IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 17, 2019, accepted May 15, 2019, date of publication May 27, 2019, date of current version June 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2919150

A Session and Dialogue-Based Social Engineering Framework

KANGFENG ZHENG[1], TONG WU[1], XIUJUAN WANG[2], BIN WU[1], AND CHUNHUA WU[1]
[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

Corresponding author: Tong Wu (wutong@bupt.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802803, and in part by the National Natural Science Foundation of China under Grant 61602052.

ABSTRACT Social engineering has been increasingly used during the past few years. Social engineering attacks have resulted in great financial losses. Research on social engineering models and frameworks is still in its elementary stage. An appropriate social engineering framework can interpret all the attack components and their relationships clearly, which will contribute to the defense of social engineering attacks. In this tutorial paper, existing social engineering models and frameworks are summarized and a new social engineering framework is proposed involving the concept of the session and dialogue. An entire social engineering attack is defined as a social engineering session (SES). A social engineering dialogue (SED) refers to a specific attack phase, which is included in a SES. A SES contains several well-organized SEDs. Then, the attack graph is used to formalize the proposed social engineering framework. The SED is treated as an atomic attack during the whole SES. The human weaknesses that an attacker can exploit are described as vulnerabilities, the information, and trust that an attacker owns as permissions. Finally, three real-world social engineering cases are analyzed using the proposed framework and attack graph. The analyses illustrate the usability of the proposed framework and provide a better understanding of various social engineering attacks.

INDEX TERMS Social engineering, social engineering session (SES), social engineering dialogue (SED), attack graph, information security.

I. INTRODUCTION

Social Engineering (SE) is an emerging threat that has developed along with networks and social media, and it has been the subject of increasing attention over the past few years. Fraud has existed long before the advent of modern technology [1]. The prevalent use of social media and cyberspace provides fertile ground for traditional fraud due to increasing sharing of personal information but little awareness and action of protecting the information [2].

Some typical SE attacks, such as phishing and phone scams, have caused hundreds of millions in monetary losses. According to the latest Internet crime report [3] of the Internet Crime Complaint Center (IC3), a formal U.S. cybercrime reporting entity, the IC3 received 10,949 complaints related to tech support fraud (phishing, phone scam, etc.) in 2017. The claimed losses amounted to nearly $15 million, which represented a 90% increase in losses from 2016. While a majority of tech support fraud involves victims in the U.S., IC3 has received complaints from victims in 85 different countries. In addition, according to 360 security center (a formal Chinese cybercrime reporting entity) [4], a total of 21,703 cases of effective SE fraud reports are received in 2018, involving a total amount of more than $58 million and an increase of 69.8% compared with the average loss in 2017.

All of these monetary losses show that social engineering achieves effective criminals with some simple means implemented in social media. The easy technique is often the hardest to prevent. There has been a considerable increase in the number of research papers on social engineering. However, there is still no effective defense method against the rapid growth of social engineering attacks. We focus our study on social engineering framework enlightened by the existing definition, with the hope of contributing to social engineering defenses.

The most popular definition of SE is that given by Kevin Mitnick, who defined it as ‘‘using influence and persuasion

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz.

to deceive people and take advantage of their misplaced trust in order to obtain insider information'' [5]. Mouton *et al.* [6] proposed definitions of social engineering, social engineer, and social engineering attacks through summarizing various previous definitions. They 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.'' According to the Oxford English Dictionary, one of the distinct meanings of ''social engineering'' involved in the domain of cyberspace is ''the use of deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer system or network'' [7]. All of the three definitions refer to the concepts of people, deception or persuasion, trust or compliance, and some actions. These words make up the key elements of a social engineering attack.

With a clear definition of social engineering, a few researchers have focused their studies on social engineering frameworks. A social engineering framework is a detailed analysis and presentation of attack patterns and mechanisms in chronological order. All the attack components and their relationships should be described as the attack process flows. Social engineering attacks can be defensed quickly and effectively only by understanding the mechanisms of each attack step adequately. Therefore, an applicable social engineering attack framework is helpful to the detection and defense of social engineering attacks.

Most of the current research applies a circular structure to describe social engineering attacks, mostly including information gathering, trust exploitation, attack development, and goal satisfaction. They state that previous phases can be repeated if more information is needed or the goal is not satisfied in a single phase [5]. However, little research discusses the phased achievements contributed to the next phase and the global goal. When a phase in the whole cycle is completed and the global goal has not been achieved, the result of this phase is still unclear in previous researches. The phased achievements are critical for the attacker, which are closely related to the global goal and information needed for the next phase. It is important to explore the phased achievements for the purpose of comprehending the mechanisms of social engineering. The relationship between each phase can be a key factor to interrupt a social engineering attack. In addition, some complex social engineering attacks are very difficult to be described using a single circular structure. A complete social engineering attack is interlinked and each phase has elaborate purposes.

Due to these shortcomings, we have designed a new social engineering attack framework using the social engineering session and social engineering dialogue. The framework breaks down the circular structure and divides a social engineering attack into multiple steps. The phased achievements and relationships between each step are discussed sufficiently.

In this tutorial paper, we make the following contributions:

- We provide a snapshot of the state-of-the-art social engineering research and a summary of social engineering models in previous works.
- A new social engineering attack framework is proposed involving of the concept of the session and dialogue.
- We describe SES and SED using attack graphs to provide formalized definitions of the proposed framework.
- We discuss three real-world cases of social engineering attacks using the proposed social engineering framework and attack graph.

The rest of this paper is organized as follows. Section II provides related works about social engineering. In Section III, we present the SES and SED frameworks. Section IV formalizes the SES and SED frameworks using attack graphs. Section V discusses three real-world social engineering attack cases. Section VI concludes our study.

II. RELATED WORK

A. THE STATE-OF-THE-ART SOCIAL ENGINEERING RESEARCH

There has been a considerable increase in the number of research papers on social engineering in recent years, indicating that social engineering has attained academic significance. The current research on social engineering mainly includes two aspects: theory and defense method. The research on social engineering theory includes its concept, taxonomy, model, etc. Social engineering defense methods include some overall detection frameworks, specific detection methods centered on a kind of SE attack, and some other research for increasing precaution consciousness. Table 1 summarizes the state-of-the-art social engineering research in recent three years.

In the area of social engineering theory, there are some outstanding representatives. For example, Joseph [7] offered a detailed history of social engineering around three fundamental ideas: epistemic asymmetry, technocratic dominance, and teleological replacement. Mouton *et al.* [6], [8]–[13] presented a wealth of research on social engineering theory, including its concept, ontological model, framework, defense method, and attack templates. Some other researchers focus their studies on human factors, such as human weakness [16], principles of persuasion [20]. In general, there are still a few studies on the theory of social engineering, and further studies are needed.

As Table 1 shows, most of the recent researches focus on social engineering defense methods, especially phishing defense including web phishing, email phishing, and short message service (SMS) phishing. Some researches use classical methods to detect phishing attacks [28] and some others develop phishing detection method in software-defined networking (SDN) environment [14], [25]. There are also several detection models designed for the overall social engineering attacks [8], [9], [17], [18]. In addition, the defense method in organizations has attracted much more attentions in order to improve employees' security awareness [22], [26], [30], [33].

B. SOCIAL ENGINEERING MODELS

This paper mainly focuses on the model of social engineering. In this subsection, several dedicated models of social engineering are presented. Table 2 shows a summary of some typical social engineering models in previous works. There are two kinds of social engineering models, phase-based model and conceptual model. A phase-based model is based on social engineering attack process, and a conceptual model is based on the key entities of a social engineering attack.

Most of the existing phase-based models are in the form of a cycle. The most commonly known model is Kevin Mitnick's social engineering attack cycle [5]. Mitnick's attack model has four phases: research, developing rapport and trust, exploiting trust, and utilizing information. In Mitnick's model, if the goal is not satisfied, the previous steps can be repeated. After this model was produced, other models and frameworks were proposed based on the attack cycle.

Mouton *et al.* [13] proposed a social engineering attack framework based on Kevin Mitnick's social engineering attack cycle. Their attack framework focuses on every step of the social engineering attack, from determining the goal of an attack up to the successful conclusion of the attack. Six phases are included in their framework: (1) attack formulation (goal identification, target identification); (2) information gathering (identify potential sources, gather information from sources, assess gathered information); (3) preparation (combination and analysis of gathered information, development of an attack vector); (4) develop a relationship (establishment of communication, rapport building); (5) exploit the relationship (priming the target, elicitation); and (6) debrief (maintenance, transition).

Algarni and Xu [35] presented a phase-based and a source-based models of social engineering threats on social networking sites. The phase-based model consisted of 8 phases: (1) using suitable gates of SNSs to gather information; (2) determining the tactic and developing a plan; (3) relying on one or more socio-psychological factors; (4) using suitable gates of SNSs to reach the victim; (5) wearing a suitable hat and playing a suitable character; (6) developing trust and a sense of safety; (7) choosing the perfect time; and (8) using professional skills. The source-based model is a supplement for the phase-based model. The three sources or gates of threats in SNSs are the following: insecure privacy settings, friendship and connection with strangers, and insecure dealing with content. The two presented models showed an intensive and comprehensive overview of social engineering attacks on social networks sites and provided a fuller picture of social engineering threats on social networks sites.

Nohlberg and Kowalski [36] created cycles describing the attacker, defender, and victim, and merged them into a model describing the cycle of social engineering. The model was then extended into a possible social engineering sphere. They provided the resulting models to educate others about social engineering, create automated social engineering attacks, facilitate better incident reporting, and understand the impact and economical aspects of defenses.

