information technology, and the amelioration of attack technologies, many new forms of social engineering attacks were created. The conceptual extension of social engineering continuously expands. At the same time, some attack methods that obviously didn't belong to social engineering were regarded as social engineering instance. Definitions that defined social engineering as an umbrella term even occurred.

On the other hand, each concepts cluster in the context of multidirectional evolution represented an evolution direction and power. What's worse is that some of these concepts were contradictory. Shoulder surfing and dumpster diving are considered as attack methods of social engineering in a large number of literature, however, Ivaturi and Janczewski [19] excluded them from the taxonomy of social engineering explicitly. Laribee [49] considered "any social engineering involves exploiting someone's trust", while Mouton et al. [50] argued that "there is not always the need to build a trustworthy relationship with the target" in the social engineering attack. Some literature hold the viewpoint that social engineering is kind of non-technical attack, while some holds the contrary viewpoint.

These phenomena led to many problems: obscure conceptual boundary, the abusive use and misuse of terminology, and the conceptual differentiation and decomposition caused by the structural tension produced by the different directional conceptual evolutions.

### 1) Social engineering concepts that emphasize deception and manipulation

Kevin Mitnick [51] defined social engineering as "using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a web site, which exploits a technical flaw and allows the hacker to take over the computer." *The Art of Deception (2002, 2011)* [48] describes that "social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology." Social engineering attack uses social means such as deception and manipulation in order to gain access to information technology [52]. Hasle et al. [53] described social engineering as "the name used for a bag of tricks used by adversaries to manipulate victims to make them say or do something they otherwise wouldn't have." Definitions come from Wikipedia and Oxford dictionary are also the similar kind. "Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information" [54]. Social engineering is, "(in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes [55]". Later works such as [56, 57, 58] inherit this kind of definitions.

Some studies emphasize the deception of social engineering. Gragg [59] considered that "in general, social engineering is the process of deceiving people into giving confidential, private or privileged information or access to a hacker." Social engineering refers that deceiving or tricking people to help attackers reach their goals [60, 61], and there is not a lot of difference between the techniques used for social engineering and the techniques used to carry out a traditional fraud [47, 59]. These people who conduct the process were called confidence men and con artists in past and social engineers today [9]. Hasan et al. [62] argued that social engineering is a process of deceiving people into giving away access or confidential information as a formidable threat to most secured networks. Literature [63, 64] considered that "in essence, social engineering refers to the design and application of deceitful techniques."

Some studies emphasize the manipulation of social engineering. Hadnagy [65] defined that social engineering is the act of manipulating a person to take an action that may or may not be in the "target's" best interest. Social engineer tries to manipulate the victims into divulging confidential information or performing social engineer's malicious objectives by using influence and persuasion [66]. Social engineering in literature [67, 68] was described as an attack method that induces victims to release information or perform an action that enables social engineer to compromise the victims' system. Similarly, social engineering "is the 'art' of utilizing human behaviour to breach security without the participant (or victim) even realizing that they have been manipulated" [69]; "is psychological manipulation, skilled or otherwise, of an individual or set of individuals to produce a desired effect on their behaviour" [13]. Thapar [21] considered social engineering is "a collection of techniques used to manipulate people into performing actions or divulging confidential information." Later works such as [63, 64, 70, 71] also holds the same type of idea.

There are also works considering social engineering is the deception and manipulation of trust. Literature [41, 44, 64] defined social engineering as the manipulation of the natural human tendency to trust. Laribee [49] considered that "any social engineering involves exploiting someone's trust".

### 2) Social engineering concepts that emphasize psychological exploitation

Traditionally, social engineering is the art of gaining access to secure objects by exploiting human psychology [72]. Peltier [73] considered that the social engineer uses a variety of psychological tricks on a computer user to get the information they need in order to access a computer or network. On the argument of the nature of social engineering, Evans [52] argued that social engineering is always psychological and sometimes technical, e.g. pretexting attack that calls to the target pretending to be the help desk is generally considered non-technical but psychological; while pretexting attack occurring over email is technical and also psychological. It is the psychological aspect of social engineering that makes the attack, not the technical aspect. Literature [74, 75] defined social engineering as the exploitation of victims' instinctual response, psychological weaknesses such as curiosity, trust and greed to conduct deception and harm for the purpose of obtaining attacks' interest. Heartfield and Loukas [17] noted that "social engineering is used as an umbrella term for a broad spectrum of computer exploitations that employ a variety of attack vectors and strategies to psychologically manipulate a user." Thornburgh [9] consisted social engineering as "a social / psychological process by which an individual can gain information from an individual about a targeted organization".

Some studies focus the application of psychological persuasion and influence in social engineering. Social engineering is the art and science of getting people to comply to your wishes [6] (focused on the psychological conformity), is the art of persuasion [62]. Mouton et al. [50] defined social engineering as "the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" (from the perspective of request - persuade - comply). Oosterloo [16] considered social engineering is "the attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data." Literature [20, 76] showed that "deceiving, persuading, or influencing people to provide information or to perform an action that will benefit the attacker is known as social engineering."

### 3) Technical features of social engineering

Social engineering is traditionally regarded as the art of gaining access to secure objects by exploiting human psychology, rather than using hacking techniques [72]. Instead of directly targeting technical controls such as firewalls and authentication systems, social engineering focus on the weakest link in the security architecture, i.e. the staff of the organization and remains a popular method of bypassing security [77, 78, 79]. As a tactic to circumvent computer security solutions, social engineering is used to avoid the risk breaking into a system by brute force or tools [80, 81]. Beckers et al. [82] argued that "social engineering is the illicit acquisition of information about computer systems by primarily non-technical means." Literature [83, 84] considered that in the context of security, "social engineering is a term that describes a non-technical kind of intrusion."

In contrast, there were also many viewpoints that social engineering can also be technical, and even social engineer need to master certain professional technology. Social engineering has become more technical and complex [72]. Literature [85, 19] showed that more and more attackers merge new technologies with traditional social engineering attack, and phishing and cross site request forgery (CSRF) are two forms of social engineer attack. Mitnick and Simon [48] also argued that the success of social engineering "often also requires a large measure of knowledge and skill with computer systems and telephone systems."

### 4) Social engineering concepts that emphasize social interaction

Social engineering is an attack on information security that is centered on some type or form of personal interaction [86]; is the process of using social interactions (social means) to obtain information about a victim's computer system [38, 86]. Ivaturi and Janczewski [19] argued that although shoulder surfing and dumpster diving help attackers in gathering intelligence in the preparation phase, these two do not involve any form social interaction with the victim, "hence we do not classify them as social engineering attack methods."

Tetri and Vuorinen [87] considered that social engineering refers to incidents in which an information system is penetrated through the use of social methods. Ghafir et al. [11] defined social engineering as "a breach of organizational security via interaction with people to trick them into breaking normal security procedures." Social engineering is an attack in which an attacker uses human interaction to obtain or compromise information about an organization or its computer system [88]. Within security world, a social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction [83].

### 5) Social engineering concepts from extensional perspective

In the information security field, the term social engineering is widely used to reference an array of techniques used by criminals who obtain sensitive information or to convince targets to perform actions that could compromise their systems [89]. Literature [90, 80] showed that social engineering is a term that encompasses a broad spectrum of malicious

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992807, IEEE Access

activity such as phishing, pretexting, baiting, quid pro quo and tailgating.

On one hand, these definitions manifests the diversity of social engineering attack approaches. There are many types of social engineering attacks, and the variety and scope of social engineering attacks is limited by only one factor, i.e. the creativity of the attacker [45, 15]. On the other hand, what's most puzzling is that "social engineering attracts such a range of definitions, covering such a range of activities (from password stealing, to scavenging through waste for useful information, to malicious misinformation) [13]."

Rather than defining social engineering concept from the intensional perspective, this kind of definitions defined social engineering concept from the extensional perspective. Although it avoids the bother to identify the essential attribute and boundary of social engineering concept, the problem is that many non-social-engineering attack methods were encompassed according to some pieces of resemblance of typical social engineering examples, e.g. signal hijacking, network monitoring, Denial of Service (DoS) [14, 15], web search [16], network sniffing [49], search engine poisoning [19], adware [17], seeking refuge in the ambiguities of metaphor. With the development of this trend of social engineering's conceptual evolution, the conceptual boundary will be even vaguer. It will finally lead to the abusive use and misuse of social engineering terminology, and further differentiation and decomposition of the social engineering concept.

### *E. ADVANCED SOCIAL ENGINEERING ATTACK*

Since approximately 2012, the developments of new environments, threats and technologies have promoted the further evolution of social engineering with more new attack features. The wide applications of Social Networking Sites (SNSs), Internet of Things (IoT), Industrial Internet, wearable devices and mobile devices, and the weakening of security zone isolation, although increased data accessibility, improved service quality and productivity, simultaneously created a larger social engineering attack surface and more attack opportunities. These phenomena also allowed attackers to easily reach and influence large numbers of victims. The big data environment with shared and open source features provides the conditions for crafting more credible social engineering attacks. The spread of social engineering tools and the open source of tools codes make large-scale social engineering attacks easier. The application of new technologies (machine learning, artificial intelligence, etc.) and the combination with new threat forms (advanced persistent threat, targeted attack, etc.) make it possible to conduct a high-efficient, targeted and intelligent social engineering attack. Social engineering with these features is posing multi-level, omni-bearing and severe security threats towards human, cyber and physical spaces.

These new attack features accelerates the trend of multidirectional evolution and concept decomposition of social engineering. Although there have been studies using words "social engineering 2.0" at different times (2008 [91], 2016 [92]) to discuss part of the new features, all these studies did not provide the concept definition of "social engineering 2.0", which continuously increases the urgent need to research the conceptual definition of social engineering.

#### 1) Social engineering with a bigger attack surface and more attack opportunities

The creation of SixDegree.com in 1997 is regarded as the sign of the emergence of SNSs. However, SNSs is still in the burgeon or conceptualization stage and not widely used. The successive creation and development of many social medias, e.g. Friendster, LinkedIn, Facebook, Twitter and Google+, since 2002, attracted more and more people to these websites creating their profiles and building relationships with others in a newfangled way. The users of Pinterest exceed 1 billion in 2012 [93]. Facebook users share more than 30 billion pieces of content each month [20]. The massive amount of data generated by the explosive growth of social media users marks the dawn of the era of big data. What's significant is that people are more exposed today than ever before [64]. Information about personal identity, activities, relationships, location, personal interest, etc. are being posted in social medias. The data like email addresses, phone numbers, birth date, work addresses, current city and school name can be obtained [72]. Social medias have become a large pool of sensitive data [94].

