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.

First Step Data Capture - Key Stroke Loggers

Keystroke logging, depending on how it is implemented, can easily bypass the best host and network security, collecting valuable key information for use in later attacks or information gathering exercises. Keystroke logging through the data it captures can also remove the requirement to brute force attack encrypted information, as pass phrases are typed and then recorded by the logger in the clear. Keystroke logging has been around since the days of the first mini-computer systems and it is still effective today as a f...

Copyright SANS Institute
Author Retains Full Rights

AD

SANS Security Essentials
(GSEC)

First Step Data Capture – Key Stroke Loggers

Nigel Lewis
SANS Security Essentials Version 1.2E

© SANS Institute 2001, Author retains full rights

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

First Step Data Capture – Key Stroke Loggers

Abstract

The SANS GIAC course highlighted the importance of Confidentiality, Availability and Integrity. This paper reviews a very old but still popular and effective technique of breaching the confidentiality of key information such as userids, passwords and pass phrases.

Selection Criteria

Key stroke logging, depending on how it is implemented, can easily bypass the best host and network security, collecting valuable key information for use in later attacks or information gathering exercises. Key stroke logging through the data it captures can also remove the requirement to brute force attack encrypted information, as pass phrases are typed and then recorded by the logger in the clear.. Key stroke logging has been around since the days of the first mini-computer systems and it is still effective today as a first step data capture utility.

Main Text

Introduction

A few days ago, one of my work colleagues decided to play a practical joke on another, he purchased a wireless mouse and plugged the receiver into the PS2 port of the victim's notebook docking station. The victim for the rest of the day was tormented by the prankster.

The victim deduced incorrectly that someone was illegally remote controlling his notebook, via the network. The victim then took the appropriate security measures to identify and remove any illegal software. He removed the notebook from the network patched it to the latest security pack, ran various anti-virus software over it and vulnerability scanned it, but because the wireless mouse was recognised by the operating system and all detection software as a valid hardware device, no vulnerability, hack or virus was detected. He then returned the notebook to the network with network and application monitoring software running, and much to his dismay the mouse once again had a mind of its own.

By this time the rest of the section who were all fully aware of what was happening, and had been egging him on with all sorts of helpful suggestions on what to do to find the perpetrator/software, broke down into fits of laughter and revealed the transceiver. The victim, very red faced, had the good grace to acknowledge his situation as the butt of the joke and with those age-old words, "It'll be your turn next", proceeded to commence plotting his revenge.

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

As interesting and as entertaining as this occurrence was it made me think: regardless of the security measures that are put into place on the network and on the desktop, valuable information is still typed and presented in the clear. Needless to say that a keyboard and a computer screen would have to be monitored for a long time before even a fraction of the information available on the magnetic media could be recovered. But that said only a small amount of critical information needs to be captured before you have they keys to the kingdom. User names, passwords, pass phrases, crypto codes are all typed in the clear: if you can capture this information you can then have access to the rest of the data. This is called first step data capturing, where information is captured at point of entry, before it has a chance to be encrypted or lost.

Over the Shoulder and Under the Mouse Pad

The easiest and least technical method of intercepting small amounts of critical information such as user id's and passwords is via social engineering a situation, where a person can be observed entering the information you require into a keyboard. Many people will not ask for you to turn around or leave the room while the information is being entered, as they do not want to appear rude or distrustful. Those people that do ask you to turn around, general after the observer's initial turn devote their full attention to the keyboard to type the information in, allowing the observer to resume their watchful attention to the key strokes. Fortunately for this type of information capturing most people still can not touch type and still type relatively slowly allowing sufficient time for key strokes to be observed and remembered.

This attack suffers from a number of weaknesses, they are:

a. All key strokes must be remembered in the correct sequence which becomes increasingly difficult if a complex password or key phrase is entered,
b. One key stroke may be missed or obscured by the person entering the information,
c. The person may become suspicious of your observation and change the critical information,
d. You maybe interrupted or observed by a third party, and
e. You must make contact with the intended target which may raise suspicions.

