Brannon McGraw

Business Proposal

**Overview**

Overseer is a bold advancement in computer security that addresses the technological advances made by computer hackers. Overseer provides all of the tools necessary to prevent attacks and to quarantine any computers that are infected with malware, trojans, or viruses. Ponderously expensive products that exist today are being overtaken even by unsophisticated attackers, because attackers are now moving faster than security experts. Security analysts are being stretched to their limit to provide band-aid solutions for an ever-increasing onslaught of attacks. With Overseer, system defenders have the advantage. In order to acknowledge the capabilities of modern attackers, Overseer combines the strength of a typical IDS with the stealth of virtualization.

The key to Overseer is virtualization, which hides the security tools and scanners that modern malware attempts to detect. If a virus or other malware is able to correctly identify what security a system is using, they obtain an incredibly important strategic advantage in planning an attack against the system. Virtualization allows us to encapsulate the entire system and interact with it externally. This makes Overseer functionally invisible from the point of view of an attacker. Although there do exist indirect methods for an attacker to infer the existence of an external security system, there is still very little that the malware can do to undermine Overseer's effectiveness.

Because Overseer runs “beneath” the virtual machine in what is known as the Hypervisor, it has a huge amount of flexibility in controlling the underlying system. Overseer can, for instance, freeze a single program that it suspects may be harboring malware. While the suspected program is analyzed, a user can still interact with the rest of the computer without being at risk from the suspicious program. Similarly, we can selectively interfere with the ability of malware to communicate with a central server while allowing a user to continue to leverage use of the network.

For its primary method of intrusion detection, Overseer uses consistency checks to known safe states of running programs. While a program is running, there is a section of memory for the code of the program. It is a common attack vector for malware to overwrite the code section of a program and usurp control. Under normal operation, the code section of a program's memory should not alter. This is an easy indicator of compromise that can be used to signal to Overseer that the system is being attacked.

When such a detection is made, Overseer will generate an incident report through the logger which gathers important information on the nature of the potential attack. With the use of a decompiler, Overseer can attempt to automatically determine if the change observed was the shellcode of an attack. All incidents and incident responses can be audited if there is a suspicion of malfeasance, addressing the issue potential attacks from internal sources. A system administrator can reverse the decision made by Overseer in an incident, but they cannot forge a fake report of an event or hide the changes they make to the system's security.

The robust logging performed by Overseer is especially important in a corporate setting, where the rich data offered by Overseer's logger can be used to generate evidence in the company's favor in the case that an attack on the company results in a lawsuit. Overseer's logs can be used to prove or disprove actual loss (e.g. of credit card numbers or trade secrets) from an attack.

Overseer's network-restricting capabilities are another key factor in loss prevention for a corporate setting; Overseer locks down network communications if it suspects the system has been compromised. This prevents successful malware from leaking sensitive information and hinders its ability to propagate through other workstations.

**Business Proposal**

Practically every company these days exists to some extent in the digital world. It's accepted as a given that a company should have security procedures to protect the company's assets, but too often these procedures neglect the digital sphere or underestimate its importance. The more sensitive information that a company has, the more critical a product like Overseer is to ensuring total security. You wouldn't leave the front doors to a convenience store unlocked, but companies are becoming increasingly aware that (from the perspective of an attacker) the “front door” to the company's digital existence is wide open.

The market for Overseer is enormous—even companies that use modern anti-malware solutions can benefit from the additional security that Overseer can provide. Because Overseer is extremely extensible, it can suit a wide range of needs from individuals to large companies with hundreds of workstations to secure. Overseer fits perfectly with companies and individuals that already use the power of the cloud and virtual workstations, but it is easily implemented on systems with only physical workstations.

The market has craved a product like Overseer for when system security is paramount. The market is saturated with IDS products, but they are usually too watered down to provide the security necessary in the rapidly changing ecosystem of cyberspace. Overseer will be the first commercially viable virtualized IDS, which provides the stealth of a network-based IDS combined with the strength of a host-based IDS.

Because Overseer can be used by individuals as well as enterprise systems, I plan on releasing the single-user version for free, in order to gain market prominence. As users secure their systems with Overseer, the strength of the brand increases and becomes more reputable. This encourages companies to become early adopters, which generates profit through enterprise subscriptions. Because Overseer is a constantly evolving project, yearly subscriptions will fund further development. This sort of software is highly sought, and few competitors exist. Overseer can immediately begin to generate revenue, and provides a useful tool to optimize the work of system administrators. Overseer's administrative interface has a suite of powerful tools that perform memory analysis, examine incident logs, and fine-tune the security settings of the system, including network permissions and firewall whitelists.

The competition to Overseer is a set of subscription-based IDS/IPS rules for malware detection. This is typically coupled with a dedicated security analyst who manually audits memory changes and firewall hits. This solution is not only expensive, it is very time-consuming and unnecessarily involved. Advanced threats typically persist on a corporate network for *years* before a malware analyst is able to detect its presence and begin removing the threat. In this time, an attacker could gain access to classified documents, customer bank information, or trade secrets.