IoT became popular around 2011 and reached the mass market in early 2014 [95]. IPv6 was introduced in 2001 and provides technical support for address space of Internet of Everything. General Electric Corporation proposed the Industrial Internet in 2012. Germany proposed Industry 4.0 in 2013 [96]. The industry is developing toward open, global, connected, customized, digital, intelligent. Mobile and wearables devices are widely used; sensors will be ubiquitous and implanted in almost any interconnected device conceivable. Many people are willing to measure all states imaginable, e.g. physiological data, location data, mood data, environment data. Large numbers of interconnected devices have become new resources, new targets and new communication channels of social engineering attack. Previously, a fraudulent email or instant message originated from your fridge would seem absurd; however, this idea does not seem so ludicrous nowadays. Lots of smart TVs, home routers and even fridge have been used to send malicious emails [97]. Besides, the incident of Stuxnet has showed that as the pivotal link of attack, social engineering has posed severe security threat to critical infrastructure (see paragraph 2 of Section II-E3).

There is no rigorous isolation between personal daily life and professional life in modern society. Social networks are widely used in work environments, which leads to information about organizational relationships, family relationship, etc. exposed to the public and meanwhile attackers. It is a common phenomenon that personal affairs are managed by organizational computers, organizational work by home computers. Employees in quite a few industries lack basic security knowledge, a case in point may be home computers connected to routers with weak or initial passwords. There are even companies encouraging the work patterns such as Bring Your Own Device (BYOD) and remote office in home. The information security boundary of the organization becomes blurred, and the traditional organization trust zone has lost its original meaning or no longer exists.

On one hand, the rapid development and wide application of Social Network Sites (SNSs), Industrial Internet and Internet of Things (IoT) improved service quality and production efficiency by connecting users and various devices together in global. On the other hand, these new applications and environments are accompanied with various kinds of vulnerabilities, providing more attack channels and a bigger attack surface for social engineering, posing multi-level, omni-bearing and severe security threat against human & cyber & physical space. What's more, the easy availability of large amounts of sensitive information about people and devices in these new environments simplifies the information gathering. All these phenomena created more and more opportunities to launch a successful social engineering attack.

### 2) High-efficient and large-scale social engineering with OSINT and software tools

The big data environments and the development of data mining technologies enable the exploitation of Open Source Intelligence (OSINT) more efficiently. No matter what information you post publicly online (Facebook, Twitter, Foursquare, etc.) might give attackers a clue on how to connect the dots on where you are and your real identity [89] and further to construct a more convincing social engineering attack. Ball et al. [98] exemplified how to conduct a spear phishing attack on organization employees by using OSINT. In the case study, *Maltego* was used to gather OSINT from the target company's websites and social networks; Simple Phishing Toolkit (SPT) was used to construct phishing emails based on employee interests. The aggregation of data from different social medias (LinkedIn and Facebook) lead to more successful social engineering attacks [99]. Edwards et al. [100] demonstrated the possibility to automatically identify employees of an organization and to harvest information pertinent to a successful social engineering attack using public visible information in Google+, LinkedIn, Twitter and Facebook.

A large group of victims can be reached and influenced at the same time, in the context of internet, mobile communication and SNSs. Besides, more and more social engineering tools have been developed, such as Social-Engineer Toolkit (SET) [101], *Maltego, Phishing Frenzy and Gophish*. These tools support multiple types of information gathering and multiple types of attack vectors creating. As a typical tool to conduct social engineering attack, SET provides functions such as spear phishing attack vectors, website attack vectors, infectious media generator, *arduino* based attack vectors and wireless access point attack vectors; many social engineering attack process will be carried out automatically after setting some parameters under the choice menu. In addition, many of which are open source, e.g. *SET, Phishing Frenzy, Gophish*. This means that non-professional hackers, e.g. script kiddies, can launch a semi-automated social engineering attack easily. These phenomena providing favorable conditions for automated, low cost and large-scale social engineering attacks. Even in the spam phishing scenario with low success rates, social engineering attacks are economically viable.

The success rate and efficiency of social engineering attack is increasing. A great deal of information about victims can be gathered manually or gathered by automated information gathering tools. Adding information about the targets increases the likelihood their falls victim to phishing [102]. The machine learning technology facilitates the exploitation of open source intelligence. Low value and low hanging fruit and spam phishing are abandoned gradually; attackers tend to select specific and valuable targets and craft more credible attacks carefully, e.g. spear phishing and context aware phishing. Employees are easily deceived and susceptible to victimization in SNSs where contextual elements provide psychological triggers to attackers [60]. There is a 90% chance at least one person will fall victim when an attacker sends out 10 emails [103]. It is very easy and effective to increase the yield of a phishing attack when an attacker exploit social network data found on the social network sites; if targets are solicited by someone appearing to be a known acquaintance, they may be over four times as likely to become victims [104].

A well planned and executed social engineering attack could succeed even among those who identify themselves as being aware of social engineering techniques [105], let alone users with low security awareness. Rich background information in social networks and Internet can be extracted freely to survey specific targets and prepare targeted social engineering attack. Benenson et al. [106] argued that by a careful design and timing of a message, it should be possible to make virtually any person click on a link, as any person will be curious about something, or interested in some topic, or find themselves in a life situation that fits the message's content and context. Functions such as recommendation and friend-finding in social networks can be abused by attackers to trick victims into contacting the attacker themselves and launch social engineering attacks passively [107]. Since the victims initiate the friend request, this attack form raise less suspicion and has the advantage to bypass filter-based detection techniques that aim to prevent large-scale unsolicited request.

### 3) Social engineering with APT, TA, ASE bot and AI

Social engineering attack can be as simple as making a phone call and impersonating an insider to elicit the required information, without having to combat antivirus software by deep coding or traverse firewall. On the other hand, Social engineering attack can also be more advanced, efficient and aggressive through the use of new technology and the combination with advanced threat.

Advanced Persistent Threat (APT) are attacks usually targeting organizations or nations for business, political or military motives, long-planned, elaborately designed and programmed, spending a lot of time and resources. Stuxnet, Duqu and Flame from 2010 to 2012 are typical examples of APT attacks. Social engineering is usually served as the approaches to establish entry point in the initial phase of APT attacks, or the methods to deal with the obstacles that other attack methods could not address. Frumento and Puricelli [108] described a common APT attack phase model, in which social engineering serve as the central core. Both APT attacks Stuxnet and Flame use social engineering (baiting) as the approach to break through the physical isolation and spread the malicious code; the difference is Stuxnet for destroying devices and Flame for monitoring the targets [109].

Compared with APT attack, Targeted Attack (TA) usually aimed at a specific company, organization or user, launched by individual hacker or hacker group around the world, for the purpose of stealing financial information, financial fraud or revenge. Targeted social engineering attacks are becoming more popular, some malwares are especially customized to implement phishing attacks aimed at a specific user or community [92]. Abraham and Chengalur-Smith [110] noted that social engineering malwares combine psychological and technical ploys, luring a computer user to execute the malware and combating existing technical countermeasures. An increasing number of malicious programs employ social engineering as the propagation approach. Social engineering malware manifests characteristics both pervasive and persistent.

There are also many works [111, 112, 113, 72, 94, 100] about automated social engineering bot (ASE bot). Some ASE bots were designed to gathering open source intelligence pertinent to targets automatically and association analysis, some even can chat with victims by combining appropriate chat logic with enhanced intelligence to conduct automated social engineering attack. A case in point mentioned in [10] is that the chat bot automated flirtatious conversations to persuade users in chat rooms to share their identity or visit websites with malicious content. The more human-like an ASE attack is, the more difficult is to detect it [94]. Lauinger et al. [112] presented a new social engineering threat in which the social chat bot takes control and forwards real conversations between human users to implement a man in the middle attack for malicious goals. The click rates of links reached to 76.1% when chat bot replaced links in the messages that the users were exchanging. The identification and detection of this automated social engineering attack on instant messaging could be difficult, since there are few differences about chat bot from true human behaviour in terms of conversations.

The application of artificial intelligence (AI) technology also contributes to the evolution of advanced social engineering attacks. HoneyPhish can be regarded as a proof of concept (PoC) of using Markov Chains for natural language processing to generate phishing emails automatically [114], which showed the possibility to harness AI in social engineering attack. Seymour and Tully [115] described an AI social engineering attack that learned to tweet phishing posts targeting specific users utilizing recurrent neural network. Bahnsen et al. [116] discussed how to leverage Long Short-Term Memory Networks to create a better algorithms, i.e. DeepPhish, to generate phishing URLs to bypass the phishing detection based on recurrent neural networks. Anderson et al. [117] leveraged Generative Adversarial Networks (GAN) to construct a deep learning based malware domain generation algorithm, which is designed to intentionally bypass a deep learning based detector. In a series of adversarial rounds, the generator learns to generate domain names that are increasingly more difficult to detect.

#### 4) The conceptual evolution in new features phase

Literature [92, 118] considered that social engineering has been used for a very long time as a well-known method of deception; 4 factors that technology, social networks, cybercrime and the users' naive behaviour contributed to the evolution of social engineering into a new multifaceted and complex phenomenon called "social engineering 2.0" Ariu et al. [118] argued that compared to old-school social engineering, the key difference of "social engineering 2.0" is the possibility to exploit the social engineering techniques on a larger scale, using automated attacks on a potentially larger number of victims. In fact, Jakobsson [91] used the words "social engineering 2.0" to discuss some new characteristics of social engineering as early as 2008. However, all of these works did not provide the specific concept and definition of "social engineering 2.0".

## III. CATEGORIZATION THEORIES AND DEFINITION METHODOLOGY

### A. CATEGORIZATION THEORIES

Classical categorization theory and prototype categorization theory are two influential categorization theories with different philosophies.

#### 1) Classical categorization theory

The classical theory of categorization has been prevalent since the time of Aristotle [119]. The classical view of categorization reflects the spirit of objectivism and essentialism. This view holds that being true is objective and mind-independent, experience is unreliable, and categorization can put it in order. Categories are the stable, abstract and logical tools for people to observe and understand the world. Entities have certain sets of properties as their identification, which means that essential properties make the thing what it is. Although other properties may be randomly allocated, a category will always include a set of essential properties.

Thus, this theory holds that 1) categories are defined by a limited set of necessary and sufficient conditions; 2) categories have clear boundaries, and a thing cannot both belong to a category and not belong to it; 3) properties are binary; and 4) all members of a category have equal status.

#### 2) "Family resemblance" and Prototype theory

Prototype theory emphasizes that subjective cognition and experience are significant during the formation of ideas, against essentialism and objectivism, reflecting the experientialism of the embodied philosophy.

Prototype theory can trace its origin back to the work of Wittgenstein [120]: "Consider for example the proceedings that we call 'games'. I mean board-games, card-games, ball-games, Olympic games, and so on...*To repeat: don't think, but look!* Look for example at board-games...When we pass next to ball-games, much that is common is retained, but much is lost...And the result of this examination is: we see a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail. I can think of no better expression to characterize these similarities than 'family resemblances'...And I shall say: 'games' form a family."

