Modelling based approach for reconstructing evidence of VoIP malicious attacks

Ibrahim, M and Dehghantanha, A

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 324-340
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

Modelling Based Approach for Reconstructing Evidence of VoIP Malicious Attacks

Mohammed Ibrahim, Mohd Taufik Abdullah and Ali Dehghantanha
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia
m.ibrahim47@yahoo.com, {mtaufik, alid}@fsktm.upm.edu.my

ABSTRACT

Voice over Internet Protocol (VoIP) is a new communication technology that uses internet protocol in providing phone services. VoIP provides various forms of benefits such as low monthly fee and cheaper rate in terms of long distance and international calls. However, VoIP is accompanied with novel security threats. Criminals often take advantages of such security threats and commit illicit activities. These activities require digital forensic experts to acquire, analyses, reconstruct and provide digital evidence. Meanwhile, there are various methodologies and models proposed in detecting, analysing and providing digital evidence in VoIP forensic. However, at the time of writing this paper, there is no model formalized for the reconstruction of VoIP malicious attacks. Reconstruction of attack scenario is an important technique in exposing the unknown criminal acts. Hence, this paper will strive in addressing that gap. We propose a model for reconstructing VoIP malicious attacks. To achieve that, a formal logic approach called Secure Temporal Logic of Action(S-TLA$^+$) was adopted in rebuilding the attack scenario. The expected result of this model is to generate additional related evidences and their consistency with the existing evidences can be determined by means of S-TLA$^+$ model checker.

KEYWORDS

Voice over IP, S-TLA$^+$, Reconstruction, malicious attack, Investigation, SIP, Evidence Generation, attack scenario

1 INTRODUCTION

Voice-over Internet Protocols (VoIP) phone services are prevalent in modern telecommunication settings and demonstrate a potentiality to be the next-generation telephone system. This novel telecommunication system provides a set of platform that varied from the subjected and closed environment offered by conventional public switch network telephone (PSTN) service providers [1]. The exploitation of VoIP applications has drastically changed the universal communication patterns by dynamically combining video and audio (Voice) data to traverse together with the usual data packets within a network system [2]. The advantages of using VoIP services incorporated with cheaper call costs for long distance, local and international calls. Users make telephone calls with soft phones or IP phones (such as Skype) and send instant messages to their friends or loved ones via their computer systems [3].

The development of VoIP has brought a significant amount of benefits and satisfactory services to its subscribers [2]. However, VoIP services are exposed to various security threats derived from the Internet Protocol (IP) [4]. Threats related to this new technology are denial of service,

host and protocol vulnerability exploits, surveillance of calls, hijacking of calls, identity theft of users, eavesdropping and the insertion, deletion and modification of audio streams [5]. Criminals take advantage of such security threats and commit illicit activities such as VoIP malicious attacks. This requires acquisitions, analysing and reconstruction of digital evidence. However, detecting and analysing evidence of attacks related to converged network application is the most complicated task. Moreover, the complex settings of its service infrastructure such as DHCP servers, AAA server, routers, SIP registrar, SIP proxies, DNS server, and wireless and wired network devices also complicate the process of analysing digital evidence. As a result, reconstructing the root cause of the incident or crime scenario would be difficult without a specific model guiding the process.

1.1 Related Work

In recent times, researchers have developed new models to assist forensic analysis by providing comprehensive methodologies and sound proving techniques.

Palmer [6] first proposed a framework with the following steps: identification, preservation, collection, examination, analysis, presentation as well as decision steps. The framework was presented at the proceeding of the first Digital Forensic Workshop (DFRW) and served as the first attempt to apply forensic science into network system. The framework was later cobble together and produced an abstract digital forensic model with the addition of preparation and approach strategy phases; the decision phase was replaced by returning evidence. However, the model works independently on system technology or digital crime [7].

Similarly, the work of Mandila and Procise developed simple and accurate methodology in incident response. At the initial response phase of the methodology, it is aimed at determining the incident, and strategy response phase is formulated and added [8]. On the other hand, Casey and Palmer [9] proposed an investigative process model that ensures appropriate handling of evidence and decrease chances of mistakes through a comprehensive systematic investigation. Also in another paper, it was reported that Carrier and Spafford [10], has adopted the process of physical investigation and proposed an integrated digital forensic process. In another approach [11] combined existing models in digital forensic and comes up with an extended model for investigating cyber crime that represents the flow of information and executes full investigation. Baryamureeba and Tushabe reorganized different phases of the work of Carrier and Spafford and enhanced digital investigation process by adding two new phases (i.e. traceback and dynamite)[12] .

Other frameworks include the work of Bebee and Clark which is hierarchical and objective based for digital investigation process[22]. However, all the aforementioned models are applied to digital investigation in a generalized form. Meanwhile, Ren and Jin [14] were the first to introduce a general model for network forensic that involves the following steps: capture, copy, transfer, analysis, investigation and presentation. The authors in [15] after surveyed the existing models suggest a new generic model for network forensic built from the aforementioned models. This model consists of preparation, detection, collection, preservation, examination, analysis, investigation and presentation.

Furthermore, many authors proposed event reconstruction attacks models for instance Stephenson [16] analysed the root cause of digital incident and applied colored Petri Nets for modelling of occurred events. Gladyshev and Patel [17] developed event reconstruction in which potential attack scenarios are constructed based on finite state machine (FSM) and neglecting scenario that deviate from the available evidence. The author in [18] uses a computation model based on finite state machine together with computer history and came up with a model that supports the existing investigation. Rekhis and Boudriga proposed in [19], [20] and [21] a formal logic entitled Investigation-based Temporal Logic of Action (I-TLA) which can be used to proof the existence or non-existence of potential attack scenario for reconstruction and investigation of network malicious attacks. On the other hand, Pelaez and Fernandez [22] in an effort to analyse and reconstruct evidence of attacks in converged network, logs correlation and normalization techniques were proposed. However, such techniques are effective if the data in the file or forensic logs are not altered.