Cullen and Armitage [37] designed a social engineering spiral model to demonstrate all social engineering targeted attacks from the very simple and straightforward to the highly complex. The social engineering attack model starts with a trigger event indicated at the center of the spiral. The attacker then analyzes the risk and carries out the initial reconnaissance. In the next phase, the attacker looks to build a relationship with the victim. Then, the attack scenario building, attack execution, and action on objectives phases are followed. At each iteration, the attacker plans for the next phase.

For the conceptual model of social engineering, there are different presentations. Some researches show the key elements separately. For example, Janczewski and Fu [38] presented a conceptual model of the major aspects of social engineering attacks, including vulnerabilities, defenses, attack methods, and consequences. The ontological model of Mouton *et al.* [6] has one social engineer, one target, one or more compliance principles, one or more techniques, one medium, and one goal. Some other researches have more different forms. Tetri and Vuorinen [39] proposed a conceptualization of social engineering, called intruder-techniques-dupe, which consisted of different dimensions of a social engineering attack. Gonzalez *et al.* [40] used two feedback loops as the idealized patterns to describe the main modes of social engineering attacks.

Almost all the existing phase-based social engineering models are performed in a cycle. The circular form shows the repeated process of a social engineering attack to achieve its final goal, but at the expense of some key details. In the next section, we will introduce a new social engineering attack framework to deal with the existing shortcomings.

III. SOCIAL ENGINEERING ATTACK FRAMEWORK

In this section, a new social engineering attack framework is presented based on previous research. This paper introduces the session and dialogue mechanisms to describe social engineering attacks. A SED is an attack phase in a whole SES and a SES contains several well-organized SEDs. The details of a SED and SES are as follows.

A. SOCIAL ENGINEERING DIALOGUE (SED)

A SED is an atomic attack in a whole social engineering attack that represents a single connection between the attacker and target. The ordered combination of several SEDs forms a complete social engineering attack process. A valid SED can prepare physical object, information and trust for the next SED step or achieve the goals of the whole SE attack. A failure of a single SED does not represent a failure of the entire attack process, because a whole SE attack process can include several SEDs. Each SED is an integrated system including the attack preparation, attack implementation, and attack gain.

TABLE 1. A summary of the state-of-the-art social engineering research.

Reference	Issues	Methodology
Joseph [7]	Concept	This paper offers a history of the concept of social engineering in cybersecurity and analyzes 134 definitions of social engineering found in academic articles written about cybersecurity from 1990 to 2017.
Mouton *et al.* [8,9]	Social engineering attack detection model	In order to formally address social engineering in a broad context, the authors propose the social engineering attack detection model using the underlying finite state machine, called SEADM and SEADMv2.
Mouton *et al.* [10]	Theory and defense (definition, framework, temples and detection model)	This paper presents a social engineering ontological model, an attack framework and a detection model. And it also proposes ten templates that provide fully detailed steps and phases throughout social engineering attacks.
Chin *et al.* [14]	Email phishing detection	This paper presents a new phishing detection and mitigation approach in software-defined networking (SDN) environment with an accuracy of 98.39%.
Sriendra and Abeywardena [15]	Email phishing detection	This paper identifies a correlation between the psychological concepts (subliminal and supraliminal) and phishing/spear phishing attacks in the domain of cybersecurity.
Fan *et al.* [16]	Theory (human weakness and defense)	This paper shapes human weaknesses for social engineering and presents a number of defense measures to fix the human weaknesses.
Heartfield *et al.* [17,18]	Semantic social engineering detection	The authors propose a human-as-a-security-sensor defense model to provide a mechanism to report social engineering attacks if some people spot them.
Bridget *et al.* [19]	Email phishing detection	The article presents a client-side sentinel to vet email header source code and alert the user to potential problems.
Sabouni *et al.* [20]	Theory(principles of persuasion)	This paper develops a preliminary radicalization framework based on social traits that may be exploited during a social engineering attack, such as principles of persuasion.
Xiangyu *et al.* [21]	Theory and defense (definition, taxonomy, personality factors, and solutions)	This paper introduces the definition, taxonomy, personality factors of social engineering and proposes solutions to reduce internet crimes.
Matthew *et al.* [22]	Social engineering defense in organizations	The article proposes an automated social engineering vulnerability scanner that organizations can use to analyze their exposure to potential social engineering attacks.
Siadati *et al.* [23]	SMS phishing defense	This paper demonstrates a robust messaging approach that can reduce the success of the most effective social engineering attack.
Abeywardana *et al.* [24]	Social engineering defense	The authors design a social engineering risk assessment framework, involving with basic building blocks for social engineering aware risk analysis and a chronological attack classification framework.
Masoud *et al.* [25]	Web phishing detection	This paper proposes a neural-network-based phishing prevention algorithm utilizing an open source software-defined networking (SDN) controller.
Pape and Beckers [26]	Social engineering defense in organizations	The authors propose a card game to elicit employees' document security requirements.
Heartfield *et al.* [27]	Semantic social engineering defense	The aim of this paper is to explore the feasibility of predicting user susceptibility to social engineering attacks through attributes that can be measured, preferably in real-time and in an automated manner.
Sawa *et al.* [28]	Social engineering detection	The authors apply natural language processing techniques to detect social engineering attacks through identifying suspicious comments.
Wilcox and Bhattacharya [29]	Social engineering defense	The purpose of this paper is to propose a social media policy framework focusing on the practical reduction of social engineering risk through security policy control.
Bakhshi [30]	Social engineering defense in organizations	This paper aims at indicating the level of user susceptibility to social engineering attacks in a cooperating corporate organization.
Gupta *et al.* [31]	A survey of phishing	The paper discusses about the phishing attack theoretically including various types of phishing attacks and prevention methods.
Algarni *et al.* [32]	Theory	This paper validates the existence of four dimensions toward the credibility of social engineering attackers on Facebook and develops a valid measurement scale for each dimension.
Ghafir *et al.* [33]	Social engineering defense	This paper examines the role and value of information security awareness efforts in defending against social engineering attacks, in order to efficiently focus on security training and awareness building.
Flores and Ekstedt [34]	Social engineering defense in organizations	This paper studies how organizational and individual factors work in shaping employees' intention to resist social engineering.

TABLE 2. A summary of existing social engineering models.

Reference	Methodology	Model type	Model form
Kevin Mitnick[5]	The model has four phases: research, developing rapport and trust, exploiting trust, and utilizing information.	Phase-based model	Cycle
Mouton *et al.* [6]	The elements in the social engineering attack model are social engineer, target, compliance principles, medium, techniques, and goal.	Conceptual model	~
Mouton *et al.*[13]	Six phases are proposed including attack formulation, information gathering, preparation, develop a relationship, exploit the relationship and debrief.	Phase-based model	Cycle
Algarni and Xu [35]	The authors propose eight phases in their phase-based model of social engineering threats on social networking sites.	Phase-based model	Cycle
Nohlberg and Kowalski[36]	The five phases in this model are goal & plan, map & bond, execute, recruit & cloak, and evolve/regress.	Phase-based model	Cycle
Cullen and Armitage[37]	A social engineering spiral model is proposed to demonstrate all social engineering targeted attacks from the very simple and straightforward to the highly complex.	Phase-based model	Spiral
Janczewski and Fu [38]	The elements in this model are vulnerabilities, defenses, attack methods, and consequences.	Conceptual model	~
Tetri and Vuorinen [39]	This paper proposes an abstract social engineering framework, called intruder-techniques-dupe.	Conceptual model	~
Gonzalez *et al.* [40]	This paper uses system archetypes as the idealized patterns to describe the main modes of social engineering attacks.	Conceptual model	~

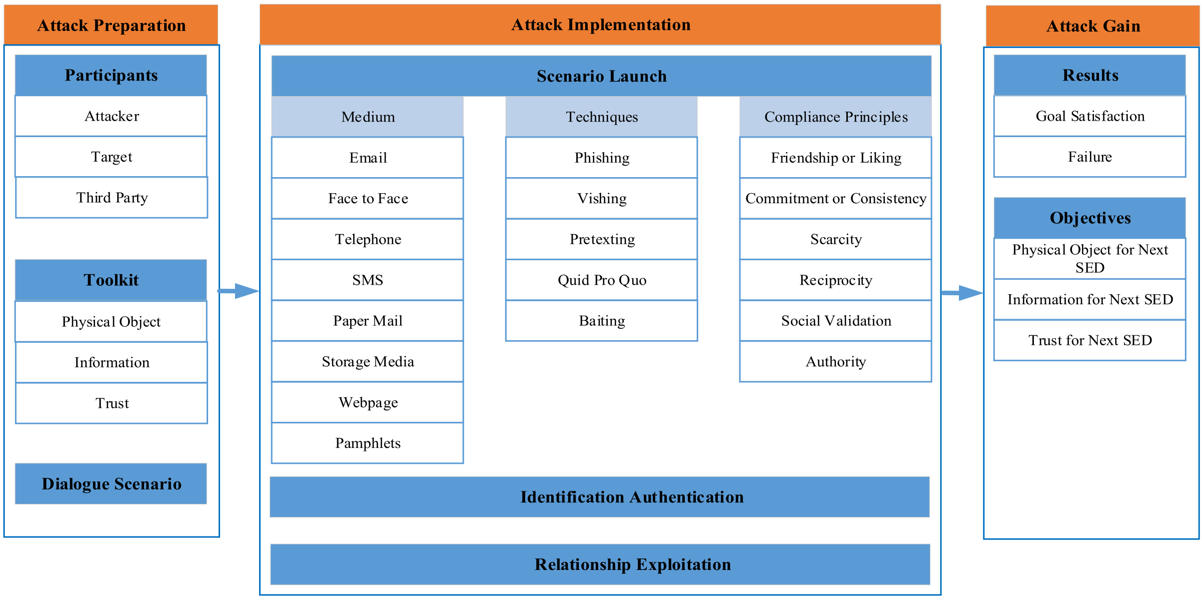

FIGURE 1. Social engineering dialogue framework.

