

Security Through Obscurity

By Nathan Ouellette

The sheer overload of information delivered through cell phones, PDAs, laptops, desktops, and other devices has created an environment in which many users are more technically savvy than in years past. While this can be viewed as a positive change, it also translates into an increasing internal threat within the corporate environment, which needs to be addressed.

As IT and information security professionals, we are bearing witness to an age of ever-increasing information overload. The ease with which information is obtained and exchanged has empowered the corporate user and the general public alike. The sheer overload of information delivered through cell phones, PDAs, laptops, desktops, and other devices has created an environment in which many users are more technically savvy than in years past. While this can be viewed as a positive change, it also translates into an increasing internal threat within the corporate environment, which needs to be addressed.

Most information security professionals, though aware the number of attacks at the perimeter remains high, would agree that the greatest threat to information assets comes from within. For example, the empowered casual user, or even the knowledgeable malicious user, can easily obtain information from various sources on ways to browse the corporate network to see what information is available. Users may not even know what they are looking for, but the sheer possibility that hosts are visible on a given network is enough to increase the risk associated with this behavior.

From an external standpoint, this casual browsing has even received a boost from the proliferation of wireless hotspots around most major cities through the use of default vendor settings and automatic wireless access point (WAP) associations. Even though policy may clearly state the ramifications of unauthorized access to any given system, we need now more than ever the controls to protect against such a threat.

The example of a casual user unknowingly connecting to a WAP helps us see that certain fundamental elements of information security are still not being addressed. One fundamental principle is to ensure that users only have access to the information or assets they need to have access to. In today's complex corporate environments, users have more identities than ever before. They are accessing more applications from more locations, and using multiple trusted and

untrusted assets to do so. The end goal of ensuring the principle of least privilege is not achieved through any silver bullet, but is a culmination of security best practices that ultimately lead to what I refer to as "security through obscurity."

Security through obscurity is a concept that has been used for centuries, largely in the military. Eastern literature based on military principles often reveals tactics used to conceal one's identity

It is true that a show of massive force can be used to intimidate an opponent, but the principles of stealth and invisibility have been used throughout history to help solidify one's own position on the battlefield, no matter how large or small that area may be.

or motive. It is true that a show of massive force can be used to intimidate an opponent, but the principles of stealth and invisibility have been used throughout history to help solidify one's own position on the battlefield, no matter how large or small that area may be. A parallel may easily be drawn to information security in the sense that invisibility and stealth in any operation are closely related to securing the availability of the resources as well as the integrity and confidentiality of the tasks themselves.

These principles have been employed over the years not only by defenders, but by attackers as well. In information security, no matter what the motive is, we all wish to secure our objective by any

means possible. For example, the black hat uses a basic brute-force attack from the Internet, attempting to cover his or her tracks by using reliable proxy servers to employ a degree of anonymity. The defender employs hardened perimeter access control devices with specific rules for filtering in order to appear stealthy, and dissuade the attacker from probing further.

From a business perspective, the principles of security through obscurity appear even more critical. An organization need lack only a few fundamental best-practice controls in order to afford end users an unobstructed path to critical hosts. A common flaw in the architecture of certain organizations is the hardened shell coupled with the soft underbelly. That is, the same philosophy used to secure the perimeter is not used to secure the internal LAN/WAN environment.

This common security posture becomes obvious in the comparison of physical security controls with technical or administrative controls. Facilities that house critical data are often secured by physical controls such as gated access, guards, proxy cards for the data center, and other sound best-practice implementations. Yet the very applications that are protected physically are exposed virtually, as we can see by examining a related grouping of missing countermeasures. Many networks fail to segment off the end-user population from critical server environments with host-based or IP-based access control. These devices are always implemented at the perimeter, but are not as prevalent on the inside. Where this common architecture is coupled with a lack of policy enforcement on the desktop, and minimal URL/content filtering, end users have unfettered access to download scripts and tools which can be used against any critical hosts clearly visible on the network.

Countermeasures for protection

There are several countermeasures that can help mitigate potential vulnerabilities, minimize the potential threat to critical information assets, and institute a fundamental practice of obscuring assets from prying eyes. However, implementing security controls and making decisions about managing risk should always be based on fundamental risk assessments. No program should lean too heavily in either direction when addressing the balance of business objectives against security.

The list below includes many best-practice items that can help achieve security through obscurity. This is by no means a comprehensive list of every security countermeasure that will aid you in this objective. It is merely a sample of some of the most common techniques.

Identity Management (IdM)

Applying role-based access control is a fundamental step to ensuring the principle of least privilege within an organization. Least privilege is ultimately the foundation and precursor to achieving security through obscurity. Properly managing identities and provisioning users for only the systems and resources they need access to is the first step. Conversely, timely deprovisioning of users from systems they no longer need access to is dually important.

Data classification

A clear and concise data classification scheme should be applied to all assets within the organization. With such a scheme in place, all future decisions regarding security for information assets can then be based on the criticality. This not only helps with decisions in regard to granting access, but it also helps save time by avoiding the

application of controls that might not be appropriate for the type of data that's being secured.

Access control

Once users are properly provisioned to applications and repositories by using roles within the company, using access control devices can appropriately enforce the same philosophy from a network perspective. Implementing granular access control between network segments is becoming increasingly popular as security decision-makers realize that firewalls are no longer just for the perimeter. Granular access control is also becoming increasingly cost-effective through the convergence of switch and firewall technologies.

Naming conventions

Logical and physical naming conventions can offer effective ways to thwart potential attacks. Administrators should be able to use standard naming conventions that provide a way to identify their devices, but which at the same time avoid obvious names that may reflect an administrator's role. For example, you would not want to give your primary financial database server the host name "Accounting." Attackers and casual browsers alike will be drawn to keywords when searching for hosts.

Access control devices are no exception. Firewalls should not be named as such; avoid obvious acronyms and abbreviations such as "FW" or common brand references such as "NG" or "PX." Effective naming of your devices within an internally recognized scheme helps provide obscurity from an external or non-IT entity, yet it makes perfect sense to those who need to know. This adds an extra layer of protection by masking a device's function from either the network browser or anyone who happens to walk by the rack in a data center.

Conclusion

In the final analysis, security through obscurity is not a new concept. The items that were previously mentioned aren't part of any new radical way of approaching security. Many security professionals understand that these items comprise a great way to protect information assets and are imperative to any approach that involves layered security.

However, the principle of obscurity is simply a way to allow subjective stakeholders to view their own posture objectively. Putting yourself in the eyes of the malicious or casual user allows you to see your own network from their perspective. The way that your assets are viewed on the wire is an important mechanism to help prioritize security projects and remediation efforts. The end result is a security posture that is much improved by implementing some key foundational best-practice items without breaking the bank in terms of capital expenditures.

About the Author

Nathan Ouellette, CISSP, is a senior information security consultant with Aon Consulting.