Эссе по “Защите информации”.
Выполнил:Николаев Константин, 911 группа.

Служба “What’s Related”, обеспечение безопасности и конфиденциальности в браузере Netscape.

Вступление.

Интернет – общедоступная сеть, состоящая из миллионов компьютеров. В сети Интернет передача данных осуществляется через общедоступные линии связи и посредством многочисленных соединений. Поэтому возможен, например, несанкционированный пассивный перехват информации без ее изменения. Браузеры, в частности браузер Netscape, содержат средства, которые обеспечивают безопасность и конфиденциальность.

В браузере Netscape 4.06 появилась новая функция, “Smart Browsing”, управляемая при помощи новой иконки “What’s related”, что является внешним интерфейсом к службе, которая предлагает сайты, которые связаны с документом, открытый в данный момент пользователем. Реализация этой функции затрагивает множество потенциально серьезных проблем, связанных с обеспечением конфиценциальности и безопасности.

В частности, URL-адреса, которые посещаются пользователем, сообщаются серверу Netscape. Эти данные могут использоваться, чтобы вести исчерпывающие досье на пользователей сети, включая их имена, адреса, и номера телефонов.

В браузере предлагается выбрать, когда автоматически загрузить службу “What’s Related”:

- "Всегда";
- "После первого использования";
- "Никогда".

Когда загружается эта служба, в дополнение к обычным запросам, открывается дополнительная HTTP-сессия с хостом www-rl4.netscape.com, на который в дальнейшем будем ссылатся, как "шпион". Обмен данными с “шпионом” продолжается, в то время как пользователь переходит от сайта к сайту, оставляя электронный след деятельности в сети на централизованном сервере. Исследуем обмен данных между браузером и “шпионом”. Это можно сделать с помощью сниффера.

Текущий URL-адрес.

URL-адрес текущей страницы посылается “шпиону”, при чём посылаются как “public”, так и “private” адреса, например, адреса страниц, находящихся в локальной сети, за исключением случая, когда они входят в группу адресов, явно исключенных пользователем в настройках браузера. HTTP-параметры запроса не содержатся в URL-адресе, посылаемым “шпиону”. Например, адрес “http://www.example.com/search.cgi?secret” пошлётся, как “http://www.example.com/search.cgi?”.

Результат запроса.

В ответе на запрос, "шпион" возвращает файл, содержащий ряд линков, которые, как считает сервер, связанны с посланным ему URL-адресом.

Ничего нет специфичного в этом файле, за исключением того, что все его линки приходят в форме

HTTP://info.netscape.com/fwd/rl/HTTP://WWW.example.com:80/

Это означает, что перед непосредственным соединением с рекомендуемым сайтом, пользователь сообщает "шпиону" на какой сайт он переходит. Это механизм обратной связи, который сообщает серверу, на какой из рекомендуемых сайтов, если таковые вообще имеются, пользователь переходит.

Cookie.

Возможно, наиболее интересным и наиболее тревожным фактом в работе с "шпионом" является это:

Cookie: NETSCAPE_ID=10010014,12f8fee8

После выхода из браузера, был исследован файл .netscape/cookies, чтобы определить, является ли это cookie постоянным во время сессии. Интересно, что файл не обновлялся в течении нескольких дней. Было обнаружено, что cookie, которое браузер посылал - *то же самое* cookie, которое посылается, когда любой сайт Netscape запрашивает его. Сайт Netcenter, сайт разработчиков Netscape, сайт поддержки, и другие.

Выводы.

Исследуемая служба затрагивает некоторые чрезвычайно серьезные проблемы секретности данных, не только для индивидуумов, но и для организаций, которые могут иметь приватную информацию, пропущенную через их firewall’ы.

Рассмотрим некоторые из заключений наблюдений.

Утечка Интеллектуальной Собственности Вне Firewall.

Наличие достаточно информативного URL-адреса, подобного HTTP://products.example.com/secret/foobar или

HTTP://products.example.com/team/some_guy/, может привести к тому, что названия еще невыпущенных продуктов, имена людей, работающие на организацию, и другая информация могут быть получены.

Появляется способность найти *внутренние* сайты организации, включенные в базу данных “шпиона”. Более того служба предоставляет, полученную из HTML-заголовка, например название документа.

Создание досье.

Один из способов обеспечения конфидециальности с помощью cookie связан с их децентрализованной природой. В частности, область, для которой cookie является активным, ограничена.

Посылая поток URL-адресов "шпиону", каждый из которых сопровождается тем самым постоянным cookie, теперь становится возможным для Netscape полностью обойти принципы конфиденциальности cookie.

