Context-Based Heuristics in Attribution

Jim Q. Chen, Ph.D.
National Defense University, U.S.A.

Abstract

In cyber forensics, attribution of an attack, which finds out details about the individual(s) who launched an attack, is more important than mere identification of an attack, since a precise response to the cyber attack heavily depends upon attribution. The identification of the initiator(s) in attribution provides precise targeting for a counter-attack. However, heuristics are typically deployed to find out information about attack actions rather than initiator(s) of attack actions. This paper proposes a mechanism that utilizes a weight system for guiding the way in which the heuristics prioritize the discovery of attacker initiator(s). Linking purpose, methods, time, location, and events with the identified device, the proposed heuristic approach can serve as a path towards accurate and prompt attribution.

Introduction

It is not uncommon that a cyber attack is reported without identification of the attacker(s). Quite often, cyber defense mechanisms and cyber forensics can help to identify the fact that a system has been hacked and compromised and the data on the system have been stolen. However, it always takes a lot more time and efforts to find out who did it and why it was done. Attribution is hard to be done even though it is possible. Without quick and accurate attribution, precise responses to the attacker(s) are delayed, and direct cyber deterrence mechanisms become less effective. In some cases, indirect deterrence mechanisms, such as diplomatic, economic, legal, military, or other national security instruments, have been employed, especially in dealing with nation-state attackers. Unfortunately, the indirect deterrence mechanisms are always taking long time to be deployed and executed, as attribution and preparation for the use of non-cyber national security instruments require extra time in this process, thus causing the delay in response or retaliation. In addition, as correctly pointed out by Sterner (2011), the indirect deterrence mechanisms have limited effect on non-nation-state attackers.

What needs to be done in order to improve the process of attribution in the cyber domain so that direct retaliation in the cyber domain can be quickly launched should it be legal and necessary? To answer this question, the key components in attribution should be identified. With this identification, a novel approach can be figured out to address these key components ahead of time so that the time needed for conducting attribution can be significantly reduced.

The paper is organized as follows: In Section 1, an introduction to the challenge is provided. In Section 2, related works are examined. The current approaches and their limitations are analyzed. In Section 3, an innovative solution is proposed. In Section 4, this novel approach is applied to a hypothetical case. In Section 5, a conclusion is drawn.

Related Works

Beebe (2009) calls for the design and implementation of smart analytical algorithms in digital forensics since the "cost of human analytical time spent sifting through non-relevant search hits is a significant issue". He holds that even though current "computational approaches for searching, retrieving and analyzing digital evidence are unnecessarily simplistic", there exists significant information retrieval overhead. He argues that smart analytical algorithms should "clearly reduce information retrieval overhead", "help investigators get to relevant data more quickly, reduce the noise investigators must wade through, and help transform data into information and investigative knowledge." In order to design such an intelligent algorithm, heuristics should be looked into.

Marti and Reinelt (2011) maintain that a good heuristic algorithm should fulfill the following properties: "A solution can be obtained with reasonable computational effort". "The solution should be near optimal (with high probability)”. “The likelihood for obtaining a bad solution (far from optimal) should be low”.

Hill-climbing algorithms belong to local search, which, according to Kokash (1998), “is a version of exhaustive search that only focuses on a limited area of the search space”. “Such algorithms consistently replace the current solution with the best of its neighbors if it is better than the current.” However, a hill-climbing algorithm “always finds the nearest local optima of low quality”. This issue is referred to as pre-mature convergence. Heuristics is used to deal with this problem.

There are several different approaches in heuristics. The best-first search selects the best state in the list. Simulated annealing allows some moves to worse states in order to explore many regions of the state space. A* algorithm, which uses a best-first search with a modified evaluation function, selects the shortest path that has the minimal total cost. However, in the first trial, as evaluation is not performed yet, it may select a path that is not the shortest one.

In the context of attribution, is there a structural configuration that helps to select the shortest path in the first trial? If there is one, what is it? How does this work? These are the questions that are addressed in the next section.

Proposal

A novel context-based heuristic approach is proposed in this section. Here, the relationship among the components for attribution is analyzed and a weight system is employed. Combining this weight system with the Contextual Binding Condition, this new context-based heuristic approach is designed to discover the shortest and the most optimal path for attribution.