On the basis of "family resemblance" principle, Rosch and her colleagues in [121, 122, 123] made a series of experiments about colours. They asked people questions such as *is red hair as good an example of your idea or image of red as a red fire engine*. Most people would give a negative answer to this question and to any other similar ones. They later extended his experiment from the colour category to other areas such as BIRD, FRUIT and FURNITURE, proposing the following prototype notion: categories form around and (or) are mentally represented by salient or information rich or highly imaginable stimuli which become prototypes for the category. The effects that prototypes have on categorization are referred to as prototype effects: the most salient features of the prototype are the first features that come to mind when the category is mentioned.

Prototype theory holds that 1) members of a category do not share certain essential properties but are linked together by family resemblances; 2) members don't enjoy equal status (some members more representative than the others, while others are on the edge), e.g. for BIRD category, robins' prototypicality is more significant than penguins and ostriches; 3) category boundaries are not clear: category prototype has the most characteristics in common with members within the same category and has lots of dissimilarities with the members of its neighbouring category; the category members have fewer similarities with its edges members which have the most similarities with members of other categories [124]; 4) categories have a polycentric structure and the prototypes are located in the central position; and 5) there are three levels in categories: superordinate level, e.g. furniture, animal; basic level, e.g. chair; subordinate level, e.g. desk chair.

The idea of family resemblances and prototype theory are not only helpful to explain how people perceive categories and deal with examples but also useful in cognitive linguistics, e.g. to explain polysemic phenomena. Taylor [125] proposed that polysemic categories are family resemblance categories and monosemic categories have prototype effect. Ungerer and Schmid [124] also showed that family resemblances worked well with cognitive categories at the superordinate level and categories at the basic level reflect more of a prototype effect.

#### 3) Comparative analysis and discussion

However, some problems cause concerns. 1) Wittgenstein encourages people to observe instead of think, which is actually returning the abstract essence to its phenomena. We have to appreciate his innovative thoughts, but sometimes objects or phenomena can be deceptive, which has already been pointed out by Aristotle as a reason for his peculiar stress on essence. When Wittgenstein was indulging himself in those illusive phenomena, he forgot that for the discussion of family resemblances that "family" should come first instead of "resemblances" [126]. That is, the family resemblances of members cannot truly unravel the process of categorization. 2) Further, a concept with prototype structure might incorrectly include an instance that is not in fact a member of that category, or incorrectly exclude instances that fail to display any of the attributes that characterize the prototype [127]. For instance, when robins serve to the prototype of BIRD category, bats are likely to be included due to their resemblances including flying, small and light bodies, thin and short legs, etc. 3) The whole internal structure of a category seems to depend on the context and, in a wider sense, on our social and cultural knowledge, which is thought to be organized in cognitive and cultural models [124]. Sparrows are the most familiar prototype of BIRD category in China. To a large extent, the choices of prototype samples are affected by contextual factors. If we change the context, the judgement will be affected; and if we increase the contextual features, the category boundaries will be affected. A further case in the point of 2) can be the following. If affected by the context and bats are regarded as a prototype of BIRD category, penguins will be excluded due to its attributes such as being flightless, having a large bodies, laying eggs and being covered with feathers. Just as Hegel says, *what is "familiarly known" (prototypicality here) is not properly known, just for the reason that it is "familiar"*. 4) The missing prototypes problem is another issue [127]. 5) The 'odd and even number paradox'. Armstrong et al. [128] found that people will grade odd numbers for centrality (3 was assigned the highest degree of membership in the ODD NUMBER category, and 2 and 4 are the highest in EVEN NUMBER category), even though the category ODD NUMBER has a clear definition in terms of the necessary and sufficient features, i.e. classical categories also exhibit typicality effects.

Given the above, family resemblances can hardly be counted as qualified criteria during the process of categorization, prototype theory is inadequate as a theory of knowledge representation, and classical categorization theory should not be abandoned.

### B. DEFINITION METHODOLOGY

This paper holds that classical categorization and prototype categorization are not incompatible. They can be complementary and combined to understand categories better from different perspectives (objectivism and essentialism vs. subjective cognition and experientialism).

Prototype effects are a consequence of recognition procedures, while classical theory examines the core definition. The distinction between the core definition and recognition procedures makes it possible, in principle, to preserve the classical theory of categorization without at the same time ignoring the empirical cognition [125]. Fuzziness is related to recognition while the core definition of categories remains intact. In addition, Taylor [125] proposed that categories can be characterized in two ways: folk categories and expert categories. Folk categories, which are more informal and experience-based, are structured around prototypical instances and are grounded in the way people normally perceive and interact with the things in their environment. Similarly, 'folk models' are based on informal observations, traditional beliefs, and even superstitions [124]. Expert categories are specifically created and defined by the imposition of a set of criteria, usually in conformity with the principles of classical categorization theory. The definitions serve to eliminate the fuzzy edges from the categories, giving them the status of technical, rather than merely pre-theoretical constructs.

Thus, this paper attempts to develop the definition of social engineering in cybersecurity (SEiCS), a concept at the basic or subordinate level, using classical categorization theory, meanwhile discuss the prototype effects reflected. A concept has its intension (connotation) and extension (denotation). The intension consists of the properties or attributes that the term connotes. The extension is composed of the members of the class that the term denotes. According to Section II, social engineering in cybersecurity is now in the situation that it has 1) a vague conceptual boundary; 2) confusing extension affiliations; 3) terminological ambiguity, overgeneralization and abuse; 4) multidirectional conceptual evolution and inconsistent conceptual intensions; 5) conceptual decomposition; etc. It is the intensional definition that gets to the root of the problem. In classical categorization theory, definitions by genus and difference are more generally applicable and achieve more adequate results than any of the other kinds of intensional definitions [129]. Two parts are necessary to compose a genus-differentia definition: a genus and the differentia. A genus-differentia definition assigns a meaning to a term being defined by identifying a genus term and one or more differentia words. Different from the meaning in biology, in logic, genus means a relatively larger class, and species means a relatively smaller subclass of the genus. The differentia is the attribute(s) that distinguish the various species within a genus. It is usually composed of the essential attribute(s) or distinctive attribute(s) rather than the common attribute(s) or accidental attribute(s).

This paper attempts to present a new definition of social engineering in cybersecurity using this method for the purpose of clarifying the conceptual intension and extension, reducing the vagueness, mitigating the structural tension caused by the multidirectional conceptual evolution, and meanwhile reflecting the mainstream conceptual intension.

## IV. DEFINING SOCIAL ENGINEERING IN CYBERSECURITY

This paper proposes the definition of Social Engineering in Cybersecurity (SEiCS) as follows:

**In the context of cybersecurity, social engineering is a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cyber security, with or without the use of technical means and technical vulnerabilities.** *(succinct definition see section end)*

In the definition, *human vulnerabilities are the human factors that are exploited by attackers to conduct a social engineering attack. These human vulnerabilities could stem from aspects of psychology, cognition, consciousness, thought, behavioural habits, neural reflexes, etc. The social interaction in social engineering is the communication between or joint activity involving two or more human roles. According to different criteria, the types of social interaction can be various, such as direct or indirect (e.g. personal interaction in the real world, user interaction in cyber space), real-time or non-real-time (e.g. phone talking, email), active or passive (e.g. reverse social engineering).* Cyber security "involves security issues that exist in electromagnetic equipment, information communication systems, operating data and system applications in cyberspace [130]". To breach cyber security, in general, is to breach the security goals (confidentiality, integrity, availability, controllability, auditability, etc.) of the four basic elements of cyberspace. These four basic elements are the Carrier (the infrastructure, hardware and software facilities of cyber space), Resources (the objects, data content that flows through the cyber space), Subjects (the main body roles and users, including human users, organizations, equipment, software, websites, etc.), and Operations (all kinds of activities of processing Resources, including creation, storage, change, use, transmission, display, etc.) [130, 131].

### *A. THE GENUS AND COMMON ATTRIBUTES*

The majority of social engineering concepts emphasize that the purpose of social engineering is obtaining information; e.g. literature [45, 132, 9, 73, 133, 134] considered that social engineering is "the practice of acquiring information through technical and nontechnical means", and usually, the information is computer network and system related. No information shall be neglected [132], even the information that seems to not be very valuable may be used by a hacker to learn the environment and assist the attack schemes.

Some social engineering concepts emphasized the assistance from victims to social engineers. Pfleeger and Pfleeger [135] stated that "the point of social engineering is to persuade the victim to be helpful." Mitnick and Simon [48] noted that "a social engineer lives by his ability to manipulate people into doing things that help him achieve his goal." Literature [60, 70, 61] also showed that the purpose of social engineering is to make the targets assist offenders in their attack or help attackers reach their goals.

In addition, obtaining physical access is included in the purpose of social engineering attacks by some studies. Typically, this includes making the victims reveal information, e.g. passwords, giving the adversary illegitimate access to buildings and granting access to restricted areas [53, 136]. Sometimes social engineering refers to going into offices and looking around for information about computer systems, such as passwords taped to monitors [137, 52].

There are some studies that very broadly defined the purpose of social engineering. The basic purposes of social engineering are the same as hacking in general, e.g. fraud, network intrusion, industrial espionage, identity theft, disrupting the system or network, and gaining unauthorized access to systems or information [41, 49, 138].

However, it will result in conceptual defects, e.g. the concept abuse and generalization, if the purpose of the social engineering concept is inappropriately defined. With regard to the definitions in which social engineering's only goal is persuasion, "an individual lying about all the break-ins he has had to convince his neighbour to build a security fence would classify as social engineering"; with regard to the definitions that take very broad approaches when explaining the goals, "the con man borrowing people's watches and never returning them constitutes social engineering" [52]. Such problems exist in almost all social engineering definitions in which the scope of the purpose is too broadly or too narrowly defined. For instance, take the social engineering definition that "the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction (direct communication or indirect communication), the persuasion or the request involves a computer-related entity [50]". The scenarios in which a little boy communicates and persuades his parents by computer to comply with his request for five dollars (with the excuse of eating lunch) is consistent with the definition; however, it is not the "social engineering (in the context of security)" that we wanted to express. These cases are likely caused by prototype effects where deception or persuasion is regarded as the prototype or criteria.

Based on the analysis of social engineering's conceptual evolution and the purpose of social engineering, this paper identifies *the genus of social engineering definition as "a type of cyber attack", and "to breach cyber security" is a corresponding common attribute.* This considered both the historicity and the evolutionality of SEiCS. (1) Though social engineering (as a polysemic term at the superordinate category level) in cybersecurity and politics domain share some conceptual (family) resemblances [29], there is not yet research shows that the conceptual connotation (not the term) of SEiCS originates from politics (Section II-A2). SEiCS evolves in the phrack community and cybersecurity domain all through, and the mainstream intension of SEiCS is different from the social engineering concept in social science (includes politics). In social science, the "social" of social engineering refers to "society" or "social system", and social engineering typically means the engineering project to address a society problem. The "social" in SEiCS refers to "social / user interaction" used during a cyber attack. The genus that a type of cyber attack separates SEiCS from "social engineering in social science". (2) The purpose attribute to breach cyberspace security not only covers the mainstream purposes such as network intrusion & disruption, identity theft, and unauthorized access of information & systems but also reserves the purpose attribute a larger evolution space. The breach of confidentiality, integrity, availability controllability or auditability is also contained.