The attack preparation stage refers to the preparation of the people, material, plans, and some other aspects needed for the SED. After the attack preparation stage, the attacker implements the attack and finally achieves some results. The framework of a SED is shown in Figure 1.

1) ATTACK PREPARATION

In the attack preparation stage, three parts are needed to be arranged, including the participants, toolkit, and dialogue scenario. To achieve a global objective in the whole SES, a dialogue scenario should be designed for one SED. After the dialogue scenario is completed, participants for this SED must be chosen and a toolkit should be collected according to the scenario.

Participants of a SED generally include an attacker and a target. Sometimes, a third party is also required in a SED. A clever attacker can better promote a criminal attack. A dialogue scenario is the script for a SED, which defines the plot, roles, and action for the participants. A dialogue scenario is devised to lure the target into a required action [10]. A successful dialogue scenario can lead the target into the role in the script, trusting the social engineer's words and acting on his instructions. A dialogue scenario needs to include the implementation process and the expected results of a SED.

An elaborate toolkit is a key factor in the whole SED process, which stores tools such as physical object, information, and trust. Physical object includes entities needed for the SED, such as bank cards and USB drives. Information is gathered about the target and everything related to the SED, such as name, profession, favorites, files, and passwords. The quality and detail level of the information largely influences the result of a SED. Information about the target usually contains some public and private data. In most cases, private information can easily gain the trust and acceptance of the target. Some private information is obtained through traditional cyber-attacks or other illegal means. According to Mitnick and Simon [5], the development of trust is a key element of a SE attack. Therefore, trust is defined as a separate tool that the attacker can exploit in the toolkit. It can illustrate an existing relationship between the participants in a SED. The trust can be obtained by the previous SED.

2) ATTACK IMPLEMENTATION

Attack implementation is the specific operational step that occurs according to the designed scenario, including the scenario launch, identification authentication, and relationship exploitation.

First, the attacker launches the designed scenario and chooses one or more mediums, techniques, and compliance principles. These three aspects guide the whole attack implementation, including the identification authentication and relationship exploitation. For example, in the case of a phone scam, an attacker calls a target and instructs him to go to the bank. This call completes the process of identification authentication and relationship exploitation. Therefore, the two processes involve a medium of telephone, a technique of vishing, and a compliance principle of authority. An appropriate medium is essential for a SED. If the selected medium cannot build the connection successfully, the attack will not be carried out effectively. Common mediums [6] are listed in Figure 1, including some physical mediums and social network mediums. Based on the research of Mouton *et al.* [6], a technique called vishing is added to the list of techniques. Compliance principles refer to the reasons why a target complies with the attacker's request, and techniques include those used to perform social engineering attacks [6].

Identification authentication is a process of building a connection and verifying the identification between the attacker and the target. Relationship exploitation is the stage of exploiting the trust relationship between the attacker and the target. In this stage, the attacker will use some psychological weakness of the target to stimulate the target's emotions. For example, some social engineers masquerade as a police officer to motivate fear in the target. Under the control of these emotions, it is easy for the target to trust the attacker and provide what the attacker needs.

3) ATTACK GAIN

The attack gain describes the results and objectives of a SED. The results represent the SED attack status (goal satisfaction or failure). The objectives show what a SED can provide for the next SED and the whole SE attack. There are three types of objectives: physical object, information, and trust. For example, in an email phishing attack, the objective of the attacker may be the password of the target's bank account. In a Dumpster Diving attack, the objective may be a flash drive. In some other scenarios, the objective of a SED may be a trust relationship between the participants in the next SED.

B. SOCIAL ENGINEERING SESSION (SES)

In this paper, a complete SE attack is defined as a SES that is an ordered combination of one or more SEDs. There are also three steps in a SES: attack preparation, attack implementation, and attack gain. A whole process of SES contains a set of several SEDs and some other global information. Figure 2 shows a detailed schematic framework of a SES.

1) ATTACK PREPARATION

The attack preparation step of a SES includes four stages: attack goal, participants, toolkit, and session scenario. The stage of the attack goal is added based on the attack preparation step of a SED. The attack preparation step of a SES contains all of the attack preparation steps of the SEDs and some other items required for the whole SE attack.

The attack goal is the overall objective that social engineers want to achieve. The attack goal of a SES is a specific purpose that can be achieved by following a set of SEDs. The whole SE attack is guided by the attack goal. For example, the attack goal of an email phishing attack is to steal the target's money in his bank account. The attacker first achieves the purpose of obtaining the target's trust using a phishing email, and then acquires the target's bank account password. In addition to the roles that appear in SEDs, attack participants of a SES also include roles, such as the organizer of the attack. Similarly, the session toolkit and session scenario of a SES assemble all of the related data needed for a SE attack.

2) ATTACK IMPLEMENTATION AND ATTACK GAIN

The attack implementation of a SES is mainly centered on the organization of SEDs, including the ordered SED implementation, phase attack gains, and SED result evaluation. A whole SES is a step-by-step process of exploiting trust and achieving phase goals. The order of SEDs in a SES is an essential element to gain the final objectives. If the order is not properly arranged, it is likely that the attack goal cannot be achieved. For example, in a vishing case, if the social engineer pretexting as a bank employee asks the attack target to transfer his money in the first SED, the target will likely

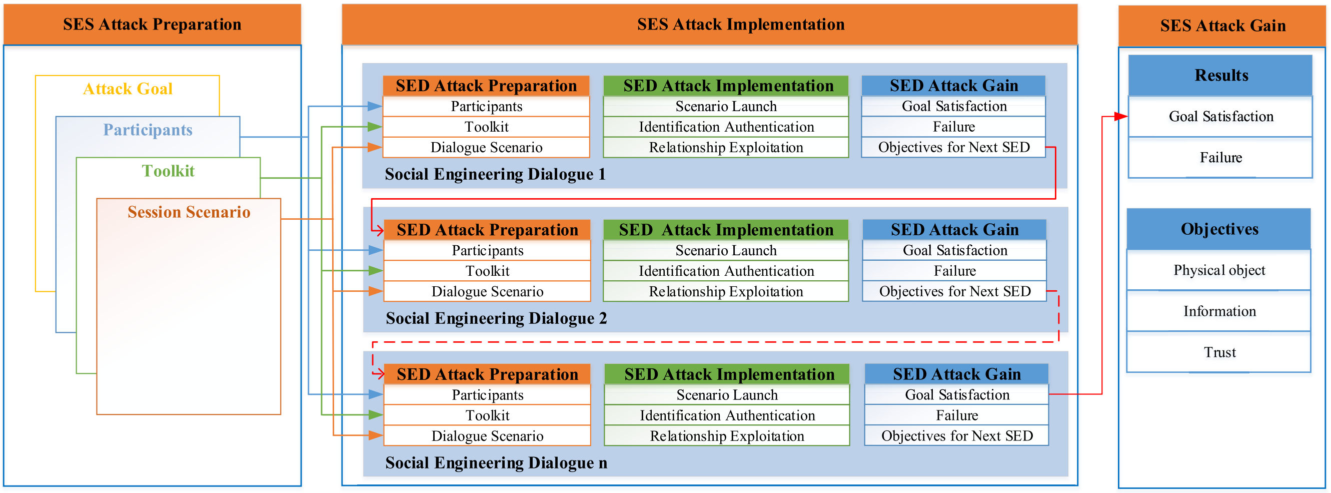

FIGURE 2. Social engineering session framework.

become more vigilant and will not believe the attacker, which will lead to the failure of the SE attack. However, if in the first SED the social engineer pretexts as a police officer to threaten the target and in the second SED pretexts as a bank employee to provide money transfer help, the target is more likely to believe the attacker and give his money to the attacker. When a SED is finished, the stage of the SED result evaluation is very important. The results that need to be evaluated include the process and objectives of previous SEDs, as well as the current psychological state of the target. The attacker needs to estimate whether the establishment of the relationship is successful, whether the trust of the target has been fully achieved and whether it can be continued to implement the next SED. The stage of the SED result evaluation plays a vital role in the integrity and continuity of a whole SES. If the evaluation is wrong and the target is not fully trusted, the attack will fail.

Some complete SESs are the combination of traditional cyber-attacks and social engineering attacks. In a whole social engineering attack, traditional cyber-attacks can be a way of acquiring information or a channel of obtaining unauthorized access. A general traditional cyber-attack also includes three stages: attack preparation, attack implementation, attack result and aftermath. This is consistent with our proposed framework. When analyzing complex attacks, it is possible to combine the steps of a traditional attack with the steps of a social engineering attack. There are lots of researches on traditional cyber-attack stages and framework. This article focuses on social engineering attack framework and does not specify traditional cyber-attack.

In view of the shortcomings of the existing social engineering frameworks, we propose a new framework to break the cycle structure and describe phased objectives, for better understanding social engineering process. In the next section, we will further describe the proposed framework using the attack graph model.

