Towards a Classification of Intrusion Strength

Yusuf M Motara <g00m2420@campus.ru.ac.za> *Rhodes University*
Barry Irwin <b.irwin@ru.ac.za> *Rhodes University*

***Abstract*— This paper proposes a new term, "intrusion strength", for use by the security community and those affected by compromised systems. It justifies the usefulness of such a term, proposes a preliminary ranking of intrusion strength factors, and concludes by mentioning the work necessary to create a full taxonomy of intrusion strength.**

I. Introduction

WHILST many can agree that an intrusion into a system is an extremely unfortunate event, it is more difficult to find agreement on how serious such an event is, especially in an environment incorporating heterogenous operating platforms. An attacker may leave instantly, having only wanted to see whether he could penetrate the system; the system could be used to attack other systems that it has a trust relationship with; or it could be compromised extensively by means of a rootkit or some similar subterfuge. These are only some of the possible outcomes of an intrusion[3].

We propose a classification of how strong a given intrusion is based on the degree of compromise over time that an attacker has obtained. We also propose the term "intrusion strength" as a useful addition to security field terminology. Both the definition of intrusion strength and its usefulness are examined in due course.

II. Intrusion Strength

Strength may be defined as "degree of potency of effect"[1]. Using this as our basic definition, we can see that any measure of the intrusion's effect can be used to define the strength of the intrusion. However, in this paper we choose to mostly disregard the effect that the intrusion has on a given organization. There are two reasons for this:

1) If two systems are attacked, and exactly the same amount of damage is done to each, then those two should logically be classified at the same level of intrusion strength. To *not* have this happen would lead to a situation wherein any classification becomes entirely subjective.
2) We do not deny that many systems exist within an organizational context, and that the organizational context is important. However, it is also a complicating factor in the classification of intrusion strength and, as a simplification, we feel justified in removing it from this discussion.

Intrusion strength may be seen as an indication of how damaging, over the long term, a given intrusion is to a system. Given the definition of "strength", we understand that intrusion strength is a matter of degree, and this is why we state that it should be assessed over time. Intrusion strength can be based on a number of factors; primary factors identified are listed below.

A. Persistence

Following in the footsteps of Catuogno and Visconti[1], [2], we define a *weak* compromise as one that is easily defeated by a reboot; that is, a compromise that is temporary and has no lasting ill effects. A *strong* intrusion is one that compromises a system over a period of time, or turns a previous weak compromise into a strong one.

In other words, one measure of intrusion strength is the persistence of the intrusion. Persistence gives some indication as to the access level than an intruder has obtained, in the case of a strong intrusion: this can be seen by the placement of files left on the system, or the extent of changes made to the system configuration. This measure also takes into account the amount of effort required by an attacker to reexploit the system: if the intrusion is weak, then the system must be continually reexploited; if it is strong, then one successful intrusion will be sufficient.

B. Damage

Intrusion strength can be assessed on the basis of how much damage is done to a system. The extent of the damage done refers to the number of files altered or deleted, the type and severity of system configuration changes, and other such malicious acts. It does not refer to organizational damage, such as the copying or deletion of documents: it is exclusively a measure of damage to the functioning of essential software.

The damage done to a system gives some indication (but not necessarily a good indication: see II-C) of how much work needs to be done in order to restore the system to a fully-functioning state. Furthermore, it indicates the level of privilege that an intruder was able to obtain: an intruder with the privileges of an ordinary user is able to cause far less damage than an intruder with the privileges of an administrator. For these reasons alone, damage done should clearly be assessed after a successful intrusion.

C. Repair Cost

Repair cost is related to damage in that it is a measure of the resources required to fix the damage caused by a given intrusion. However, it is not *directly* related to damage since it takes into consideration the difficulty of replacing or recreating organizational files that have been removed. For example, a system that is badly damaged may be fixed at a very low repair cost by an automated reinstallation of the operating system and associated utility programs; however, a lightly damaged system that has simply had several important documents wiped out may have a repair cost that is orders of magnitude greater.

The assistance of the National Research Foundation (NRF), the Deutscher Akademischer Austausch Dienst (DAAD), and the Telkom Center of Excellence (CoE) is gratefully acknowledged and appreciated.