Thus, the ambiguity and confusion of the social engineering concepts of different disciplines are eliminated. It also avoids the term abuse and conceptual overgeneralization of SEiCS. Scenarios such as picking a lock and sneaking through a door, deception or fraud discussed above, are excluded from the SEiCS concept since these cases are not relevant to cyber security.

### B. THE DISTINCTIVE ATTRIBUTE AND ESSENTIAL ATTRIBUTE

Compared to traditional attack forms such as brute-force password cracking and software vulnerabilities exploiting, the distinctive attribute of SEiCS that manifests on the attack subject attackers usually involves the utilization of approaches such as deception, manipulation, persuasion, influence and induction (prototypes). It covers the intension of Section II-D1. However, this attribute does not reflect SEiCS's essential attribute, since there will be various kinds of skills (not limited to the five above) for conducting a social engineering attack with the development of information technology, the transformation of environment and the variation of attack scenarios.

The distinctive attribute of SEiCS that manifests on the attack object victims is the exploitation of human vulnerabilities such as gullibility, curiosity, conformity, greed, sloth, intuitive judgement and fixed-action patterns. It covers the intension of Section II-D1 from another perspective and Section II-D2 (psychological exploitation as prototype). Exploiting human vulnerability is one aspect of the essential attribute of SEiCS. Whatever the attack approaches or skills are, attackers exploit the human vulnerability of some aspects to make SEiCS a success in the final analysis.

The distinctive attribute manifests on the SEiCS's realization form is social interaction, which can be various kinds of forms such as direct or indirect, real-time or non-real-time, and active or passive. It covers the intension that relies heavily on social interaction of Section II-D4 of conceptual multidirectional evolution. Social interaction reflects another aspect of the essential attributes of SEiCS.

With regard to the technical attributes of SEiCS, this paper does not make any stipulations on the use of technical means and technological vulnerabilities in the attack process. The attack can be conducted with or without technical means and technical vulnerabilities. The development of technology will reconstruct the implementation methods and forms of social engineering attacks, and the viewpoints in Section II-D3

**TABLE 1.** Definition of SEiCS covers the mainstream intension of conceptual evolution

| Evolution phase | Attributes related to vulnerability exploitation | Attributes related to social interaction | Technical attributes | Concept genus and common attributes |
|---|---|---|---|---|
| Origin | Pretexting | Calling | | To get information |
| Phreak | Posing as a telecommunications company employee. Convincing. Persuasion. Exploit nice and helpfulness of someone inside a telecommunications company. | Calling | | To get information about phone network systems. |
| Phrack | Pretexting, impersonation, persuasion, deception to exploit the help desks, support services, employees in telephone industry | Calling; Conversation; Social interaction | | To get information about phone network systems, targets' computer system. To break into computer Systems. |
| Hack | Psychological exploitation and physical exploitation by methods such as manipulation, deception, persuasion, impersonation masquerading. Psychological subversion. Getting people to comply. Physical penetration. | Calling; Physical; Online | Technical social engineering e.g. email phishing. | Hacker purposes |
| Multi-directional evolution | More and more method to take advantage of human psychology and behaviour. | (Personal, Social, Huaman) interaction. | Non-technical; technical. | Many kinds of purposes (discussed in section IV-A). |
| | Discussion of extensional definition see section II-D5, cases analysis see table 3. | | | |
| Advanced attack | Inherit attributes in previous phase | Inherit attributes in previous phase | Non-technical; More technical (factors) | Inherit attributes in previous phase |
| SEiCS | 1 exploit human vulnerabilities (through any method such as influence, deception, manipulation, persuasion, induction) | 2 by means of social interaction | | Social engineering is a type of attack (1,2) to breach cyber security (confidentiality, integrity, availability controllability, auditability, etc.). |

The mainstream conceptual intensions of social engineering concept in different phase of conceptual evolution are covered by SEiCS definition, coloured with grey.

that social engineering is completely a type of non-technical attack is just an interim cognition.

Based on the discussion of the distinctive attributes of SEiCS above, *the "differentia" is "exploit human vulnerabilities by means of social interaction"*. It is also the criteria to tell whether a cyber attack case belongs to SEiCS.

Thus, the proposed definition can be expressed in a succinct way: "**Social engineering in cybersecurity (SEiCS) is a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cyber security.**" Cases of SEiCS have to satisfy attributes described in the definition.

## V. PERFORMANCE ANALYSIS OF THE SEICS DEFINITION

### A. COMPARATIVE ANALYSIS OF THE DEFINITION INTENSION

Table 1 shows a comparative analysis of the definition intension of SEiCS and the mainstream intension in each phase of the conceptual evolution. These intensions fall mainly in four attribute dimensions, i.e. attributes related to vulnerabilities exploitation, attributes related to social interaction, technical attributes, concept genus and common attributes. Definition attributes of SEiCS are placed in the last row, and each attribute is coloured with grey. If the attributes in a certain table cell is covered by the attribute of SEiCS in the corresponding dimensions, the table cell is also filled with grey. Areas without colour are discussed where labeled. As is shown by the table, the mainstream intensions and prototypes in different phases of the conceptual evolution are covered by SEiCS.

Table 2 shows a comparative analysis of SEiCS with typical social engineering definitions in the literature. In order to scatter the corresponding attribute description of a definition in literature as much as possible into three attribute columns for comparison, the definition is broken down into necessary component parts, each of which is marked with a number (1.2.3.4.5...) according the position sequence in original definition. Three attribute columns are a column with the concept genus and common attributes, a column with vulnerability exploitation (Attribute 1) and a column with social interaction (Attribute 2). If an attribute of a certain definition is limited by SEiCS's attribute in the same column (e.g. for reasons discussed in section IV-A), the corresponding table cell will be coloured with Goldenrod. If an attribute of a certain definition is covered by SEiCS's attribute in the same column, the corresponding table cell will be coloured with Gainsboro. If a definition largely embodies the corresponding attribute of SEiCS, but the definition does not explicitly state it, then the table cell will be coloured with LightBlue.

For example, the definition in literature [51] is broken into "1. Social engineering is 2. using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, 3. and the request

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992807, IEEE Access

**TABLE 2.** Comparative analysis of the SEiCS definition with typical definitions in the literature

| Definitions | Concept genus and common attributes | Attribute 1 | Attribute 2 |
|---|---|---|---|
| SEiCS | 1. In the context of cybersecurity, social engineering is a type of attack wherein 4. in order to breach cyber security (such as confidentiality, integrity, availability controllability and auditability). | 2. the attacker(s) exploit human vulnerabilities (through any method such as influence, deception, manipulation, persuasion, induction) | 3. by means of social interaction |
| Kevin Mitnick [51] | 1. Social engineering is 3. and the request is usually to release information or to perform some sort of action item that benefits that attacker. | 2. using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, | (unspecified, but many social skills) |
| Mitnick and Simon [48] | 1. Social engineering uses 3. As a result, the social engineer is able to 5. to obtain information with or without the use of technology. | 2. influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. 4. take advantage of people | (unspecified, but many social skills) |
| Wikipedia [54] | 1. Social engineering, in the context of information security, 3. into performing actions or divulging confidential information | 2. refers to psychological manipulation of people | 🟧 |
| Oxford dictionary [55] | 1. In the context of information security, 3. into divulging confidential or personal information that may be used for fraudulent purposes | 2. social engineering is the use of deception to manipulate individuals | 🟧 |
| Mouton et al. [50] | 1. The science of using 4. from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity | 3. as a means to persuade an individual or an organization to comply with a specific request | 2. social interaction |
| Hadnagy [65] | 2. to take an action that may or may not be in the "target's" best interest. | 1. Social engineering is the act of manipulating a person | 🟧 |
| Harley [13] | 2. to produce a desired effect on their behaviour. | 1.Psychological manipulation, skilled or otherwise, of an individual or set of individuals | 🟧 |
| Manske [45] | Social engineering is the practice of acquiring information through technical and nontechnical means. | 🟧 | |
| Fiery [35] | 3. of the system into revealing all that is necessary to break through the security barriers. | 1. Social engineering is the attempt to | 2. talk a lawful user |
| Cruz [88] | 1. In the information security field, social engineering is defined as an attack in which an attacker uses 3. to obtain or compromise information about an organization or its computer system | 🟧 | 2. human interaction |
| Nohlberg [67] | 1. Social engineering denotes, within the realm of security, a type of attack 3. to release information or perform actions they should not. | 2. against the human element during which the assailant induces the victim | 🟧 |
| Winkler and Dealy [38] | 1. Social engineering is the term the hacker community associates with the process of using 3. to obtain information about a "victim's" computer system | 🟧 | 2. social interactions |
| Thornburgh [9] | 2. an individual can gain information from an individual about a targeted organization | 1. Social engineering is a social / psychological process by which | 🟧 |
| Gragg [59] | 2. into giving confidential, private or privileged information or access to a hacker. | 1. In general, social engineering is the process of deceiving people | 🟧 |
| Rapid7 [68] | 1. Social engineering is an attack method that 3. to release information or perform an action that enables social engineer to compromise the victims' system. | 2. induces victims | 🟧 |
| Gulati [69] | 2. to breach security without the participant (or victim) even realizing that they have been manipulated. | 1. Social engineering is the 'art' of utilizing human behaviour | 🟧 |
| Mills [86] | 1. Social engineering is an attack on information security that is centered on some type or form of | 🟧 | 2. personal interaction |
| Ghafir et al. [11] | 2. a breach of organizational security via 5.into breaking normal security procedures. | 1. Social engineering can be defined as 4. to trick them | 3 interaction with people |
| Oosterloo [16] | 2. revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or data. | 1. Social engineering consists of the successful or unsuccessful attempts to influence a person(s) into either | 🟧 |

The number (1.2.3.4.5...) in every row is the order of component parts of the definition.
🟧 SEiCS limit the attribute. ⬜ SEiCS cover the attribute. 🟦 SEiCS specify the attribute.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2992807, IEEE Access

**TABLE 3.** Analysis of confusing cases, which are regarded as social engineering in the literature, yet by the definition of SEiCS which are not.

