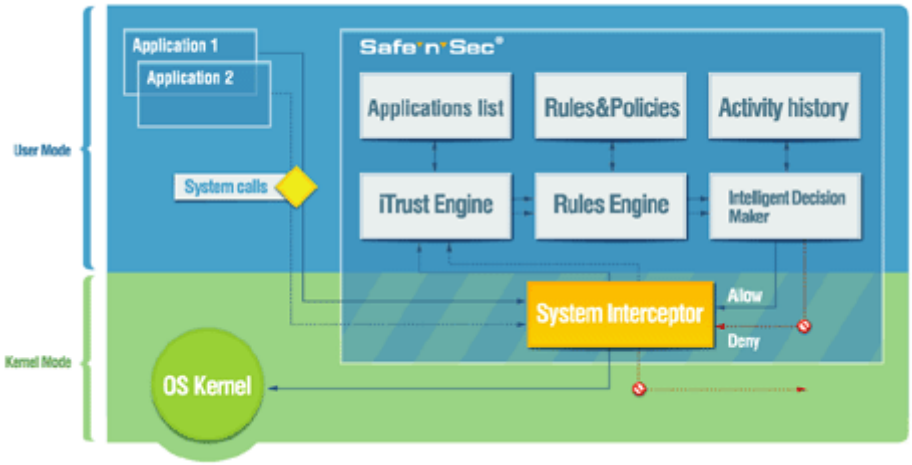
S.N.Safe&Software
Altufievskoe shosse 5/2
127106, Moscow, Russia
Tel. +7(495) 967-1451
Fax. +7(495) 967-1452
www.safensoft.com
e-mail: sns@safensoft.com

S.N.Safe&Software
Алтуфьевское шоссе 5/2
127106, Москва, Россия
Тел: +7(495) 967-1451
Факс: +7(495) 967-1452
www.safensoft.ru
e-mail: sns@safensoft.com

Технология Safe'n'Sec

В основе технологии Safe'n'Sec лежит перехват вызовов системных функций (system calls) на уровне операционной системы. При старте операционной системы System Interceptor загружается одним из первых как модуль расширения ядра и встраивается в цепочку вызовов системных функций. Это позволяет перехватывать все системные вызовы любых приложений, при необходимости, блокировать доступ (*deny*) к системным ресурсам. Если System Interceptor получает команду, что доступ разрешен (*allow*), то вызов передается ядру операционной системы для дальнейшего выполнения.



Для анализа и принятия решения System Interceptor направляет полную информацию о системном вызове и приложении в модуль идентификации приложений iTrust Engine. Правильная идентификация необходима для того, чтобы отличать активность вредоносных приложений от активности обычных приложений пользователя.

Идентификация происходит по уникальным свойствам приложения (расположение на диске, действующий цифровой сертификат, состав модулей и т.д.) и не зависит от версии приложения или операционной системы. Список легальных приложений Application List содержит перечень самых распространенных приложений (MS Office, системные утилиты и сервисы Windows, графические пакеты и т.д.), которые были однозначно идентифицированы. Технология iTrust позволяет значительно снизить долю ложных срабатываний (false alarms) при работе Safe'n'Sec. Например, программа автоматического обновления Windows скачивает очередное обновление во временный каталог, запускает установку обновления, переписывает некоторые системный файлы и изменяет системный реестр. Действия в такой последовательности очень похожи на активность вируса. Однако Safe'n'Sec не блокирует такую активность, т.к. имеет идентификационные данные этой программы. Другая программа, которая маскируется под программу обновления Windows, используя то же имя модуля, расположение на диске и т.д., будет заблокирована.

Далее, запрос обрабатывается модулем управления правилами Rules Engine. В базе правил и политик Rules & Policies задаются потенциально опасные действия приложений (удаление системных файлов, несанкционированный доступ к данным пользователя, изменение настроек операционной среды и т.д.). Набор таких правил и действия над ними

(заблокировать/разрешить/ спросить пользователя и т.д.) составляют политику контроля активности. Политик контроля активности может быть несколько, в зависимости от потребностей пользователя. Если запрос соответствует одному из правил, то Rules Engine выносит заключение о действии, которое должно быть применено согласно установленной политики, и передает его дальше для принятия окончательного решения.

Поступающие в модуль принятия решения Intelligent Decision Maker данные анализируются с учетом истории активности приложения Activity History. В истории фиксируются действия приложения, проанализированные ранее, но этой информации было недостаточно для принятия решения о вредоносности активности.

Последовательность действий, их количество, периодичность и повторяемость помогают Intelligent Decision Maker принять правильное решение. Для примера можно рассмотреть действия, совершаемые в системе при распространении сетевого червя (network worm). Если каждое действие червя анализировать по отдельности, то оснований для блокировки активности нет – файл скачивается из Интернета, запускается на выполнение, процесс открывает адресную книгу Outlook и рассылает email. Но если рассмотреть последовательность действий целиком, поведение приложения выглядит вредоносным. Собрав и проанализировав эти данные, Intelligent Decision Maker может принять решение о блокировании активности сетевого червя без многократных оповещений пользователя на каждое действие.

Другие системы будут посылать оповещения системному администратору, такие как "Приложение А открыло адресную книгу" или "Программа была загружена из Интернет и выполняется", каждое из которых должно быть проанализировано, чтобы принять решение об атаке или нормальном поведении.

Intelligent Decision Maker собирает данные об активности приложения от других компонентов Safe'n'Sec: информацию об идентификации приложения от iTrust Engine, заключение о выполняемом действии приложения от Rules Engine, историю активности приложения от Activity History. По этой информации делается окончательный вывод – разрешить (Allow) или запретить выполнение запроса. Затем System Interceptor блокирует запрещенные запросы или передает к выполнению разрешенные запросы на системном уровне.