Hal Berghel

Better-Than-Nothing Security Practices

Security for general audiences.

There are a number of different digital security models recommended by professionals and organizations in the information security business, including time-based security, principle of least privilege, defense-in-depth, baseline security, perimeter hardening, intrusion detection, and intrusion prevention. All of these models attempt to circumscribe and quantify some measure of risk as the function of real or potential vulnerabilities and threats.

To illustrate the difference in strategies, consider time-based security (TBS) and the principle of least privilege (POLP). Time-based security uses time as the primary measure of risk. On this account, our safety margin increases with advance warning. As long as our advance warning exceeds the sum of the detection and response times, we should remain protected. The greater the difference, the greater the safety margin.

Conversely, the principle of least privilege relies on controls. POLP holds that security varies inversely with the degree of control given an application or user. The idea comes from physical security—the employees have keys to their desks, the supervisor has the sub-master for their area of authority, and the general manager has the master keys.

Perhaps the most visual reinforcement of POLP in the digital world for many of us is found in the task manager of Windows Vista. You may have noticed that in XP/2003 services and applications ran at the same priority level as the local user who invoked them; if the user were logged in as administrator, the invoked services and applications ran at the highest level—Session ID=0. This is a breach of the POLP, since most of the applications do not need to run at that level. This leads to the infamous "shatter" attacks against Windows. In Vista, only the kernel Windows services run at Session ID=0; user-invoked services and applications always start at a lower (non-0) level. This particular implementation of POLP falls under the rubric of "service hardening." Curious readers can easily verify POLP presence in Vista and absence in XP within Task Manager (press <CTL-ALT-DEL> and enable "Session ID column" from "view").

There are organizations that promote specific security standards, such as the Control Objectives for Information and related Technology (COBIT), the Federal Information System Controls Audit Manual (FISCAM), the

SERGE BLOCH

Certified Information Systems Auditors (CISA), the BSI 7799/ISO 17799/ISO 27001 standards for best practices, to name but a few. In each case, these standards map to government legislation or mandates, such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA), to provide standards by means of which one might determine compliance. A good overview of the issues is available in the NIST Handbook (see csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf).

The Better-Than-Nothing Security Practices Model

To enrich our security model landscape, I offer the following modest example: the "Better-Than-Nothing" Security Practices (BTNSP) model. I developed this model in the immediate post-Y2K time frame as a result of two simultaneous events: (1) Windows NT and 2000 were suffering from severe security vulnerabilities (buffer overflows, simple file sharing/"null session" attacks, NTLM password attacks, unauthorized guest account logins, elevated privilege hacks, and so forth); and (2) the innovation of administering security policy through Active Directory (AD) and domain controllers. Event (1) became an enormous and very costly problem, while (2) was both difficult to understand and nearly impossible to implement completely and correctly in the early years. Many of my clients asked for inexpensive partial solutions that didn't require retraining their IT staff, and my vision of a security model that was better than doing nothing sprang to life. I originally focused on XP.

1. Disable Simple File Sharing

1. Open "My Computer"
2. Open "Folder Options..." from the Tools menu
3. Click the "View" tab
4. In the Advanced Settings scroll menu, go to the bottom
5. Inspect the checkbox: Unchecking "Use simple file sharing (Recommended)" is more secure.

2. Change Access Privileges to Hard Drives

1. Make sure **Simple File Sharing is off** (above step)
2. Open "My Computer"
3. For each hard drive :
    1. Right Click on the drive
    2. Select Properties
    3. Click on the "Security" tab
    4. Click on the "Advanced" button
    5. Highlight the "Everyone" list item by clicking once on it
    6. It is most secure to click "Remove"
    7. Click OK to exit the Advanced Security Settings window
    8. Click OK to exit the drive properties window

Figure 1. Disabling file sharing and modifying hard drive access privileges.

Here's the way it worked. I would encourage clients to undertake some basic risk management assessment by assessing the cost and relevance of known threat vec-

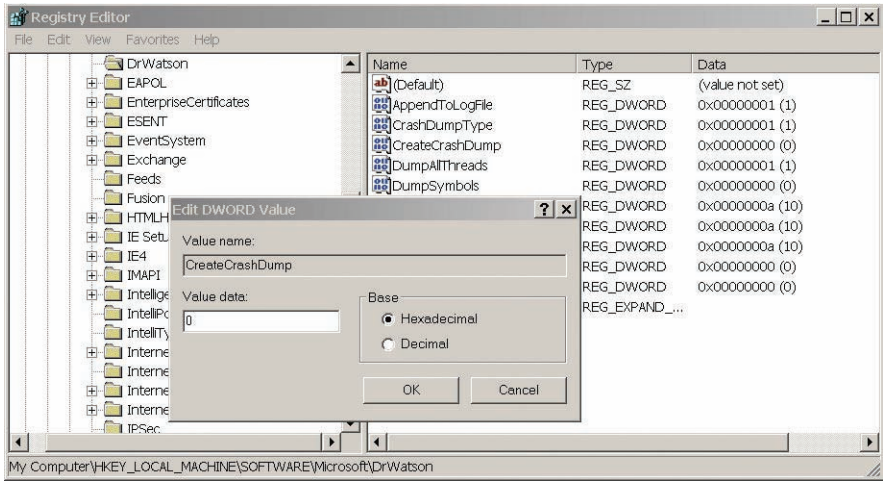

Figure 2. Instructions 1–6 of Figure 3 from the perspective of Registry Hive.

tors for their IT infrastructure. Then, I'd provide a spectrum of alternatives to mitigate this risk within their security policy, ranging from "make sure this vulnerability can't ever happen to me" to "try to avoid if it doesn't break anything." The clients could then pick and choose based on their own assessment.

