Response to NTIA RIN 0660-XC018
Stakeholder Engagement on Cybersecurity in the Digital Environment

by

John E. Savage
Computer Science Department
Brown University
John_Savage@brown.edu, 401-863-7600

Introduction

Security vulnerabilities in computer systems are unavoidable. An attacker who is able to exploit such vulnerabilities can compromise their operation.

Networks depend on communication between computers. Rogue agents can use their computers or those that they have compromised to interfere with the expected behavior of communication protocols and disrupt communication networks. Denial-of-service attacks are examples of such misuse. Below we list some security challenges that are likely to benefit from multistakeholder evaluation.

Disruption of Computer Host Exploitation (CHE) Campaigns

A CHE campaign begins by finding and exploiting a security vulnerability. Not only it is very difficult to design hardware and software that does not contain security vulnerabilities, no testing procedure can be constructed to guarantee that no such vulnerabilities are present. Thus uncertainty concerning the presence of vulnerabilities is a permanent condition of computer hardware and software.

Several well-known steps should be taken to protect against exploitation of *host security vulnerabilities*. They include firewalls, antivirus detection, intrusion detection, data loss protection, application whitelisting, and IP address blacklisting. They can also include experimental techniques such as automated diversity.

We propose to add **state restoration** to this list, that is, restoring the state of hardware and software to a known good state. State restoration will not fix vulnerabilities but it will eliminate malware that has been injected into software. It is highly unlikely to do the same for firmware, although that might be addressed by replacing firmware with non-writable firmware.

The exploitation of host vulnerabilities is a component in a campaign, which typically involves reconnaissance, injection of a remote access tool, lateral movement to find lucrative targets, data collection and exfiltration, etc. Such campaigns are time-consuming. If state restoration is used, a campaign will be disrupted. To restore it will typically require work by an attacker. Although an attacker can use knowledge acquired on previous penetrations to make later penetrations easier, if a disruption occurs frequently enough, the attacker may be discouraged enough to look for an easier target.

State restoration is another name for the concept of SteadyState that has been available in the past from Microsoft as a utility. It cached all changes to the system to a file, which were discarded on reboot, restoring the machine to its original state. Commercial solutions from other companies are now available.

State restoration appears to be sufficiently valuable that it should be explored by the security community, its pluses and minuses assessed, and a decision made as to whether to include it in the repertoire of security solutions. The conditions under which it might be recommended need to be identified.

I. The computer science community should debate the feasibility and desirability of partial and complete state restorations.
II. Good solutions to this problem have the potential to significantly improve computer security.
III. A discussion of several hours combined with design experiments offline should help to understand the issues this approach presents.
IV. Actionable outcomes could consist of new architectural designs and products offering a variety of more and less complete restoration and recommendations for their use depending on security needs.
V. Several vendors offer clients the option of state restoration.

Related Issues

Botnet mitigation can profit greatly from state restoration. If computer owners were to do state restoration when then are sleeping or absent, botnets would be more difficult to maintain.

The **Internet of Things** will be marked by the proliferation of inexpensive computers for which manufacturers will have little to no incentive to update faulty software. Since compromised computers can be harvested and used in DDoS attacks, manufacturers must be encouraged to invoke state restoration periodically.

State restoration is a stopgap measure. Combined with **upgrades** of firmware and software, it can lead to a gradual improvement in computer security. To make this happen will require the installation of a system for the **secure distribution of upgrades**. For such a system to materialize, demand for it must be created along with support for an infrastructure to implement it. This is an opportunity for an effective public/private partnership.

Policing the Internet

DNS resolvers that are openly accessible to users outside the ISPs hosting these servers can be used in DDoS reflection attacks. To avoid such misuse, ISPs should be encouraged by local governments to make these resolvers inaccessible to outsiders. Similarly, governments can cooperate in ensuring that their domestic autonomous systems do not make false BGP announcements. Since the number of such ASes is small, policing them should be feasible.

International cooperation will be necessary to police the web in this fashion. Nation states have a common interest in reducing the influence of radicalized elements in their midst, such as terrorists. Using terrorism as a vehicle, perhaps nation states can be persuaded to do the mundane policing of the Internet that will increase its security.

Algorithmic Denial of Service Attacks

Algorithmic denial of service attacks occur whenever an attacker finds a way to make a host computer do more work than anticipated by a designer. Such attacks have been demonstrated against a web server that uses a known deterministic hashing algorithm (Bernstein's hash function) to hash gets and puts to provide a fixed length internal name for them. These attacks are likely to grow in importance. Awareness of them can help designers to avoid problems with them.