Chapter XLVIII
Taxonomy for Computer Security Incidents

Stefan Kiltz
Otto-von-Guericke University Magdeburg, Germany

Andreas Lang
Otto-von-Guericke University Magdeburg, Germany

Jana Dittmann
Otto-von-Guericke University Magdeburg, Germany

ABSTRACT

The adaptation and extension is necessary to apply the CERT-taxonomy to malware in order to categorise the threat (e.g., Trojan horses, Viruses etc.) as a basis for countermeasures. For the adaptation of the taxonomy to include malware a new entry in the tools section is needed (malicious software). This entry will cover the Trojan horses mentioned earlier. The proposed extension of the CERT-taxonomy will include the attacker-model, the vulnerability and the objectives. Within the attacker-model a new entry should be added, the security scan. This type of penetration testing by security-experts is similar to the works done by 'white hat'- hackers. However, such penetration testing is done by contractors on request, within strict margins concerning ethics and the assessment of potential damages before such testing takes place. The objectives within the CERT-taxonomy need a supplement, the security evaluation. This of course is the addition necessary to complement the introduction of the security scan. A very important vulnerability, social engineering, should be added to the taxonomy as well. It describes a very effective way to attack an IT-System. Two types can be distinguished, social engineering with the use of computers (e.g. e-mail content, phishing) and social engineering using human-based methods (e.g. dumpster diving, impostors).

INTRODUCTION

Since its introduction in 1998 in Howard and Longstaff (1998), the *CERT-taxonomy* for computer security incidents has been a very useful tool in finding a common language to describe computer security-related incidents. This ability to use a standardized language can be of great use, especially in situations where swift action is required (e.g., during incident response actions).

The authors propose a couple of extensions to this taxonomy, in order to adapt it to the environment that is found in the field of computer security today. Although the general nature of computer security incidents has not changed much, the proposed extension seems necessary to cover a new range of malicious tools, techniques, and motivations for an attack on a computer system or network.

BACKGROUND

The taxonomy was created in order to standardize the terminology used when dealing with incidents. It is useful for computer *security* incidents; *safety* aspects are not yet considered.

Safety deals mostly with incidents that appear at random or are caused by negligence or natural events. They often relate to material damage on physical objects. Security, however, is interested in malicious attacks against mostly immaterial entities like information, such as stored data.

Using the taxonomy, computer- and network security-related incidents can be reconstructed precisely and measures needed to be taken to remedy the situation can be discussed.

MAIN THRUST OF THE CHAPTER

The CERT-Taxonomy

The taxonomy was published in Howard and Longstaff (1998). Its objective was to provide a common language for security experts when dealing with security-related incidents. Their taxonomy classifies a computer security-related incident into the event, the attack, and the whole incident. It lists several items in the categories of attacker, tool, vulnerability, action, target, result, and objective.

The incident, therefore, includes the attacker, the objectives, as well as the attack itself. This attack is then divided into the tools used, the exploited vulnerability, the event, and the (unauthorized) result. The event consists of the action taken and target of the attack. The taxonomy can be interpreted as follows: An attacker using certain tools on a known vulnerability of a computer system that enables him to perform actions on a target. The outcome is the unauthorized result that allows the attacker to achieve his objectives.

It shows that the actual event is only a part of the whole incident. To fully understand the incident, the whole chain of the taxonomy has to be considered. For it can be vital to look at the attacker as well as the objective; this allows for conclusions to be drawn for similar events. Certain characteristics can be considered, for instance, a hacker will most likely leave the system after a successfully breaking in, where as a spy is most likely to gather as much data as possible.

The Attacker

Certain known types of attackers are listed here. Some subcategories can be formed (e.g., the so-called white-hat hackers or the black-hat hackers). Politically or monetarily motivated attackers can be considered highly dangerous who often stop at nothing to achieve their objectives.

The Tools

The taxonomy tries to classify the tools used for a computer security incident. As can be seen in the picture, the tools range from physical access up to *distributed attack tools* (e.g., to be used distributed denial of service attacks).

The Vulnerability

Vulnerabilities are used by exploiters. The hardest one to remedy is design vulnerability, as it can only be overcome by employing a new design, which in turn implies a new implementation. Vulnerabilities based on a false implementation of a correct design are likely to be fixed more easily. Although configuration vulnerabilities do not imply a redesign or r-implementation, fixing them (e.g., in a complex networked environment) is of a nontrivial nature.