1.	Start>Run...
2.	Type in "regedit" and click OK
3.	Navigate to HKEY_LOCAL_MACHINE> SOFTWARE> Microsoft> Windows NT> CurrentVersion> AeDebug
4.	Double Click on "Auto"
5.	Inspect the value. The most secure setting is to change the value to 0
6.	Click OK
7.	Navigate to HKEY_LOCAL_MACHINE> SOFTWARE> Microsoft> DrWatson>
8.	Double Click on "CreateCrashDump"
9.	Check the value. The most secure setting to change the value to 0 (should be set correctly by default on some systems—double check)
10.	Click OK
11.	Right Click on the Start Button
12.	Choose Explore
13.	Go to Documents and Settings>All Users>Shared Documents>DrWatson
14.	If found, it is more secure to delete User.dmp and Drwtsn32.log if found

Figure 3. How to prevent Dr. Watson from storing debugging files.

To illustrate, consider Windows simple file sharing. This service was originally enabled by default in Windows OSs. What are the implications of leaving this open? On the positive side, files and folders may be shared in networked workgroups. On the negative side, workgroup simple file sharing isn't part of the AD structure and access is not controlled. Thus, if one computer in the workgroup is compromised, all file shares on all computers in the workgroup that have simple file sharing enabled are also compromised—a serious problem for sensitive information. So, the spectrum runs from leave it on to shut it off. For those who needed some file sharing but with greater control, we encouraged them to consider using the Access Control List (ACL) feature that is available for every folder. This is a middle ground that may fall within the organization's comfort zone. The next step is to show the client how to accomplish this, so we offered the step-by-step instructions shown in Figure 1.

While this was a more labor-intensive approach to managing file sharing security through AD and a domain controller, it led to the same results: closing a security hole. For XP, I offered explanations and recommendations for a wide variety of security issues from password protection to disabling memory dumping and Dr. Watson. Figure 2 illustrates how one

URL PEARLS

Time-based security is presented in a book of the same name by Winn Schwartau. Information about COBIT is available at the ISACA Web site; www.isaca.org. FISCAM is promoted by the General Accounting Office; see www.gao.gov/special.pubs/ai12.19.6.pdf. CISA is an ISACA certification for information systems auditors at www.isaca.org/cisa.

The ISO/IEC 17799 standard (to be updated and renamed soon) is a popular international information security standard based on the earlier British Standards Institute 7799 standard. Details are available online at www.standardsdirect.org/iso17799.htm or iso17799.safemode.org, as well as the BSI and ISO Web sites at www.bsi-global.com/ and www.iso.org. C

The original motivation for BTNSP for XP to help organizations administer security through local security policy was replaced by their need for simple and useful security guides for other aspects of their IT infrastructure.

would implement the instructions shown in Figure 3 within the registry editor.

BTNSP Online

After the initial foray into XP security, I added BTNSP for Web browsers, 802.11 wireless infrastructures, and firewalls. I even added BTNSP for Linux and dabbled with the idea of RFID and Bluetooth, though I never got them ready for prime time. The same general interactive format was followed throughout. Of course, the computing and network world changes rapidly, so the original motivation for BTNSP for XP to help organizations administer security through local security policy was replaced by their need for simple and useful security guides for other aspects of their IT infrastructure. At this point, implementing security policy for entire domains through AD is the norm in the enterprise. However, BTNSP may provide a useful checklist for AD administrators, and it remains relevant for small home office and business users who do not have domain controllers.

While originally used only internally in my lab, and later by my clients, BTNSP is now available online via my Web site at www.berghel.net/btnsp. I hope you find Better-Than-Nothing Security Practices lives up to its name. C

Hal Berghel is associate dean of the Howard R. Hughes College of Engineering at the University of Nevada-Las Vegas, the director of the Center for Cybersecurity Research (ccr.i2.nscee.edu), and co-director of the Identity Theft and Financial Fraud Research and Operations Center (www.itffroc.org).

Coming Next Month in Communications

BEYOND SILICON: NEW COMPUTING PARADIGMS

Computer hardware has been dominated by silicon-based technology for over 40 years. However, new computing paradigms have emerged in recent years and while extensive practical use of these devices is yet to be seen, these ideas have stimulated the scientific community for their fundamental nature, novelty, and potential for new forms of information processing and applications. This special section will present an overview of these non-silicon-based paradigms, namely, atomic/molecular computing, quantum computing, optical, and micro/nanofluidic computing.

Also in September:

Parallel Computing on Each Desktop
Not All Interface Characteristics are Created Equal
Domain Expert User Development
What Really Matters When New IT is Introduced
SOX, Compliance, and Power Relationships
What's Wrong with Online Privacy Policies?