БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ ВІДНОСНО ВИКОРИСТАННЯ COOKIE

Землянська О.В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Сітко Д., студ. (гр. ФІ-51, ФТІ КПІ ім. Ігоря Сікорського)

Cookie це механізм для запам'ятовування браузером текстових даних. Сайт просить браузер запам'ятати деяку (невелику) кількість інформації. Браузер, якщо він налаштований відповідним чином, запам'ятовує цю інформацію і передає її сайту з кожним наступним запитом. Сайт може отримати тільки власні cookie, інформація з чужих сайтів йому не доступна [1].

Механізм Http-cookie

Сервер може встановити cookie у відповідь на запит браузера. Для цього служить заголовок відповіді (response header) Set-cookie.

Cookie також може бути встановлений і самим браузером через Javascript, який підтримується більшістю сучасних браузерів.

Браузер повинен зберігати cookie на період визначений для її часу життя і посилати cookie на сервер в заголовку запиту (request header) Cookie.

У запиті посилаються тільки ті cookie, які відповідають домену, шляху і протоколу для яких cookie була встановлена.

Вищевикладений механізм застосовний і для будь-якого іншого, відмінного від браузера, клієнтського застосування, що обмінюється інформацією з веб-сервером по протоколу HTTP/HTTPS [3].

Самі по собі cookies не можуть робити нічого, це тільки лише деяка текстова інформація. Однак сервер може зчитувати інформацію, яка міститься в cookies і на підставі її аналізу здійснювати ті чи інші дії. Наприклад, в разі авторизованого доступу до чого або через WWW в cookies зберігається login і password протягом сесії, що дозволяє користувачеві не вводити їх знову при запитах кожного документа, захищеного паролем.

На використанні cookies також часто будують функції оформлення замовлень в онлайнових магазинах, зокрема, в найбільшому віртуальному книжковому магазині Amazon Books реалізована своєрідна віртуальна корзина покупця, як в звичайному реальному супермаркеті, в яку сервер записує інформацію про всі замовлені книги. Користувач просто позначає книги які його цікавлять, а потім оформляє покупку відразу всіх зазначених книжок.

Ще одна поширена область використання cookies – при налаштуванні індивідуального профілю кожного зареєстрованого користувача.

І, нарешті, остання область – використання механізму cookie в рекламному бізнесі на Інтернет. Ще рік тому реклама в Інтернет за гроші була досить екзотичною послугою, а зараз цей бізнес вже устоявся і стрімко розвивається. Однак рекламодавці починають пред'являти більш жорсткі умови до оцінки ефективності своїх витрат. Cookie використовуються для орієнтування реклами (визначення цільової аудиторії, наприклад, за географічним положенням користувачів), відстеження інтересів користувачів,

обліку кількості показів і проходів крізь банери [4].

Cookie бувають двох видів: збережені і сеансові (сесійні). У першому випадку вони зберігаються вказаний при їх установці час, у другому – до закриття браузера. Для ідентифікатора сесії зазвичай використовуються сеансові cookie – немає причин зберігати цей ідентифікатор після закриття браузера. Збережені cookie, на відміну від сеансових, зберігаються на диск. Вони часто використовуються для реалізації сервісу «запам'ятати мене», тобто дозволяють не вводити пароль на сайтах при кожному відвідуванні. Пароль зберігається в cookie і автоматично відсилається на сайт під час входу на нього.

Деякі комерційні сайти включають вбудований рекламний матеріал, який обслуговується з інших сайтів, і для таких оголошень використовуються cookie для цього стороннього сайту, що містить інформацію, передану йому з сайту – така інформація може включати ім'я сайту, а також переглянутих продуктів, відвідуваних сторінок і т. п. Коли користувач пізніше відвідує інший сайт, що містить аналогічну вбудовану рекламу з одного і того ж стороннього сайту, рекламодавець зможе прочитати cookie-файл і використовувати його для визначення деякої інформації про історію перегляду користувача. Це дозволяє видавцям обслуговувати рекламу, націлену на інтереси користувача. Тим не менш, багато людей бачать такі «файли відстеження», як вторгнення в приватне життя, оскільки вони дозволяють рекламодавцю створювати профілі користувачів без їх згоди.

