EasyChair Preprint

№ 628

Causal Modeling for Cybersecurity

Suchitra Abel, Licheng Xiao and Hairong Wang

November 12, 2018

Causal Modeling for Cybersecurity

Dr. Suchitra Abel
Dept. of Computer Engineering
Santa Clara University
Santa Clara, CA, United States
sabel@scu.edu

Licheng Xiao
Dept. of Computer Engineering
Santa Clara University
Santa Clara, CA, United States
lxiao@scu.edu

Hairong Wang
Dept. of Computer Engineering
Santa Clara University
Santa Clara, CA, United States
hwang1@scu.edu

***Abstract*—Causal modeling is very useful in the pursuit of cybersecurity since it often helps us to execute actions leading to fruitful results, without performing unnecessary computations that might affect the values of other variables. The causative factors that are necessary and sufficient, are explored, with the help of modeling a real-life example taken from 2017, United States cybersecurity case. One can recommend future company policies, based on the causal modeling results. It also makes us understand how an event such as a breach of cybersecurity occurs, and how it can be dealt with.**

***Keywords*—causal modeling, data leakage, preventing computational virus, graph maneuvered according to causal modeling**

I. Introduction (Scientific Method for cybersecurity based on Causation)

We offer a scientific method based on the notion of causation, which is productive in the field of cybersecurity. Our goal in this paper is to develop this notion, in terms of which practical cases of cybersecurity can be understood and evaluated. An example of such a practical case is that of an internet infrastructure company called Cloudflare, that suffered from a severe data security breach. The problem was solved by a Google employee who isolated the cause of the data breach and fixed the problem; however, he did not perform any formal causal modeling of the situation, which could have helped the public to be informed about similar future investigation modes. Here we propose the method of causal analysis and describe how it is to be handled, by recommending that the problem at hand is to be accomplished by causal modeling, in order to provide support for future cases. This shows that the problem at hand is the effect of some particular cause; this way, we can transform indeterminate situations into more determinate ones.

II. Description and importance of the topic of causal modeling for cybersecurity

New methods for tackling the modern problem of cybersecurity are critical. Instead of trying to fit the new phenomenon into the framework we already have, we should try a new approach. [1].

This paper covers some important aspects of handling modern cases of cybersecurity, with the new approach of causal modeling.

In 2017, the internet infrastructure company Cloudflare stated that a (computational) virus in its platform caused accidental escape of potentially vulnerable customer data. Cloudflare offers performance and security services to about six million customer websites (including companies that have a large incoming traffic, such as Fitbit and OKCupid), so though the leaks were occasional and only involved small pieces of data, they drew from a vast collection of information. The flaw was uncovered and fixed by a Google vulnerability researcher, in the early part of 2017.[2] However, if proper causal modeling accompanied this protection, then future cases could also benefit.

According to the Google researchers who discovered the virus, now known as "Cloudbleed," the problem or vulnerability had been sending data to the browsers of the users when they visited a web page hosted by the company. This was extremely costly to the companies, and also to the economy overall.

The first impulse can be to use statistical modeling. Statistical modeling, a widely used technique, can handle some of this data breach problems, but not all.

One can draw from past experiences, and try to build a probability distribution. [3] Standard probability theory has been productive in these problems and similar ones, when the past experiences are readily available for analysis. But there are instances where it fails to provide adequate concepts and mathematical methods, particularly when the past experiences are either not available, or are not similar.

A context like breach of data can interact with the phenomena of interest in ways that standard probability theory does not productively capture; that is, in ways that standard probability theory does not provide insights and methods for useful modeling and fails to capture key concepts. Some of these key concepts are the necessary and sufficient conditions that produce the essential model of the cause-effect relationships involved.

A necessary condition is one that is required if a certain effect is to follow. For example, it is necessary for the data security in cases like Cloudflare, that the information is given out to companies, without there being bugs in the system. A sufficient condition, on the other hand, is enough for certain effect to follow. So, it is sufficient for data security that there not be bugs (like computational viruses) in the system where it can originate. Thus, in systems like Cloudflare, data security signifies the absence of bugs, which constitutes both necessary and sufficient conditions.