The existing models stated above are more of generic not specific to a particular kind of attacks. Therefore, the need for reconstructing the evidences of malicious attacks against VoIP is highly needed because it plays an important role in revealing the unknown attack scenario. As a result, the reliability and integrity of analysis of evidence in VoIP digital forensic would be improved and enhances its admissibility in the court of law. In view of that, the work in this paper is focused on reconstruction of Session Initiation Protocol (SIP) server malicious attacks. Hence, the VoIP evidence reconstruction model (VoIPERM) is proposed that categorized the previous model in [23] into main components and subcomponents. The model described VoIP system as a state machine through which information could be aggregated from various components of the system and formulates them into hypotheses that enable investigator model the attack scenario. Following the reconstruction of attack scenario, actions that contradict the desirable properties of the system state machine are considered to be malicious [23]. Consequently, the collection of both legitimate and malicious actions enables the reconstruction of attack scenario that will uncover new more evidence. To determine the consistency of additional evidences with respect to the existing evidence, a state space representation was adopted that depict the relationship between set of evidence using graphical representation. The graphical representation enables investigators understand if generated evidences can support the existing once. Hence, it reduces the accumulation of unnecessary data during the process of investigation [23]. Additionally, the model is capable of reconstructing actions executed during the attack that moves the system from the initial state to the unsafe state. Thus, all activities of the attacker are conceptualized to determine what, where and how such an attack occurred for proper analysis of evidence [23]. To handle ambiguities in the reconstruction of attack scenario, S-TLA$^+$ is to be applied. Essentially, the application of S-TLA$^+$ into computer security technology is efficient and generic. On the other hand, S-TLA$^+$ is built on the basis of logic formalism that accumulate forward hypotheses if there is deficient details to comprehend the compromised system [19].

In addition there were several works on malware investigation [24,25], analysis of cloud and virtualized environments [26-28], privacy issues that may arise during forensics investigation[29-34], mobile

device investigation [35-37] and greening digital forensics process [38].

The main contribution of this paper is to propose a novel model in VoIP digital forensic analysis that can integrate digital evidences from various components of VoIP system and reconstruct the attack scenario. Our objective is to reconstruct VoIP malicious attacks to generate more additional evidences from the existing evidence. The remaining of the paper is arranged as follows: next section discusses VoIP malicious attacks; 3 discuss VoIP digital forensic investigation, section 4 introduces the new model, section 5 discusses S-TLC model checker, section 6 case study and 7 conclusions.

2 VoIP MALICIOUS ATTACKS

In general, an appropriate term used related to software built purposely to negatively affect a computer system without the consent of the user is called a malware [39]. And the increased number of malicious activities during the last decade brought most of the failures in computer systems [40]. Nevertheless, Voice over IP is prone to those malware attacks by exploiting its related vulnerabilities. Having access to VoIP network devices, intruders can disrupt media service by flooding traffic, whip and control confidential information by illicit interception of call content or call signal. Through impersonating servers, intruders can hijack and make fake calls by spoofing identities [3]. Consequently, the confidentiality, integrity and availability of the users are negatively affected. Also VoIP services are utilized by spammers to deliver instant messages, spam calls, or presence information. However, these spam calls are more problematic than the usual email spam since they are hard to filter [3]. Similarly, attacks can transverse gateways to an integrated network system like traditional telephony and mobile system. Meanwhile, compromising VoIP applications composed a link to break out security mechanisms and attack internal networks [39]. Also, attackers make use of malformed SIP messages to attack embedded web servers through Database injection vectors or Cross Script attacks [39].

2.1 SIP Malicious Attack

As previously explained, this paper considers SIP Server attacks. Several attacks are related to SIP server, but the most concern threat within research community is VoIP spam. Generally, spam is an unwanted bulk email or call, deliberated to publicize social engineering. The author in [3] discusses that "Spam wastes network bandwidth and system resources. It exists in the form of instant message (IM), Voice and presence Spam within a VoIP setting" [3]. It affects the availability of network resources to legitimate users which can result to denial of service (DoS) attack. Spam originates from the collection of session initiation in an effort to set up a video or an audio communications session. If the users accepted, the attacker continues to transmit a message over the real-time media. This kind of spam refers to as classic telemarketer Spam and is applicable to SIP protocol and is well known as Spam over IP Telephone (SPIT). However, spam is categorized into instant Message (IM spam) and presence Spam (SPPP). The former is like email spam, but it is bulky and unwelcome set of instant messages encapsulated with the message that the attacker wishes to send. IM spam is delivered using SIP message request with bulky subject headers, or SIP message with text or HTML bodies. The latter, is like the former, but it is placed on presence request (that is, SIP subscribes requests) in an effort

to obtain the "white list" of users to transmit them an instant message or set off another kind of communication [3].

3 VoIP DIGITAL FORENSIC INVESTIGATION

Lin and Yen [41] define digital forensic science to preserve, identify, extract, record as well as interpret the computer and network system evidence and analyse through complete and perfect methods and procedures." On the other hand, forensic computing is particularly important interdisciplinary research area founded from computer science and drawing on telecommunications and network engineering, law, justice studies, and social science [42]. However, to convene with the security challenges various organizations developed numerous models and Methodologies that satisfy their organizational security policy. Presently, more than hundreds of digital forensic procedures developed globally [43]. Also the increase number of security challenges in VoIP persuades researcher to developed several models. On the other hand, in VoIP digital forensic a standard operating procedure called VoIP Digital Evidence Forensic Standard Operating Procedure (VoIP DEFSOP) is established [41].

Moreover, previous study noted that there was not established research agenda in digital forensic; to resolve that, six additional research areas were proposed at the 42nd Hawaii international conference, which include Evidence Modelling. In evidence modelling investigation procedure is replicated for practitioners and case modelling for various categories of crimes [44]. However, the increase number of crimes associated with computers over the last decade pushes product and company to support in understanding what, who, where and how such attack happened [45]. To fulfil this current development, in this paper the proposed model can support investigation and analysis of evidence by reconstructing attack scenario related to VoIP malicious attacks. Afterwards, the reconstruction of potential attack scenario will assist investigators to conceptualize what, where, and how does the attack happened in the VoIP system.

