

Система автоматического мониторинга

Заказчик

Клиент – американско-английская компания, специализирующаяся на разработке программных продуктов в сфере родительского контроля за детьми, детской безопасностью в интернете, борьбой с детской порнографией, сетевой безопасности.

Задача

Основными задачами программного комплекса являлись:

- Журналирование посещаемых пользователем(предположительно ребенком) интернет-сайтов (перехват информации в браузерах типа IE, FireFox, AOL, MSN Explorer и др).
- Журналирование переписки в интернет-чатах (msn, aol, yahoo, icq, trillion и др).
- Получение удаленного доступа к компьютеру (аналог функции «удаленный рабочий стол»).
- Удаленное управление и ограничение доступа ребенка к компьютеру в целом, к интернету, к отдельным приложениям.
- Уведомление родителя о посещении ребенком запрещенных веб-сайтов, а также наличия запрещенных слов в чате, посредством sms, email.
- Режим «невидимости» клиента для приложений типа «Антивирус» и «Брандмауэр».
- Высокая загрузка серверной части проекта. Ориентировочное пиковое количество транзакций в сутки: 20миллионов.
- Большие объемы обрабатываемых данных. Ориентировочный дневной объем получаемых данных от клиентов составляет ~10Гб.

Решение

Поскольку риски по разработке некоторых функций проекта были довольно высоки, было принято решение разработать пилотные версии некоторых модулей, которые в дальнейшем легли в основу всей системы. В процессе создания пилотного проекта были разработаны такие основные модули системы, как: модуль межпроцессного обмена и взаимодействия, модуль «невидимой» отправки, модуль синхронизации, а также основные протоколы обмена данными и взаимодействия. В дальнейшем были созданы остальные модули системы в соответствии со спецификациями и функциональными требованиями к системе. Данный проект является сложной распределенной системой перехвата данных внутри компьютера. Продукт работает под управлением ОС Windows XP и выше и позволяет отслеживать и блокировать доступ к тем или иным данным и процессам. Теоретически, система может осуществлять мониторинг любых действий пользователя на компьютере. Для обеспечения безопасности от взлома использовался алгоритм шифрования данных BLOWFISH. В целях обеспечения совместимости с предыдущими версиями в качестве базы данных использовался сервер MSSQL2005.

Основные функции

- Клиентская часть:
 - Функция включения/выключения невидимого режима.
 - Автоматическое обновление и загрузка настроек.
 - Защита от удаления программы.
 - Диагностика и самовосстановление системы.
 - Перехват и журналирование посещаемых сайтов.
 - Перехват сообщений в чатах.

- Блокировка (на различном уровне) доступа к компьютеру, интернету, веб-сайту, интернет-чату, отдельному приложению.
- Видеозапись действий пользователя во время работы за компьютером.
- Серверные функции:
 - Прием логов и упаковка их в базу данных
 - Отправка настроек на клиентский компьютер.
 - Трансляция запросов «телевизора» (просмотр, запись и тд.).
 - Трансляция запросов удаленной загрузки файлов.
 - Рассылка уведомлений посредством sms и email.
- Веб-интерфейс:
 - Управление настройками на уровне отдельных пользователей и компьютеров.
 - Управление настройками установленных компьютеров.
 - Управление настроек доступа к компьютеру, интернету, веб-сайту, интернет-чату, отдельному приложению.
 - Просмотр логов.
 - Удаленное управление рабочим столом компьютера («телевизор»).
 - Удаленное закрытие открытых программ.
 - Удаленное блокирование, перезагрузка, выключение компьютера.
 - Удаленная загрузка файлов с/на управляемый компьютер.

Технологии

VisualStudio 2005, QT, MFC, WinAPI, FSDDK, C++,ASM, reverse engineering, C#/ASP.NET, MSSQL, MSProject, MSVisio

Название продукта

SAH

Результаты

Продукт получил оценку «Must Have» («Каждый должен иметь») популярного великобританского онлайн-журнала www.Telegraph.co.uk

Объем работ

Более 150 человеко-месяцев