To accurately attribute an event to an individual, all the following elements should be addressed: “who”, “what”, “when”, “where”, “how”, and “why”. To do so, it is crucial to find out the relationship among these elements.

Sinek (2009) does a very good job in explaining the relationship among some components, such as “what”, “how”, and “why”, via the Golden Circle, as shown in Figure 1 below:

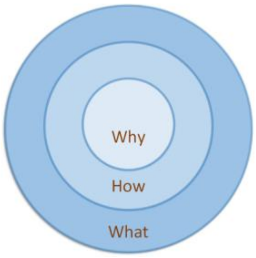

Figure 1. Golden Circle

The Golden Circle is used for inspirational leadership. The idea is to have a goal figured out and made known first, come up with a method or craft a strategy based on the purpose, and then figure out what to do to achieve the goal.

As shown in this figure, the component “what” represents actions or events. The component “how” represents the method or the strategy used in orchestrating these events. It is relatively less obvious than the component “what”. The component “why” represents the goal to be achieved via the method or the strategy employed. It is the least comprehensible element of these three components. However, once an understanding of the goal is gained, an understanding of the whole picture and the relationship of all these events is acquired.

Given the representation in circles, this process can be depicted as being inside out. In Sinek’s term, it all starts with why. Sinek (2009) even looks at how this representation corresponds with the major levels of the brain. The “what” level corresponds with neocortex, while the “how” level and the “why” level correspond with limbic brain. Neocortex is responsible for rational and analytical thought as well as language but it does not drive behavior. Limbic brain, which drives behavior, is responsible for feelings, such as trust and loyalty, as well as all human behavior and decision making.

This model demonstrates that a purpose (i.e. the “why” component) drives methods or strategies (i.e. the “how” component), which, in turn, drive actions (i.e. the “what” component). From this perspective, the “why” component is more important than the “how” component, and the “how” component is more important than the “what” component.

It has to be pointed out that as the purpose of the Golden Circle is not for attribution, other important components such as “who”, “when”, and “where”, are not included in the Golden circle. However, to build the Attribution Circle on the basis of the Golden Circle, these three components have to be included. What needs to be discovered is the relationship among all these components.

It needs to be noted that the component “who”, which represents the human component, possesses the highest priority in any investigation as it directly pinpoints to the individual(s) who conducted the action. Other factors, such as the reason why the action was conducted, the way the action was conduct, the action that was conducted, the place where it was conducted, and the time when it was conducted, are all directly associated with the human component, i.e. the “who” component. To a certain extent, they are the attributes of the “who” component, which represents the initiator of an action. It is the human who has a purpose or a goal. It is the human who comes up with a method or a strategy to archive the goal. Of course, the method or the strategy has to be associated with location and time. It is the human who conducts the action based on the method or the strategy. The action has to occur in a specific location within a specific time. This is why this human component should hold relatively the highest weight in the Attribution Circle. Also, the component "who" is closely tied to all other components as it is the initial driver who makes all these happen.

The component "why" is the second most crucial element, as it drives the component "how", which, in turn, drives the component "what". This is why it should possess the second highest weight in the Attribution Circle. For the same reason, the component "how" should hold a weight that is less than that of the component "why" but more than that of the component "what". As location (i.e. the component "where") and time (i.e. the component "when") are the attributes for a method (i.e. the component "how") or an action (i.e. the component "what"), they should hold a weight that is less than that of the component "how". Naturally, a weight system comes into being.