4 VoIP EVIDENCE RECONSTRUCTION MODEL (VoIPERM)

The idea proposed in [43] is to assist investigators in finding and tracing out the origin of attacks through the formulation of hypotheses. However, our proposed model considered VoIP system as a state machine (which observed the system properties in a given state) and the model is built up from four main components as shown below.

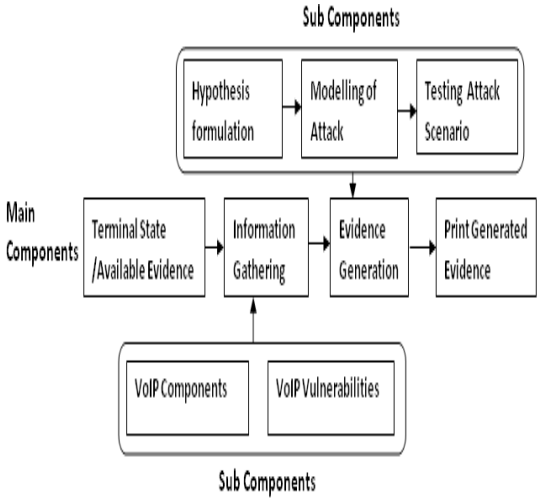

Figure 1. VoIP evidence reconstruction model

The explanation of each component is as follows:

4.1 Terminal State/Available Evidence

This component observes the final state of the system at the prevalence of the crime; it

is the primary source of evidence and is characterized by the undesirable system behavior. The terminal state provides available evidence and gives an inside about the kind of action acted upon on the compromised system [23]. Other properties of system compromise described by [21] include any of the following:

- Undesirable safety property of some system components
- Unexpected temporal property

Given $(s_0 \ldots s_f) \in S$ be the set of all reachable states in VoIP system and $D_p = \{p_1 \ldots p_n\}$be the collection of all desirable properties in a given state. If $\{\exists p \in s_f : p \notin Dp\}$ then the final state s_f of the system is said to be unsafe and can be represented as$\neg$ safe(s_f). For all actions $(A_0 \ldots A_f) \in A$ where A is the sequence of actions associated with each reachable state; then A_f is said to be a malicious action. So A_f is signifying one of the available evidence [23].

4.2 Information Gathering

This component is aimed to collect and gather information that gives details about VoIP system state. It requires the following subcomponents.

- *VoIP components*: these components provide services such as voice mail access, user interaction media control, protocol conversion, and call set up, and so on. The components can be proxy servers, call processing servers, media gateways and so on, depends on the type of protocol in use [23]. Moreover, software and hardware behaviours are observed to assist the investigator with some clue about VoIP system state. VoIP system states are defined as the valuation of component variables that change as a result of actions acted upon them. If$v_1 \ldots v_n$ are components variables that change by executing action in a given state. These variables are referred to as flexible variables given as $V_F = v_1 \cup v_2 \cup \ldots \cup v_n$and for any action A that transforms $v \rightarrow v'$. Where v and v' are respectively variables in old and new state X and Y . Then the properties of v and v' are observed to decide whether they belongs to the system desirable properties [23].
- *VoIP vulnerabilities*: These refer to any faults an adversary can abuse and commit a crime. Vulnerabilities make a system more prone to be attack by a threat or permit some degree of chances for an attack to be successful [46]. In VoIP systems, vulnerabilities include weaknesses of the operating systems and network infrastructures. Some weaknesses formed from poor in design and implementation security mechanism and Mis-configuration settings of network devices. VoIP protocol stack also associated with weaknesses that attacker exploits and access text based credentials and other private information.

4.3 Evidence Generation

In this component, hypotheses are formulated based on information gathered in the previous stage. The formulated hypotheses are used in the process of finding and generation of additional evidence. The formal logic of digital investigation is applied to consider available evidence collected from different sources and handle incompleteness in them by generating a series of crime scenario according to the formulated hypotheses. This stage involves the following subcomponents:

- *Hypothesis formulation*: To overcome the lack of system details encountered during the investigation, hypotheses are formulated based on intruder's anticipated knowledge about the

system and the details of information captured from VoIP components. The basis of hypothesis formulation is to predict the unknown VoIP malicious attack. In this case, there is a need to have specific variables attached to hypotheses and VoIP components respectively and make an assumption to establish a relationship between the variables. This determines what effect of such hypothesis if it is applied to VoIP components. To achieve this, three main requirements are set out:

- Hypotheses should establish a relationship between system states (that is, VoIP component states in this regard), to avoid violating the original properties (Type Invariant) of the system under investigation.
- All hypotheses found to be contradictory are eliminated to avoid adding deceptive hypotheses within a generated attack scenario.
- To efficiently select and minimize the number of hypotheses through which a node is reached, the relationship among the hypotheses should be clearly expressed [19].

Moreover, the process of investigation relied on the formulation of hypotheses to describe the occurrence of the crime. At the lowest levels of investigation, hypotheses are used to reconstruct events and to abstract data into files and complex storage types. While at higher levels of investigation, hypotheses are used to explain user actions and sequences of events [45]. An investigation is a process that applies scientific techniques to formulate and test hypotheses. At this point, VoIP variables are signifying as (indigenous Variable), while variables formed by hypotheses are denoted as (Exogenous Variable). Consequently, it describes how VoIP components are expected to behave if formulated hypotheses are executed. However, Assumptions are obviously made based on the expected knowledge of the attacker about the system. The sets of hypotheses are said to be variables signifying attacker's expected knowledge about the system which is different from the flexible variables V_F as has been mentioned. However, all the variables derived from hypothesis formulation are referred to as constrained variables denoted by $V_C = v_1 \cup v_2 \cup ... \cup v_n$. Meanwhile, while hypotheses are aggregated care should be taking to stay away from adding ambiguous hypothesis that can prevent the system from moving to the next state. In S-TLA$^+$ it is signifies inconsistency and denoted as $\perp$ [19]