| Attack in literature | Description | A1 | A2 | A3 |
|---|---|---|---|---|
| Cases that fit the definitions of some literature (discussed in Section IV-A. Table 2), but are not social engineering in cybersecurity (SEiCS). | Do some break-ins, and convince the neighbor to build a security fence (e.g. exploit gullibility, nervous, neuroticism.) | × | ✓ | ✓ |
| | Con man borrowing watches and never returning (e.g. exploit credulity, helpness). | × | ✓ | ✓ |
| | Children get their parents to give in to their demands; doctors, lawyers, or psychologists manipulate and obtain information from their patients or clients; a con man convince his target to take actions that lead to loss for them [65] | × | - | ✓ |
| | The one-cent cell phone: pretending to be a salesman of chain store, manipulating and deceiving other salesmen in another branch to comply with a request (asking for a favor) and get a phone in a marketing campaign without paying [48]. | × | ✓ | ✓ |
| | Little boy communicates and persuades his parents by computer to comply with his request of five dollars (with the excuse of eating lunch; exploit e.g. trust, habit and carelessness). (A case fit the definition in [50]) | × | ✓ | ✓ |
| | Property theft (financial criminals) by means of cracking a crib (picking a lock and sneaking a door) or deceiving the entrance guard. | × | - | ✓ |
| | In economic life, financial fraud taking advantage of victims' greed. | × | ✓ | ✓ |
| | Induce or influence an individual to purchase something unnecessary (exploit greed, fear of scarcity, etc.) | × | ✓ | ✓ |
| Signal hijacking [14, 15] | Hijack the signal between two or more entities such as computer and electronic device, e.g. to replay for authentication. | ✓ | × | × |
| Network monitoring [14, 15] | To perform network monitoring or capture propagating waves of wireless connection. | ✓ | × | × |
| Denial of Service [14, 15] | Disrupting services of a host connected to the Internet accomplished typically by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems. | ✓ | × | × |
| Web search [16] | To search valuable corporate and personal information in web. | - | - | × |
| Trashing [41, 18] | Dumpster Diving. "In which the perpetrator goes through the mark's garbage to find information" [67]. | - | - | × |
| Network sniffing [49] | To examine network traffic for passwords. | ✓ | × | - |
| Search engine poisoning [19] | Using search engine optimization tactics to get some web page high in the rankings for relevant search results without buying advertisements. | ✓ | × | × |
| Adware [17] | Software that generates revenue for its developer to generate online advertisements. | × | - | - |
| XSS [20] | Cross-site scripting attack exploits web applications vulnerability that enables attackers to inject client-side scripts into web pages viewed by other users to bypass access controls such as the same-origin policy. | ✓ | × | - |
| CSRF [19] | Cross-site request forgery is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. | ✓ | × | - |
| Drive-by download [94, 17] | The attack exploits vulnerabilities in the browser or plugins to run malicious code (download software) without the user's knowledge. | ✓ | × | - |
| Pharming [110, 139] | Pharming is a cyber attack intended to redirect a website's traffic to another, fake site by exploitation of a vulnerability in DNS server software. | ✓ | × | × |

A1: concept genus and common attributes, i.e. a type of cyber attack to breach cyber security.
A2: attribute that "exploit human vulnerability". A3: attribute that "by means of social interaction".
"✓", "×" and "-" means "match", "mismatch" and "match or mismatch depending on the attack details" respectively

is usually to release information or to perform some sort of action item that benefits that attacker." Part 2 is put into the third column and compared with the attribute "exploit human vulnerabilities" of SEiCS. The table cell (part 2) is coloured with Gainsboro since the "exploit human vulnerabilities" covers the meaning of part 2. This definition does not explicitly assign "social interaction"; however, many social interaction factors (manipulation, influence, deception, etc.) are contained. Thus, this table cell is coloured with LightBlue. The remaining content (parts 1 and 3) of the definition are put into the second column to compare with the meaning that "in the context of cybersecurity, social engineering is a type of attack in order to breach cyber security such as confidentiality, integrity, availability controllability and auditability" of SEiCS. Since the meaning scope of "perform some sort of action item that benefits that attacker" is larger than the meaning scope of SEiCS in the corresponding column (i.e. the meaning is limited by SEiCS), the table cell (parts 1 and 3) is coloured with Goldenrod. Definitions in other rows are processed with the same way (e.g. "to take an action that may or may not be in the target's best interest [65]" and "or perform actions they should not [67]" are coloured with Goldenrod due to the corresponding attribute was broadly defined).

As shown by the coloured areas in the Table 1 and 2, the intensional definition of SEiCS manifests the lexical implication (i.e. social interaction), limits the conceptual boundary and bestows a larger evolution space appropriately (discussed in section IV-A), covers the mainstream intension and prototypes of the conceptual evolution, and mitigates the structural tension caused by concept multidirectional evolution.

## B. EXTENSIONAL ANALYSIS

This section analyses the attributes of confusing cases and prototype effects, summarizes the popular social engineering attack scenarios, and discusses the social-engineering-based attacks in order to further clarify the SEiCS concept.

During the literature survey, the authors find that there are many items that belong to mediums, human vulnerabilities, social skills or effect mechanisms are regarded as social engineering by some studies. The following are examples of these situations. Email, software, web sites and instant

**TABLE 4.** The analysis of popular social engineering attack scenarios in cybersecurity

| Attack scenarios | Description | Ref. e.g. |
|---|---|---|
| Pretexting | A classical social engineering attack where attacker elicits classified or sensitive information from victims by using pretext scenarios (face to face or via some mediums,telephone typically). It can be very simple, e.g. posing as someone who needs help asking for help or information directly, or complex, e.g. posing as inner staff, technical support to obtain useful help with a prior survey to know better the lingo, organization and victims. (exploit e.g. kindness, credulity, ignorance, sympathy, helpfulness) | [84, 52, 48, 50] |
| Shoulder surfing | The attacker collects information by surfing/observing over the victim's shoulder (e.g. snooping through username, password on computers, sticky notes or papers) when the victim is not paying attention or relax the vigilance during a social interaction. (exploit e.g. gullibility, friendliness, ignorance, carelessness) | [64, 9, 16] |
| Piggybacking | An authorized person provides access to an unauthorized person by keeping the secured door open (for providing help or other reasons. Most employees do not know every colleagues at large organizations and will hold a door for politeness). | [140, 141] |
| Trailing & Pretending | Attacker who lacks the proper authentication by following individuals with permission into a restricted area of security, usually with suitable disguises such as uniform, fake badge to convince or bypass security guard. (exploit e.g. helpfulness, sloth) | [19, 64] |
| Baiting | The attacker leaves a medium (e.g. USB stick) containing malicious codes in a location that is likely to be found and waits for the victims' trigger. Cases like Item Dropping, Road Apple [10, 16] are included. (exploit e.g. curiosity, greed) | [142, 143, 50] |
| Phishing | A network attack in which attackers use spoofed emails typically to trick, to lure victims into sharing sensitive information such as usernames and passwords (other actions, e.g. click a link). It is can be conducted by network mediums such websites, SNSs, instant messaging, pop-up windows and WiFi [92, 73, 67, 49, 19, 17]. | [104, 144] |
| Spear phishing | Spear phishing is a phishing that targets a specific organization or individual. Usually, attackers gather information about the targets, such as personal and professional relationships and other personal details from SNSs, job sites corporate websites, etc. to craft a personalized message that looks and sounds authentic to increase the probability of success. | [106, 104, 65] |
| Whaling | Whaling is a spear phishing attack directed specifically at high-value targets such as senior executives, CEO or CFO. Usually, the whaling baits such as emails and websites are highly customized and personalized, in which the target's name, job title, employee functions, internal phone numbers, organizational logos, email footer and other relevant information are incorporated. The high-level customization makes it difficult to detect a whaling attack. | [18] |
| Vishing | Voice phishing, in which victims are exploited to divulge sensitive information in voice form. Usually, it is conducted by mediums such as phone, Voice over IP (VoIP) and Interactive voice response (IVR). | [145] |
| Smishing | SMS phishing. Attacks uses Short Message Service (SMS), typically cell phone text messages, to deliver the bait to induce people to divulge sensitive information. Since the mobile phone market is now saturated with smartphones which all have fast internet connectivity, a malicious link sent via SMS can yield the same result as it would if sent via email, instant message, SNSs, etc. | [138] |
| Trojan attack | Trojan attack seeks to damage, disrupt, steal, control or in general inflict some other harmful action on targets' computer and network. In trojan attacks, malicious code or malwares are designed to disguise as legitimate software to lure or deceive targets into loading and activating on computer. Interesting malwares, fake mobile App are cases in point. E.g. an attacker (orally or via a note for a certain/tempting software) manages to convincing the victim to disable their firewall/anti-virus, under the pretext of allowing the software's installation, or further breaches cybersecurity by the software installed. (exploit human vulnerabilities credulity, greed, obey to authority/software note, etc.) | [10, 110, 17] |
| Water-holing | A watering hole attack is a strategy, in which attacker infects websites that targets are likely to visit (mainly by exploiting websites vulnerabilities), then waits for the targets to visit and be compromised by e.g. by downloading malwares or click malicious links (exploit targets' visit habits that they often or regularly visit the websites and trust in familiar websites). | [18, 64] |

messages were classified as technical-based social engineering attacks [15], when in fact, they are just mediums to deliver attacks. Friendliness, conformity, sympathy, guilt and ignorance were classified as human-based social engineering attacks [49]. Actually, these items are human vulnerabilities exploited by social engineering attacks. Equivocation was regarded as a human-based social engineering attack [49] and 'authoritative voice' was classified as a non-technical attack vector [21]. In fact, equivocation and 'authoritative voice' are social communication tricks (social skills). Authority, commitment & consistency, scarcity, diffusion of responsibility, moral duty, and reciprocation were classified as human-based attacks [146, 49]. Actually, these items are effect mechanisms that can be used to explain why targets fall victim to social engineering attack. This section for social engineering extension analysis does not focus on these items.

Table 3 shows the attributes analysis of confusing cases that are not regarded as social engineering by SEiCS. Some scenarios that fit certain definitions in the literature but do not fit the concept genus and common attributes of SEiCS (i.e. not a type of attack that breaches cyber security) are analysed in the top half of the table. These scenarios contain some cases discussed in section IV-A. The attacks that appeared in section II-D5 and the attacks classified as social engineering by certain studies are analysed in the bottom half of the table. Prototype effects can be found in these cases: e.g. trashing and social engineering are two different concepts in the beginning (Section II-A1); when it is mistakenly regarded as a prototype of social engineering category, it is not strange that *web search* is included due to resemblances such as non-technical and information gathering. These attacks are all cases that do not satisfy certain attributes of SEiCS, and some attacks are especially confusing because the attack process some time involves user interaction, such as XSS, CSRF and drive-by download. Nonetheless, these attacks can be analysed and identified through the attributes match. For instance, XSS, CSRF and drive-by download are attacks that exploit software vulnerabilities, and themselves do not involve the exploitation of human vulnerabilities.