Tucked away under the mouse pad, keyboard or some other desktop decoration, userids and passwords can still be found allowing easy recovery. Unfortunately for security staff this practise still goes on in most organisations.

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

Key Stroke Logging Techniques and Devices

Electronic Over the Shoulder

Another simple technical technique to observe keyboards and monitors is the careful placement of a camera or cameras. One or more properly positioned cameras can allow for all key entry to be captured and if necessary played back frame by frame or frozen so that correct key sequences can be captured. Multiple login and critical data entries can be observed increasing the accuracy of the targeted information. The monitor as well as the keyboard can be placed under surveillance allowing for confirmation of the application that the captured data is pertinent to. There are many types of small inconspicuous surveillance cameras, many have on board data storage and others transmit the information to receiver stations located elsewhere.

Disadvantages to this method are:

a. That access to the building must be obtained for placement of the camera(s),
b. Replacement of the storage media, if used,
c. If using transmitter based cameras, electrical interference may interfere with the signal; and
d. Discovery of the camera(s) may alert the target that they are under surveillance.

Advantages to this method are:

a. Small amount of technical skill is required,
b. Can be used as evidence, if correct and valid legal warrant has been issued, and
c. Easily defeats encryption systems as pass phrase are captured in the clear.
d. Links key stroke data to application if monitor is being captured as well.

Key Stroke Logging using Hardware

With the advances in encryption and the easy availability of free/shareware encryption products it is getting harder for law enforcement and other authorised groups to access criminal data. One way to by-pass the requirement to undertake a brute force attack, to decrypt the targeted data, is to capture the key strokes that make up the pass phrases.

Hardware key stroke loggers are attached between the keyboard port of the motherboard and the keyboard itself. Hardware loggers can work in two ways: the first is effectively eavesdropping, where the signal sent from the keyboard it is detected and recorded. The second is store and forward where the signal is received recorded and then forwarded to the motherboard. The delay introduced by both methods are so small as to be undetectable. Only careful observation of the keyboard cable may discover the hardware device, but the devices are made so innocuous they are easily overlooked. The hardware device can either store the information on board or transmit it via wireless technology to a receiving station. Unfortunately both

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

methods suffer problems, batteries and on board storage memory limit, which requires regular access to the device to correct.

While I was conducting research for the paper I found a good example, of hardware key stroke loggers being used by law enforcement in the United States of America (U.S.A.). The Federal Bureau of Investigations (FBI) used a hardware key stroke logger in the apprehension of an alleged criminal Nicodemo S. Scarfo. The FBI were aware that Nicodemo S. Scarfo Jr an alleged mobster was using sophisticated encryption products to protect his records on loansharking and bookmaking. Rather then trying to break the encryption, FBI surveillance agents accessed Scarfo's residence under a court order and installed an electronic device that allowed for the remote monitoring of his every keystroke. This device allowed them to record the critical pass phrases they required to be able to unencrypted the critical evidence[iiiiii] which was later used in court by the prosecution.

The hardware key stroke logging device that was used by the FBI in this case is now publicly available.

"Such a device is available through DSI Investigations and inquiries can be directed to us via email. …. Email us at jdallas@dallassecurity.com and we will email you details."[iv]

A number of other hardware key stroke capture and recording devices are also now commercially available and are listed at Annex A.

The advantages of hardware capture devices are:

a. Privileged accounts are not required for installation,
b. No change to the operating system or use of any system resources therefore undetectable by anti-virus and other security vulnerability/scanning software,
c. Easy to install, no technical skill required,
d. All key strokes captured and recorded,
e. Will also capture BIOS passwords before boot up,
f. Not susceptible to software upgrades,
g. Operating system independent.

The disadvantages are:

a. Limited storage, if onboard memory used, and
b. Access to the PC required for installation and data collection.