- *Modelling of Attack scenario*: Digital forensic practices demands for the generation of temporal analysis that logically reconstruct the crime [26]. Also according to [47], in crime investigation it is likely to reason about crime scenarios: explanation of states and events that change those states that may have occurred in the real world. However, due to the complexity of understanding attack scenario, to handle them, it is vital to develop a model that simplifies their description and representation within a collection of information and set aside new attacks to be regenerated from the existing ones [19]. For this reason, it is essential to model VoIP malicious attacks to enable investigators understand the attack scenario and describes how and where to acquire digital evidence. In this regard, instead of modelling both the system and witness statement as a finite automata like in [40] an S-TLA$^+$ is used to model attack scenario as its

support logic formulation with uncertainty. In addition, evidences can easily be identified with S-TLA$^+$ using a state predicate that evaluates relevant system variables [19]. Moreover, S-TLA$^+$ is an advancement over a temporal logic of action (TLA). However, a system is signified in TLA by a formula of the form x: $Init \Lambda \Box[\mathbb{N}]_v \Lambda L$, relating the set of all its authorised behaviours. It expresses a system whose initial behaviour satisfies $init$ and where every state satisfies the next state relation $\mathbb{N}$, or leaves the tuple of specification variable unchanged. The infinite behaviour of the system is constrained by the Liveness property L(written as a conjunction of weak and strong fairness conditions of actions). In this regard, TLA can be used in S-TLA$^+$ to illustrate a system's progress from a state to another, in advance of the execution of an action under a given hypothesis [11].Meanwhile, in S-TLA$^+$ a constrained variable with hypothesis not yet express out, assumed a fictive value denoted as ∇ [19].

An action A is a collection of Boolean function true or false if $A(\forall v \in V_F : S(v)\ /v,\ t(v)/v') =$ true i.e. each unprimed variable v in the state s is replaced with prime variable v' in state t the action A become true [19].

$A(\forall v \in V_C : S(v)\ /v,\ t(v)/v'') =$ true i.e. each non-assumed constrained variable v in state s is replaced with assumed constrained variable v'' in state t. The action A becomes true, and if $\{\exists A_l \subseteq A: A_l(s,t) = true \wedge \exists\, p \in t: safe(t)\}$then the set of actions A_l is said to be legitimate actions. Likewise if $\{\exists A_m \subseteq A: A_m(s,t) = true \wedge \exists\, p \in t: \neg safe(t)\}$ then the set of actions A_m is said to be malicious actions, where p is the property satisfying the behaviour of t [23], Attack scenario fragment are the collection of both legitimate and malicious actions that move the system to an unsafe state. Thus, attack scenario denoted as α is defined $\alpha = A_m \cup A_l$[23]

- Testing Attack scenario**:** the purpose of testing generated attack scenario is to ascertain its reliability in respect to the system behaviours. The properties of the system at a given state is examined, the investigator should compare the properties of the generated attack scenario with the system final state. If any of the scenarios satisfied the properties of the final state, then the investigator should then generate and print digital evidence else the hypotheses should be reformulated [23]. Let $\alpha = \langle \alpha_0 \dots \alpha_f \rangle$ be the set of the generated attack scenario and $(s_0 \dots s_f) \in S$ be the set of VoIP system states. If $\{\exists p \in s: \neg safe(s)\}$ and $\{\exists \alpha_i \in \alpha: p \epsilon \alpha_i\}$ then α_i satisfied the properties of the system final state, where p is the property satisfying the behaviour of s and $s \in (s_0 \dots s_f)$ otherwise known as $EvidenceState$ [23].

4.4 Print Generated evidence

Evidences can be generated from attack scenario using forward and Backward chaining phases adopted from inferring scenarios with S-TLC [19]. However, the proposed model after being logically proof by the S-TLA$^+$, it is expected to reconstruct malicious attack scenario in the form of specifications that can be verified using S-TLA$^+$ model checker called S-TLC. S-TLC is a directed graph founded on the basis of state space representation that verifies the logical flow of specifications written in S-

TLA^+ formal language. Therefore, absolute reconstructions of attack scenario fragments are represented and the logical relationships between them are illustrated on a directed graph [23]. At this point, the investigator is likely to realize what, how, where and why such an incident was accomplished in the VoIP system. Also the resulting outcome of the graph is to generate new evidence that matches the existing evidence. For all generated attack scenarios $\alpha = \langle \alpha_0 \dots \alpha_f \rangle \exists s \in \alpha$ such that all the flexible variables $V_F \in s$ and constrained variable $V_C \in s$ are evaluated as s_n and s_c respectively, where $s_n$is the valuation of all non-constrained variables called a node core ands_c is the valuation of all constrained variables called node label. Then, each reachable state s can be represented on the directed graph G with their node core and node label as$\langle s_n, s_c \rangle$, respectively.

5 S-TLC MODEL CHECKER, STATE SPACE REPRESANTATION

A state can be represented on the generated graph as a valuation of all its variables including the constrained ones. It involves two notions:

- Node core: it represents the valuation of the entire non-constrained variables and
- Node label: is a valuation of the entire constrained variables under a given hypothesis.

Given a state t, t_n is used to denote its equivalent node core, t_c to describe its resulting environment (is a set of hypotheses) and Label (G, t) to refer to its label in graph G.

The S-TLC algorithm is built on three data structures G, U_F and U_B , G refers to the reachable directed graph under construction. U_F and U_B are FIFO (first in first out) queues containing states whose successors are not yet computed, during forward and backward chaining phases respectively. The S-TLC model checker works in three phases [19].

