Intrusion Tolerance to Mitigate Attacks that Persist

Arun Sood
Professor (Computer Science) and Co-Director International Cyber Center
George Mason University, Fairfax, VA
asood@gmu.edu

The variety and complexity of cyber attacks is increasing, and so are the numbers of successful intrusions to mission and business systems. Recent breach reports show that intruders were in the system for long periods. For example, in Network Solutions\(^1\) compromise reported in mid-2009 the compromise was detected after 2 months; Wyndham Hotels\(^2\) reported compromise detection in February 2010 and the bad guys were in the system since October 2009. So we conclude that not only did the IDS/IPS fail to prevent the intrusion, these systems were not able to detect the presence of the intruder after the compromise.

Intrusion detection is a hard problem, and current cyber defense systems reportedly detect 40% of the malware. Verizon Business Data Breach Investigations Report\(^3\) underscores this problem by noting that only 11% of the compromises were detected in minutes or hours: 22% were detected in days, 37% were detected in months and 7% in years. Thus, the current cyber defenses cannot protect against customized malware and other zero day attacks and once an attack is successful, it can persist for many weeks. Any strategy that will mitigate the effects of the attack would be useful, and if the breach duration is reduced it would lead to reduced losses.

Motivated by the above observations, the focus of our research has been on methods to address two important issues to enhance cyber defense. First, we recognize that intrusion detection is a hard problem, and intrusions are inevitable.

---

1\ http://about.networksolutions.com/site/data-security-alert-problem-fix-and-customers-notified/
2\ http://www.wyndhamworldwide.com/customer_care/data-claim.cfm
Hence, we ask is it possible to work through a successful intrusion? Can we address the problem by shifting our focus to containing the losses that result from an intrusion? If this strategy is successful, we anticipate, that the demands on the IDS will be reduced and this in turn will lead to fewer false alarms (false positives). This has the potential of reducing the security operations cost. We note that in this scenario our solution is looked at as another layer of defense that works with the intrusion detection system. The overall system is more effective than each of the parts. In fact, the potential synergy leads to a system that is more effective than the sum of the parts.

Secondly, we focus on reducing the costs that result from an intrusion. We have to achieve this goal in spite of the fact that intrusion detection is a hard problem. Thus, our objective is to achieve this reduction without relying on IDS systems. The key question is – what do we have to give up? In our approach, we stipulate that providing an upper bound on the time between compromise and recovery has many advantages. For example, for the crown jewels we would like to keep the upper bound as low as possible. To achieve this goal we note that our strategy cannot assume that we will be able to detect either the intrusion attempt or the compromise.

We have developed an intrusion tolerance approach that explicitly addresses these two issues. We have built systems where the duration of the compromise is upper bounded at 1 minute. Our approach has the side effect of reducing the time between detection and recovery. We note that the above cited Verizon study shows that for more than 85% of the cases the recovery process took days, weeks, months and even years.
**Self Cleansing Intrusion Tolerance**

In a series of papers\(^4\), we have introduced a new approach to this problem – Self Cleansing Intrusion Tolerance (SCIT). Our basic premise is to reduce the exposure time of the servers to the internet. SCIT servers reduce losses because of intrusions by making the exploitation of vulnerabilities more difficult by limiting the effective exposure time of the server to the internet. We have achieved sub-minute exposure time for servers without service interruption. SCIT supplements existing security approaches, thus augmenting the value of existing investments. SCIT servers provide (1) threat independence, and (2) mission resilience, while (3) automatically recovering from a successful intrusion.

**How SCIT Technology Works**

Using virtualization technology, SCIT rotates pristine virtual servers and applications every sixty seconds or less. In the graphic, five online virtual servers (shown in red) are processing transactions while three offline servers are being cleaned and restored to a pristine state. The online servers are assumed compromised the instant they are brought online. Every cycle a pristine “green” server is swapped out with a “red” server and the SCIT process begins again, seamlessly without effecting overall performance.

The SCIT approach converts static sitting duck servers into dynamic systems. This strategy has the advantage of avoiding some failures, and in the case of a failure, there is a fast recovery mechanism. In our approach, we do not rely on failure detection.

\(^4\) www.scitlabs.com
Benefits of SCIT

SCIT technology mitigates two kinds of faults – (1) faults that result because of external malicious activity, and (2) faults because of inadvertent software or configuration errors. In the cyber security context, we deal with malicious activity often leading to a successful intrusion. Our intrusion tolerance approach discussed above addresses these faults. However, SCIT is also useful for operational resilience to protect against progressive failures – these failures are not visible in the short term but lead to reduced performance with aging or even a system crash. Because our approach restores the system performance every rotation cycle, it leads to higher service availability. This, in turn, reduces the redundancy requirements of server farms and consequently, the overall cost. The SCIT technology has the following advantages:

Cyber Security Benefits

Using the rotation and swapping strategy of SCIT servers removes malware every rotation cycle. This malware deletion does not require detection. This strategy effectively leads to automatic recovery from website defacement or software deletion attacks. Effectively SCIT reduces the time between compromise detection and recovery to the rotation time. In addition, when the SCITized servers are supported by network or host IDS, the system reduces data exfiltration.

Operational Resilience Benefits

SCIT rotation strategy facilitates the application of patches without rebooting the server. This property also has the potential for fast recovery from bad patches. In some cases, this ability for fast recovery has the potential for reducing the regression testing typically used to validate a patch. The SCIT rotation strategy also protects against progressive faults, i.e. faults that accumulate and become visible with increasing time or increasing users, etc. Memory leaks are one
example of a progressive fault. SCIT rotations eliminate memory leak induced performance degradation or even system crashes.