УДК 004.7+65

СПОСОБЫ ЗАЩИТЫ БРАУЗЕРОВ ОТ СЕТЕВЫХ АТАК

Сиволап Ірина Юріївна, Баранов Анатолій Анатолійович
Державний вищий навчальний заклад «Національний гірничий університет»
irochka911@gmail.com, tocea@yandex.ru

В работе рассмотрены вопросы безопасности использования современных интернет-технологий, а также способы защиты браузеров от сетевых атак.

Каждый производитель интернет-браузеров имеет свои широко декларируемые преимущества, которые находят отклик в глазах определённой группы пользователей, и обеспечивают тому или иному браузеру ярых приверженцев и широкую популярность.

Индустрия браузеров существует, в основном, за счёт косвенных источников дохода. Все популярные браузеры либо можно установить бесплатно, либо же встроены в ту или иную операционную систему. Напомним, что Internet Explorer встроен в Microsoft Windows, начиная с Windows 98, а Safari интегрирован в Mac OS. Соответственно, конкурировать производителям интернет-браузеров с использованием экономических рычагов влияния — невозможно.

Зачастую пользователи отдают предпочтение тому или иному браузеру из-за красивого интерфейса, скорости и удобства в работе или наличия каких-то расширений. Следовательно, в ход идут иные методы борьбы «за сердце пользователя» - с использованием таких, весьма претенциозных, лозунгов как «самый быстрый браузер», «самый удобный браузер», «самый функциональный браузер», «самый настраиваемый браузер» и другие. Но при этом часто забывается или специально умалчивается о степени безопасности самого браузера. А ведь непосредственно через браузер пользователь просматриваем содержимое веб-сайтов. Через браузер он заходим на сайты интернет-банков, производим оплату товаров и услуг, пользуемся онлайн-сервисами или обмениваемся конфиденциальной информацией. Именно на браузер ложится первичная ответственность за безопасность в сети.

Согласно результатам исследований компании Net Applications браузер Microsoft Internet Explorer, оставаясь самым востребованным, постепенно сдает свои рыночные позиции. Так, по состоянию на конец августа 2011 г. с ним работало чуть меньше 67% всех опрошенных пользователей, в то время как в июле 2011-го их было 67,7%, а в августе 2010-го — 75,1%. Второе место вслед за Internet Explorer занимает набирающий популярность Firefox: 22,5% пользователей в июле и 23% в августе. Доля расположившегося на третьем месте Apple Safari составляет 4,1% — она за два летних месяца не изменилась. Зато количество пользователей Google Chrome за это же время немного увеличилось — с 2,6% в июле до 2,8% в августе. Доля Opera на протяжении нескольких месяцев остается на уровне 2%.

Ниже, для каждого браузера, приведена информация, на которой акцентируют своё внимание производители браузеров по поводу безопасности их продуктов для интернет-сёрфинга, ибо подача такой информации во многом выявляет приоритеты этих производителей в реализации технологий безопасности в выпускаемых ими продуктах. При этом будет предложен обзор информации, приведённой на официальных сайтах соответствующих браузеров, без углубления в технические блоги разработчиков и другую информацию подобного рода, так как пользователи обычно руководствуются именно информацией, расположенной на официальных сайтах. Также, в качестве ограничения, введём такой параметр, как русскоязычность такой информации, т.к. данный обзор ориентируется, в первую очередь, на русскоязычных пользователей.

Apple Safari

Компания Apple, говоря о безопасности, в первую очередь акцентирует внимание на функции защищённого просмотра. В данном режиме Safari не записывает историю посещаемых сайтов, загружаемого ПО и документов, не сохраняет поисковые запросы, cookies, и данные веб-форм. В Safari также присутствуют функции блокировки всплывающих окон.

В Safari встроены и продолжают развиваться технологии, противодействующие атакам с использованием межсайтового скриптинга (XSS, Cross Site Scripting, такая аббревиатура используется для исключения путаницы с аббревиатурой Cascading Style Sheets (CSS) – каскадные таблицы стилей). Также в браузер встроены репутационные технологии блокировки вредоносных сайтов: фишинговых, мошеннических, а также сайтов, распространяющих вредоносные программы. Также встроена поддержка EV-сертификатов (Extended Validation), что позволяет легко выделять легитимные сайты.