Software Key Stroke Capture

Software key loggers have been around for a long time: I remember while at high school in 1980, with a couple of other students writing a password capture program to run on a Vax 11/70 system. The first time we ran it, it only captured one login ID and password and it was fairly crude, it returned a standard error message to the user before automatically logging out of one of our accounts, but by the end of the year it was executing from a virtual terminal using a dummy account (to prevent being

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

tracing back to a specific terminal/user, we had already been caught by the sys admin that way once) and it automatically logged out and the logged the user into their own account after recording their userid/password.

Most software key stroke loggers these days are targeted at PC users, and these have some limitations. The software key stroke logger requires the installation process to be executed by a user who has create and modify permissions to the local C drive. Unfortunately for the DOS based operating systems, this is everyone but with newer operating systems such as NTFS and Linux, users can be restricted in their permissions on the C drive. Most well written software key stroke loggers will install without producing any memory conflicts, poorly written programs may cause memory conflicts that may give the user a clue that something is wrong. A number of software products are available to allow you to capture the key strokes, a summarised list of the ones I found via a quick web search are attached at Annex A.

An interesting example of the use of a software key storke logger, is where two Russian hackers were targeting U.S.A. financial institutions. The FBI identified the hackers and approached Russian authorities for assistance, the Russian authorities were less then helpful, so the FBI provided the Russian hackers with a utility that had a software key stroke logger embedded into it. Once the hackers executed the software the FBI were able to monitor every key stroke they made. By using this technique the FBI were able to locate the Russian server which contained all of the stolen information. The two hackers were eventually lured to the U.S.A where they were arrested.[v]

Software key stroke loggers store there data various ways:

a. by writing to a log file which is hidden away amongst valid systems files,
b. by emailing the key strokes to a pre-configured recipient, or
c. by embedding the key strokes into valid network protocol packets which are then transmitted to a target system.

Advantages of software key stroke loggers are:

a. Difficult to detect, unaided,
b. No physical device to be installed,
c. Can transmit the key strokes externally via the network, alleviating the requirement for physical visiting the site,
d. Can be deployed remotely,
e. Large selection of products available,
f. No limit on the size of log files, and
g. Proven technology.

Disadvantages of software key stroke loggers are:

a. May be detected by anti-virus programs or specialist key stroke logger detection programs.
b. Must be installed by a user with create and modify permissions.
c. May cause software conflicts if poorly written.
d. Cannot capture BIOS passwords

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

e. Technical skills maybe required for its deployment.
f. Operating system dependent.
g. If transmitting captured data by network maybe blocked by the firewall.

Malicious Software Key Stroke Loggers

A variation to the software key stroke logger is the Trojan program. A Trojan is generally not a virus as in the majority of cases it is unable to replicate itself. A Trojan is a malicious piece of software which is hidden in a valid system file. Most Trojans arrive via email and unsuspecting end users execute them and thereby install the Trojan software onto their systems. A large number of Trojans are written specifically to capture key strokes and send the results back to the Trojan master. An interesting article extract below describes the use of a Trojan Horse virus that captures key strokes and then emails the details back to a specified address.

"A Trojan Horse Virus has been found recently which captures key-strokes of unknowing computer users. Once this interior program is deployed it will record key-strokes of the individual that it is deployed against, and then e-mail the captured data back to the individual who deployed it. This Trojan Horse key-stroke capture program is installed and operates on a computer without the user's knowledge. The program can be activated when a user receives it as an attachment to e-mail and clicks on the attachment. Users who receive the Trojan Horse program may have no indication that it has infected their computers. Once deployed and active, this program can capture the user's private communications and is impervious to encryption."[vivii]

The web site http://net-security.virtualave.net/page11.html has a very comprehensive details on Trojans and a good list of Trojans including ports used.

Key Stroke Detection Programs[viii]

In the military there is a saying: if you build better armour someone will build a better bullet. There are a number of products on the market to detect key stroke logging programs, this includes all major anti-virus programs which will detect Trojan programs, as well as some specialist products such as AntiSnoop Password Dropper[ixx].