IV. SOCIAL ENGINEERING ATTACK DEFINITION USING AN ATTACK GRAPH

To formalize the proposed social engineering framework, we define the proposed social engineering framework using the attack graph model. The graph aims at finding the specific attack actions and privileges that an attacker needs to achieve his goals. Two attack graphs are designed to show the attack process of the SES and SED.

A. ATTACK GRAPH

In the 1990s, Cynthia and Painton [41] first proposed the concept of an attack graph and applied it to network vulnerability analysis. An attack graph is a directed graph that shows the attack order and attack effect, making it possible to describe all the critical network nodes and all the possible attack ways. There are two typical types of attack graphs, the state attack graph [42]–[44] and the attribute attack graph [45]. In this paper, the attribute attack graph is used to describe the proposed SE framework.

Beckers *et al.* [46] provided a structured threat analysis method for combining the analysis of social engineering attackers and technical attackers using attack graphs, in order to identify relevant actors that could become victims of a social engineering attacker. They defined social engineering patterns and identified social engineering vulnerabilities using access control lists and some information about the system, then combined social engineering vulnerabilities with network vulnerabilities using attack graph. Finally, possible attacks were quantitatively viewed. This paper provides the inspiration of using attack graphs to analyze social engineering attacks. It also demonstrates the rationality of combining social engineering attacks with traditional attacks in an attack graph. These provide a basis for us to define our framework with attack graphs.

The main contribution of our method is that the proposed attack graphs spread around human elements. Attack graphs of traditional cyber-attacks are used to describe network security related elements, such as the host, service, vulnerability, and permission. Because the critical difference between a social engineering attack and a traditional attack is the utilization of human elements, we regard human as a system and abstract human elements into attack graphs. We regard the human cognitive weaknesses that an attacker can exploit as vulnerabilities, the information and trust that an attacker owns as permissions. The proposed attack graphs clearly show the process that an attacker uses people's information, utilizes people's weaknesses, gains people's trust and finally achieves the objectives.

It should be noted that in a traditional attack graph, when all of the pre-conditions are met, the vulnerability utilization can be completed, thus satisfying all the post-conditions. However, in SE attacks, for different attackers and targets, all of the post-conditions may not be satisfied after all of the pre-conditions and SEDs. This situation is determined by human's cognitive complexity. Based on this essential characteristic, the proposed attack graphs are just simple representations of the existing SE attack processes and results through summarizing real-world SE cases, but not a comprehensive analysis, including all of the possible attack ways of a whole target system.

In order to correspond to the proposed framework, we design two attack graphs, a SES attack graph and a SED attack graph. For a whole SES, a SED can be treated as an atomic attack. Therefore, in a SES attack graph, a SED can be represented as an attack vertex. In order to analyze the process of each SED, a SED also can be described using a separate attack graph in detail according to the proposed SED framework. When a whole SE attack needs to be analyzed, a SED can be treated as a node for the sake of brevity of the overall analysis. When analyzing complex attacks, each SED can also be analyzed as a single complete attack graph. These two attack graphs not only correspond to our proposed framework, but also facilitate the diversified analysis of social engineering attacks.

B. ATTACK GRAPH OF SES

According to the definition of an attack graph, the attack graph of a SES is defined as $Graph_{SES} = \{S, A, E\}$. S is a collection of resource state nodes, $S = \{s_1, s_2, \ldots s_n\}$. A is the set of action nodes, $A = \{a_1, a_2, \ldots, a_m\}$. E is the edge set $E = \{e_i | e_i \in ((A \times S) \cup (S \times A))\}$. In the proposed framework, six types of S are needed for specifying the SES, that is $S = \{$*Participants, Physical object, Information, Trust, Scenario, Attack goal*$\}$, in which the physical object, information, and trust can form the node called *Toolkit*. There are two kinds of action nodes, traditional attack and SED, that is, $A = \{$*Traditional attack*, *SED*$\}$. The information of all of the nodes is marked in the parentheses, such as *Information*(*Email*). The information of a SED action node includes three parts, which are scenario launch (SL), identification authentication (IA), and relationship exploitation (RE). The information of a trust node, (a, b), represents that a trusts b.

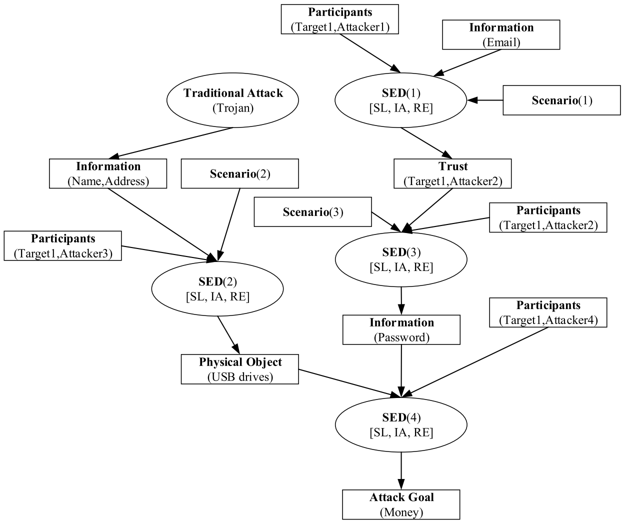

FIGURE 3. An example SES attack graph.

Figure 3 shows an attack graph example of a SES. The example describes how a social engineering criminal organization achieves its attack goals through several traditional network attacks and SEDs. They obtain the required physical objects, information, and trust to eventually achieve their attack goal. First, the criminal organization begins the attack by launching a SED attack utilizing the target's email address according to the designed scenario(1). The SED attack called SED(1) achieves the objective of obtaining the trust of target1. The SED attack builds a foundation for the next SED. On the basis of SED(1), SED(3) involves attacker2 and scenario(3) for the purpose of obtaining some additional information, such as the password from the target1. A traditional attack is implemented to acquire the needed information. Then, SED(2) is launched, utilizing the acquired information, and achieves the objective of getting a physical object, such as a USB drive. Finally, SED(4) is implemented using tools from the former attacks and achieves the final attack goal of the whole SES.

To formalize the attack graph, a table is designed to present the attack path, pre-conditions, and post-conditions in the SES. Table 3 shows the details for the attack graph example in Figure 3. In the attack path, "→" represents a progressive relationship between two attacks and "∧" represents the separation of the attack steps. As shown in Table 3, SED(1) provides a trust relationship for SED(3) and a traditional attack provides some information for SED(2). Then, SED(2) and SED(3) contribute a physical object and a password to SED(4), separately. Finally, the social engineers obtain the target's money in SED(4). The pre-conditions include a list of participants, a set of information, and several scenarios. The post-conditions include some physical objects, information, and trust relationships, which are also the objectives of each SED. Table 3 describes all of the elements of the example SES while Figure 3 shows all of the elements as an attack graph. These methods facilitate the analysis of social engineering attacks.

TABLE 3. A description of the example SES attack graph.

SES Detail	Description
Attack Path	*SED*(1)→*SED*(3)∧ *Traditional attack*(Trojan)→*SED*(2)∧ *SED*(4)
Pre-conditions	*Participants*={*Target1*, *Attacker1*, *Attacker2*, *Attacker3*, *Attacker4*}∪ *Information*={*E-mail*}∪ *Scenario*={*Scenario(1)*, *Scenario(2)*, *Scenario(3)*}
Post-conditions	*Physical object*={*USB*}∪ *Information*={*Name*, *Address*, *Password*}∪ *Trust*={*Trust*(*Target1*, *Attacker2*)}∪ *Attack goal*={*Money*}

C. ATTACK GRAPH OF SED

As shown in the SED framework, each SED is a complete attack including attack preparation, attack implementation and attack gain. Therefore, a SED can be also defined as an attack graph. In addition, it is convenient to analyze each SED in detail for a separate SED attack graph.

Most of the SED attack graph node representations are common to the SES. Only three unfolded nodes are specifically shown in the SED attack graph. One is a resource state node that includes the information of the medium, techniques, and compliance principles. The others are two unfolded action nodes, *SL* and *IA&RE*. When the participants, toolkit, and scenario are prepared, the scenario launch process starts. This action deploys the use of one or more mediums, the adoption of one or more techniques, and the application of one or more compliance principles. The three resources guide the next two implementation actions, including the identification authentication and relationship exploitation in a SED. Finally, one or more objectives are obtained through the scenario launch, identification authentication, and relationship exploitation. Three types of objectives are the physical object, information, and trust, which are in accordance with their description in a SES. To provide a concise expression, a SED in a SES is presented as $SED[SL(Medium, Techniques, Principles), IA\&RE(P_1, P_2)]$. P_1, and P_2 represent the two participants in a SED. For example, a SED can be defined as *SED*[*SL*(*Telephone*, *Pretexting*, *Authority*), *IA&RE*(*Attacker*, *Target*)] in a SES.

SES and SED attack graphs provide formally graphical definitions for the proposed SES and SED framework. The two attack graphs can show social engineering attacks more briefly. In the next section, we will analyze some attack cases using the proposed framework and attack graph.

V. SOCIAL ENGINEERING ATTACKS CASE STUDY

In this section, we analyze three typical social engineering attack cases in real-world scenarios using the proposed method. The three cases include one phone scam case, one email phishing scheme, and one watering hole attack case. Some cases are complete social engineering attacks and some others are the combination of traditional cyber-attacks and social engineering attacks. Due to the space constraints, we use different diagrams to illustrate different examples.

