Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Users Wary of Microsoft's .NET

Everyone who uses a computer has heard of Internet security issues such as viruses, e-mail scams, and hacker attacks. Many computer users don't see the need for security or feel helpless in the face of hacker attacks. Both of these assumptions are false as will be discussed in this paper. This paper is written for non-technical computer users who need to know the security risks of the Internet and how to protect their important digital information.

Copyright SANS Institute
Author Retains Full Rights

AD

Users wary of Microsoft's .NET

By: Jeffrey Hudack

SANS GSEC Practical v1.2e

Every day more of our personal information is stored on digital media. Countless advertisers and retailers spend much their resources on identifying their target audience and gearing their products towards those desired individuals. Doctors keep files on your history, allowing them to access it quickly and efficiently. Financial institutions have massive databases outlining your entire financial history. The digital world is becoming a part of every aspect of our life, from oil changes to supermarket buying habits.

In some ways this progression is inevitable as technology is used to control, maintain and track various aspects of your life. The mass digital storage of information allow us to quickly access our data and extrapolate useful conclusion from our habits and schedules which allow us to work faster and more efficiently. Were all of this information contained in one database, the potential for technology to adapt itself to the user's lifestyle becomes possible, which is an enticing prospect.

Microsoft wants to bring it to this level with their .NET product line, bringing all of your data into a central repository where it can be accessed in its entirety at any time. Although this could be considered an inevitable step for technology, there are those who are concerned with the risks associated with this emerging technology model.

HailStorm

The first of Microsoft's .NET products to be announced is HailStorm, which will initially provide text messaging, automatic scheduling and online storage of personal files to its users. The goal, however, is to eventually have it hear and observe the user while they are in the office or at home, allowing it to wait until you are available before giving you messages.

The Microsoft white paper, "Building User-Centric Experiences, An Introduction to Microsoft HailStorm" gives the following description:

> The core HailStorm services use this architecture to manage such basic elements of a user's digital experience as a calendar, location, and profile information. Any solution using HailStorm can take advantage of these elements, saving the user from having to re-enter and redundantly store this information and saving every developer from having to create a unique system for these basic capabilities.

This capability, while increasing efficiency, also presents some serious concerns about security, privacy and availability. Many questions have been raised concerning Microsoft's ability to administer this complex system while maintaining the integrity of the data.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Due to the prevalence of Microsoft critics, it will be a long road to gaining acceptance of the Hailstorm product among the user community. However, the veracity with which these opponents analyze and criticize this software could be the deciding factor in providing for the necessary attention given to addressing problems and making sure they are eliminated in a timely and efficient manner. Without such opponents, Microsoft would be free to implement their product regardless of the readiness state, which would assuredly be an unwise decision.

Security

Security has long been a concern when creating Internet-based software. The prevalence of easy-to-use cracking tools has empowered those with little or no knowledge of their target to gain substantial power with minimal effort. Because of this fact, it is necessary to make sure your product will stand up to time when exposed to the skills of those who would wish to compromise it. When looking at this product, there are some points of vulnerability: data on the server, the client itself, IP traffic en route, and the users.

As it is the most recognizable name in the PC industry, it should come as no surprise that Microsoft is the #1 target for cracking attacks, ranging from Denial of Service to data theft. Although Microsoft has proven to be fairly secure so far when you consider the sheer number of attacks that must be mounted against them daily, once there exists a database of such massive proportions it is likely that some crackers will step up their efforts to gain access to it. The foundation for the entire .NET line of products is going to be trust; if the customer can not trust Microsoft to protect their data they will not use the product. It is therefore quite necessary that extra security precautions are taken to protect the .NET data store, such as large key length encryption and very limited access rights.

Client Woes

A large point of vulnerability lies at the client PC, which is not necessarily secured by the user properly. Through the use of keystroke logging, a would-be attacker could easily gain the information entered into the system, including any personal information disclosed. Also, it is feasible that a trojan virus could be created specifically for this product, gathering information from the client while it is logged in and forwarding it to the attacker. Such a virus could be distributed through e-mail, Java or ActiveX controls, or through any 'backdoors' introduced by this product. By allowing the HailStorm application to be accessed from anywhere the likelihood of a compromised PC being used increases considerably. Although there is little that can be done, aside from requiring certain updates, to address the vulnerabilities on the client machines, this should be taken into serious consideration if they wish to ensure the safety of the data submitted.