Conclusion

High grade encryption products are readily available on the Internet, and with the increase in security functionality on the basic operating systems it is becoming harder to access data either legally (with a warrant) or illegally. Key stroke loggers once again are becoming an essential tool for capturing primary data to allow access to the full data store. There is a proliferation of software key loggers available and also a small number of hardware key loggers. These loggers all perform the same basic function of recording each key stroke entered via the keyboard, but they can store and deliver the information to the perpetrator differently. Some software key stroke loggers send the key stroke to a log file while others can transmit the keystrokes out to

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

the Internet through different methods such as email, or buried within valid TCP/IP requests.

Most of the major virus scanning packages will detect the majority of Trojan key stroke loggers to various degrees and there are also speciality key logger detection packages available but unfortunately the only way to detect hardware key loggers is observation.

Due to its very nature as a first step data capture system, key logging is still one of the best methods for capturing userids, passwords and pass phrases.

© SANS Institute 2001, Author retains full rights

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

ANNEX A TO
GSEC ASSIGNMENT
DATED 14 AUG 2001

All information in this page has been **copied** directly from the web site referenced by the footnotes and is not original work. It is intended **for information only** and is not submitted as part of the assignment.

Software Key Stroke Loggers

Got your KeyStrokes! - 2.0 by Customized Computer Software

This application was developed as a tool for parental control, system administrators, corporate environments, or anywhere that it would be beneficial to have a log of what the user was doing on the computer system. Basically, the software is hidden from the user and records all keystrokes that were used within any program that was opened.[xi]

HackerWacker Advanced Edition - 9.25.0 by Streiff Information Services

Provides advanced sevices and features to monitor and log most user activity on your computer. This includes All URLS browsed, key stroke logging, and Active Window Logging. All logs can be optionally encrypted and also emailed to multiple destinations. Contains the Echelon Word System to define and flag strings or words you define. Includes Database support, for logging to a database source across your network or the Internet (MS access 2000 db included). Other features include screen captures, advanced security, stealth mode, inherited settings between users, and much more! Perfect for business, educators, administrators, parents, spouses, branch offices, and more. Volume discounts and other options available.[xii]

PC#Protect –

This stealth-type keystroke logger runs invisibly in the background, logging all keystrokes to an encrypted textfile. This is ideal for tracking the activities on your home and office computers for Web usage statistics and details.

ZDNet Software Library - Stealth Keyboard Interceptor Pro

Stealth Keyboard Interceptor Pro 01-04-99 ANNA Ltd.

Stealth Keyboard Interceptor Pro silently monitors your PC, intercepting keystrokes and saving them to a text-based .log file. The log is surprisingly complete, retrieving time/dates, application and dialog names, file names, pasted text, and keystroke actions. The result is a clear picture of all activity that has transpired on your PC. Users won't see the program in the task list, task bar, or system-tray area. For added security, you can choose to encrypt the log file.

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

A number of settings are available to customize the behaviour of the program: you can record mouse clicks, control keys, keyup events, keydown events, and more. An automatic scheduler is also available.

Although not well documented, Stealth Keyboard Interceptor Pro is easy to use and provides superb monitoring of your computer with no noticeable loss of performance.[xiii]

More

Tempest Phreaking[xiv]
Desktop Detective[xvxvi]
WinGuardian[xvii]
winadm - Freeware
007 Stealth Activity Monitor (SAM) - Shareware
KeyKey 2000 - Shareware [xviii]
Got your KeyStrokes – Shareware
DIRT[xix]
Invisible Activity Spy - Shareware[xx]
SILENT WATCH v.1.1[xxi]