5.1 Initialization Phase

Initialization phase is the first stage in S-TLC algorithm and involve the following steps:

1. G as well as U_F and U_B are created and initialized respectively to empty set $\emptyset$ and empty sequence$\langle\rangle$. At this step, each step satisfying the initial predicate *init* is computed and then checked whether it satisfies the invariant predicate Invariant (that is a state predicate to be satisfied by each reachable state).
2. On satisfying the predicate Invariant, it is appended to graph G with a pointer to the null state and a label equal to the set of hypotheses relative to the current state. Otherwise, an error is generated. If the state does not satisfy the evidence predicate $EvidenceState$ (i.e. a predicate characterized by system terminal state that represent digital evidence), it is attached to U_F, otherwise it is considered as terminal state and append to U_B which can be retrieved in backward chaining phase [19].

5.2 Forward Chaining U_F

In this phase, all the scenarios that originate from the set of initial system states are inferred in forward chaining. This involves the generation of new sets of hypotheses and evidences that are consequent to these scenarios. During this phase and until the queue becomes empty, state s is retrieved from the tail of U_F and its successor states are computed. For every successor state t satisfying the predicate constraint (specified to assert bound on the set of reachable

states), if the predicate Invariant is not satisfied, an error is generated and the algorithm terminates otherwise state t is appended to G as follows:

1. If a node core t_n does not exist in G, a new node (set to t_n) is appended to the graph with a label equal to t_c and a predecessor equal to s_n. State t is appended to U_B if satisfied predicate $EvidenceState$, otherwise it is attached to U_F.
2. If there exists a node x in G that is equal to t_n and whose label includes t_c, then a conclusion could be made stating that node t was added previously to G. In that case, a pointer is simply added from x to the predecessor state s_n.
3. If there exists a node x in G that is equal to t_n, but whose label does not include t_c, then the node label is updated as follows:
   - t_c is added to Label (G, x).

- Any environment from Label (G, x), which is a superset of some other elements on this label, is deleted to ensure hypotheses minimality.
- If t_c is still in Label (G, t) then x is pointed to the predecessor state s_n and node t is appended to U_B if it satisfies predicate *EvidenceState* .
- Otherwise, it is attached to U_F [19]

The resulting graph is a set of scenarios that end in any state satisfying the predicate *EvidenceState* and/or Constraint.

5.3 Backward Chaining Phase

All the scenarios that could produce states satisfying predicate $EvidenceState$, generated in forward chaining, are constructed. During this phase and until the queue becomes empty, the tail of U_B, described by state t, is retrieved and its predecessor states (i.e. the set of states s_i such that (s_i, t) satisfy action Next) which are not terminal states and satisfy the predicate Invariant (States that doesn't satisfy predicate Invariant are discarded because this step aims simply to generate additional explanations) and Constraint are computed. Each computed state s is appended to G as follows:

1. If s_n is not in G, a new node (set to s_n) is appended to G with a label equal to the environment s_c. Then a pointer is added from node t_n to s_n and state s is appended to U_B.
2. If there exists a node x in G that is equal to s_n, and whose label includes s_c, then it is stated that node s was been added previously to G. In that case a pointer is simply added from t_n to the predecessor state s_n and s is appended to U_B.
3. If there is x in G that is equal to Sn, but whose label doesn't include s_c, then Label (G, t) is updated as follows:
   - s_c is added to Label (G, x).
   - Any environment from Label (G, x) which is a superset of some other elements in this label is deleted to ensure hypotheses minimality.
   - If s_c is still contained in the label of state x then the node t is pointed to the predecessor state x and the node s is appended to U_B.

The outcome of the three phases is a graph G containing the set of possible causes relative to the collected evidence. It embodies different initial system states apart from those described by the specification [19].

6 CASE STUDY

To investigate VoIP malicious attack using the proposed model, the following case study on the reconstruction of spam over Internet Telephony (SPIT) attack is proposed, to investigate the denial of service experienced by some of the VoIP users as a result of VoIP spam. A direct

investigation shows that the network bandwidth and other resources has been exhausted by the server as it was busy receiving and sending audio message request to SIP URIs(Uniform Resource Identifiers).

According to the VoIP evidence reconstruction model, the first stage emphasis on the identification of the terminal state and the available evidence of the attack.

6.1 Terminal State/Available Evidence

Exhausting of bandwidth and other resource/sending an audio message request to SIP URIs.

6.2 Information Gathering

This includes the following:

- VoIP Components: these comprise both signalling and media infrastructure. The former is based on session initiation protocol (SIP) in particular, that include: SIP STACK (SS) (which is responsible for sending and receiving, manufacturing and parsing SIP messages) and SIP addressing (SA) (is based on the URI). The latter, considered Real Transmission Protocol (RT) (RTP stacks) which code and decode, compress and expand, and encapsulate and demultiplex of media flows.
- VoIP vulnerabilities: it can be as a result of the following:
  a. Unchanged default passwords of deployed VoIP platforms can be strongly vulnerable to remote brute force attack,
  b. Many of the services that exposes data also interact as web services with VoIP system and these are open to common vulnerabilities such as cross-site request forgeries and cross- site scripting.
  c. Many phones expose service that allows administrators to gather statistics, information and remote configuration settings. These ports open the door for information disclosure that attackers can use to gain more insight to a network and identify the VoIP phones.
  d. Wrong configure access device that broadcast messages enable an attacker to sniff messages in VoIP domain.
  e. The initial version of SIP allows plain text-based credentials to pass through access device.

6.3 Evidence Generation

This stage involves the following:

- Hypothesis formulation. Using the hypothesis that a VoIP running a service on a default password can grant an access to an intruder after a remote brute force attack. A hypothesis stating that service ports on VoIP phones expose data, also interact as web services, an intruder that have access to VoIP service can exploit such vulnerability in the form of cross-site scripting to have an administrator access.

. Some phones expose a service that allows administrators to gather statistics, information and remote configuration, a hypothesis stating that such phones can grant an intruder with direct access to administrative responsibility.

  a. A hypothesis stating that there is a wrong configured access device which broadcast SIP messages. This enables the attacker to intercept SIP messages.

b. A hypothesis stating that the messages are running on the initial version of SIP, which has a vulnerability that send a plain text SIP message. The intruder that intercepts the messages can extract user information from the message.
c. An intruder who is equipped with administrator function can create, decode and send a request message
d. An intruder can extract SIP extension/URIs by sending an OPTION message request after searching all ports running on 5060 in SIP domain, to send a SIP message.
e. A hypothesis stating that the credentials were encrypted with cipher text requires an encryption engine to enable the intruder to digest SIP message header and obtain other information.