Some of the usage of the necessary and sufficient conditions are as follows: we have to look for causes that are common in the cases where the effect also occurs. Thus, some event is not a necessary condition if it occurs without the effect occurring. [4] [5]

Thus, a necessary condition for a normal transfer of information is the absence of bugs. The sufficient condition of detecting that the presence of bugs causing security breach has taken place, is as follows: if an instance of the lack of security (in data transfer) occurs (bugs) and an instance in which this lack of security does not occur, (absence of bugs), the circumstance(s) in which the two situations differ is an indispensable part of the cause – a sufficient condition.

One can view cause-effect relationships via directed acyclic graphs; one should also link these types of causal parameters and observed data, as well as approaches to estimation of the resulting statistical parameters. [6] The method of using Directed Acyclic Graphs for viewing causal relationships has been successfully utilized in the fields of Biometrics and Biostatistics. [7] It is also useful in the field of cybersecurity.

We can explore causal modeling on observational data. This is important in cases like the cybersecurity of Cloudflare, because controlling the situation of data leakage will require knowing which independent factors actually cause the outcomes, so that we may create changes in the scenario of information pool in a manner that will be predictable and useful in the future.

One may look for correlation, but one might be fooled by spurious association; so can the method of regression. We must move beyond correlation to causation as a methodology, if we want to make use of cause and effect relationships.

Suppose that we tried to confront this problem with *only* the knowledge of the joint distribution of a set of random variables. Then we cannot deal with certain mechanisms, such as leading to actionable intelligence better than models based on statistical methods. Ultimately, we will be able to identify practices, methods, and tools that improve how software is built.

But if we are able to formulate the causal structure and the joint distribution among a set of random variables, then we can predict the effects of intervening in the system by maneuvering the values of certain variables. For example, if we can identify or discern that the computational virus in the platform caused the data leakage (not just a joint distribution between them), we can predict that stopping those bugs will prevent the leakage. Predicting the effects of interventions is important.

Fortunately, in this case, the cause of the data leakage (bugs in the system) were strongly suspected and also identified. One could use the domain knowledge to solve the problem at hand.

One could utilize the method of causal modeling to predict the effects of interventions and policies of the company, and also to recommend company policies.

Let us consider the case where the causal structure is known (the case of the company with data leakage). The population actually sampled is that of the known case; that is the non-maneuvered population. The hypothetical population for which these bugs are taken out is the causally maneuvered population.

Studying this case, we find that if the policy of taking out the bugs in the system were put into effect by the company, it would be effective in stopping the leakage, but it would not affect the value of any other variable in the population, except through its effect on stopping the leakage. In this case, we can say that the leakage-stopping has been maneuvered. However, the other variables are not affected. For example, the distribution of the number of people accessing the web sites does not change. This way, causal modeling operates by performing less unnecessary computational processes.

In this exploratory analysis, we can show that one can generate a plausible graph explaining the occurrence of the lack of cybersecurity.

The graphs for the causally maneuvered and the non-maneuvered populations will be different. The distribution of the data leakage will be different.

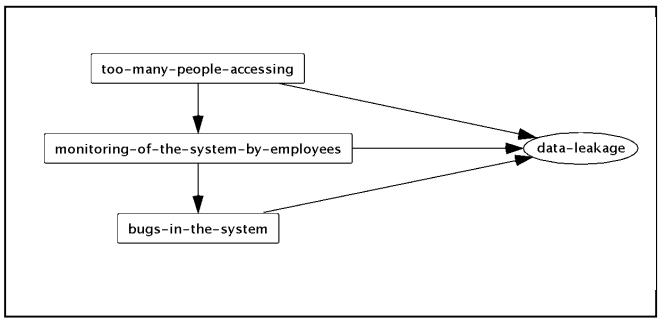

Fig. 1. Non-maneuvered graph (before proper modeling was accomplished)