One possible solution would be to implement a software firewall using dynamic packet filtering as a part of the HailStorm product, moderately protecting the machine from unwanted data transfer and/or the compromise of the system. Although this is not a complete solution for the apparent security problems, it would provide a significant improvement over the current security implemented by the Windows operating system in its current state, allowing transmission of only traffic identified as 'acceptable'.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In Transit
The data transmission itself also presents a point of compromise that is out of the control of both the client and host. Were an attacker able to intercept data via a 'man in the middle' attack and decode the encryption, he/she could easily record, publish, or alter the data almost instantaneously. When you sending the names and addresses of contacts this may not be a major concern, but when dealing with credit cards and other sensitive information, it becomes mission critical, even life-threatening. Were a cracker able to alter your prescription data, for example, it could result in death or illness. Or, should the proposed camera and microphone interfaces exist, the cracker could 'hijack' the stream and use it to spy on the user. Once compromised, this product could act much like a Trojan virus, providing the attacker with a large amount of data to monitor or exploit the victim.

An obvious security measure would be the use of encryption. By encoding the data stream in an unreadable format, the attacker must first decrypt the data before he/she can identify and utilize the data. Although encryption can be very secure, many other such data obfuscation techniques that were thought to be unbreakable were eventually cracked as computing power increased exponentially. With this in mind, it would be a good idea to have the .NET line of products to allow for updates to the security model should the utilized encryption no longer be secure. This way, if Microsoft's encryption is broken, the vulnerability can be addressed with the release of a necessary security update.

User Beware
The largest security vulnerability, by far, is going to be the users themselves. Because the .NET system is based on a universal password it is going to be up to the end-users to protect that password, else open up their entire life to someone else. Lacking the proper knowledge most people do not recognize attempts to gain access to their system, be it a trojan placed through their DSL/cable modem or well-acted social engineering used to gain the password. Unlike an employer, Microsoft cannot feasibly educate all of their users on the threats to their security and how to protect against them. As a result, unknowing users could easily be tricked into sharing their user information, including the universal password. Once this password is compromised, all other lines of defense have been rendered useless.

By gaining access to credit cards, your spending habits, your address, your friends, and just about anything else the attacker wishes to know, they have, in effect, gained access to your life. A would-be stalker, credit card thief, or murderer could get everything they needed to commit their crime at the most opportune moment.

Privacy
So far, the largest point of contention against the centralized storing of user data is the level of privacy. Protection of data has become a highly publicized topic, creating warranted concern among the online community about misuse of personal data. There are even proposals in Congress to limit the collection and use of this data, which could feasibly limit Microsoft's .NET products before they are even made available.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Although Microsoft insists the data is stored only for your convenience, many are still skeptical, and for good reason. Even the Unites States Federal government, which strictly prohibits its web sites from collecting user information, has unknowingly been tracking users through use of cookies on sites such as NASA and the General Services Administration. In some cases, it is the large number of administered web sites make it difficult to effectively police them all for privacy violations.

In Microsoft's "white paper" outlining their Hailstorm product, they contend that the various applications we use make things more complicated, requiring multiple entries of the same data across several programs. In some ways this can be problem, leading to inefficiency unnecessary repetition. However, from a privacy perspective it is this separation between the personal data that provides us with a sense of control over the information we wish to share. By assembling all of this information in one location, the comfort level for the users is diminished by knowing that this information is easily assembled and abused. According to Scott Rosenberg of Salon.com, "Many of us worry less about having to learn a new set of rules every now and then than about the forbidding prospect of somebody assembling all that 'important data and personal information' into one cross-referenced master profile."