Table 4 summarizes twelve popular social engineering

**TABLE 5.** Cases analysis of social-engineering-based attacks

| Attack | Description of non-social-engineering part | Description of social engineering part |
|---|---|---|
| XSS & phishing | The attacker finds website A containing a non-persistent (reflected) XSS vulnerability that enables attacker to inject client-side scripts into web pages, and then crafts an innocent-looking URL that call attack scripts (e.g. exp.js) prepared in sites B to exploit the vulnerability. | The attacker sends the malicious link to targets (e.g. some authenticated user of website A) via email, instant message, etc. to trick targets into clicking. Once clicked, the attack script exp.js in site B is triggered to load in victims' browser as if it originated from website A and to execute malicious functions such as cookie theft and privilege escalation. |
| CSRF & spear phishing | When a web server A is designed to receive a request from a client without sufficient mechanism for verifying, then it might be possible for an attacker to conduct a CSRF attack. E.g., targets are currently authenticated on website A, and credentials associated with website A, such as the user's session cookie, IP address, Windows domain credentials are saved in browser. | The attacker embeds forged request into website B in advance, and lures targets to visit website B via e.g. instant message. If the target is not logged into website A, a (spear) phishing email can be used to trick targets into logging in website A and clicking a link points to website B. Once the targets opened the website B, the forged request in website B inherits the identity and privileges of the targets on website A to perform malicious functions on website A automatically through targets' browser. |
| Drive-by Download & phishing | Attackers first create malicious content (e.g. a computer virus, spyware or malware) and host it on their own server or a compromised legitimate website, and then prepare the "drive-by webpage" by compromising other websites and injecting small pieces of code with download functions inside. | Attackers send a link in an email, text message, or social media post that tells targets to look at something interesting or awards on "drive-by webpage" (exploit human vulnerabilities such as curiosity and greed). Once the link opened, without requiring further victims' interaction to click or accept any software, the malware can be download and even executed in the background without victims' knowledge (exploit the vulnerabilities in the browser, plugins or system). |
| APT | Advanced Persistent Threat is a cyber security threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. | Social engineering usually serves as an important attack stage of APT, to gain access to a physical location to enable further network attacks in initial stage, to bridge other attack vectors in the intermediate stage, etc. Stuxnet and Flame are cases in point. |

The implementation and success of these attacks usually depends on social engineering, but they themselves are not social engineering (Table 3).

attack scenarios. Some of them are accepted by the majority of studies and are familiar to the public, such as pretexting, shoulder surfing, phishing and vishing (typical instances or prototypes). There are also some new attack scenarios that this paper identified again, such as baiting, trojan attack and watering hole attack. The description of attack scenario in every row embodies the attributes of SEiCS, and some notes are marked to make them easy to understand. For instance, the possible forms of social interaction, the human vulnerabilities that may be exploited by the attack scenario and the possible attack mediums are annotated.

As a type of cyber attack vector, the co-relation between social engineering and other kinds of attack vectors can be assistance, enhancement, connection, substitution, etc. Social engineering can be used to assist or enhance other kinds of attack vectors and make them simpler and more efficient. Social engineering can be used in the beginning of an attack to establish an attack entry point, can be used in the intermediate stage to bridge other attack vectors to form a complete attack chain, and can be used in the final stage to achieve the attack goals. Social engineering can also be used as a preferred or alternative scheme to replace other kinds of attack vectors to conduct the entire attack process independently.

There are some attacks in which their implementation and success usually depend on social engineering, but they themselves are not social engineering, such as XSS, CSRF and drive-by download (Table 3). This paper calls them social-engineering-based attacks, and some cases are discussed in Table 5. The non-social-engineering part and the social engineering part of these scenarios are described separately to illustrate the attack role of social engineering.

## VI. CONCLUSION

For the purpose of addressing conceptual deficiencies of social engineering in cybersecurity (SEiCS), this paper attempts to provide a new definition after the literature survey, the problems analysis and the definition methodology. The original meaning, the conceptual evolution and many relevant conceptual problems of SEiCS are investigated, analysed and discussed in a systematic way, which serve as materials for the defining work. The methodology of definition is developed based on the analysis of merits and demerits of different kinds of categorization theories. The proposed definition eliminates the conceptual inconsistencies, vagueness and confusion; covers the mainstream intension in conceptual evolution; clarifies the conceptual boundary; and avoids the overgeneralization, abuse and decomposition. Meanwhile, this new definition manifests the lexical implication and appropriately bestows a larger concept evolution space. Five tables are used to analyse and discuss the performance of the proposed definition from both intensional side and extensional side, which further clarifies the concept of SEiCS.

Although the definition proposed in this paper seem to be similar with the definitions in literature, but in fact they are different. A concept definition typically contains many attributes or properties and a very small disparity in certain attribute will lead to a large difference on conceptual scope, conceptual denotation (cases), etc. To propose a definition is something that needs to be carefully considered and dealt with. The discussion of differences and comparative analysis are presented in Section IV-A, Section IV-B, Table 2, Table 3, etc. Our philosophy of innovation is to make a solid step in the right direction. We attempt to get the right direction and solid material by the survey, analysis and discussion of conceptual evolution (Section II), and make a solid progress (even if it may be small) by proposing a new definition which is more precise, proper and compatible. That is why the scope of this paper does not limited to the history of the term "Social Engineering". Although providing a conceptual paradigm (the generally accepted perspective of a particular object at a given time) of social engineering in cybersecurity is difficult, this paper makes its best efforts to achieve it.

In future work, we will systematically research the human vulnerabilities and effect mechanisms used in social engineering.

## REFERENCES

[1] Dimensional Research, The Risk of Social Engineering on Information Security: A Survey of It Professionals, Technical Report, 2011. URL: https://pdftopng-converter.online/storage/documents/2070510db1af82d3af55786b20afb38f.pdf.

[2] 2016 Cybersecurity Snapshot, 2016. URL: https://www.isaca.org/pages/2016-cybersecurity-snapshot.aspx.

[3] Cyberthreats Increasing but Shifting, with Ransomware Attacks Down 17 Percent, 2018. URL: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2018/Pages/Cyberthreats-Increasing-but-Shifting-with-Ransomware-Attacks-Down-17-Percent.aspx.

[4] Ponemon Institute LLC, Accenture, Ninth Annual Cost of Cybercrime Study, Technical Report, 2019. URL: https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

[5] M. Nohlberg, Social Engineering Audits Using Anonymous Surveys: Conning the Users in Order to Know if They Can Be Conned, in: 4th Security Conference, Las Vegas, USA, March 30–31, 2005, 2005. URL: http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-1714.

[6] Harl, People Hacking : The Psychology of Social Engineering, 1997. URL: http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html.

[7] Kevin Mitnick, My first RSA Conference, SecurityFocus (2001). URL: http://www.securityfocus.com/news/199.

[8] Exclusive: Snowden persuaded other NSA workers to give up passwords..., Reuters (2013). URL: https://www.reuters.com/article/net-us-usa-security-snowden-idUSBRE9A703020131108.

[9] T. Thornburgh, Social Engineering: The "Dark Art", in: Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD '04, ACM, New York, NY, USA, 2004, pp. 133–135. URL: http://doi.acm.org/10.1145/1059524.1059554.

[10] T. L. Thomas, Cyberskepticism: The Mind's Firewall, Technical Report, FOREIGN MILITARY STUDIES OFFICE (ARMY) FORT LEAVENWORTH KS, 2008.

[11] I. Ghafir, V. Prenosil, A. Alhejailan, M. Hammoudeh, Social Engineering Attack Strategies and Defence Approaches, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 145–149.

[12] D.-J. van Mourik, Targeted attacks and the human vulnerability (2017).

[13] D. Harley, Re-floating the titanic: Dealing with social engineering attacks, European Institute for Computer Antivirus Research (1998) 4–29.

[14] E. Nyamsuren, H.-J. Choi, Preventing social engineering in ubiquitous environment, in: Future Generation Communication and Networking (FGCN 2007), volume 2, IEEE, 2007, pp. 573–577.

[15] F. Mohd Foozy, R. Ahmad, M. F. Abdollah, R. Yusof, M. Z. Mas'ud, Generic Taxonomy of Social Engineering Attack, UTHM, Batu Pahat, Johor, 2011. URL: http://eprints.utem.edu.my/191/.

[16] B. Oosterloo, Managing social engineering risk: making social engineering transparant, Ph.D. thesis, University of Twente, 2008. URL: http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf.

[17] R. Heartfield, G. Loukas, A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks, ACM Comput. Surv. 48 (2016) 37:1–37:39. URL: http://doi.acm.org/10.1145/2835375.

[18] K. Krombholz, Heidelinde Hobel, Markus Huber, E. Weippl, Social Engineering Attacks on the Knowledge Worker, in: Proceedings of the 6th International Conference on Security of Information and Networks, ACM, New York, NY, USA, 2013, pp. 28–35. URL: http://doi.acm.org/10.1145/2523514.2523596.

[19] K. Ivaturi, L. Janczewski, A taxonomy for social engineering attacks, in: International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, 2011. URL: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2011.

[20] A. Algarni, Y. Xu, Social engineering in social networking sites : phase-based and source-based models, International Journal of e-Education, e-Business, e-Management and e-Learning 3 (2013) 456–462. URL: http://eprints.qut.edu.au/67455/.

[21] A. Thapar, Social Engineering: An Attack Vector most Intricate to Tackle, CISSP: Infosec Writers (2007).

[22] The Kid & Co., The Shadow, MORE ON TRASHING, 2600: The Hacker's Quarterly Volume 1, Number 9 (1984). URL: http://www.hackcanada.com/ice3/2600/2600_01-9_p50.txt.

[23] Anonymous, Vital Ingredients: Switching Centers and Operators, 2600: The Hacker's Quarterly (1984).

[24] T. Shadow, How to Run a Successful Teleconference, 2600: The Hacker's Quarterly (1985).

[25] unknown, The history of The Legion Of Doom, Phrack Magazine Three (1990). URL: http://phrack.org/issues/31/5.html.

[26] B. Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Bantam, 1993.

[27] K. Hafner, J. Markoff, Cyberpunk: outlaws and hackers on the computer frontier, revised, Simon and Schuster, 1995.

[28] BlackOpsPro07, The Secret History of Hacking, 2001. URL: https://www.youtube.com/watch?v=PUf1d-GuK0Q.

[29] J. M. Hatfield, Social engineering in cybersecurity: The evolution of a concept 73 (2018) 102–113. URL: http://www.sciencedirect.com/science/article/pii/S0167404817302249.

[30] P. Lapsley, Exploding the phone: The untold story of the teenagers and outlaws who hacked Ma Bell, Grove Press, 2013.

[31] J. Quittner, Interview With Ice Man And Maniac, Phrack Magazine 4 (1992). URL: http://phrack.org/issues/40/14.html#article.

[32] H. M. Kluepfel, In search of the cuckoo's nest [computer security], in: Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, 1991, pp. 181–191.

[33] Social Engineering, Phrack Magazine Volume Two (1988). URL: http://phrack.org/issues/20/8.html#article.

[34] H. M. Kluepfel, Foiling the wiley hacker: more than analysis and containment, in: Proceedings. International Carnahan Conference on Security Technology, 1989, pp. 15–21.

[35] D. Fiery, Secrets of a Super Hacker, The Knightmare, 1994: Secrets of a Super Hacker, Bukupedia, 1994. Google-Books-ID: pEBtD-wAAQBAJ.

