The Future is Grey

An Introduction to Unmanaged Systems Problem Resolution

Draft 0.4

Erick Engelke
Engineering Computing
University of Waterloo

Introduction

Computer viruses and vulnerabilities are being discovered at ever increasing rates. There are two solutions to control the threats they pose: good management to reduce the risk of exposure, and quick cleanup of infected systems before they bring down other systems or risk loss or exposure of user data.

Computers in managed campus environments (such as Ads and Nexus) are usually safe because teams of professionals tend to them regularly, updating the operating system, applications and antivirus definitions when vulnerabilities are discovered. Staff can mitigate risks in large numbers of machines using automated delivery systems, so the process is very efficient and scalable.

Computers living outside these managed environments are more prone to attacks, and result in significant staff time spent finding, diagnosing and fixing these systems. The cost to the university in staff time per unmanaged system is significantly greater than the cost per similar managed system. Much of this effort could be avoided if we could convince these users to use an antivirus product and automatically download Microsoft OS patches.

Client managed computers in offices, laptops and the residences are all sources of security problems.

In the four months leading up to this writing, there were 4,600 security warnings issued by IST, approximately 1150 per month, 38 per day.

Designation	Warnings Issued	% of Total	Average Per Day
Residences	2031	44 %	17
Wireless	750	16 %	6
Wired Offices	1819	40 %	15

One of the factors keeping the wireless numbers somewhat manageable was the introduction of MinUWet, a UW-written security agent which frisks laptops once per week before allowing access to our wireless environment. It uses technology to see if the computer meets our profile of an acceptable system: that there is an up-to-date antivirus client, and to ensure the laptop receives Microsoft Windows patches.

Computers which pass MinUWet's tests are rewarded with unfettered network access. Computers which fail are restricted to web-only access. Rewards and consequences help guide our users to responsible system management.

A more detailed description of MinUWet can be found at http://www.eng.uwaterloo.ca/~erick/presentations/06wirelesscanheit.pdf .

We continue to observe wireless threats despite the presence of MinUWet. We expect MinUWet to catch most problems, but the presence of a well-intentioned loophole appears to be the main source of wireless security threats.

When MinUWet was introduced, we decided to retain some minimal internet access for computers which either failed MinUWet or whose users decided not to run MinUWet.

This minimal service is necessary so that users can download antivirus updates from their providers. In effect, we left enough access that any laptop could be fixed by the user to pass MinUWet, and thus become a fully functional client on our wireless again.

Some users know that their systems always fail MinUWet, or they are suspicious of our tool, so they choose not to run MinUWet. These few laptops generate almost all of the observed wireless security issues.

For both wireless and wired environments, staff try to contact owners of compromised systems by Email and inform them of the need to fix their computers. Often this Email is ignored, perhaps because the user is suspicious of possibly fraudulent Email claiming to be from administrators (technically known as phishing).

After enough unheeded warnings, frustrated staff sometimes *blacklist* the user or laptop, meaning that future wireless access is denied until the user contacts an appropriate help desk to indicate the problem is resolved. Even then, users frequently claim resolution although the threat has never been adequately addressed.

Security warnings remain frequent, we are at risk of attacks and time is unnecessarily spent trying to track down and fix computers. The problem is not manageable today, and current methods will not scale for expected growth.

Greylisting

In June 2006, an experimental *greylisting* feature was added to MinUWet and deployed for Engineering wireless systems. Unlike blacklisting, the resolution can be achieved entirely by the user and requires almost no staff effort.

If we can harness the concept of self-remediation, we will improve reliability of campus systems, and reduce all the risks to the client owned machines, all while decreasing staff effort. This strategy scales well.

To implement greylisting on our wireless, we will still grant web-only access to those who fail or do not run MinUWet. This is our good faith that the client system is not an immediate security threat and to enable easy user-initiated updates.

However, if a computer is issued an important security warning, this indicates the machine poses a risk to itself and to others. We simply do not want these machines on our network until the risk is mitigated.

We have a system administrator inspect the automated warning to rule out possible false positives. If the warning seems important, the system administrator simply adds the computer or user to a list called our greylist.

Subsequent attempts by the user to log onto our wireless environment are issued a general statement about security problems and the user is directed to a web page which explains how to fix most systems in five easy steps.

The laptop is also restricted to only the minimal network access to complete these steps, rendering the system almost useless for any normal network activity.

The user can complete the steps unassisted in about 20 minutes, or they can seek assistance at a help desk or from a friend.

Upon completion of the steps, the user is required to run MinUWet. A passing grade restores full network access. Failure leaves the system with almost no network access.

There are several key points to the greylist strategy.

- It only affects users whose systems represent real security threats.
- There are real consequences for ignoring our warnings.
- The user becomes focused on fixing the problem.
- Security risks are removed from our networks.
- Staff time is used more efficiently.
- Users can fix their systems without assistance, including when help desks are closed for the day or weekend.
- The solution can scale with anticipated laptop growth

We are concerned that users will be cut off the network, but it will only be those whose systems represent a risk to the campus and to themselves.

What is particularly appealing is that these concepts and most of the technology could also be applied to wired systems. Since we are currently averaging more than 1150 security warnings per month, we should further investigate this strategy to decrease that number, the associated staff time and ultimately user risks.