All these relations can be successfully captured in the Attribution Circle proposed in Figure 2 below:

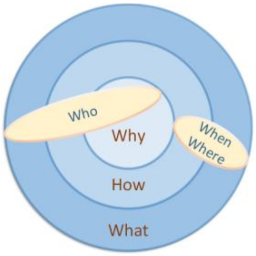

Figure 2. Attribution Circle

In the leadership environment, an effective directional relationship is inside out. Similarly, a well-designed attack follows this directional relationship. An attacker has a goal to achieve. To achieve that goal, the attacker needs to figure out a method or a strategy. The attacker then orchestrates various actions in different locations at different times according to the method or the strategy. This clearly reflects an inside-out directional relationship, which is displayed in Figure 3 below:

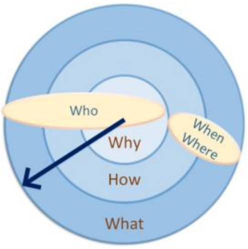

Figure 3. Inside Out

However, in the cyber forensics environment, an effective directional relationship is outside in. Investigators usually observe seemingly irrelevant actions in different locations at different times. The analysis helps them to link the dots of these actions and eventually to figure out the method or the strategy used. Based on the understanding of the method or the strategy used as well as the link between an action and an actor, the suspect(s) can be eventually attributed to. This reflects an outside-in directional relationship, which is displayed in Figure 4 below:

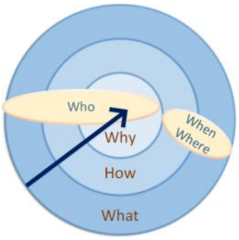

Figure 4. Outside In

Evidently, the directional relationship truly reflects the order of events. The Attribution Circle can effectively capture the relationship.

Based on the above analysis, the following stipulation can be made to capture the proportion of weight of probability for each component in attribution:

(1) Weight of probability for each component:
"who": W1 = 0.3
"why": W2 = 0.25
"how": W3 = 0.15
"when": W4 = 0.1
"where": W5 = 0.1
"what": W6 = 0.1

The total weight of probability equals 1.

If a component is known, it carries the value "1". Otherwise, it has the value "0".

The probability of successful attribution can be express as follows:

(2)

$$\mathrm{P}(X) = \sum_{i=1}^{6} (Xi * Wi)$$

Given the weight of each component listed in (1), the formula in (2) can be expanded as follows:

(3)

$$P(X) = \sum_{i=1}^{6} (Xi * Wi)$$

$$= (X_1*W_1) + (X_2*W_2) + (X_3*W_3) + (X_4*W_4) + (X_5*W_5) + (X_6*W_6)$$
$$= (1*0.3) + (1*0.25) + (1*0.15) + (1*0.1) + (1*0.1) + (1*0.1)$$
$$= 0.3 + 0.25 + 0.15 + 0.1 + 0.1 + 0.1$$
$$= 1$$

This means that if all the six components are known, the individual who launched the attack can be successfully attributed to.

Also, when the attributes represented by these components are all properly addressed in an expected way, the Revised Restrictive Contextual Binding Condition proposed in Chen (2016) is satisfied, as the variables are properly bound by their corresponding contextual operators. This binding condition is listed below:

Assume X is an entity, and CO is a contextual operator.

(4) In a specialized time, location, environment, and background, if X is directly related to CO with respect to all the attributes such as action-initiator (who), action (what), action-recipient (who/what_recipient), time (when), location (where), method (how), and purpose (why) in such a setting:
COi[WHO1, WHAT2, WHAT_RECIPIENT3,
WHEN4, WHERE5, HOW6, WHY7]
{……Xi[WHO1,WHAT2,
WHAT_RECIPIENT3,
WHEN4, WHERE5, HOW6, WHY7]……}
then Xi is contextually bound by COi in a restrictive way.

As pointed out in Chen (2016), this is a typical representation of Type 1 Binding as all the attributes in the variable are contextually bound by the attributes in the contextual operator. "If one contextual attribute in the variable is not directly related to the corresponding attribute in the contextual operator, the variable is not contextually bound by the contextual operator in the restrictive sense."

Putting (3) and (4) together, if all the attributes of a variable (i.e. "who", "why", "how", "when", "where", and "what") are known, then P(X) = 1, and the variable is properly, (i.e. 100%) bound by the contextual operator (CO). However, if only "what", "when", and "where" are known, then P(X) = (1*0.1) + (1*0.1) + (1*0.1) = 0.3, and the variable is 30% bound by the CO.