- Modelling of Attack Scenario: in this case, we are to use $STLA^+$
  The specification describes the available evidence with predicate $EvidenceState$ which uses the function *request* to state that the machine is busy sending invite audio messages.

  In this segment we are to represent hacking scenario fragment inform of hypothetical action as described below.
  a. $\underline{VoIPBrfor}$: There is a Hypothesis stated that there is vulnerability that VoIP running service on a default password, an intruder can easily brute force and gain access and raise up his privilege from no access($acss = NA$) to access level ($acss = AL$) on the VoIP network, by performing brute force on VoIP($VoIPBrfor$) default password.
  b. $\underline{ExpSerVul}$: using the hypothesis stating that the service ports on VoIP has some vulnerabilities if it is exploited can raise the accessibility level of an attacker from ($acss = Al$) to administrator access($acss = AA$) by exploring service port vulnerability ($ExpSerVul$).
  c. $\underline{ExpPhnVul}$: A hypothesis stating that some VoIP phones expose service that allows administrators to gather information for remote configuration. Such vulnerability can grant a direct access from ($acss = NA$) to an administrator access ($acss = AA$), if it's exploited by exploring phone vulnerability ($ExpPhnVul$).
  d. $\underline{IntcSIPmsg}$: hypothesis stating that if there is wrong configured access devices, which allow messages to be broadcast a SIP has vulnerabilities that send messages with plain-text credentials. If it's exploited, an intruder can intercept SIP messages ($IntcSIPmsg$) and eavesdrop.
  e. $\underline{MaFacSIPMsg}$: a user with administrative access can manufacture ($MaFacSIPMsg$), decode and encapsulate SIP messages using SIP STACK (SS).
  f. $\underline{AccSIPURIs}$: the user requires SIP extension or URIs to send an invite messages, being equipped with administrative access the intruder sends OPTION message request to extract SIP URIs ($AccSIPURIs$) provided that the

service port is running on 5060 ports.

g. *MsgDecrypt*: the intruder takes advantage of vulnerability that the device has an encryption engine, it will enable him digest the cipher text on SIP message header field value to extract other information related to SIP message credentials.

h. *SendInvMsg*: the intruder with administrative access and manufactured SIP message then send an invite audio message (*SendInvMsg*) to the server as a message request.

i. *Logout*: the user then logout from the VoIP domain.

The S-TLA$^+$ attack scenario fragment module is depicted in the figure below.

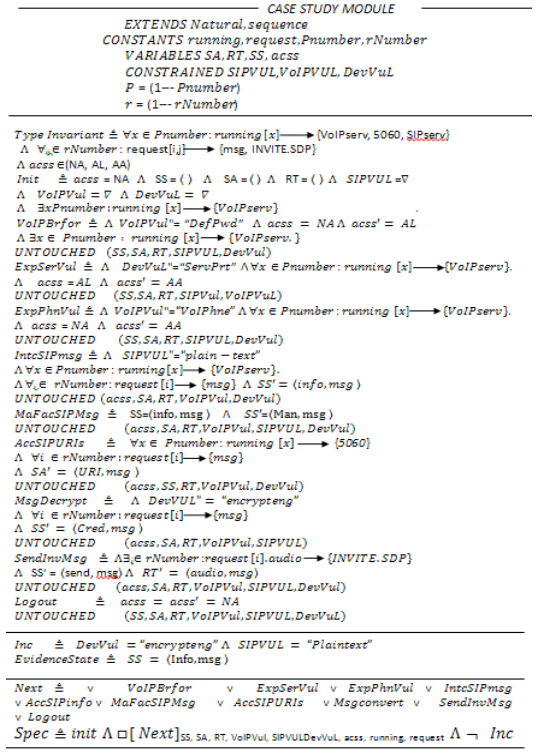

Figure 2. Generated attack scenario fragment using S-TLA$^+$

- Testing Generated Scenario: given a set of a generated attack scenario, if any of the scenarios satisfies the terminal state of the system under investigation, then digital evidence is generated and printed otherwise the hypothesis is reformulated. In the case study presented above, an action *sendInvMsg* in the generated scenarios satisfied the available evidence of the terminal state of the system.
- Print Generated evidence: To generate evidence from the attack scenario fragment presented in Figure 2, we used forward and backward chaining phases as explained above. This has been adopted from inferring scenarios with S-TLC[19].

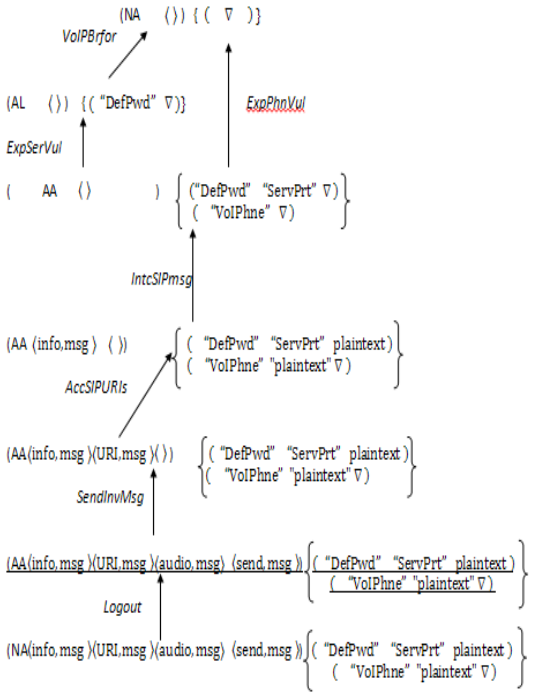

Figure 3. Forward chaining phase VoIP attack scenario

The graph of Figure 3 shows the main possible attack scenario on VoIP. Initially, there is no user accessing the VoIP system. The default password was not changed during implementation of the system. An