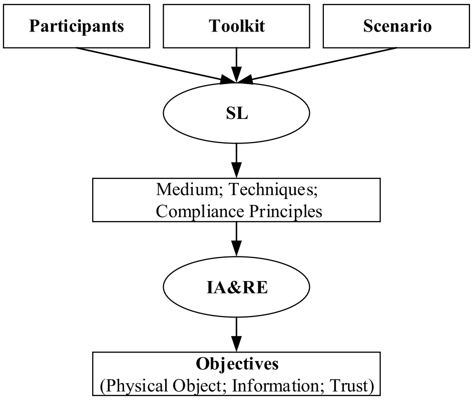
Participants
Toolkit
Scenario
SL
Medium; Techniques; Compliance Principles
IA&RE
Objectives
(Physical Object; Information; Trust)

FIGURE 4. Attack graph of SED.

A. CASE 1: A PHONE SCAM ATTACK

The case of Yuyu Xu is an infamous phone scam event, which has promoted the modernization of the rule of law in China. On August 21, 2016, Yuyu Xu, a preparatory college student, died of a sudden cardiac arrest after being defrauded of ¥9,900 (around $1,468.3) by a phone scam. This was a typical social engineering attack. It took advantage of the loopholes in human nature and the system, combined a traditional cyber-attack and social engineering attacks, and achieved the purpose of illegally obtaining another person's money. The attack process is shown as follows.

➢ Step 1: An attacker, Du, hacked the College Entrance Examination Online Registration Information System of Shandong Province in 2016 and implanted a Trojan horse virus. He illegally stole a large amount of personal information from senior high school graduates through the virus. Then, he sold all of this personal information for money.

➢ Step 2: An attacker, Chen, purchased the personal information of 1,800 senior high school graduates from Du at a price of ¥0.5 (around $0.07) for each piece. Chen planned to use the information for a phone scam. He formed a criminal organization and then started committing phone scam attacks. The criminals used the senior high school list to randomly choose victims. They devised a scenario to provide fake grants for the graduates to deceive them.

➢ Step 3: First, a member of the criminal organization called Yuyu Xu and told the student he was an education officer. The attacker told Xu the name of her school and her parents' names. He also told Xu about the amount of her student grant (¥2680, around $397.5). The attacker told Xu that if she wanted to receive it, she needed to contact the staff of a certain financial bureau now

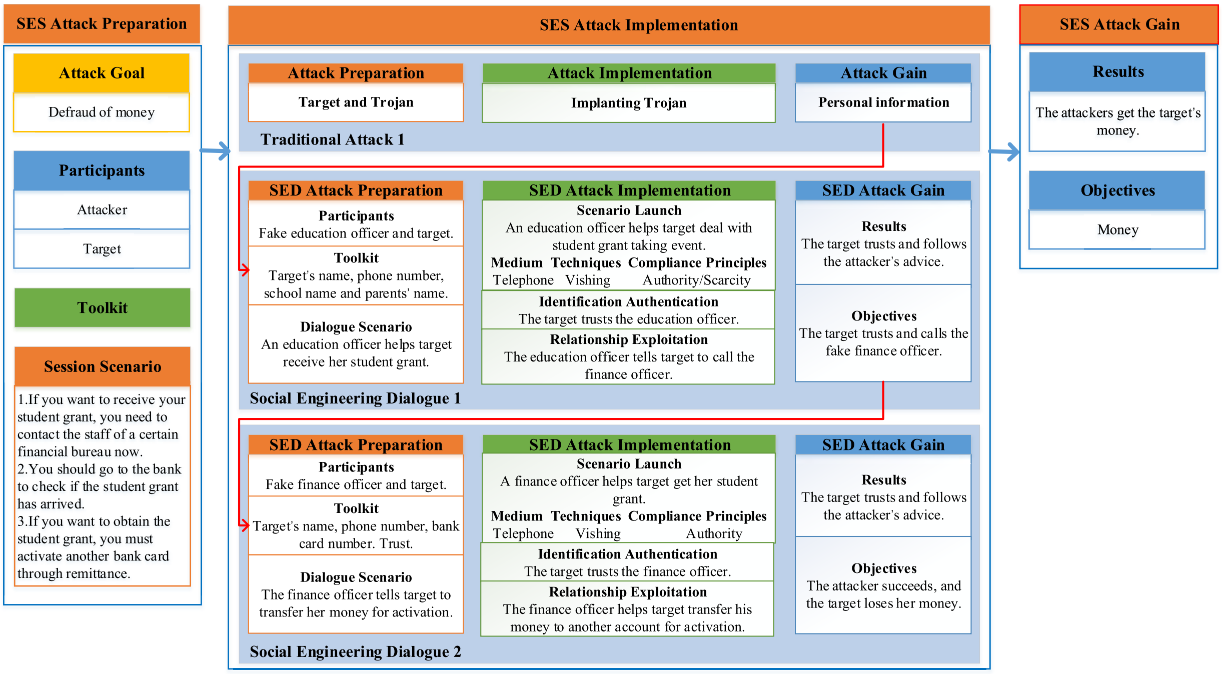
SES Attack Preparation
Attack Goal
Defraud of money
Participants
Attacker
Target
Toolkit
Session Scenario
1.If you want to receive your student grant, you need to contact the staff of a certain financial bureau now.
2.You should go to the bank to check if the student grant has arrived.
3.If you want to obtain the student grant, you must activate another bank card through remittance.
SES Attack Implementation
Attack Preparation
Target and Trojan
Attack Implementation
Implanting Trojan
Attack Gain
Personal information
Traditional Attack 1
SED Attack Preparation
Participants
Fake education officer and target.
Toolkit
Target's name, phone number, school name and parents' name.
Dialogue Scenario
An education officer helps target receive her student grant.
SED Attack Implementation
Scenario Launch
An education officer helps target deal with student grant taking event.
Medium Techniques Compliance Principles
Telephone Vishing Authority/Scarcity
Identification Authentication
The target trusts the education officer.
Relationship Exploitation
The education officer tells target to call the finance officer.
SED Attack Gain
Results
The target trusts and follows the attacker's advice.
Objectives
The target trusts and calls the fake finance officer.
Social Engineering Dialogue 1
SED Attack Preparation
Participants
Fake finance officer and target.
Toolkit
Target's name, phone number, bank card number. Trust.
Dialogue Scenario
The finance officer tells target to transfer her money for activation.
SED Attack Implementation
Scenario Launch
A finance officer helps target get her student grant.
Medium Techniques Compliance Principles
Telephone Vishing Authority
Identification Authentication
The target trusts the finance officer.
Relationship Exploitation
The finance officer helps target transfer his money to another account for activation.
SED Attack Gain
Results
The target trusts and follows the attacker's advice.
Objectives
The attacker succeeds, and the target loses her money.
Social Engineering Dialogue 2
SES Attack Gain
Results
The attackers get the target's money.
Objectives
Money

FIGURE 5. SES framework of Xu's case.

because today was the last day to obtain the money. He then confirmed Xu's phone number. Xu was a student in a poor family, and she did apply for a grant from the Education Bureau, so she believed the attacker.

➢ Step 4: Xu dialed the telephone number given by the first attacker. The person answering the telephone was another attacker in the criminal organization acting as a finance officer. The attacker asked Xu to go to the bank to check if the student grant had arrived. After Xu went to a nearby bank, the attacker told Xu that if she wanted to obtain the student grant, she must activate another bank card through remittance. Xu followed the attacker's demands to obtain the student grant because of her particularly urgent need. She took out all of her tuition fee of ¥9,900 and then deposited it all in the bank account sent by the attacker for activation. While she was anxiously waiting for the remittance (in the rain), the third member in the criminal organization withdrew all of her money in another province.

The case is a typical phone scam case combining a traditional cyber-attack and social engineering attacks. In this case, we regard all the four steps as a whole social engineering attack. Figure 5 and Figure 6 show the detail analyses using the proposed SES framework and attack graph. In Figure 5, the whole phone scam is broken in three parts which are SES attack preparation, SES attack implementation and SES attack gain according to the proposed framework. In the attack preparation stage, the attack goal is to defraud of money. All the participants in the whole attack includes several attackers and some senior high school graduates. In this case, the target is Yuyu Xu. According to the characteristics of the target group, the attackers design three steps session scenarios in order to achieve the final attack goal. After all the preparation works, the attackers start attack implementation. First, a traditional attack is launched for the purpose of acquiring personal information. Second, a SED starts using the personal information. The attacker uses a medium of telephone, a technique of vishing and two compliance principles of authority and scarcity. The pretending position of education officer makes the target believe that it's official. The words, ''today is the last day'', increase urgency of this event. These all exploit human's weakness for believing in authority and pursuing scarcity. The objective of this SED is

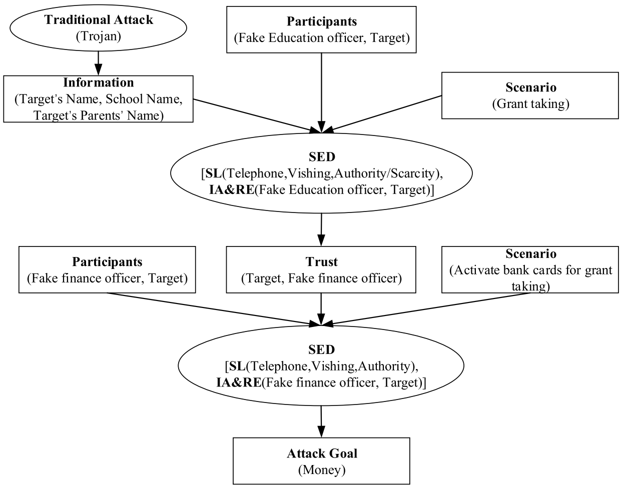
Traditional Attack
(Trojan)
Participants
(Fake Education officer, Target)
Information
(Target's Name, School Name, Target's Parents' Name)
Scenario
(Grant taking)
SED
[SL(Telephone,Vishing,Authority/Scarcity),
IA&RE(Fake Education officer, Target)]
Participants
(Fake finance officer, Target)
Trust
(Target, Fake finance officer)
Scenario
(Activate bank cards for grant taking)
SED
[SL(Telephone,Vishing,Authority),
IA&RE(Fake finance officer, Target)]
Attack Goal
(Money)

FIGURE 6. SES attack graph of Xu's case.