As the attribute "who" possesses the highest weight, i.e. 0.3, and the attribute "why" possesses the second highest weight, i.e. 0.25, the missing of these two attributes immediately points out a new path of search, namely, the quest for the attributes "who" and "why". Once these two attributes are known, 55%, i.e. (1*0.3) + (1*0.25) = 0.55, of the puzzle is solved. Let us compare the pair of the attributes "who" and "why" with the pair of attributes "how" and "what". As the weight of the attribute "how" is 0.15 and the weight of the attribute "what" is 0.1, the total weight of the latter pair is P(X) = (1*0.15) + (1*0.1) = 0.25. This means that getting to know these two attributes solves 25% of the puzzle. Evidently, 25% is less than 55%; and the pair of the attributes "how" and "what" has less priority than the pair of the attributes "who" and "why" does. With such a weight system in place, the attribute "who" is always the first one to go after if it is unknown. The attribute "why" is the second one to go after, and the attribute "how" is the third one to go after. The pair of the attributes that possesses the highest weight, i.e. the attributes of "who" and "why", which possesses 55% of the total weight, is the first one to go after as a pair. The pair of the attributes that holds the second highest weight, i.e. the attributes of "who" and "how", which holds 45% of the total weight, is the second one to go after as a pair. As shown here, the weight system proposed in this paper helps to set up the priority in the search and helps to heuristically choose an optimal path for the quest. This structural configuration helps to select the shortest path in the first trial, thus making heuristic algorithms more optimal and more efficient, especially in the quest for attribution.

In addition, this weight system can help the process of intelligence collection for the sake of prevention in the cyber domain. If a request for a service is received from a device that is unknown, the server service should hold the normal response and immediately start the query for the unknown factors. Picking up the component with the heaviest weight in the list, the server service goes after the component "who". The server service now engages the device of the attack-initiator into a dialog by asking it questions related to the "who" attribute. The idea is to make the device of the attack-initiator to reveal its identity information. If no answer or unsatisfactory answer is received, the request from the attack device is immediately rejected and the normal response is not provided at all. If a satisfactory answer is received, the server service goes after the component "why", which possesses the second heaviest weight in the list. The server service now asks the device that makes the request to provide reasons for its request. Again, if no answer or unsatisfactory answer is received, the request from the attack device is immediately rejected and the normal response is not provided at all. Otherwise, a normal response is provided. The questions related to the "why" attribute can help to detect a zombie since a zombie either does not have a good reason for the request or has to wait for the attack-initiator to provide a reason. The unsatisfactory answer or the delay in response is a good indicator in detecting a zombie system. Evidently, this new context-based heuristic approach can help intelligence collection for the sake of prevention.

Chen and Dinerman (2016) examine the unique characteristics of cyber conflicts and discover the following three cyber feature sets, namely intelligence collection, stealth maneuvers, and surprise effect. They argue that these unique feature sets can be turned into unique cyber capabilities that serve as force multipliers, if they are integrated appropriately into conventional conflicts as complementary military capacities. As shown in this paper, this new context-based heuristic approach not only can assist intelligence collection but also can speed up the attribution process. This capability is exactly what is needed for force multipliers.

Case Study

In this section, the proposed context-based heuristics is applied to a hypothetical case, which is a typical attribution challenge.

Let us assume that a server suddenly receives 2,000 repetitive packets within a second from the same source right at 5:00 PM on Monday. This abnormal behavior immediately triggers the context-based heuristics for investigation, as the server usually receives less than 1,000 different packets within a minute. A quick scrutiny reveals the packets are all echo packets utilizing UDP Port 7. The message echoed is exactly the same. This started a minute ago. It only occurs on this particular server at that time.

This quick scrutiny discloses the attributes of "what", "when", "where", and "how". The fact that the server is hit by 2,000 echo packets per second accounts for the attribute of "what". The time at 5:00 PM on Monday accounts for the attribute of "when". The location of the server accounts for the attribute of "where". Echo packets utilizing UDP Port 7 in that particular location at that particular time accounts for the attribute of "how". So far, the known attribute are "what", "when", "where", and "how". The unknown attributes are "who" and "why". Given the weighted system, the weight of the known attributes is ((1*0.15) + (1*0.1) + (1*0.1) + (1*0.1) = 0.15 + 0.1 + 0.1 + 0.1 = 0.45, namely, 45% of the puzzle is known. The context-based heuristics recommends an inquiry for the attribute "who" first as it possesses 30% of the total weight.