[1]Merriam-Webster Online, *http://www.m-w.com/*

D. System Criticality

This refers to the importance of a system in an organizational context. For example, a web-based business may count their web-server as a "critical" system, whereas an accounting firm may count it as a subsidiary system. It is assumed that the more critical a system is, the more intrusion strength will be required to breach it; therefore, system criticality is a reasonable measure of intrusion strength.

However, the truth of the matter is that system criticality has little to do with intrusion strength since certain critical systems (such as a web server) must be exposed to the public, and certain others (such as an internal file-server) may not be. Compromising the former, given its public nature, seems easier than compromising the latter; in addition, the assumption that the more critical a system, the more protected it is can demonstrably be shown to not always hold true.

E. System Location

Many organizations have several layers of network indirection that protect the core network. This leads to a DMZ that the outside world is allowed to see, and is frequently used to keep an intranet (or several intranets) out of direct contact with the internet. Consequently it is more difficult for an intruder to gain access to an intranet system than it is for him to gain access to a system directly connected to the internet; therefore, we may say that the deeper within such a network a system is located, the more difficult it is to reach.

III. Classification

Having discussed some methods for determining intrusion strength, we now propose a system for classifying intrusions according to intrusion strength.

Characteristic	Explanation	Indicates
Persistence	How enduring	Compromise duration, access level obtained
Damage	How destructive	Access level obtained
Repair Cost	How costly	No. of resources required
System Criticality	How disruptive	Amount of work disrupted
System Location	How extensive	No. of systems compromised

Table 1: Comparison of Intrusion Strength factors

Referring back to our discussion of "strength" (see II), we can see that persistence and damage are the two main factors to be considered, with persistence being more indicative of intrusion strength than damage. Repair cost and system criticality are indicators of organizational disruption rather than intrusion strength[2]; they are useful to assess on a per-organizational basis, but only manage to skew any attempt to create an objective classification for a given intrusion. Lastly, system location refers to the extent of a compromise in a networked situation and is not useful when determining the intrusion strength used to compromise a single machine.

[2]However, the temporal component of repair cost may be valuable to assess since strength is a matter of *degree*

Though it is beyond the scope of this paper to create even a semi-complete taxonomy of intrusions, it is evident that certain factors must be weighted as more relevant than others.

IV. Usefulness

A term is useless unless it promotes greater clarity of communication between participants in a discussion. It is therefore important to examine whether intrusion strength does promote such clarity.

Firstly, it is important to note that the term is *practical*, by which we mean that (given an appropriate set of commonly-available tools) the intrusion strength can be readily determined after an intrusion has occurred, and the actions that are taken following an intrusion may be determined on the basis of intrusion strength. The intrusion strength for any two machines compromised should be approximately the same, which means that an organization may be able to set down policy guidelines that specify which actions should be taken in the event of a compromise.

Secondly, "intrusion strength" is general enough to cover all intrusions, no matter the device type or platform. The factors that relate to intrusion strength are also all factors that require discussion whenever a break-in occurs. Having a single term that is general enough to refer to any intrusion and specific enough to allow comparisons to be made between intrusions is worth consideration.

Lastly, there is some benefit in creating a taxonomy of intrusion strength so that security discussions can focus more readily on how to deal with a particular intrusion strength value rather than discussing each factor individually. This would cut down on redundancies in such discussions: for example, it may not be necessary to discuss the specific level of access obtained as this could be inferred from the intrusion strength category alone.

V. Conclusion

It is clear that more work needs to be done on the subject of intrusion strength to clarify and more narrowly define the term. We have defined intrusion strength, presented factors that may contribute to it,

More research should also be undertaken to select additional important factors, if any, that may have an impact on intrusion strength. What has been presented in this paper is merely a proposal to create terminology that is relevant and useful to security-related discussions.

References

[1] Luigi Catuogno and Ivan Visconti. A Format-Independent Architecture for Run-Time Integrity Checking of Executable Code. In *Proceedings of the Third Conference on Security in Communication Networks*. Dipartimento di Informatica ed Applicazioni, Universita di Salerno, September 2002. Available: http://libeccio.dia.unisa.it/wlf/scn02/index.html.

[2] Luigi Catuogno and Ivan Visconti. An Architecture for Kernel-Level Verification of Executables at Run Time. *The Computer Journal*, 47(5), September 2004.

[3] Ed Skoudis and Lenny Zeltser. *Malware: Fighting Malicious Code*. Prentice Hall, November 2003.

Yusuf Moosa Motara is currently reading for his Masters degree at Rhodes University, South Africa, in the area of computer security.