Competing products rely on manual analysis to prevent and detect the worst intrusions, but they don't provide the same integration with analyst tools. These products progress slowly, in part because they have to maintain rulesets for many different operating systems and configurations. Because Overseer is virtualized, many different systems can be protected with a few tweaks to the configuration.

As cloud computing becomes more popular, securing assets on virtual machines becomes more and more critical. Current products treat virtual and physical systems as the same, ignoring the power and stealth provided by bringing the IDS out of the machine into the hypervisor. Overseer can maintain a competitive advantage by boldly exploring the potential of virtual systems.

As Overseer gains popularity amongst individual users and companies, the strength of Overseer's modularity truly shines. A security analyst can interact with a single instance of Overseer with the same ease as managing an entire network of protected workstations. Overseer automatically has configurations set up for custom internal network permissions and external communication protocols. If a system is under attack, Overseer has a network channel safe from attack that can be used to coordinate network-wide quarantine and malware eradication. Because Overseer is polymorphic (constantly adapting to current conditions), most of the focus of development after the initial rollout will be for performance and optimization. This ensures minimal disruption from the overhead that any IDS imposes on the system.

Overseer is, however, in a very experimental stage currently. Early attempts at IDS virtualization have failed due to the difficulty of providing machine introspection (getting useful information to protect the system while existing outsize of the workstation). Other attempts have had entirely too much overhead to be responsive enough for standard users. Although security is touted as being of critical importance, in reality they often forgo such measures in the interest of speed and responsiveness. As virtualized computers become more standard, there will be more comprehensive libraries for interacting with virtual machines and accessing information from the machine on a level necessary for security analysis. Even Overseer can't be made to be a feasible consumer product today, with each year advances are made in computing that can make Overseer faster and more accurate.

With that in mind, Overseer should seek to take the market now rather than later. Eventually, a product that works on the same principle of Overseer is bound to emerge from a large computer security firm. Our competition now is focused on software it considers “safe”; we have a unique opportunity to introduce something new and innovative enough to drastically change the landscape of computer security.

**Social Impact**

If Overseer was a commonplace solution for providing system security, malware developers would be dealt a blow many would struggle to recover from. Think of Overseer as being akin to a home security system: if a burglar can see that you are being protected by company X, they can revise their approach to first subvert company X's security, then invade your home while the security is disabled. By contrast, Overseer is an invisible security system that can even trap the burglars inside a portion of the house until police can arrive. Even just the *possibility* that a computer may be secured with Overseer can be a powerful deterrent that most low-level attackers would balk from.

Specially crafted malware could potentially penetrate Overseer (no IDS can have perfect performance, especially against top-level attackers), but even successful attacks can be rendered useless by Overseer's powerful network control. When even successful attacks on a system are nullified, hackers no longer see a profit to their activities. If hackers no longer have a financial incentive to craft new malware, the ecosystem of malware developers could collapse or see a dramatic shift in structure.

For every one malware developer that actively produces new attacks, there are hundreds of low-level attackers called script kiddies (or “skiddies”) that simply use the attacks already developed and given to them. This results in a very bottom-heavy organization structure that is easily disrupted by removing very few of high-level threats. If Overseer is widely adopted, some high-level hackers may focus their efforts elsewhere, effectively stopping many thousands of attacks before they even begin!

One of the more exciting prospects to entertain if Overseer becomes widely used is the ability for community involvement. Overseer is built to be modular and extensible, with industry-standard I/O specifications. If an aspect of Overseer doesn't work well for one set of customers, they can develop and use a modified version. For instance, some users may wish to perform annual audits of their security logs. Although Overseer may not initially have the ability to perform the audit in the same format as the users desire, they may develop and release their own log auditing plugin that can be used by anyone. In this way, development of Overseer can be diffused over dozens or even hundreds of developers, each contributing a relatively small amount of code while collectively making huge improvements.

Because Overseer is a system defense program, there is no way to weaponize the project—an attacker cannot repurpose Overseer to perform attacks or lock a user out of their own workstation. The default settings of Overseer are appropriate for a wide array of needs, so the average user has no need to have the technical knowledge necessary to configure an IDS. For those that do wish to manually interact with Overseer, the controls are straight-forward, high-level, and powerful. From the administrative control panel, a user can quickly freeze or unfreeze a suspicious program, add new programs to watch, or even send the system into paranoid mode, which closely inspects and restricts all network access. Parents can use Overseer as a safeguard to ensure their child's online experience is safe and age-appropriate with a set of widely-available networking rules.

Even should attackers have the source code of Overseer leaked, there are few avenues of attack against a virtualized IDS—even knowing exactly how Overseer works doesn't significantly simplify an attacker's task. Because of the structure and setup of Overseer, it is impossible to install Overseer on a workstation that you don't own, eliminating the ability for individuals to put Overseer to unethical use. Overall, many groups stand to benefit from Overseer, while only exploiters, hackers, and other attackers are negatively affected.