intruder exploit this vulnerability by performing an action $VoIPBrfor$ and gained access to the VoIP Service and the intruder further exploits vulnerability in the service ports with an action $ExpSerVul$ and gain and administrator access. Or exploit VoIP phones vulnerability with an action $ExpPhnVul$ that grants access to administrative functions and obtain Administrator access. The hacker can intercept all the incoming messages into the server by executing an action $IntcSIPmsg$, as a result of exploiting a vulnerability in which messages are sent as plain text based on the initial version of SIP. With administrative power, the intruder access SIP URIs from the intercepted messages after executing an action $AccSIPURIs$ and send an audio invite messages to the collected URIs by performing an action $SendInvMsg$ without any hypothesis been established in the last two actions. Therefore the node labels remain the same and then logout and leave evidences within the system. The underlined texts in the generated graph are the available evidence, while others are new evidence generated during an investigation.

The generated attack scenario stopped inconsistency from occurring. The action ($MsgDecrypt$) is not part of the generated scenario as a result of contradicting with action $IntcSIPmsg$.

The generated graph after execution of forward and backward chaining phase is shown in Figure 4. It shows a new generated scenario. It follows the same pattern with the forward chaining phase, but in this case the VoIP system is holding information on received messages that are not accessible to the intruder. The intruder performs the same actions as in the forward chaining phase and was granted an administrator access. Thereafter, the intruder manufactured a SIP invite messages by executing an action $(MaFacSIPMsg)$. The intruder access SIP URIs and send a SIP invite audio message to the collected URIs by performing actions $AccSIPURIs$ and $SendInvMsg$ respectively. No any hypotheses have been established for these actions to be executed, the intruder then logout from the system after executing an action $Logout$ and leave digital evidence. The underlined texts in the generated graph are the available evidence, while other texts are new evidences generated during reconstruction of attack scenario.

Figure 4. Backward chaining phase, scenario attacks on VoIP

7 CONCLUSIONS

In this paper, we proposed a model for reconstructing Voice over IP (VoIP) malicious attacks. This model generates more specified evidences that match with the existing evidence through the reconstruction of potential attack scenario.

Consequently, it provides significant information on what, where, why and how a particular attack happens in VoIP System. To harmonize our study, there is a need for reconstruction of anonymous and Peer-to-peer SIP malicious attacks.

REFERENCES

1. Yun-Sheng Yen, I-Long Lin, Bo-Lin Wu. A: Study on the Mechanisms of VoIP attacks: Analysis and digital Evidence. Journal of Digital Investigation 8, 56–67 Science direct (2011).
2. Jaun C. Pelaez: Using Misuse Patterns for VoIP Steganalysis. 20th International Workshop on Database and Expert Systems Application (2009).
3. Patric Park. Voice over IP Security. Cisco press ISBN: 1587054698 (2009)
4. Hsien-Ming Hsu, Yeali S. Sun, Meng Chang Chen. Collaborative Forensic Framework for VoIP Services in Multi-network Environments. In: Proc. 2008 IEEE International workshops on intelligence and security informatics, pp. 260-271 Springer-Verlag Berlin Heidelberg (2008)
5. Jill Slay and Mathew Simon: Voice over IP: Privacy and Forensic Implication. International Journal of Digital Crime and Forensics (IJDCF) IGI Global (2009).
6. Palmer G. : A road map for digital forensic research. In: First digital forensic research workshop. DFRWS Technical Report New York (2001).
7. Mark Reith, Clint Carr and Gregg Gunsch: An Examination of Digital Forensic Models. International Journal of Digital Evidence. Vol. 1Issue 3. Fall (2002)
8. Mandia K, Procise C.: Incident Response and Computer Forensics. In: Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi: Network Forensic Frameworks: Survey and Research Challenges. Digital Investigation pp.1-14, Elsevier(2010).
9. Casey E, Palmer G.: The investigative process. In: Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi: Network Forensic Frameworks: Survey and Research Challenges. Digital Investigation pp.1-14, Elsevier(2010).
10. Barian Carrier, Eugene Spafford.: Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, Vol.2 Issue 2. Fall(2003).
11. Ciarduhain O.S.: An extended Model of Cybercrime Investigation. International Journal of Digital Evidence, Vol.3 Issue1. Summer(2004).
12. Baryamureeba V. Tushabe F.: The Enhanced Digital Investigation Process Model. In : Proceedings of the fourth digital forensic research workshop (DFRWS); (2004). www.makerere.ac.ug/ics
13. Beebe NL, Clark JG: A Hierarchical, Objectives-Based Framework For the Digital Investigations Process. Digital Investigation 2(2) pp146-66. Elsevier(2005)
14. Ren W , Jin H. : Modeling the Network Forensic Behavior. In: Security and Privacy for Emerging Areas in Ccommunication Networks, 2005. Workshop of the 1st International Conference pp 1-8 IEEE(2005)
15. Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi: Network Forensic Frameworks: Survey and Research Challenges. Digital Investigation pp.1-14, Elsevier(2010).
16. Peter Stephenson.: Modeling of Post-incident Root Cause Analysis. International Journal of Digital Evidence 2, pp. 1-16 (2003).
17. Pavel Glydyshev and Ahmed Patel :Finite State Machine Approach to Digital Event Reconstructions, International Journal of Digital Forensic & Incident, ACM pages 130-149,(2004)
18. Brian D. Carrier and Eugene H. Spafford: An Event-Based Digital Forensic Investigation Framework. In: Proc. 2004 DFRWS 2004, pp. 1-12 (2004).
19. Slim Rekhis: Theoretical Aspects of Digital Investigation of Security Incidents. PhD thesis, Communication Network and Security (CN&S) research Laboratory (2008).
20. Slim Rekhis and Noureddine Boudriga: Logic Based approach for digital forensic investigation in communication Networks. Computers & Security pp 1-21, Elsevier (2011).
21. Slim Rekhis and Noureddine Boudriga: A Formal Logic- Based Language and an Automated Verification Tool for Computer Forensic Investigation in communication Networks. 2005 ACM symposium on Applied Computing pp. 287-289 (2005)
22. Jaun C. Pelaez and Eduardo B Fernandez. Network Forensic Models for Converged Architectures. International Journal on Advances in security, Vol 3 no 1 & 2 (2010).
23. Mohammed Ibrahim, Mohd Taufik Abdullah, Ali Dehghantanha: VoIP Evidence Model : A New Forensic Method For Investigating VoIP Malicious Attacks. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE International Confence, Malaysia (2012).