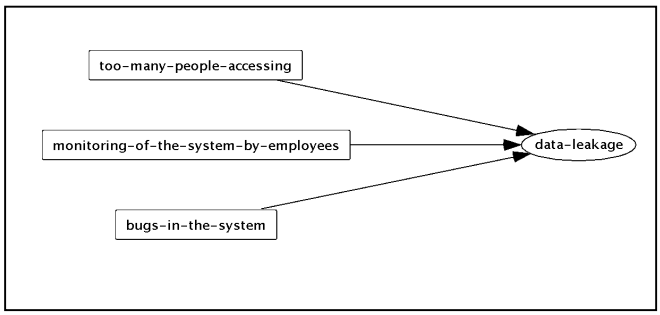

Fig. 2. Graph maneuvered by causal modeling

The Figure 2 shows 3 possible paths to data leakage; but the predominant cause is dealt with first (bugs) and the connection leaves it open for the other vertices to be considered later. Some vertices that are parents of the causally maneuvered variable in the non-maneuvered graph may not be parents of the maneuvered variables of the causally maneuvered graphs (notice the arrows being absent in the second graph).

Next, we have to describe the change in the distribution of the bugs in the system that will result by taking the bugs out in this case (that is, so far).

The value of a variable that represents the company policy is different in the two populations.

So, we can introduce another variable in the causal graph. This is the "dispense with the bugs" variable. In the non-maneuvered population, this particular variable has the value off, and in the hypothetical population, it is on. In the non-maneuvered population we measure

$$P(\text{bugs} \mid \text{“dispense with the bugs”} = \text{off}) \quad (1)$$

In the causally maneuvered population that would be produced if bugs were dispensed with, the case can be represented as

$$P(\text{bugs} = 0 \mid \text{“dispense with bugs”} = \text{on}) = 1 \quad (2)$$

What, and how, empirical evidence legitimizes a cause-effect connection?

David Heckerman of Microsoft Corporation covered this important topic [8].

In this elaboration of concepts behind causation, we clarify as to how a causal structure can be legitimately acknowledged. Dr. David Heckerman [9] introduced the notion of responsiveness, a fundamental relation underlying causation. One can use this notion to define causal dependence.

In general, to determine whether or not an uncertain variable x (the supposed effect – in our case, it is the purported data leakage) is responsive or unresponsive to decision d (for example , leakage is due to the bugs in the system), we have to answer the query "Would the outcome of x have been the same had we chosen a different alternative for d?" Queries of this form are counterfactual queries.

We need some definitions of the counterfactual world and also of the concepts of responsiveness and unresponsiveness, in order to understand this.

Definition of the Counterfactual World: there are some uncertain variables, X (of which x is an instance), such as data leakage (including some uncertainty as to why, and are we sure about the leakage?) in the scenario; there is also the set of potential causes C. In our case, possible candidates for the potential causes in C are: (a) too many people accessing, (b) employees monitoring the system poorly, and (c) bugs in the system.

Given the uncertain variables $X \subseteq U$ (where U is the total set of possible variables that can be and could have been contenders as effects to be determined correctly) and the set of decisions D (for example, the decision that the data leakage is, indeed, there, and that it is there because of the bugs, in our case; the other contenders can be leakage because of people accessing, and leakage because of poor monitoring by employees), a counterfactual world of X and D is any instance assumed by $X \cup D$ after the decision maker chooses a particular instance of D.

Definitions of unresponsiveness and responsiveness are to be understood next. Given uncertain variables X and decisions D, X is unresponsive to D, denoted $X \nleftarrow D$, if X assumes the same instance in all counterfactual worlds of $X \cup D$. (In other words, instances of X do not affect the status of $X \cup D$).

In our case, D contains, for example:

Case 1: data leakage is because of the bugs, or possibly.

Case 2: leakage because of people accessing.

Case 3: leakage because of poor monitoring by employees.

X (the set of the effect or effects for which we are seeking the cause) is the same in all counterfactual worlds of $X \cup D$, if D is Case 2 or Case 3. One should remember, at this stage, that we have chosen a particular instance of D, namely, decision regarding data leakage in the case of Cloudflare, February 2017. So, $X \cup D$ will be any instance in the case of their union (set containing data leakage as the only member) with Cloudflare data problem (a set containing only that case as a member).

(Note that there can still be, in theory if not in practice, more than one instances of the union).

X is responsive to D, denoted $X \leftarrow D$, if X can assume different instances in different counterfactual worlds of $X \cup D$. We should go back to our chosen instance of D, namely, the Cloudflare data problem; if our element in the set of X is the problem of data leakage, then $X \cup D$ is such that X can assume different instances in the different counterfactual worlds of $X \cup D$.

X refers to the collections of events (indicating, for example, different states of data leakage) some of which occur after decision(s) D have been made

(A side-remark at this stage is that this can explain, in many cases, as to how a robot can acquire causal information from the environment. However, Robotics is not the main concern of this paper.)

Now we can come up with a formal definition of a cause.

Given decisions D, the variables in the set C are causes for x with respect to D if all the following three conditions are met.

Condition 1: x is not a member of C.

Condition 2: x is responsive to D.

Condition 3: C' is a minimal set of variables such that x is unresponsive to D in worlds limited by C' (that is, $x \leftarrow D$, and C' is a minimal set such that $x \nleftarrow c' D$).

The third condition can be difficult to understand. It is saying that C has a definite influence on x being responsive to D. The influence is that the relevant cause (or causes) must be included in whichever set of variables that also necessarily differ (being responsive) in accord with x being responsive to D. So, the set C' that limits the relation of x with D (regarding responsiveness) is a minimal set.

The following are the brief explanations with regard to the system discussed here.

Condition 1 is affirming that the effect is not a member of the set of causes.

Condition 2 is ffirming that for x (data leakage) to be caused with respect to decision D (data leakage must have been caused by the bugs in the system) , it must be responsive to that decision.

Condition 3 is explaining the following: suppose that one can find a set of variables Y such that x, data leakage, can be different in different counterfactual worlds only when Y is different. In that case, Y must contain a set of causes (that is, include the bugs in the system, in our case).

III. Conclusion

The authors are currently undertaking the causal program for cybersecurity; it is showing the progress towards the advances in our effort, and promises to bring forth the results shortly. The program will be tested with several real-world cases where cybersecurity is needed.

Acknowledgment

We acknowledge the support and facilitation by the Dept. of Computer Engineering, Santa Clara University, towards

our effort. We also thank Berkeley Institute for Data Science, UC Berkeley, CA where we presented an info-graphic poster in 2018. [9]

REFERENCES

[1] Feynman, Richard, QED: The strange theory of light and matter, Princeton University Press. ISBN 0-691-08388-6, 1985.

[2] Bogart, N., "What you need to know about "Cloudbleed" the latest internet security bug," www.globalnews.ca, February 27, 2017.

[3] Zornig, P. Probability Theory and Statistical Applications, De Gruyter.. ISBN-13: 978-3110363197

[4] McLaughlin, Brian, On the Logic of Ordinary Conditionals, Buffalo, NY: SUNY Press, 1990.

[5] Pearl, Judea, Causality: Models, Reasoning, and Inference, Cambridge: Cambridge University Press, 2000.

[6] Pearl, Judea, Causality, 2nd edition, Cambridge University Press, 2009.

[7] Thornley, S., Marshall, R.J., Wells, S., and Jackson R., "Using Directed Acyclic Graphs for Investigating Causal Paths for Cardiovascular Disease," Journal of Biometrics & Biostatistics, 2013, 4:182. doi:10.4172/2155-6180.1000182

[8] A Decision-Based View of Causality, Heckerman, D. Microsoft Research and Shachter, R. Stanford, CA. Retrieved from AAAI Technical Report SS-95-07. Compilation copyright © 1995, AAAI (www.aaai.org).

[9] Abel, Suchitra, Xiao, Licheng and Wang, Hairong, "Data Security in the Scenario of Uncertainty," presentation at the 2018 BIDS Data Science Faire, Berkeley Institute for Data Science, UC Berkeley, CA, May 8, 2018.