Safari поддерживает технологии безопасного шифрования для предотвращения перехвата сеансов связи, мошенничества при работе в Интернете. Также поддерживается аутентификация на основе регистрации на безопасных веб-сайтах и наиболее популярные прокси-протоколы. Интересна также функция Безопасные загрузки, благодаря которой при первом открытии каждого сайта отображается источник, из которого была взята та или иная страница.

Google Chrome

Раздел русскоязычного сайта Google, посвящённый обзору возможностей безопасности браузера Google Chrome, является весьма лаконичным. В нём говорится о том, что в данном браузере существует защита от мошеннических и фишинговых сайтов, сосредоточенная в технологии «Безопасный просмотр».

Также выделяется функциональная возможность под названием «песочница» (в англоязычных

материалах соответствующее термину sandboxing), с помощью которого браузер может предотвратить установку в систему вредоносных программ, а также имеет возможность отслеживать влияние кода, который выполняется в одной вкладке браузера на содержимое других открытых вкладок. В Chrome 12 появился фильтр вредоносных файлов на основе репутационных технологий, который при дальнейшем развитии может составить конкуренцию технологии Application Reputation от Microsoft.

В англоязычных источниках можно узнать о возможностях обеспечения безопасности более подробно. В частности, в Google Chrome существует технология обеспечения непрерывности HTTPS-соединения и защиты его от компрометации, защита от XSS-атак и другие полезные функции. Поэтому, автор обзора надеется, что компания Google, активно рекламирующая свою продукцию и на территории России и Украины, в том числе – с помощью дорогостоящей телевизионной рекламы, выделит ресурсы для того, чтобы перевести на русский язык столь важную для пользователей информацию, дабы способствовать дальнейшей популяризации данного браузера среди интернет-пользователей российского сегмента.

Microsoft Internet Explorer

Компания Microsoft, говоря о безопасности своего браузера, в первую очередь делает упор на фильтрацию ActiveX-содержимого. В общем-то, проблема небезопасного ActiveX-содержимого актуальна именно для данного браузера, т.к. без дополнительных плагинов в конкурирующих браузерах взаимодействие с активным содержимым, расположенным на интернет-страницах, производится посредством других технологий.

Также акцент делается на противодействие XSS-атакам, просмотр в приватном режиме InPrivate и функция защиты от слежения. Также реализовано выделение домена второго уровня в адресной строке браузера, жирным цветом, что позволяет легко определить, находится ли пользователь на настоящем сайте, на который хотел зайти, или же на мошенническом, адрес которого сильно похож на адрес настоящего сайта.

В качестве уникальной функциональной особенности безопасности можно указать широко рекламируемый фильтр SmartScreen, который в 9-ой версии Internet Explorer имеет возможность фильтровать не только вредоносные сайты по URL, но и, собственно, вредоносные файлы посредством технологии Application Reputation, которая основана на репутационных технологиях.

Следует заметить, что актуальная версия Internet Explorer, по мнению автора, значительно усовершенствовалась в плане повышения стандартов информационной безопасности по сравнению с предыдущими версиями данного браузера, и его вполне можно рекомендовать к использованию начинающим интернет-пользователям для совершения операций интернет-банкинга и других потенциально-опасных операций при чётком следовании рекомендациям производителя.

ВЫВОДЫ

Поддержка работы с EV-сертификатами, наличия режима приватного просмотра, а также возможности соединений с веб-узлами по защищённому протоколу HTTPS - все это реализовано во всех сравниваемых браузерах.

С защитой от компрометации HTTPS -соединения ситуация обстоит несколько хуже. Из известных технологий по данному поводу можно упомянуть только возможность слежения за непрерывностью HTTPS-соединений у Google Chrome и закреплённые сайты (pinned sites) у Internet Explorer 9 при использовании совместно с Windows 7.