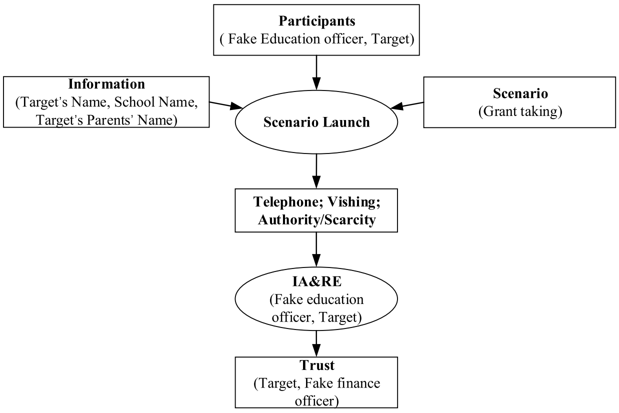
Participants
(Fake Education officer, Target)
Information
(Target's Name, School Name, Target's Parents' Name)
Scenario
(Grant taking)
Scenario Launch
Telephone; Vishing; Authority/Scarcity
IA&RE
(Fake education officer, Target)
Trust
(Target, Fake finance officer)

FIGURE 7. The first SED attack graph of Xu's case.

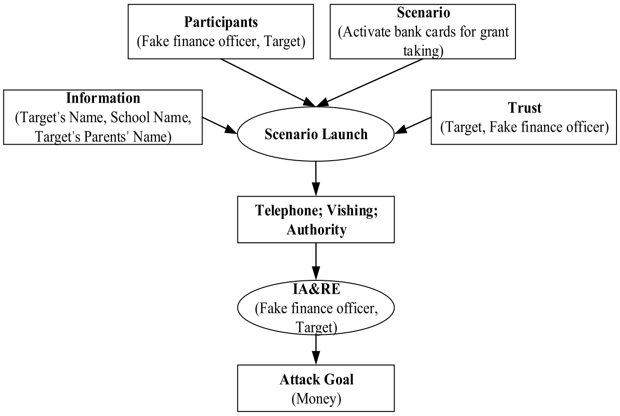
Participants
(Fake finance officer, Target)
Scenario
(Activate bank cards for grant taking)
Information
(Target's Name, School Name, Target's Parents' Name)
Trust
(Target, Fake finance officer)
Scenario Launch
Telephone; Vishing; Authority
IA&RE
(Fake finance officer, Target)
Attack Goal
(Money)

FIGURE 8. The second SED attack graph of Xu's case.

gaining trust for the attacker in the next SED. Finally, another SED is implemented involving trust from the first SED. The attackers achieve the attack goal and acquire target's money.

Figure 6 illustrates the case of Xu with the proposed SES attack graph. The attack graph involves five types of resource nodes S, which are participants, scenario, information, trust and attack goal. One traditional attack action and two SED actions are presented as three action nodes A. In order to show the operation of a separate SED attack graph, Figure 7 and Figure 8 present two detailed SED attack graphs. The SES and SED attack graphs describe the whole SE attack involving all of the elements in the attack, which is more streamlined and concise than the proposed framework.

B. CASE 2: A PHISHING ATTACK

Phishing is a harmful social engineering technique that the threat actors use to find a chance to gain access to critical information systems. A common approach in phishing is through the use of email communication with an embedded hyperlink [14]. In the presented case, the social engineer steals the target's money through a phishing email and a phishing website. First, the attacker sends a phishing email to the target. In this email, the attacker pretexting as a bank officer tells the target that his bank card is frozen and it is needed to validate his identification for the use of his bank card. A URL is embedded in this email for the target's click. Then, if the target trusts this phishing email, he will click the URL and enter a phishing website. When the target inputs his bank card password, the attacker will quickly withdraw the target's money.

A typical email phishing scheme is analyzed using both the proposed SES framework and SES attack graph. Figure 9 and Figure 10 show the detailed framework and attack graph. As shown in the framework, there are two SEDs in this phishing attack. The first SED is when the attacker sends a phishing email to the target. A relationship is established

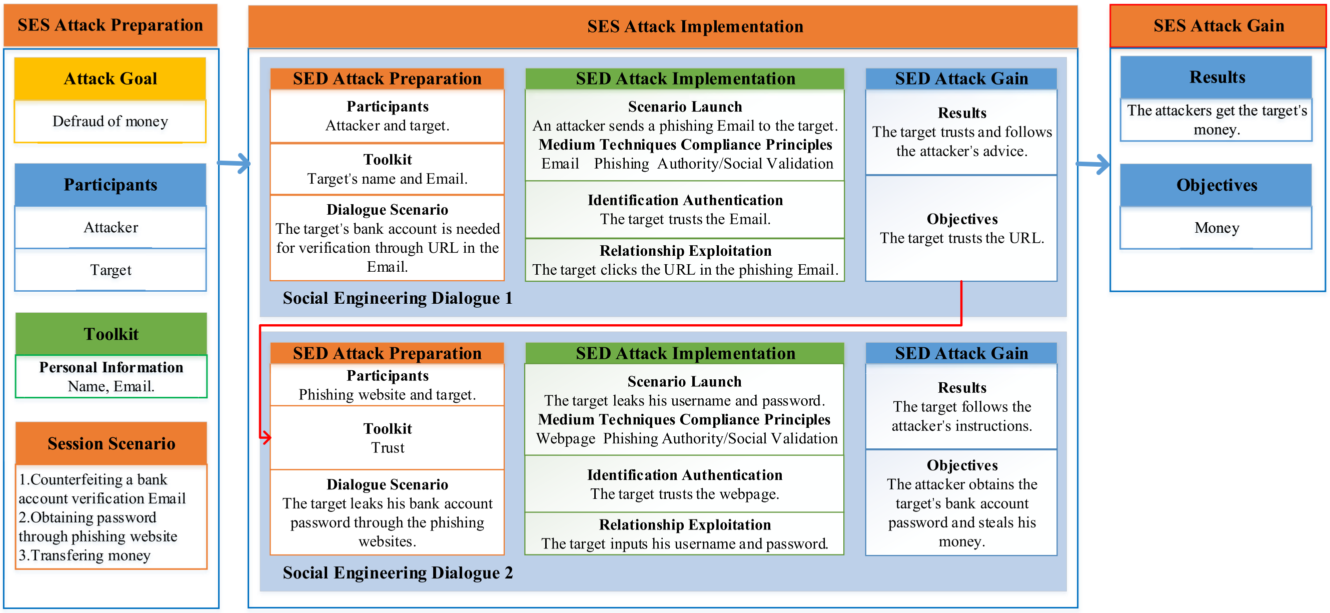
SES Attack Preparation
Attack Goal
Defraud of money
Participants
Attacker
Target
Toolkit
Personal Information
Name, Email.
Session Scenario
1.Counterfeiting a bank account verification Email
2.Obtaining password through phishing website
3.Transfering money
SES Attack Implementation
SED Attack Preparation
Participants
Attacker and target.
Toolkit
Target's name and Email.
Dialogue Scenario
The target's bank account is needed for verification through URL in the Email.
SED Attack Implementation
Scenario Launch
An attacker sends a phishing Email to the target.
Medium Techniques Compliance Principles
Email Phishing Authority/Social Validation
Identification Authentication
The target trusts the Email.
Relationship Exploitation
The target clicks the URL in the phishing Email.
SED Attack Gain
Results
The target trusts and follows the attacker's advice.
Objectives
The target trusts the URL.
Social Engineering Dialogue 1
SED Attack Preparation
Participants
Phishing website and target.
Toolkit
Trust
Dialogue Scenario
The target leaks his bank account password through the phishing websites.
SED Attack Implementation
Scenario Launch
The target leaks his username and password.
Medium Techniques Compliance Principles
Webpage Phishing Authority/Social Validation
Identification Authentication
The target trusts the webpage.
Relationship Exploitation
The target inputs his username and password.
SED Attack Gain
Results
The target follows the attacker's instructions.
Objectives
The attacker obtains the target's bank account password and steals his money.
Social Engineering Dialogue 2
SES Attack Gain
Results
The attackers get the target's money.
Objectives
Money

FIGURE 9. SES framework of email phishing scheme.

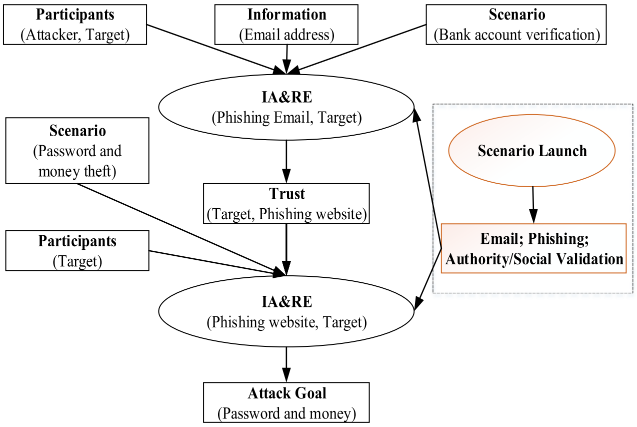

FIGURE 10. SES attack graph of email phishing scheme.

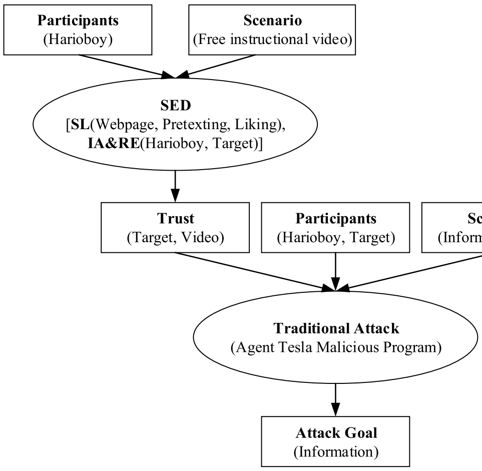

FIGURE 11. SES attack graph of watering hole case.

when the target reads this phishing email and trusts it. The objective of the first SED is gaining the trust of the embedded hyperlink. The second SED starts when the target clicks the URL. The objectives of the second SED are obtaining the password and stealing the target's money.

Figure 10 shows this phishing case with the unfolded SES attack graph. The SEDs in this SES are guided by the same medium, technique, and compliance principles, which are telephone, vishing, and authority/social validation. Generally, the phishing email and phishing webpage are often pretended as some official template. Most people would like to believe an email or a webpage with a famous head. The trust will be reinforced if they have seen similar templates. These are part of human cognitive weaknesses. It is these weaknesses that make such phishing attacks success.

C. CASE 3: A WATERING HOLE ATTACK

A watering hole attack is a seemingly simple, but highly successful, social engineering attack. Targets are mostly specific groups, such as organizations, industries, and regions. Attackers first identify the websites that the target often visits, and then invade one or more websites and plant malwares. A hacker (or hacker organization) whose network ID is Harioboy attacked hundreds of thousands of personal machines using a watering hole attack to control the targets' computers. The attack steps were as follows.

Harioboy deployed a malicious code-embedded hacker tool (a free RC7 Cracked and Discord cracking tool) and put instructional videos on video websites (such as YouTube) to teach users how to crack RC7 and Discord. Some gamers, hackers, or crackers found the videos and the tool through search engines. They downloaded and ran the tool on their computers using the instructions from the videos. Once the hacker tool ran on the victim's computer, it executed Harioboy's pre-embedded malicious code and downloaded Harioboy's custom Trojan horse. Hackers then used the Trojan horse to monitor and control the victims' computers, and even steal sensitive information, such as victims' bank accounts, game accounts, and Bitcoin.

Figure 11 and Figure 12 shows the attack process using the proposed SES framework and attack graph. The two figures show that this attack does not require personal

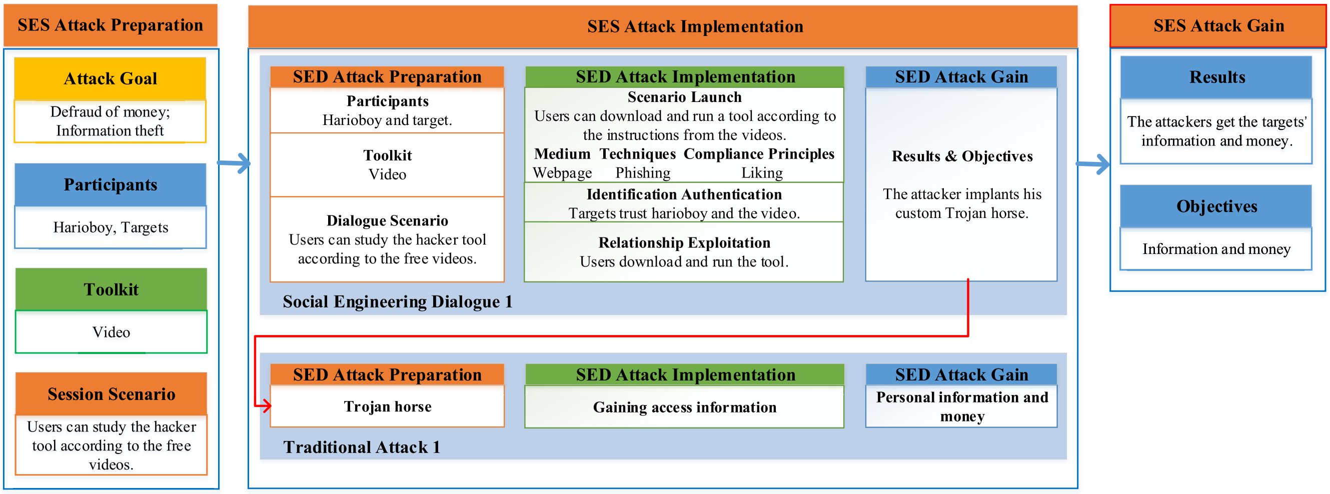
SES Attack Preparation
Attack Goal
Defraud of money; Information theft
Participants
Harioboy, Targets
Toolkit
Video
Session Scenario
Users can study the hacker tool according to the free videos.
SES Attack Implementation
SED Attack Preparation
Participants
Harioboy and target.
Toolkit
Video
Dialogue Scenario
Users can study the hacker tool according to the free videos.
SED Attack Implementation
Scenario Launch
Users can download and run a tool according to the instructions from the videos.
Medium Techniques Compliance Principles
Webpage Phishing Liking
Identification Authentication
Targets trust harioboy and the video.
Relationship Exploitation
Users download and run the tool.
SED Attack Gain
Results & Objectives
The attacker implants his custom Trojan horse.
Social Engineering Dialogue 1
SED Attack Preparation
Trojan horse
SED Attack Implementation
Gaining access information
SED Attack Gain
Personal information and money
Traditional Attack 1
SES Attack Gain
Results
The attackers get the targets' information and money.
Objectives
Information and money

FIGURE 12. SES framework of watering hole case.

information, which is different from the previous cases. This lack of required personal data is a characteristic of the watering hole attack. Another difference is the compliance principle used in this attack (Liking). The attacker takes full advantage of the target group's preferences. The purpose of the first SED is gaining the target's trust in the video and luring the target to run the malicious code. The SED attack establishes a basis for the next traditional attack. This case illustrates the many possibilities of a combination of traditional cyber-attacks and SE attacks. In a complete SE attack, not only do traditional cyber-attacks provide information for SE attacks, but the SE attacks can lay a foundation for traditional cyber-attacks.

Three typical types of social engineering attacks (phone scam, email phishing and watering hole) are described smoothly using the proposed framework and attack graph. The analyses of three typical social engineering attack cases clearly demonstrate phased achievements and the correlation between each phases in the whole social engineering attacks. All the analyses figures clearly show the establishment of trust and acquirement of physical objects and information. The frameworks and attack graphs will help to break the chain of trust established during social engineering attack, thereby enabling social engineering defenses.

VI. CONCLUSIONS

Due to the serious threat posed by social engineering attacks, a proper understanding of these attacks is critical to develop efficient countermeasures. In this paper, a new social engineering framework is proposed that uses the concept of session and dialogue. A social engineering session (SES) and a social engineering dialogue (SED) are described in this paper. A whole social engineering attack can be regarded as a SES. Each phase in a social engineering attack is depicted as a SED. A SES contains several SEDs that are well-organized and closely connected. Each SED can achieve one or more objectives and provide useful material for the next SED. To formalize the proposed SE framework, we define formal representations for the proposed SES and SED using the attack graph. Finally, three real-world social engineering attack cases are discussed using the proposed framework and attack graph. The proposed framework clearly describes all the components and the attack process of a social engineering attack, which provides a theoretical basis for social engineering defense. Based on our proposed framework, a social engineering attack threat assessment and detection model in a real network environment will be considered in our planned future work.

The social engineering attacks in the cyber age have evolved from simple scams to systematical and sophisticated attacks. Today's social engineering attacks spread rapidly involving with networks and social medium. Social engineering attacks are becoming more diverse. The implementation of social engineering attacks are more automated. The target and objective of social engineering attacks are more precise. The defense of social engineering attacks is based on a comprehensive understanding of the operation mechanism of social engineering attacks. Social engineering defense is not unilateral. It should strengthen the technical defense method with improvement of people's security awareness.

REFERENCES

[1] M. Bidgoli and J. Grossklags, "'Hello. This is the IRS calling.': A case study on scams, extortion, impersonation, and phone spoofing," in *Proc. IEEE APWG Symp. Electron. Crime Res. (eCrime)*, Scottsdale, AZ, USA, Apr. 2017, pp. 57–69.

[2] R. Borsack and M. Lifson. The truth about social media identity theft: Perception versus reality. Business Wire, Accessed: Jun. 21, 2010. [Online]. Available: https://www.businesswire.com/news/home/20100621005370/en/Truth-Social-Media-Identity-Theft-Perception-Reality

[3] (2018). *2017 Internet Crime Report*. [Online]. Available: https://pdf.ic3.gov/2017_IC3Report.pdf

[4] (2019). *The 2018 Internet Fraud Trends Research Report*. [Online]. Available: http://zt.360.cn/1101061855.php?dtid=1101062366&did=610070297

[5] K. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN, USA: Wiley, 2002.

[6] F. Mouton, L. Leenen, M. Mercia Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *Proc. IFIP Int. Conf. Hum. Choice Comput.* Berlin, Germany: Springer, 2014, pp. 266–279.

[7] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, Mar. 2018.

[8] F. Mouton, A. Nottingham, L. Leenen, and H. S. Venter, "Underlying finite state machine for the social engineering attack detection model," in *Proc. IEEE Inf. Secur. South Africa (ISSA)*, Johannesburg, South Africa, Aug. 2017, pp. 98–105.

[9] F. Mouton, M. Teixeira, and T. Meyer, "Benchmarking a mobile implementation of the social engineering prevention training tool," in *Proc. IEEE Inf. Secur. South Africa (ISSA)*, Johannesburg, South Africa, Aug. 2017, pp. 106–116.

[10] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, Jun. 2016.

[11] F. Mouton, M. M. Malan, and H. S. Venter, "Development of cognitive functioning psychological measures for the SEADM," in *Proc. Int. Symp. Hum. Aspects Inf. Secur. Assurance (HAISA)*, Crete, Greece, Jun. 2012, pp. 40–51.

[12] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack detection model: SEADMv2," in *Proc. IEEE Int. Conf. Cyberworlds (CW)*, Visby, Sweden, Oct. 2015, pp. 216–223.

[13] F. Mouton, M. Mercia Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *Proc. IEEE Inf. Secur. South Africa (ISSA)*, Johannesburg, South Africa, Aug. 2014, pp. 1–9.

[14] T. Chin, K. Xiong, and C. Hu, "Phishlimiter: A phishing detection and mitigation approach using software-defined networking," *IEEE Access*, vol. 6, pp. 42516–42531, Jun. 2018.

[15] D. I. Sriendra and K. Y. Abeywardena, "The use of subliminal and supraliminal messages in phishing and spear phishing based social engineering attacks; feasibility study," in *Proc. 13th Int. Conf. Comput. Sci. Educ. (ICCSE)*, Colombo, Sri Lanka, Aug. 2018, pp. 1–5.

[16] W. Fan, K. Lwakatare, and R. Rong, "Social engineering: I-E based model of human weakness for attack and defense investigations," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 1, pp. 1–11, Jan. 2017.

[17] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," *Comput. Secur.*, vol. 76, pp. 101–127, Jul. 2018.

[18] R. H. Loukas and D. Gan, "An eye for deception: A case study in utilising the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks," in *Proc. IEEE 15th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, London, U.K., Jun. 2017, pp. 371–378.

[19] B. Opazo, D. Whitteker, and C.-C. Shing, "Email trouble: Secrets of spoofing, the dangers of social engineering, and how we can help," in *Proc. 13th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Guilin, China, Jul. 2017, pp. 2812–2817.

[20] S. Sabouni, A. Cullen, and L. Armitage, "A preliminary radicalisation framework based on social engineering techniques," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment (Cyber SA)*, London, U.K., Jun. 2017, pp. 1–5.

[21] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social engineering and insider threats," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Nanjing, China, Oct. 2017, pp. 25–34.

[22] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analysing online social engineering attack surfaces," *Comput. Secur.*, vol. 69, pp. 18–34, Aug. 2017.

[23] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, "Mind your SMSes: Mitigating social engineering in second factor authentication," *Comput. Secur.*, vol. 65, pp. 14–28, Mar. 2017.

[24] K. Y. Abeywardana, E. Pfluegel, and J. M. Tunnicliffe, "A layered defense mechanism for a social engineering aware perimeter," in *Proc. SAI Comput. Conf. (SAI)*, London, U.K., Jul. 2016, pp. 1054–1062.

[25] M. Masoud, Y. Jaradat, and Q. A. Ahmad, "On tackling social engineering web phishing attacks utilizing software defined networks (SDN) approach," in *Proc. 2nd Int. Conf. Open Source Softw. Comput. (OSSCOM)*, Beirut, Lebanon, Dec. 2017, pp. 1–6.

[26] K. Beckers and S. Pape, "A serious game for eliciting social engineering security requirements," in *Proc. IEEE 24th Int. Requirements Eng. Conf. (RE)*, Beijing, China, Sep. 2016, pp. 16–25.

[27] R. Heartfield, G. Loukas, and D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access*, vol. 4, pp. 6910–6928, 2016.

[28] Y. Sawa, R. Bhakta, G. Ian Harris, and C. Hadnagy, "Detection of social engineering attacks through natural language processing of conversations," in *Proc. IEEE 10th Int. Conf. Semantic Comput. (ICSC)*, Laguna Hills, CA, USA, Feb. 2016, pp. 262–265.

[29] H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," in *Proc. IEEE 11th Conf. Ind. Electron. Appl. (ICIEA)*, Hefei, China, Jun. 2016, pp. 1039–1044.

[30] T. Bakhshi, "Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors," in *Proc. 13th Int. Conf. Emerg. Technol. (ICET)*, Islamabad, Pakistan, Dec. 2017, pp. 1–6.

[31] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Noida, India, Apr. 2016, pp. 537–540.

[32] A. Algarni, Y. Xu, and T. Chan, "Measuring source credibility of social engineering attackers on Facebook," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Koloa, HI, USA, Jan. 2016, pp. 3686–3695.

[33] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Vienna, Austria, Aug. 2016, pp. 145–149.

[34] W. R. Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," *Comput. Secur.*, vol. 59, pp. 26–44, Jun. 2016.

[35] A. Algarni and Y. Xu, "Social engineering in social networking sites: Phase-based and source-based models," *Int. J. e-Educ., e-Business, e-Manage e-Learn.*, vol. 3, no. 6, pp. 456–462, Jan. 2013.

[36] M. Nohlberg and S. Kowalski, "The cycle of deception: A model of social engineering attacks, defenses and victims," in *Proc. 2nd Int. Symp. Hum. Aspects Inf. Secur. Assurance (HAISA)*, Plymouth, U.K., Jul. 2008, pp. 1–11.

[37] A. Cullen and L. Armitage, "The social engineering attack spiral (SEAS)," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Secur.)*, London, U.K., Jun. 2016, pp. 1–6.

[38] L. J. Janczewski and L. Fu, "Social engineering-based attacks-model and New Zealand perspective," in *Proc. Int. Multiconf. Comput. Sci. Inf. Technol.*, Wisla, Poland, Oct. 2010, pp. 847–853.

[39] P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behaviour Inf. Technol.*, vol. 32, no. 10, pp. 1014–1023, Oct. 2013.

[40] J. J. Gonzalez, J. M. Sarriegi, and A. Gurrutxaga, "A framework for conceptualizing social engineering attacks," in *Proc. CRITISs 1st Int. Conf. Crit. Inf. Infrastructures Secur.*, Samos, Greece, Aug. 2006, pp. 79–90.

[41] P. Cynthia and S. L. Painton, "A graph-based system for network-vulnerability analysis," in *Proc. Workshop Secur. Paradigms (NSPW)*, Charlottesville, VA, USA, Sep. 1998, pp. 71–79.

[42] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Proc. 15th IEEE Comput. Secur. Found. Workshop*, Cape Breton, NS, Canada, Jun. 2002, pp. 49–63.

[43] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2002, pp. 273–284.

[44] O. M. Sheyner, "Scenario graphs and attack graphs," Ph.D. dissertation, School Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, USA, 2004.

[45] S. NoelSushil and J. Jajodia, "Managing attack graph complexity through visual hierarchical aggregation," in *Proc. ACM Workshop Vis. Data Mining Comput. Secur.*, Washington, DC, USA, Oct. 2004, pp. 109–118.

[46] K. Beckers, L. Krautsevich, and A. Yautsiukhin, "Analysis of social engineering threats with attack graphs," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Cham, Switzerland: Springer, 2015, pp. 216–232.

KANGFENG ZHENG received the Ph.D. degree in information and signal processing from the Beijing University of Posts and Telecommunications, in 2006, where he is currently an Associate Professor with the School of Cyberspace Security. His research interests include networking and system security, network information processing, and network coding.

TONG WU is currently pursuing the Ph.D. degree with the Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. She has participated in one of the National Key Research and Development Programs of China and one of the National Natural Science Foundation of China Programs. Her research interests include information security, social engineering, biometrics, and pattern recognition techniques.

XIUJUAN WANG received the Ph.D. degree in information and signal processing from the Beijing University of Posts and Telecommunications, in 2006. She is currently an Instructor Lecturer with the Faculty of Information Technology, Beijing University of Technology. Her research interests include information and signal processing, network security, and network coding.

BIN WU received the Ph.D. degree in information and signal processing from the Beijing University of Posts and Telecommunications, in 2008, where he is currently an Instructor Lecturer with the Information Security Center, School of Cyberspace Security. His research interests include network security, intrusion detection, social engineering, and artificial intelligence security.

CHUNHUA WU received the Ph.D. degree in information and signal processing from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008, where she is currently an Assistant Professor with the Information Security Center, School of Cyberspace Security. She is in charge of one of the National Natural Science Foundation of China Projects. Her current research interests include machine learning, attack detection, malware detection, and identity authentication.