Hardware Key Stroke Loggers

The KeyGhost Box

So here enters the "Sovereign" class starship of KeyLoggers. The KeyGhost. But this round, it's not software based. It's hardware based. The KeyGhost is a revolutionary product, a simple 30cm long cable with a white cylinder at the middle, that when is connected to a computer, LOGS EACH AND EVERY keystroke a user enters. And can spill it all on demand, Form the same terminal being monitored, or from a computer 50km away. All you need is a computer terminal with a PS/2 port and a text editor. No need for software. No need for external drivers, No need to to reboot computer. No need for any special action. Simply connecting the KeyGhost to a PS/2 Keyboard port will activate it. Allowing it to feed power from the host computer (no need for any external power connector, no need for a battery, no need for an outlet), and will quiltlly, in the background, without ever interfering with the computer operations, without taking any system recourses will start logging every keystroke the user enters. and in the end of the day, when the user begin monitored logs off from his terminal, thinking no one will ever get access to sensitive information, you walk by the computer, pull the KeyGhost from the PS/2 port. And take it home. Once you arrive,all you need to do connect it to your computer PS/2 port, go into a text editor, and type the default password. "Vghostlog" In a single word. Without making a backspace, and to your instant sense of gratification, the KeyGhost operation menu will open up inside the text editor.[xxii]

KEYKatcher

The KEYKatcher Monitors computer use in the home or the office and insures computer usage policy compliance. The KEYKatcher is a tiny recording device that

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

clips onto your keyboard cable. It's used to log keystrokes typed on the computer. It doesn't require any external power source and it installs in less than 10 seconds. The KEYKatcher records all keystrokes, and stores them in a non-volatile memory. Even if the device is unplugged, or your computer is turned off, the KEYKatcher will continue to store the information

[redacted]

© SANS Institute 2001, Author retains full rights

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

References:

[i] http://www.usatoday.com/life/cyber/tech/cti881.htm last accessed 17 Jul 01
[ii] http://irights.editthispage.com/discuss/msgReader$1047?mode=day last accessed 17 Jul 01
[iii] http://www.techlawjournal.com/alert/200012/20001206.asp last accessed 17 Jul 01
[iv] http://www.dallassecurity.com/Newsletters/Inquirer_Spring01/inquirer_spring01.html
[v] http://legalminds.lp.findlaw.com/list/intpil/ msg00296.html last accessed 17 Jul 01
[vi] http://newyork.fbi.gov/contact/fo/nyfo/fraudalert.htm last accessed 17 Jul 01
[vii] http://net-security.virtualave.net/page11.html last accessed 20 Jul 01
[viii] http://www.xblock.com/ last accessed 19 Jul 01
[ix] http://www.fileguru.com/security/security.asp last accessed 18 Jul 01
[x] http://www.pcworld.com.eg/protect_may2000.htm last accessed 20 Jul 01
[xi] http://www.downlinx.com/proghtml/232/23276.htm last accessed 17 Jul 01
http://www.code-it.com/security/got_em.htm last accessed 19 Jul 01
[xii] http://www.downlinx.com/proghtml/233/23311.htm
[xiii] http://icfcst.kiev.ua/panorama/OFM/index.shtml#Keystrokelogutilities
[xiv] http://www.webisers.com/investigations/Investigation/ucanhack.htm last accessed 17 Jul 01
[xv] http://www.yippee.net/html/win/utilities/title12598.htm last accessed 17 Jul 01
[xvi] http://www.electronickits.com/spy/finish/finish.htm last accessed 17 Jul 01
[xvii] http://www.webroot.com/wgresale8.htm last accessed 18 Jul 01
[xviii] http://www.supershareware.com/Apps/15681.asp last accessed 19 Jul 01
[xix] http://www.codexdatasystems.com/cdsnews.html last accessed 20 Jul 01
[xx] http://www.fileguru.com/security/security.asp last accessed 18 Jul 01
[xxi] http://twhk.com/Products_Adavi.htm last accessed 19 Jul 01
[xxii] http://www.geekvortex.f2s.com/reviews/keyghost/ last accessed 18 Jul 01

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

Last Updated: May 21st, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced