Profense SDK User Manual

Profense SDK is a professional software kit for fast developing of any kind of security applications for Microsoft Windows. Simple APIs of Profense SDK include powerful functions: multi layer packet filter (transport layer and channel layer), system services monitor (SDT monitor), IDT monitor, GDT monitor, LDT monitor, registry and filesystem access monitor, NT object manager monitor, filesystem filtering interface, executive objects monitor (processes and threads), executable objects monitor (executable images and sections), state-of-art hidden executive objects monitor (SMM based), abnormal activity monitor (SMM based), abnormal activity monitor (VMM based, including VMX & SVM interfaces), executive objects manipulation interface (using for hidden objects in-memory heuristic search), Patch Guard manipulation interface (using for internal purposes), interface for search of non-exported symbols in kernel environment, real-time instruction tracer interface (using for catching suspicious interception of system services), interface for heuristic detection of exploits (any kind of exploits, Trojans and viruses), IRP_MAJOR procedures monitor (using for proactive defense's purpose), hardware interrupt monitor (IRQ monitor, using for low-level control of system activity), journal and history logger interface (applicable to any kind of monitor), transport layer network monitor (TDI based filter), low-level network monitor (NDIS based), TcpIp protocol suite (using for avoiding any malicious interception of network traffic), driver – application communication interface (with two simultaneous channel type – Command channel and Data channel, which renders asynchronous interface to communicate with kernel modules), virtual address manipulation interface (search and enumeration of VAD list on per-process basis), finite state machine for behavior-based detection (proactive defense decision module), network firewall interface with flexible rule system (ALLOW/DENY/CONTENT_BLOCK/CONTENT_MODIFY methods on any active network interface).

Use Profense SDK to add proactive security capabilities to applications that will operate on the Internet to ensure that your application is safe from various attacks, and that once identified, an Intruder can be blocked from accessing the system on any level (including non-network vectors of attack), without incurring high CPU usage.

Supporting OS:

Windows 2000
Windows XP
Windows 2003 Server
Windows Vista
Windows 2008 Server
Windows 7

Supporting platforms:

IA-32
AMD-64
EM64T
IA-64 (request for quote)

Supporting containers:

Microsoft Visual Studio 6.0 and later
Microsoft Visual Basic 6.0 and later
Microsoft Visual C++ 6.0 and later
Microsoft Visual J++ 6.0 and later
Microsoft Office 97 and later
Microsoft Outlook
Borland C++ Builder 3 and later
Borland Delphi 3.0 and later

Features:

Application Programming Interface being encapsulated by DLL is simple and powerful.
Engine of SDK provide full range of a professional security suite functions, including, but not limited:

- Flexible system of vectors to implementation grants incredible ability for secure end user.
- Double layer packet filter (transport layer and channel layer) can manage and control data packets of all kinds network protocols quickly and correctly in safe manner;
- Supports filtering of packets both incoming (to the local machine) and outgoing (packets attempting to leave the local machine), including packets from kernel mode malicious modules and rootkits;
- Allows filters to be set up by specifying ranges of IPs and ports, by specific ranges of system points of interest, by specific behavior models and signatures. Behavior analysis allows detection and prevention measures against new malicious software (not known to antivirus vendors at the moment);
- Allows monitors to be set up to block all events by default, or to let all events pass by default;
- Multi-threaded design ensures that high rate of packets filtered does not interfere with the main thread of your application;
- Allows an access to packet filtering via an ActiveX component (can be used by any environment that can use an ActiveX component);
- Allows filtering and inline modifications on TCP, UDP, ICMP, and other protocols;
- Allows filters to be set up by specifying ranges of IPs and ports;
- Allows packet filters to be set up to block all traffic by default, or to let all traffic pass by default;
- Allows filtering of packets both incoming and outgoing;
- Multi-threaded design ensures that high rate of packets filtered does not interfere with the main thread of your application;
- Provides IP address identification for all local NIC cards (multi-homed);

Modules

Application layer interface module: PFSDK.DLL
Kernel mode helper module: pfsdk.sys
Kernel mode monitors:

- sdtmon.lib, sdtmon.h – SDT monitor module
- idtmon.lib, idtmon.h – IDT monitor module
- gdtmon.lib, gdtmon.h – GDT monitor module
- ldtmon.lib, ldtmon.h – LDT monitor module
- objproc.lib, objproc.h – NT object manager monitor module
- reg.lib, reg.h – registry & filesystem callback interface module
- fsmf.lib, fsmf.h – filesystem filtering interface(FilterManager) module
- psthr.lib, psthr.h – processes and threads monitor(PsNotify) module
- ccmgr.lib, ccmgr.h – cache manager load & run monitor module
- etm.lib, etm.h – external thread monitor (SMM) module
- vmm.lib, vmm.h – abnormal activity monitor (VMM) module
- smm.lib, smm.h – abnormal activity monitor (SMM) module
- objlist.lib, objlist.h – in-memory heuristic search for objects module
- pg.lib, pg.h – Patch Guard interface manipulation module
- sym.lib, sym.h – non-exported symbols resolver module
- trace.lib, trace.h – instruction tracer module
- nox.lib, nox.h – no exploit interface module
- irp.lib, irp.h – IRP_MAJOR procedures monitor module
- irq.lib, irq.h – IRQ handler monitor module
- log.lib, log.h – monitor logger module
- tdi.lib, tdi.h – transport layer network monitor module
- ndis.lib, ndis.h – NDIS layer network monitor module
- tcp.lib, tcp.h – TcpIp suite module
- link.lib, link.h – kernel – user communication interface module
- vad.lib, vad.h – virtual address descriptor interface module
- fsm.lib, fsm.h – decision finite state machine module

- netmon.lib, netmon.h – network filtering interface monitor
- sscan.lib, sscan.h – signature based scanner module
- pfsdk.lib, pfsdk.h – consolidated module

Profense API: PFAPI.DLL
PFAPI.h API C++ header
PFAPI.lib API C++ import library

How the engine of SDK Works

Profense SDK engine intercepts control flow of various points of interest in Windows OS kernel. Finite state machine control sequence of events on per-thread basis and make decision (if any behavior signature found). Filtering interface render ability for inline modification or blocking specified packets with defined patterns of data. Flexible system of rules renders ability for host intrusion prevention on system wide basis. Anti-exploit interface renders ability for prevention of execution and API offset resolving for any "run-not-from-image" code, including exploits, viruses and any other suspicious code. TcpIp protocol suite interface grants safe access to any remote resources, avoiding malicious interception. Registry and filesystem monitors of any kind grants full control on autorun sections of Windows Registry and filesystem. Signature based scanner grants detection for malicious software with known signatures (MD5 hash of PE sections). Behavior based signature scanner grants detection for malicious software with unknown signatures, by determined behavior. Application level library grants simple and easy interface to any type of application to full power of Profense SDK in easy way.

Mission of Profense SDK – grants ability for fast development of professional grade security products to any developer in any programming language (including VB, VBA, VB.NET, C#, C++, C).

Licensing Requirements

The component is licensed on a CPU basis, and is not Royalty Free. For each developer that will be developing concurrently with Profense SDK you must purchase one license. Each license allows one developer to develop with the SDK, as well as deploy the component on one (1) CPU. This means
that if you have one developer developing, and are deploying to a dual processor machine (or to two
separate machines), you must purchase two licenses. Similarly, if you have two developers developing
but are deploying to one CPU, you must still purchase two licenses. Corporate and Site Licenses are available. Please email sales@profense-sdk.com if you have any questions regarding pricing or licensing.
Licenses can be purchased securely online directly from our web site at www.profense-sdk.com. Licensing terms and conditions are as per the License Agreement.

License Agreement

PROFENSE SOFTWARE DEVELOPMENT KIT
END-USER LICENSE AGREEMENT

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and FXSEC LTD Software Team. For the software product identified above, which includes computer software and may include associated media, printed materials and «online» or electronic documentation («SOFTWARE PRODUCT»). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE.

This EULA grants you the following limited, non-exclusive rights:
Software Product. You may install and use one (1) copy of the SOFTWARE PRODUCT to design, develop, and test your software application ("Application"), and then you may deploy to 1 machine (computer). This constitutes one (1) license.

SAMPLE CODE. You may modify any sample source code located in the SOFTWARE PRODUCT's "samples" directories ("Sample Code") if provided, to design, develop, and test your Application. You may also reproduce and distribute the Sample Code in object code form only along with any modifications you make to the Sample Code, provided that you comply with the Deployment Requirements described below. For purposes of this section, "modifications" shall mean enhancements to the functionality of the Sample Code.

DEPLOYABLE CODE.

You may deploy SDK files ("Deployable Code") to one machine (computer). You may not otherwise copy or redistribute this code. This SOFTWARE PRODUCT is not royalty free.

DEPLOYMENT REQUIREMENTS.

You may deploy any Sample Code and/or Deployable Code to one machine (collectively "DEPLOYABLE COMPONENTS") as described above, provided that

(a) you deploy the DEPLOYABLE COMPONENTS only in conjunction with, and as a part of, your Application;

(b) your Application adds significant and primary functionality to the DEPLOYABLE COMPONENTS;

(c) you do not permit redistribution of the DEPLOYABLE COMPONENTS;

(d) any deployment of Deployable Code is only in conjunction with your Application and includes each and every file contained therein deployed as a single set. The SDK files may not be individually reproduced or distributed.;

(e) you include a valid copyright notice on your Application; and

(f) you agree to indemnify, hold harmless, and defend FXSEC LTD and it's distributors from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or deployment of your Application

(g) you do not use the same application names, filenames, or binary compilations as those that are deployed with the SOFTWARE PRODUCT

(h) any Sample Code or Deployable Code, whether enhanced and/or modified, may only be deployed in compiled form. FXSEC LTD reserves all rights not expressly granted to you.

2. COPYRIGHT.

All rights, title, and copyrights in and to the SOFTWARE PRODUCT (including, but not limited to, any names, images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT) and any copies of the SOFTWARE PRODUCT are owned by FXSEC LTD. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material, except that you may either

(a) make one copy of the SOFTWARE PRODUCT solely for backup or archival purposes, or

(b) install the SOFTWARE PRODUCT on a single computer, provided you keep the original solely for backup or archival purposes. You may not copy printed materials (if any) accompanying the SOFTWARE PRODUCT.

3. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

LIMITATIONS ON REVERSE-ENGINEERING, DECOMPILATION, AND DISSASSEMBLY. You may not reverse- engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

RENTAL. You may not rent, lease or lend the SOFTWARE PRODUCT.

SOFTWARE TRANSFER. You may permanently transfer all of your rights under this EULA, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, this EULA, and the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must include all prior versions of the SOFTWARE PRODUCT.

RUN-TIME DEPLOYMENT. You may deploy the run-time modules of the Software to one (1) computer provided that:

(a) you deploy the run-time modules only in conjunction with and as a part of your software product;

(b) you include valid copyright notices on your software product;

(c) you agree to indemnify, hold harmless, and defend FXSEC LTD and its suppliers and distributors from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or deployment of your software product; and

(d) you do not embed the run-time modules in a toolkit which allows users to build and use or distribute applications containing the run-time modules;

(e) your Application adds significant and primary functionality to the DEPLOYABLE COMPONENTS. The "run-time modules" refers to the PFSDK.SYS, PFSDK.DLL, PFAPI.DLL and any of librarian component files that are required for execution of your software program. The run-time modules are limited to run-time files and install files.

TERMINATION. Without prejudice to any other rights, FXSEC LTD may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

4. EXPORT RESTRICTIONS.

You agree that neither you nor your customers intend to or will, directly or indirectly, export or transmit

(a) the SOFTWARE PRODUCT or related documentation and technical data, or

(b) your Application as described in Section 1 of this EULA (or any part thereof), or process, or service that is the direct product of the SOFTWARE PRODUCT to any country to which such export or transmission is restricted by any applicable government regulation or statute, without the prior written consent, if required, by such governmental entity as may have jurisdiction over such export or transmission.

MISCELLANEOUS. If any provision of this Agreement is found to be unlawful, void or unenforceable, then that provision shall be severed from this Agreement and will not affect the validity and enforceability of any of the remaining provisions.

NO WARRANTIES. To the maximum extent permitted by applicable law, FXSEC LTD expressly
disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation are provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties of merchantability or fitness for a particular purpose. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

LIMITATION OF LIABILITY. FXSEC LTD's entire liability and your exclusive remedy under this EULA shall not exceed five dollars ($5.00 USD).

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall FXSEC LTD or its suppliers or distributors be liable for any damages whatsoever (including, without limitation, damages for loss of business profit, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of, or inability to use, this product, even if FXSEC LTD has been advised of the possibility of such damages. Because some states/provinces/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

RIGHT OF PUBLICITY. You agree that FXSEC LTD is hereby granted the right to promote SOFTWARE PRODUCT and your use of it in it's online portfolio, it web site, its press kits, its press releases, and any other promotional materials.
Profense SDK is a trade name of FXSEC LTD.