Так как cookie для каждого из запросов к “шпиону” - *то же самое* cookie, используемое для посещений всех сайтов Netscape, включая сайт для скачивания браузера, теперь, мало того, что можно потенциально связать все просматриваемые сайты с определенным пользователем, но и можно связать его со всеми запросами к любым страницам Netscape, которые пользователь делал.

Добавление имени пользователя к досье.

Чтобы скачать продукт фирмы Netscape, пользователь обязан указать своё имя, адрес, и номер телефона, что и позволяет Netscape связать детальную историю посещенных страниц с определенным индивидуумом.

Методы защиты.

Есть несколько методов, которые могут быть предприняты, чтобы нейтрализовать эффекты нарушения конфиденциальности службой “What’s Related”.

Первый метод – фильтрование чрезмерно информативных URL-адресов. Это можно реализвать на шлюзах организации.

Второй метод - отказ от cookies. Это может помочь предотвратить создание точного досье на пользователей, но полностью эту проблему решить не может. Вместо cookies могут быть использваоны вторичные признаки, например, что пользователь, посещающий в данный момент определенный сайт является тем же самым пользователем, который посетил его вчера. Эти механизмы, тем не менее, являются гораздо менее эффективными чем использование cookie.

Третий метод – использвание анонимных прокси. Могут быть использвованы такие продукты, как Anonymizer, Lucent Personalized Web Assistant, Crowds, а также корпоративные firewall'ы и web-прокси. Этот метод является наиболее эффективной защитой. Фунции, такие как фильтрация cookie и скрытия отправителя запросов, сами по себе эффективны против потенциальных нарушений конфединциальности.

К сожалению, браузер Netscape недостаточно хорошо обеспечивает секретность и конфиденциальность. Помимо проблем со службой "What's Related", даже в самых последних версиях есть уязвимости.

Mozilla – браузер с открытым исходным кодом. Для создания браузеров Netscape, начиная с 6-ой версии, использовался этот исходный код .В результате, Netscape имеет многие из тех уязвимостей, что и Mozilla. Другие браузеры, такие как Galeon, Phoenix, Camino (Chimera) также используют исходный код браузера Mozilla и могут быть иметь те же уязвимости.

Был проведен тест на уязвимость браузера Netscape одной из последних версий на сайте http://bcheck.scanit.be/bcheck/. Испытываемая версия Netscape 7.0 Preview Release 1(на данный момент последняя версия 7.02). Было обнаружено несколько уязвимостей. Практически все из которых по словам разработчиков исправлены в новых версиях.

Но одна уязвимость не устранена на данный момент. Её название – "Mozilla Link Onclick Cross Domain Scripting Vulnerability". Эта уязвимость позволяет сайту злоумышленника получить доступ к вашим данным о других сайтах. Например, это может использоваться, чтобы читать вашу электронную почту из почтовой системы с web-интерфейсом.

Когда браузер начинает загружать новую страницу в окне, различные объекты на старой странице остаются доступными в течение короткого периода времени. Однако домен изменяется немедленно на домен новой страницы. В течение этого короткого периода возможно выполнить JavaScript код, определенный на старой страницей в контексте новой страницы.

Эта проблема может быть использована следующим образом:

1. Когда пользователь заходит на страницу сайта злоумышленника, открывается новое окно со страницей с этого же сайта. Эта страница

должна содержать гиперссылку, для которой определено событие "onclick".

2. Код на первой странице сохраняет ссылку на функцию onclick гиперссылки другого окна.

3. Затем начинается загружаться любая интересующая страница во втором окне.

4. Пока новая страница загружается, вызывается функция “onclick” при помощи сохраненной ссылки на неё.

5.Функция выполняется в контексте загружаемой страницы и имеет доступ к cookies и другой информации о этом веб-сайте.

Демонстрацию этого подхода можно найти на сайте http://www.securityfocus.com/archive/1/318777.Возможное(но очень неудобное) решение этой проблемы – отключение поддержки JavaScript.

Также был протестирован браузер Microsoft Internet Explorer 6 SP1. Были обнаружены несколько уязвимостей, но все они устранялись соответствующими “пачами” (исправлениями продукта).

Используемая литература:

1. “What's Related?”
Everything But Your Privacy.

http://www.interhack.net/pubs/whatsrelated/

2. Netscape Communications Corporation. 1998. *What's Related FAQ* [online]. Available from World Wide Web: http://home.netscape.com/escapes/related/faq.html.

3. Netscape DevEdge.

http://devedge.netscape.com/

4. Known Vulnerabilities in Mozilla

http://mozilla.org/projects/security/known-vulnerabilities.html