В Інтернеті багато побоювань, що файли cookie можуть пошкодити ваш жорсткий диск, скопіювати ваші дані, чи принести з собою вірус, що пошкодить вашу операційну систему. Але це не так. Файли cookie не є небезпечними для вашого комп'ютера.

Трохи про проблеми, пов'язані з використанням cookie.

Головною проблемою є початкова недовіра користувачів до того, що віддалені сервера без їх відома і згоди записують на їх власні локальні диски якусь інформацію. Побутували також чутки про те, що за допомогою механізму cookie можна прочитати будь-яку інформацію з будь-якого комп'ютера. Це неправда, до того ж сучасні версії браузерів дозволяють контролювати прийом cookie або зовсім блокувати його. Крім того, з'явилося безліч спеціальних утиліт для управління прийомом cookie, так звані Cookie Managers.

Інша сторона цієї проблеми полягає в тому, що на вузлах мережі акумулюються величезні масиви даних з персональною інформацією, необхідні для комерційних серверів. Ось тут і з'являються підвищені вимоги до захисту від несанкціонованого доступу до цих даних. Користувачі таких серверів повинні бути впевнені, що їх імена, адреси електронної пошти, номери телефонів та ін., не потраплять в чужі руки. В іншому випадку наслідки можуть виявитися катастрофічними для комерційних серверів, що «проштрафилися» [4].

У cookie склалася репутація «дірки» безпеки, деякі надто старанні додатки для знищення шкідливих програм навіть попереджають про це користувача. Справа в тому, що, запам'ятовуючи відвідувача, в принципі

можна стежити за всіма його діями – які сторінки він відвідує, якими товарами і послугами цікавиться. Правда, це можливо тільки в межах одного сайту, що сильно лімітує можливості [1].

Реальною проблемою безпеки є те, що, вкравши чужі cookie, зловмисник може увійти на запаролений сайт під логіном жертви. Це, однак, при використанні сесій може статися завжди, незалежно від механізму зберігання ідентифікатора.

Основні проблеми з безпекою викликають саме збережені cookie, як раз з їх допомогою можна відстежувати смаки користувача протягом періодів, достатніх для аналізу (а це набагато більше звичайного часу життя сеансових cookie). І саме в них зберігаються паролі при реалізації механізму «запам'ятання паролю». Тобто слід розрізняти сеансові і збережені cookie і, якщо вже відключати, то тільки останні.

Однак, оскільки деякі веб-сайти або програми вимагають використання файлів cookie для правильної роботи, ви можете втратити певні функції, якщо ви вирішите видалити або відключити всі файли cookie з вашого веб-браузера.

Відключення ж і сеансових cookie ніяких видимих переваг в безпеці не дає, навіть породжує додаткові проблеми, зокрема змушуючи відключати укупі з ними і передачу referer'a.

Але є й альтернативні способи отримання персональної інформації з cookie. На відміну від інтернет-компаній, яким необхідно розробляти спеціальні програми, вашим знайомим досить вставити тільки флешку в ваш комп'ютер і завантажити cookie. Цього достатньо, щоб отримати доступ до вашої персональної інформації в Інтернеті [2].

Саме тому, безпека приватних даних залежить в особливості від особистої недбалості.

Наслідками крадіжки ваших персональних даних можуть бути:

1. Фінансові збитки, в разі крадіжки приватної інформації, що стосується банківських операцій (паролі, номера телефонів, коди);
2. Моральні збитки, в разі користування вашими персональними даними (наприклад в соціальних мережах, чи просто електронною поштою) з метою наклепу чи введення в оману. Як наслідок можлива психологічна травма.

Література

1. http://xpoint.ru/know-how/Security/Cookie
2. http://serfock.ru/browser/cat-mozilla-firefox/cookie-descript
3. https://uk.wikipedia.org/wiki/%D0%9A%D1%83%D0%BA%D0%B8
4. http://citforum.ru/internet/html/cookie.shtml