Chapter 14
Deception Detection in Cyber Conflicts:
A Use Case for the Cybersecurity Strategy Formation Framework

Jim Q. Chen
DoD National Defense University, Washington D.C., USA

ABSTRACT

Deception is a strategy that has been widely used in cyber conflicts. How to detect deception in a timely manner is always a challenge, especially for a cyber commander who is at the point of making decisions with respect to the actual target to go after, the exact location of the target, the starting and ending time of a cyber operation, the type of cyber operation, the way of launching the cyber operation, and the amount of resources and support needed. It is absolutely important for a cyber commander to know for sure that he/she is not deceived by an adversary so he/she will be able to make right decisions. Varied solutions do exist. However, they are either too narrow or too broad. The solutions represented by signature technology are narrow in scope, so that they are not capable of dealing with the deception that they have not handled before. The solutions represented by behavioral analysis are relatively broad, so that they require extra time to re-adjust their focuses, incorporate contextual information, and combine heterogeneous data resources in order to get to what is exactly needed. In addition, the use of contexts in analysis is at random and not in a systematic way in most cases. Even when contexts are included in analysis, their relations with the relevant events are not well explored in all these solutions. To address these issues, this paper proposes a new strategic and systematic solution applying the Operational-Level Cybersecurity Strategy Formation Framework. This new solution employs purpose analysis, contextual analysis, and risk analysis. A case study is provided to test the effectiveness of this solution in detecting deception in a timely manner. The benefits and limitations of this solution are discussed. The capabilities of the Operational-Level Cybersecurity Strategy Formation Framework are evidently proved via this use case.

DOI: 10.4018/978-1-7998-2466-4.ch014

INTRODUCTION

Cyber deception is a strategy that has been widely used in cyber conflict. How to detect it in a timely manner is always a challenge.

Caddell (2004) defines two criteria for deception in general: "first, it is intentional; and second, it is designed to gain an advantage for the practitioner". He further makes a distinction between two forms of deception in the economic and political arenas, i.e. fabrication and manipulation. He states, "If false information is created and presented as true, this is fabrication." "Manipulation, on the other hand, is the use of information which is technically true, but is being presented out of context in order to create a false implication." These two forms of deception also exist in the cyberspace. A hacker may create a piece of malware, attach it to a seemingly innocent email, and send the email to a specific group of potential victims. An ignorant user of the group may open the email and click the attached file. Immediately, the user's system is infected with the malware. This is an example of spear phishing. It is also an example of fabrication in cyberspace. A hacker may also inject a true error message for one application into another irrelevant environment, say another application. Every time when the second application is activated and runs normally, that error message pops up on the screen, confusing the ignorant user and making the application seemingly unusable. This is an example of manipulation. How can these forms of deception be detected in a timely manner? This is the challenge that we are facing.

Besides, Caddell (2004) puts deception into active and passive categories. He states, "Put simply, passive deception is designed to hide real intentions and capabilities from an adversary. You are hiding something which really exists. Active deception, on the other hand, is the process of providing an adversary with evidence of intentions and capabilities which you do not, in fact, possess. Here you are showing your enemy something which is not real." In cyberspace, a honeypot is a good example of passive deception on the defense side. A honeypot appears to be a regular system, but it contains extra functionalities, such as logging the attack pattern of an attacker and collecting the attack evidence for prosecution. The use of an appropriate indicator of mutual exclusion (MUTEX) to confuse a zero-day worm in its propagation is a good example of active deception on the defense side. Having seen the indicator, the worm may stop its infection process as it considers the system being infected already. This method helps defenders to gain some valuable time in figuring out an effective countermeasure.

To deal with deceptions, Caddell (2004) suggests understanding the "enemy's intentions and capabilities" and "never relying on a limited number of sources of information or a limited number of collection methodologies". He notes that "the more one knows, the harder it is for someone to manipulate information out of context. The more one knows, the more likely one will detect a fabrication". However, he argues, "A comprehensive methodology for dealing with deception will never be written", as "it is nebulous and ever changing field of virtually infinite proportion". "We can never be confident we are not being deceived."

Rowe (2004a) also discusses different types of deception. He argues for the use of deception in defending information systems "as a second line of defense when access controls have been breached on those systems". He considers honeypots and honeynets developed by the Honeynet Project (2002) as "a simple passive form of deception". He scrutinizes other researches on deception methods such as Barber and Kim (2001)'s work, Carofiglio, deRosis, and Castelfranchi's work (2001), and considers them as being "good at identifying categories of effect but do not explain how deception occurs". He proposes a deeper theory of deception "developed from semantic cases of computational linguistics" initiated by Fillmore's case grammar theory (1968). Rowe's claim is "deception operates on an action to change