24. F. Daryabar, A. Dehghantanha, HG. Broujerdi, *Investigation of Malware Defence and Detection Techniques,"* International Journal of Digital Information and Wireless Communications(IJDIWC), volume 1, issue 3, pp. 645-650, 2012.
25. F. Daryabar, A. Dehghantanha, NI. Udzir, "*Investigation of bypassing malware defences and malware detections*," Conference on Information Assurance and Security (IAS), pp. 173-178, 2011.
26. M. Damshenas, A. Dehghantanha, R. Mahmoud, S. Bin Shamsuddin, "*Forensics investigation challenges in cloud computing environments*," Cyber Warfare and Digital Forensics (CyberSec), pp. 190-194, 2012.
27. F. Daryabar, A. Dehghantanha, F. Norouzi, F Mahmoodi, "*Analysis of virtual honeynet and VLAN-based virtual networks*," Science & Engineering Research (SHUSER), pp.73-70, 2011.
28. S. H. Mohtasebi, A. Dehghantanha, "*Defusing the Hazards of Social Network Services*," International Journal of Digital Information, pp. 504-515, 2012.
29. A. Dehghantanha, R. Mahmod, N. I Udzir, Z.A. Zulkarnain, "*User-centered Privacy and Trust Model in Cloud Computing Systems*," Computer And Network Technology, pp. 326-332, 2009.
30. A. Dehghantanha, "*Xml-Based Privacy Model in Pervasive Computing*," Master thesis-University Putra Malaysia 2008.
31. C. Sagaran, A. Dehghantanha, R Ramli, "*A User-Centered Context-sensitive Privacy Model in Pervasive Systems*," Communication Software and Networks, pp. 78-82, 2010.
32. A. Dehghantanha, N. Udzir, R. Mahmod, *"Evaluating user-centered privacy model (UPM) in pervasive computing systems*," Computational Intelligence in Security for Information Systems, pp. 272-284, 2011.
33. A. Dehghantanha, R. Mahmod, "*UPM: User-Centered Privacy Model in Pervasive Computing Systems*," Future Computer and Communication, pp. 65-70, 2009.
34. A.Aminnezhad,A.Dehghantanha,M.T.Abdullah , "A Survey on Privacy Issues in Digital Forensics," International Journal of Cyber-Security and Digital Forensics (IJCSDF)- Vol 1, Issue 4, pp. 311-323, 2013.
35. S. Parvez, A. Dehghantanha, HG. Broujerdi, "*Framework of digital forensics for the Samsung Star Series phone*," Electronics Computer Technology (ICECT), Volume 2, pp. 264-267, 2011.
36. S. H. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, "*Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone*," International Journal of Digital Information and Wireless Communications (IJDIWC),volume 1, issue 3, pp. 651-655, 2012.
37. FN. Dezfouli, A. Dehghantanha, R. Mahmoud ,"*Volatile memory acquisition using backup for forensic investigation*," Cyber Warfare and Digital Foresnsic, pp. 186-189, 2012
38. Y. TzeTzuen, A. Dehghantanha, A. Seddon, "*Greening Digital Forensics: Opportunities and Challenges*," Signal Processing and Information Technology, pp. 114-119, 2012.
39. Mohammed Nassar, Radu State, Olivier Festor: VoIP Malware: Attack Tool & Attack Scenarios In: 2009 IEEE International Conference on Communications (2009).
40. Mouna Jouini, Anis Ben Aissa, Latifa Ben ArfaRabai, Ali Milli: Towards quantitative measures of Information Security: A cloud computing case Study" International Journal of Cyber-Security and Digital Forensic (IJCSDF) 1(3):248-262. The society of Digital Information and Wireless communications.(ISSN:2305-0012)(2012)
41. I-Long Lin, Yun-Sheng Yen: VoIP Digital Evidence Standard Operating Procedure. International Journal of Research and Reviews in Computer Science 2, pp. 173 (2011).
42. Jill Slay and Mathew Simon: Voice over IP forensics. In: e-Forensics 08 Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia workshop. Adelaide, Australia (2008).
43. Siti Rahayu Selamat, Robiah Yusof, Shaharin Sahib, Nor Hafeizah Hassan, Mohd Faizal Abdollah, Zaheera Zainal Abidin. Traceability in Digital Forensic Investigation Process. In: 2011 IEEE Conference on Open Systems, pp. 101-106 (2011).
44. Kara Nance Brian Hay, Matt Bishop. Digital Forensic: Defining a Research Agenda Incident Response. In: Proc. 42nd Hawaii International Conference on system science (2009).
45. Karen Kent Suzanne Chevaliar, Tim Grance, Hung Dang. Integrating Forensic Techniques into Incident Response. A white paper submitted by Guidance Software Inc. UK (2006).
46. Tamjidyamcholo A, Dawoud R A.: Genetic Agorithm for Risk Reduction of Information Security. International Journal of Cyber-Security and Digital Forensic(IJCSDF) 1(1):59-

66 (ISSN:2305-0012) the society of Digital Information and wireless communications (2012).

47. Jeroen Keppens and John Zeleznikow. "A Model Based Approach for Generating Plausible Crime Scenarios from Evidence. In: Proc. of the 9th International Conference on Artificial intelligence and Law (2003).