На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.,** ректор ОНАХТ.

Співголови :
Капрельянц Л.В. – д.т.н., проф., проректор з наукової роботи та міжнародних зв′язків,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., доц., директор ННІМАтаКС ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри автоматизації виробничих процесів ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри технології і автоматизації виробництва радіоелектронних і електронно-обчислювальних засобів ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СПіСКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., директор інституту комп'ютерних технологій Національного авіаційного університету.

<u>Члени оргкомітету:</u>
Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ.
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ.
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ.
Грищенко І.В. – к.т.н., заступник декана ФІТта КБ ОНАХТ.
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

Prefab(Префаб - каркас) - являє собою ще один тип ресурсів призначений для зберігання та багаторазового використання ігрових об'єктів з доданими до них компонентів та встановленими значеннями властивостей. *Prefab* виступає в ролі шаблону для створення екземплярів об'єкта на сцені. Будь-які зміни у префабі відображаються на усіх екземплярах, при цьому розробник має можливість перевизначити компоненти і налаштування для кожного екземпляра окремо. Також у випадку експериментування з перевизначенням існує можливість відмінити зміни до початкового стану префаба.

***Tag*(Тег - ознака)** – ключове слово яке може бути назначене ігровим об'єктам. Завдяки цьому розробники мають можливість групувати ігрові об'єкти. Тег допомагає програмістам звертатися зі скрипта, одразу до декількох об'єктів, яким призначений однаковий тег. Для розширення можливостей існує можливість створювати власні теги.

Список літератури

1. Will Goldstone. Unity Game Development Essentials (2009) Birmingham, B27 6PA, UK. ISBN 978-1-847198-18-1

МЕТОДИ ЗАХИСТУ ВІД КРАДІЖОК ГРОШЕЙ З БАНКІВСЬКИХ КАРТОК

Ткаченко В.Ю., Ткаченко Є.О. студенти ОКР „бакалавр" ФІТ та КБ ОНАХТ
Керівник – ст. викл. каф. КІ Бондаренко В.Г.

В даний час більшість населення активно користується банківськими картками.

Перевага банківських карток очевидно - це зручність при оплаті, контроль витрат, знижки та бонуси, гігієнічність і безпеку.

Але говорячи про безпеку, необхідно зробити застереження.

Як показує практика, коли з банківських карт зникають гроші, клієнт звертається в банк, там найчастіше знизують плечима, громадянин приходить в поліцію, але і там допомогти можуть в лічених випадках. В результаті власник картки залишається без грошей. За статистикою 0.1% громадян щомісяця втрачають гроші з карток. Почавши користуватися пластиковою карткою, і не виконуючи елементарних правил безпеки, кожен з нас автоматично стає потенційною жертвою. Як тільки Ви втратите пильність, Вас пограбують. Без вжиття заходів безпеки, це лише справа часу. В інтернеті задоволене велика кількість однакових статей на тему крадіжок з банківських карт. У них описуються неможливі і рідкісні для нашого часу речі: наприклад, технічні накладки на клавіатуру банкоматів (скімінг), приховані камери, фальшиві банкомати та інші страшилки для обивателя. Всі ці десятки тисяч сторінок створюють інформаційно-шумовий бар'єр, який не дає можливості користувачеві знайти по-справжньому що стоїть інформацію про те, як себе убезпечити.

Завжди, коли Ваша картка потрапляє в руки до чужої людини, Ви ризикуєте втратити гроші. Шахраєві досить запам'ятати 16 цифр (номер картки), і

гроші можуть піти на чужий рахунок. Нижче представлені найпопулярніші місця крадіжки даних з карти:

Кафе. Якщо при оплаті Ви дасте офіціантові в руки карту, і він з нею піде за терміналом, є ймовірність що дані будуть викрадені. Офіціант може їх: записати, сфотографувати або запам'ятати.

Магазин. При оплаті Ви даєте карту в руки касирові, і є ризик, що десь поруч встановлена мікрокамера, якої достатньо продемонструвати карту з двох сторін і дані будуть вкрадені. Також відомі випадки скіммінгу в торгових точках.

Інтернет. Якщо Ви розраховуєтесь в інтернет - магазинах, є ймовірності:

- що сервіс, через який Ви зробили оплату, збереже дані Вашої картки, які пізніше будуть використані зловмисниками;
- що ви зайдете на фішингових (від англ.- Fishing - ловля на гачок) сайт-імітатор інтернет - банку (як правило точна копія) і введені дані підуть до зловмисників, після чого Вас переадресовують на інший сайт;
- що Ваш комп'ютер заразять шкідливою програмою (вірусом) яка буде відправляти на адресу зловмисників паролі, логіни і PIN - коди.

Мобільні банківські додатки менш захищені, оскільки, при певному старанні можна дістати дублікат SIM карти і отримувати одноразові паролі при платежах. Не виключається і крадіжка телефону або смартфона (після збору даних з комп'ютера паролів і логінів). Статистика компанії Zecurion стверджує, що кількість громадян, які втратили гроші з рахунків, або в результатах хакерських атак і крадіжок смартфонів, становить мільйони чоловік.

Окремо потрібно сказати про такий спосіб зняття інформації з карти, як RFID - reader. Зчитувачі подібного типу дозволяють вважати дані з Вашої картки на відстані і визначити цей момент досить важко. Як правило це відбувається в людному місці, в натовпі, або громадському транспорті. Шахраєві - кардеру досить знати номер карти, термін дії, прізвище, ім'я та CVV / CVC код - 3 цифри на зворотній стороні карти. Далі він навіть без підтверджень по СМС зможе зняти гроші з Вашої картки. Щоб цього не сталося, досить захистити свій CVV / CVC і PIN коди.

Список літератури

1. В. А. Гамза, Банківська безпека: сучасна ситуація // InformationSecurity [Електронний ресурс] – Режим доступу: http://www.itsec.ru/articles2/tema/bank_ bezopasn_sovremen_situac (дата звернення 20.03.16);
2. Шахрайство з банківськими картами // Банкі.ру - інформаційний портал [Електронний ресурс] - Режим доступу: http://www.banki.ru/ (дата звернення 20.03.16);
3. Статистика пошуку в інтернеті // Яндекс - [Електронний ресурс] - Режим доступу: https://wordstat.yandex.ru/ (дата звернення 20.03.16)/