Now, the engagement mechanism is triggered, and the intelligence collection process gets started. It examines the source MAC address and the source IP address within the echo packets. As the source MAC address is the address of the switch that the server is directly connected to, the server asks the switch for the source MAC address of the packet that the switch receives. The switch will ask the router that it directly connects to for the source MAC address and the source IP address within the echo packets that the router receives. The router provides the information. Now, the MAC address and the IP address that sends the echo packets to the router are discovered. The engagement mechanism approaches that device and asks the same question. This process keeps running until it reaches to the device that launches these echo packets.

Once it gets to the device that launches these echo packets, the engagement mechanism makes an inquiry about the attribute "why", which possess 25% of the total weight. If this device is a zombie, it may provide an unsatisfactory reason; or it may be slow in providing the reason as it waits for it from the command and control (C2) server. Note that this type of control requires connectivity. If the engagement mechanism further asks for the current status of its connectivity, and if the zombie device provides the answer, the IP address of the C2 server is revealed.

Using the same back-tracking method, the engagement mechanism can eventually trace to the C2 server. From the neighboring device of this C2 server, the engagement mechanism is able to find out the MAC address as well as the IP address of the C2 server. Once discovered, the engagement mechanism makes an inquiry about the attribute "why". The C2 server either refuses to provide an answer or provides an unsatisfactory answer. This may give up its real intention. At this point, a close surveillance is initiated in order to find out the host name of the devices and the user name if possible. In addition, the engagement mechanism tries to verify if the device is used by the real attack initiator and if the owner/user of the device is the real attacker. Eventually, 100% of the puzzle is solved, or at least a very higher percentage of the puzzle is solved.

Note that this operation is conducted at the very early stage of a denial of service attack. So, deterrence mechanisms, defense mechanisms, and recovery mechanisms can be immediately launched to halt the denial of service attack. In cyber operations, every minute counts. The sooner an attacker can be identified, the sooner a counter-attack can be launched, and the less impact can be left on the affected systems and networks. Meanwhile, the evidence collected can be used for prosecution and retaliation purpose. This supports cyber deterrence.

As shown in this hypothetical case, the context-based heuristics plays a significant role in search for a target and in collecting intelligence and evidence about the target. With no doubt, it helps accurate attribution.

Conclusion

Attribution is a challenge in the cyber domain. However, as shown in this paper, heuristics can guide the most optimal search based on some structural configurations with a weight system. Eventually, it is capable of limiting the search time of information discovery heuristics in supporting cyber operations. Linking purpose, methods, time, location, and events with the identified device, the proposed heuristic approach can serve as a path towards accurate and prompt attribution.

References

Beebe, N. 2009. Digital Forensic Research: the Good, the Bad and the Unaddressed. *Advances in Digital Forensics V*, Springer. pp. 17-36.

Chen, J. 2016. Contextual Binding and Intelligent Targeting. *Proceedings of the 2016 IEEE/WIC/ACM International Conference on Web Intelligence*. pp.701-704.

Chen, J. & Dinerman, A. 2016. On Cyber Dominance in Modern Warfare, *Proceedings of the 15th European Conference on Cyber Warfare and Security*. pp.52-57. Reading, UK: Academic Conferences & Publishing International (ACPI) Limited.

Kosash, N. 1998. An Introduction to Heuristic Algorithms. University of Trento, Italy.

Marti, R. & Reinelt, G. 2011. Heuristic Methods. The Linear Ordering Problem, Exact and Heuristic Methods in Combinatorial Optimization 175, DOI: 10.1007/978-3-642-16729-4_2. pp.17-40. Berlin: Springer-Verlag.

Sinek, S. 2009. *Start with Why: How Great Leaders Inspire Everyone to Take Action*. USA: Penguin Group.

Sterner, E. 2011. Deterrence in Cyberspace: Yes, No, Maybe. *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*. pp. 27. Washington DC: George C. Marshall Institute.