[36] A. Berg, Cracking a social engineer, Computers & Security 8 (1995) 700. URL: https://www.infona.pl//resource/bwmeta1.element.elsevier-80e104e1-fd04-39e8-b957-5b80efca285d.

[37] J. Quann, The hack attack - Increasing computer system awareness of vulnerability threats, Dec. 7-11, 1987, United States, 1987. URL: https://ntrs.nasa.gov/search.jsp?R=19880038985.

[38] I. S. Winkler, B. Dealy, Information Security Technology?...Don'T Rely on It: A Case Study in Social Engineering, in: Proceedings of the 5th Conference on USENIX UNIX Security Symposium - Volume 5, SSYM'95, USENIX Association, Berkeley, CA, USA, 1995, pp. 1–1. URL: http://dl.acm.org/citation.cfm?id=1267591.1267592.

[39] Anonymous, Telco Trashing Yields Big Rewards, Phrack Magazine 4 (1992). URL: http://phrack.org/issues/40/2.html#article.

[40] I. S. Winkler, Social Engineering and Reverse Social Engineering (1998).

[41] S. Granger, Social engineering fundamentals, part I: hacker tactics, Security Focus, December 18 (2001). URL: http://www.academia.edu/download/33172114/04SocialEngineeringWebQuest.pdf.

[42] T. Jordan, P. Taylor, A sociology of hackers, The Sociological Review 46 (1998) 757–780. URL: http://onlinelibrary.wiley.com/doi/10.1111/1467-954X.00139/abstract.

[43] S. Higgins, Physical penetrations: the art of advanced social engineering (2001).

[44] S. Granger, Social engineering fundamentals, Part II: Combat strategies, Security Focus. Retrieved October 12 (2002).

[45] K. Manske, An introduction to social engineering, Information

systems security 9 (2000) 1–7.

[46] H. Dang, The origins of social engineering, McAfee security journal (2008) 4–9. URL: https://www.wired.com/images_blogs/threatlevel/files/mcafee_security_journal_fall_2008.pdf#page=4.

[47] J. J. Rusch, The "social engineering" of internet fraud, in: Internet Society Annual Conference, http://www. isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm, 1999.

[48] K. D. Mitnick, W. L. Simon, The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons, 2011. (Similar citation of version 2001, 2002 are merged to avoid duplicate).

[49] L. Laribee, Development of methodical social engineering taxonomy project, Master's Thesis, Monterey, California. Naval Postgraduate School, 2006. URL: https://calhoun.nps.edu/handle/10945/2734.

[50] F. Mouton, L. Leenen, M. M. Malan, H. S. Venter, Towards an Ontological Model Defining the Social Engineering Domain, in: ICT and Society, IFIP Advances in Information and Communication Technology, Springer, Berlin, Heidelberg, 2014, pp. 266–279. URL: https://link.springer.com/chapter/10.1007/978-3-662-44208-1_22.

[51] CNN.com - A convicted hacker debunks some myths - Oct 7, 2005, 2005. URL: http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html.

[52] N. J. Evans, Information technology social engineering: an academic definition and study of social engineering-analyzing the human firewall (2009).

[53] H. Hasle, Y. Kristiansen, K. Kintel, E. Snekkenes, Measuring Resistance to Social Engineering, in: Information Security Practice and Experience, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2005, pp. 132–143. URL: https://link.springer.com/chapter/10.1007/978-3-540-31979-5_12.

[54] Social engineering (security), 2019. URL: https://en.wikipedia.org/w/index.php?title=Social_engineering_(security)&oldid=885978090, page Version ID: 885978090.

[55] social engineering | Definition of social engineering in English by Oxford Dictionaries, 2019. URL: https://en.oxforddictionaries.com/definition/social_engineering.

[56] M. Nohlberg, S. Kowalski, The cycle of deception : a model of social engineering attacks, defenses and victims, in: DIVA, University of Plymouth, 2008, pp. 1–11. URL: http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-3622.

[57] I. Gulenko, Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness, Information Management & Computer Security 21 (2013) 91–101. URL: http://www.emeraldinsight.com/doi/abs/10.1108/IMCS-09-2012-0053.

[58] W. Fan, K. Lwakatare, R. Rong, Social Engineering: IE based Model of Human Weakness to Investigate Attack and Defense (2016).

[59] D. Gragg, A multi-level defense against social engineering, SANS Reading Room, March 13 (2003). URL: http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf.

[60] M. Silic, A. Back, The dark side of social networking sites:Understanding phishing risks, Computers in Human Behavior 60 (2016) 35–43. URL: http://www.sciencedirect.com/science/article/pii/S0747563216301029.

[61] M. Schaeken, Information security awareness measuring & social engineering 2.0. Assessment of information security awareness (ISA) in the Belgian healthcare sector using an enhanced HAIS-Q., Master's thesis, Open Universiteit Nederland, 2018.

[62] M. Hasan, N. Prajapati, S. Vohara, Case Study On Social Engineering Techniques for Persuasion, International Journal on Applications of Graph Theory In wireless Ad Hoc Networks And sensor Networks 2 (2010) 17–23. URL: http://arxiv.org/abs/1006.3848, arXiv: 1006.3848.

[63] R. Samani, C. McFarland, Hacking the Human Operating System The role of social engineering within cybersecurity, Santa Clara, CA: McAfee (2015).

[64] F. Breda, H. Barbosa, T. Morais, SOCIAL ENGINEERING AND CYBER SECURITY (2017).

[65] C. Hadnagy, Social engineering: The art of human hacking, John Wiley & Sons, 2010.

[66] M. Huber, M. Mulazzani, S. Schrittwieser, E. Weippl, Cheap and Automated Socio-technical Attacks Based on Social Networking Sites, in: Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security, AISec '10, ACM, New York, NY, USA, 2010, pp. 61–64. URL: http://doi.acm.org/10.1145/1866423.1866435.

[67] M. Nohlberg, Securing information assets: understanding, measuring and protecting against social engineering attacks, PhD Thesis, Institutionen för data-och systemvetenskap (tills m KTH), 2008.

[68] rapid7.com, Best Practices for Social Engineering Attacks, 2018. URL: https://www.rapid7.com/docs/download/Metasploit_Best_Practices_for_Social_Engineering_Attacks.pdf.

[69] R. Gulati, Gulati, R. (2003). The threat of social engineering and your defense against it, Technical Report, 2003. URL: http://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=925964.

[70] J.-W. Bullee, Experimental social engineering: investigation and prevention (2017). URL: https://research.utwente.nl/en/publications/experimental-social-engineering-investigation-and-prevention.

[71] J. Stewart, M. Dawson, How the modification of personality traits leave one vulnerable to manipulation in social engineering, International Journal of Information Privacy, Security and Integrity 3 (2018) 187–208. URL: https://www.inderscienceonline.com/doi/abs/10.1504/IJIPSI.2018.092057.

[72] Y. Boshmaf, I. Muslukhov, K. Beznosov, M. Ripeanu, The Socialbot Network: When Bots Socialize for Fame and Money, in: Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11, ACM, New York, NY, USA, 2011, pp. 93–102. URL: http://doi.acm.org/10.1145/2076732.2076746.

[73] T. R. Peltier, Social Engineering: Concepts and Solutions, Information Systems Security 15 (2006) 13–21. URL: http://dx.doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3.

[74] F. Lu, Social engineering leading non-traditional information security, China Computer News (2006).

[75] J. Z. Fan, Hacker Social Engineering Attack, Jinan Qilu Electronic Audio and Video Publishing House, 2008.

[76] A. A. M. Algarni, The impact of source characteristics on users' susceptibility to social engineering Victimization in social networks, Thesis, Queensland University of Technology, 2016. URL: https://eprints.qut.edu.au/95604/.

[77] M. Hermansson, R. Ravne, Fighting Social Engineering - Increasing information security in organizations by combining scenario based learning and psychological factors of persuasion, University of Stockholm/Royal Institute of Technology (2005).

[78] M. Nohlberg, Social engineering: understanding, measuring and protecting against attacks, University of Skövde (2007).

[79] T. Bakhshi, M. Papadaki, S. Furnell, A Practical Assessment of Social Engineering Vulnerabilities., in: HAISA, 2008, pp. 12–23.

[80] N. Y. Conteh, P. J. Schmick, Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced Computer Research 6 (2016) 31.

[81] R. Larson, L. Cockcroft, CCSP: Cisco Certified Security Professional Certification All-in-One Exam Guide (Exams SECUR, CSPFA, CSVPN, CSIDS, and CSI)., McGraw-Hill Osborne, 2003.

[82] K. Beckers, S. Pape, V. Fries, HATCH: Hack And Trick Capricious Humans – A Serious Game on Social Engineering, 2016.

[83] R. E. Indrajit, Social Engineering Framework: Understanding the Deception Approach to Human Element of Security, International Journal of Computer Science Issues (IJCSI) 14 (2017) 8–16.

[84] J. R. Whiteman, Social Engneering: Humans are the Prominent Reason for the Continuance of These Types of Attacks, Master's thesis, 2017. URL: https://search.proquest.com/docview/2007620740/abstract/C5C35D60F2914052PQ/1.

[85] M. Jakobsson, Modeling and Preventing Phishing Attacks(full-text), in: Financial Cryptography and Data Security, volume 3570, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 89–89. URL: http://link.springer.com/10.1007/11507840_9.

[86] D. Mills, Analysis of a Social Engineering Threat to Information Security Exacerbated by Vulnerabilities Exposed Through the Inherent Nature of Social Networking Websites, in: 2009 Information Security Curriculum Development Conference, InfoSecCD '09, ACM, New York, NY, USA, 2009, pp. 139–141. URL: http://doi.acm.org/10.1145/1940976.1941003.

[87] P. Tetri, J. Vuorinen, Dissecting social engineering, Behaviour & Information Technology 32 (2013) 1014–1023. URL: https://doi.org/10.1080/0144929X.2013.763860.

[88] J. A. A. Cruz, Social engineering and awareness training, Technical Report, Technical report, Walsh College, 2010. URL:

http://www.talktoanit.com/SE/Social%20Engineering%20and%20Information%20Awareness.pdf.

[89] K. Lab, SOCIAL ENGINEERING, HACKING THE HUMAN OS, 2013. URL: https://www.kaspersky.com/blog/social-engineering-hacking-the-human-os/3386/.

[90] D. Bisson, 5 Social engineering attacks to watch out for, Tripwire. Viitattu 8 (2015) 2016.

[91] M. Jakobsson, Social Engineering 2.0: What's Next, McAfee security journal (2008) 13–15. URL: https://www.wired.com/images_blogs/threatlevel/files/mcafee_security_journal_fall_2008.pdf#page=4.

[92] E.Frumento, R.Puricelli, F.Freschi, D.Ariu, N.Weiss, C.Dambra, I.Cotoi, P.Roccetti, M. Rodriguez, L.Adrei, G.Marinelli, G.Kandela, B.Pachego, The role of Social Engineering in evolution of attacks, Technical Report, 2016. URL: http://www.doganaproject.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf.

