360 IS

information Security

Perspectives Q2/07

There are over 10 million Skype users online at any point in time, most people only have 20 buddies on their whitelist.

There are 236000 items of malware in existence, yet most people need less than 10 applications.

In 10 years you might have Email correspondence with a few hundred people out of tens of millions of Internet users.

The Growing Trend Of Security Whitelists

There is a developing trend among security professionals, tired of being trapped in a continuous cycle of virus signature updates and anti-spam tuning. The Whitelist approach promises to break this cycle by proscribing any and all activities that are not expressly permitted. An "activity" might be the opening a file, the execution of an application, or perhaps the acceptance of an Email. Those of you who have been around network security for long enough will recognise this as the "default deny" strategy long adopted by Firewall administrators to combat the tidal wave of "bad" network traffic that accompanied widespread Internet adoption in the early 1990's. The alternative to a whitelist is a blacklist, a list of all the bad things you don't want to happen, all the viruses, all the spam Email senders, all the network protocols you don't need, all the instant message users you don't want to talk to. The trouble with blacklists, is that they get very large or are incomplete (or both). Fortunately there are some very clear signs that an area of IT security is ripe for the whitelist approach:

Are you are constantly in a reactive mode, scrambling for patches and signatures, updating lists of "bad things" on a regular basis?

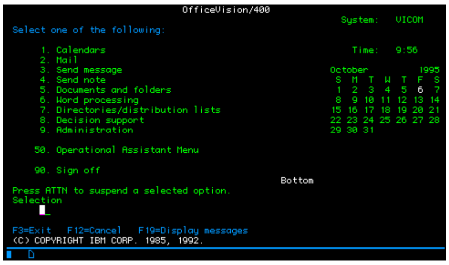
Is the amount of undesirable "stuff" far greater than the amount of good "stuff"? Stuff being applications, Emails, network protocols, or messages.

Have you been disappointed time after time by vendor's promises of fixes, always coming "in the next version" or "with the new update".

Although "whitelists" or buddylists within Instant Messaging are ubiquitous, and one hopes that Firewalls are deployed in a "default deny" mode, application whitelisting is still the subject of some debate. In a way this is surprising because application whitelisting isn't new. It was once common for mainframe and minicomputer administrators to make only certain applications available to members of particular user groups. Originally driven by the high cost of licenses and scarcity of hardware capacity, the welcome side effect was that ordinary users could not install and run anything the administrator had not expressly sanctioned.

Application Whitelisting Today

Today the Microsoft desktop is king and people expect to see a general purpose-computing environments, not text menus. Application whitelisting software resides on the desktop PC as a sort of shim between the operating system and the executable code you are attempting to run. If the target application, executable or macro is on the whitelist for that user then it runs as normal. If not then execution is prevented and an error message can be displayed. My application whitelist only has about 10 items in it, plus some essential OS components. Virus executables cannot run, Email attachments will not execute, and I can't install (inadvertently or deliberately) any toolbars, unlicensed software, or malware. Of course whitelisting cant fix everything, if your operating system has a vulnerability in it like a buffer overflow, whitelisting will not fix that flawed OS, but it can stop execution of applications on the disk (such as a rootkit) that further exploit your system. Increasingly we are recommending whitelisting to companies running large numbers of similar or identical Microsoft desktops, who are suffering a high cost of user support due to the installation and execution of non-business-critical software by their users.



```
                              OfficeVision/400
                                                        System:   VICOM
 Select one of the following:

     1. Calendars                                         Time:   9:56
     2. Mail
     3. Send message                                   October        1995
     4. Send note                                       S  M  T  W  T  F  S
     5. Documents and folders                           1  2  3  4  5  6  7
     6. Word processing                                 8  9 10 11 12 13 14
     7. Directories/distribution lists                 15 16 17 18 19 20 21
     8. Decision support                               22 23 24 25 26 27 28
     9. Administration                                 29 30 31

    50. Operational Assistant Menu

    90. Sign off
                                             Bottom
 Press ATTN to suspend a selected option.
 Selection
     _

 F3=Exit   F12=Cancel   F19=Display messages
 (C) COPYRIGHT IBM CORP. 1985, 1992.
```

IBM OfficeVision/400, users were not offered the option of "pressing 10 to run a virus or 11 to install a spyware toolbar". Those mainframe/mini guys had this licked years ago!