Availability

Once your data has been stored on the .NET servers it becomes necessary for this information to be available on demand. In the wake of their recent DNS failure, there is much concern about Microsoft's ability to maintain this database and make sure that it can be reached anytime, anywhere. With a business model revolving around 24-hour uptime, even a minor glitch can result in large amounts of lost business and revenue. It is quite likely that the cracker community will realize this and begin to target the .NET systems specifically.

It is likely that DOS attacks will become more commonplace, and perhaps even coordinated between multiple DDOS attacks for maximum efficiency. With this in mind, much thought should be given to finding ways to prevent these attacks and fix any discovered DOS vulnerabilities within in minutes of their publication. With Microsoft being a popular target, even the smallest vulnerability could lead to disaster for the entire .NET line should the integrity of customer data be compromised.

Accountability

With such a comprehensive store of data controlled solely by Microsoft, there are some well-founded worries about the use and integrity of the data held within. Even Microsoft has issued a Terms of Use agreement for the Microsoft Passport product, the software that provides for the communication between the various Hailstorm clients and the database, which allows them to delete, alter, or even sell data which they see fit without retribution. The following is an excerpt from the Terms of Use:

> MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY, RELIABILITY, AVAILABILITY, TIMELINESS, AND ACCURACY OF THE

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS CONTAINED ON OR OBTAINED THROUGH THE PASSPORT WEB SITE OR SERVICE FOR ANY PURPOSE. ALL SUCH INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

While such disclaimers are common practice, with such large amount of sensitive data are at stake many worry that Microsoft, by freeing themselves from liability of any sort, have invalidated the security and privacy necessary for such a robust system. Even if all of their data was irreparably damaged or changed, the user is powerless to pursue an action, legal or otherwise, to rectify the situation.

Vaporware?

Although Microsoft has, at its expense, a large amount of resources to put into this project, there is no way we can be sure the anticipated project will be finished on time with all of the proposed features. Since it has become almost commonplace to release software on a schedule before making sure many of the bugs and exploits have been worked out, there is a good chance this software will require quite a few patches before it is ready for trusted deployment. In environments where security and reliability are a must, the Hailstorm product may never actually become the central repository that Microsoft claims it will one day be.

The Next Step

Microsoft has long been the leading force in many of the innovations that have taken place in the software industry. Although such a centralized management system is a logical next step in collaborative software, one must wonder if Microsoft will take the risks involved seriously enough to make this a viable product that people can use without worry. To do this, it will be necessary to commit resources to security, privacy and availability before the product begins deployment. Should this product be rushed to market before proper security measures are taken Microsoft could be setting itself up for a public relations disaster and tarnish their image among their many users. With user trust being a primary component of this system, they can not afford to alienate those that may be seriously considering their product.

Hailstorm will usher in a new age of vendor responsibility for a product, one that should provide users with a new sense of trust in the technologies that may someday dictate our behavior and schedule. If done correctly, Microsoft stands the chance of extending their reach to the personal level, their software becoming the backbone of our highly-organized, schedule-driven society. Otherwise, it runs the risk of becoming yet another innovation that has been lost to poor implementation.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

List of References

Dudley, Brier. “Microsoft's 'HailStorm' service stirs up online privacy issues”. 8 April 2001. URL: http://archives.seattletimes.nwsource.com/cgi-bin/texis/web/vortex/display?slug=micrprivacy080&date=20010408 (19 June 2001).

Mearian, Lucas. “Government Still Guilty of Using Cookies”. 18 April 2001. URL: http://www.pcworld.com/news/article/0,aid,47703,00.asp (19 June 2001).

Microsoft Corporation. “Building User-Centric Experiences An Introduction to Microsoft HailStorm”. 11 June 2001. URL: http://www.microsoft.com/net/hailstorm.asp (19 June 2001).

Microsoft Corporation. “Microsoft Passport Web Site and Services Terms of Use and Notices”. 4 April 2001. URL: http://www.passport.com/Consumer/TermsOfUse.asp (19 June 2001).

Rosenberg, Scott. “Microsoft storm warning”. 28 March 2001. URL: http://www.salon.com/tech/col/rose/2001/03/28/hailstorm/index.html (19 June 2001).

© SANS Institute 2001, Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**