[93] Pinterest, 2018. URL: https://en.wikipedia.org/w/index.php?title=Pinterest&oldid=873992162, page Version ID: 873992162.

[94] P. Kaul, D. Sharma, Study of automated social engineering, its vulnerabilities, threats and suggested countermeasures, International Journal of Computer Applications 67 (2013).

[95] Why it is called Internet of Things: Definition, history, disambiguation, 2014. URL: https://iot-analytics.com/internet-of-things-definition/.

[96] Industry 4.0, 2018. URL: https://en.wikipedia.org/w/index.php?title=Industry_4.0&oldid=872950801, page Version ID: 872950801.

[97] D. Gan, R. Heartfield, Social engineering in the internet of everything, Cutter IT Journal 29 (2016) 20–29.

[98] L. D. Ball, G. Ewan, N. J. Coull, Undermining-social engineering using open source intelligence gathering, in: KDIR 2012: Proceedings of the 4th International Conference on Knowledge Discovery and Information Retrieval, Barcelona, Spain, October 4-7, SciTePress-Science and Technology Publications, 2012.

[99] Y. Scheelen, D. Wagenaar, M. Smeets, M. Kuczynski, The devil is in the details: Social Engineering by means of Social Media, A Project Report on System & Network Engineering, Universiteit van Amsterdam (2012).

[100] M. Edwards, R. Larson, B. Green, A. Rashid, A. Baron, Panning for gold: Automatically analysing online social engineering attack surfaces, Computers & Security 69 (2017) 18–34. URL: http://www.sciencedirect.com/science/article/pii/S0167404816301845.

[101] trustedsec, trustedsec/social-engineer-toolkit, 2018. URL: https://github.com/trustedsec/social-engineer-toolkit, original-date: 2012-12-31T22:01:33Z.

[102] W. Rocha Flores, H. Holm, G. Svensson, G. Ericsson, Using phishing experiments and scenario-based surveys to understand security behaviours in practice, Information Management & Computer Security 22 (2014) 393–406.

[103] B. Green, D. Prince, J. Busby, D. Hutchison, The Impact of Social Engineering on Industrial Control System Security, in: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC '15, ACM, New York, NY, USA, 2015, pp. 23–29. URL: http://doi.acm.org/10.1145/2808705.2808717.

[104] T. N. Jagatic, N. A. Johnson, M. Jakobsson, F. Menczer, Social Phishing, Commun. ACM 50 (2007) 94–100. URL: http://doi.acm.org/10.1145/1290958.1290968.

[105] D. Kvedar, M. Nettis, S. P. Fulton, The Use of Formal Social Engineering Techniques to Identify Weaknesses During a Computer Vulnerability Competition, J. Comput. Sci. Coll. 26 (2010) 80–87. URL: http://dl.acm.org/citation.cfm?id=1858583.1858595.

[106] Z. Benenson, F. Gassmann, R. Landwirth, Unpacking Spear Phishing Susceptibility, in: M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, M. Jakobsson (Eds.), Financial Cryptography and Data Security, Lecture Notes in Computer Science, Springer International Publishing, 2017, pp. 610–627.

[107] Danesh Irani, M. Balduzzi, D. Balzarotti, E. Kirda, C. Pu, Reverse Social Engineering Attacks in Online Social Networks, in: Detection of Intrusions and Malware, and Vulnerability Assessment, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2011, pp. 55–74. URL: https://link.springer.com/chapter/10.1007/978-3-642-22424-9_4.

[108] E. Frumento, R. Puricelli, An innovative and comprehensive framework for Social Driven Vulnerability Assessment, Magdeburger Journal zur Sicherheitsforschung 2 (2014) 493–505.

[109] D. Kushner, The real story of stuxnet, ieee Spectrum 50 (2013) 48–53.

[110] S. Abraham, I. Chengalur-Smith, An overview of social engineering malware: Trends, tactics, and implications, Technology in Society 32 (2010) 183–196. URL: http://www.sciencedirect.com/science/article/pii/S0160791X10000497.

[111] M. Huber, S. Kowalski, M. Nohlberg, S. Tjoa, Towards Automating Social Engineering Using Social Networking Sites, in: 2009 International Conference on Computational Science and Engineering, volume 3, 2009, pp. 117–124.

[112] T. Lauinger, V. Pankakoski, D. Balzarotti, E. Kirda, Honeybot, Your Man in the Middle for Automated Social Engineering, in: LEET, 2010.

[113] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, C. Kruegel, Abusing Social Networks for Automated User Profiling, in: Recent Advances in Intrusion Detection, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2010, pp. 422–441. URL: https://link.springer.com/chapter/10.1007/978-3-642-15512-3_22.

[114] R. Gallagher, Where Do the Phishers Live? Collecting Phishers' Geographic Locations from Automated Honeypots, 2016 ShmooCon (2016).

[115] J. Seymour, P. Tully, Weaponizing data science for social engineering: Automated E2e spear phishing on Twitter, Black Hat USA (2016) 37.

[116] A. C. Bahnsen, I. Torroledo, L. D. Camacho, S. Villegas, DeepPhish: Simulating Malicious AI (2018).

[117] H. S. Anderson, J. Woodbridge, B. Filar, DeepDGA: Adversarially-Tuned Domain Generation and Detection, in: Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, AISec '16, ACM, New York, NY, USA, 2016, pp. 13–21. URL: http://doi.acm.org/10.1145/2996758.2996767.

[118] D. Ariu, E. Frumento, G. Fumera, Social Engineering 2.0: A Foundational Work: Invited Paper, in: Proceedings of the Computing Frontiers Conference, CF'17, ACM, New York, NY, USA, 2017, pp. 319–325. URL: http://doi.acm.org/10.1145/3075564.3076260.

[119] B. Aristotle, et al., The Categories, Minerva italica, 1971.

[120] L. Wittgenstein, Philosophical investigations, John Wiley & Sons, 2009.

[121] E. H. Rosch, Natural categories, Cognitive psychology 4 (1973) 328–350.

[122] E. Rosch, Cognitive representations of semantic categories., Journal of experimental psychology: General 104 (1975) 192.

[123] E. Rosch, B. B. Lloyd, Cognition and categorization (1978).

[124] F. Ungerer, H.-J. Schmid, An introduction to cognitive linguistics, Routledge, 2013.

[125] J. R. Taylor, Linguistic Categorization: Prototypes in Linguistic Theory, Oxford University Press, 2003.

[126] P. LingYu, The Compatibility Between Classical View of Categorization and Prototype Theory From the Perspective of Meaning Holism, Master's thesis, University of Electronic Science and Technology of China, 2014.

[127] V. Evans, M. Green, Cognitive linguistics: An introduction, Routledge, 2018.

[128] S. L. Armstrong, L. R. Gleitman, H. Gleitman, What some concepts might not be, Cognition 13 (1983) 263–308.

[129] P. J. Hurley, A concise introduction to logic, Nelson Education, 2014.

[130] B. Fang, The definitions of fundamental concepts, in: Cyberspace Sovereignty, Springer, 2018, pp. 1–52.

[131] B. Fang, Define cyberspace security, Chinese Journal of Network and Information Security 4 (2018) 1–5.

[132] Y. Lafrance, Psychology: A precious security tool, SANS GSEC Certification, Practical Assignment (2004).

[133] S. Lineberry, The Human Element: The Weakest Link in Information Security, Journal of Accountancy; New York 204 (2007) 44–46,49. URL: https://search.proquest.com/docview/206792454/abstract/60BDA918B1444D61PQ/1.

[134] McAfee, Social Engineering in the Internet of Things (IoT), 2015. URL: https://securingtomorrow.mcafee.com/executive-perspectives/social-engineering-internet-things-iot/.

[135] C. P. Pfleeger, S. L. Pfleeger, Security in Computing, Prentice Hall Professional, 2003.

[136] S. Uebelacker, S. Quiel, The Social Engineering Personality Framework, in: 2014 Workshop on Socio-Technical Aspects in Security and Trust, 2014, pp. 24–30.

[137] I. Winkler, Corporate Espionage: What it Is, why it is Happening in Your Company, what You Must Do about it, Prima Pub., 1997. Google-Books-ID: ge7a68kDIXEC.

[138] P. Dhiman, S. A. Wajid, F. F. Quraishi, A Comprehensive Study of Social Engineering-The Art of Mind Hacking (2017).

[139] M. Spinapolice, Mitigating the risk of social engineering attacks, Theses (2011). URL: http://scholarworks.rit.edu/theses/394.

[140] R. Barber, Social engineering: A People Problem?, Network Security 2001 (2001) 9–11. URL: http://www.sciencedirect.com/science/article/pii/S1353485801007164.

[141] P. S. Maan, M. Sharma, Social engineering: A partial technical attack, International Journal of Computer Science Issues 9 (2012) 1694–0814. URL: https://pdfs.semanticscholar.org/7e51/0456042c26cade06d74ea755c774713c46cf.pdf.

[142] S. Stasiukonis, Social engineering, the USB way, Dark Reading 7 (2006). URL: http://tonydye.typepad.com/main/files/HO05-DarkReading.doc.

[143] M. Jodeit, M. Johns, Usb device drivers: A stepping stone into your kernel, in: Computer Network Defense (EC2ND), 2010 European Conference on, IEEE, 2010, pp. 46–52. URL: http://ieeexplore.ieee.org/abstract/document/5663316/.

[144] S. Gupta, A. Singhal, A. Kapoor, A literature survey on social engineering attacks: Phishing attack, in: 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 537–540.

[145] E. M. Maseno, Vishing Attack Detection Model For Mobile Users, Thesis, KCA University, 2017. URL: http://41.89.49.13:8080/xmlui/handle/123456789/1276.

[146] K. C. Redmon, Mitigation of Social Engineering Attacks in Corporate America, Greenville: East Carolina University (2005).

ZUOGUANG WANG is a doctoral student of the School of Cyber Security, University of Chinese Academy of Sciences. He is currently pursuing his PhD in Information Security at Institute of Information Engineering, Chinese Academy of Sciences, and has participated in one of the National Key Research and Development Programs of China. His main research interests include Social Engineering, Industrial Control System security and IoT security.

LIMIN SUN holds a PhD from National University of Defense Technology, and is a professor of Institute of Information Engineering, Chinese Academy of Sciences. He is the Secretary General of the Select committee of CWSN, the director of Beijing Key Laboratory of IOT information security. His main research interests include IoT security, Industrial Control System security and Social Engineering.

HONGSONG ZHU holds a PhD from Institute of Computing Technology, Chinese Academy of Sciences, and is a professor of Institute of Information Engineering, Chinese Academy of Sciences. He is the Member of the Select Committee of China Computer Federation Technical Commission on Sensor Network (CWSN). His main research interests include IoT security, network measurement and Social Engineering.