власного фото для зображення профілю; доступ до головної сторінки та сторінки допомоги; свій персональний простір.

V. Програмне забезпечення та технології

В процесі реалізації системи, використаємо наступні засоби: Microsoft Visual Studio, Microsoft SQL Server, ASP.Net MVC, HTML, CSS, Bootstrap, Javascript, Ajax, JQuery. Приклад основного меню системи, зображено на рис.3.

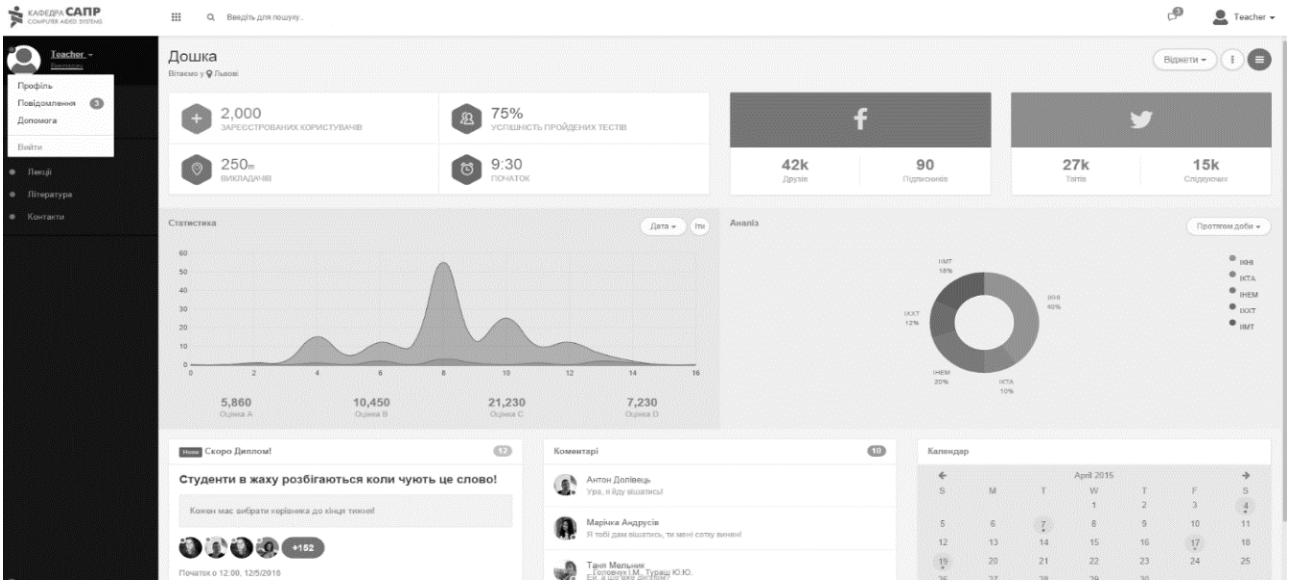

Рисунок 3 - Приклад основного меню системи

Висновок

Побудована система дає змогу автоматизувати процес формування тестів та тестування знань студентів.

Список використаних джерел

1. В.С.Фетісов. Комп'ютерні технології в тестуванні: навч.-метод. посіб. – Ніжин: Видавець ПП Лисенко М.М., 2011. – 140 с.
2. Опарін А.В., Британська О.П. Досвід контролю базових знань студентів за допомогою системи комп'ютерного тестування, Інформаційно-аналітичний портал «Вища освіта», 6.12.2012.
3. Троелсен, Эндрю. Язык программирования C# 5.0 и платформа .NET 4.5, 6-е изд. : Пер. с англ. — М. : ООО "И.Д. Вильямс", 2013. — 1312 с.
4. Н. Б. Шаховська, В. В. Литвин. Проектування інформаційних систем: навчальний посібник. - Львів: "Магнолія-2006", 2011. - 380 с.

УДК 681.518

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РОЗПІЗНАВАННЯ ЗАШИФРОВАНОГО ТРАФІКУ У VOIP СИСТЕМАХ

Гончар Л.І.[1)], Вавренюк А.Р.[2)]

Тернопільський національний економічний університет

[1)] к.е.н., доцент; [2)] магістрант

За минулі кілька років технологія Voice-over-IP (VoIP) стала привабливою альтернативою більш традиційним формам телефонії. Природно, з ростом її популярності у щоденному вжитку весь час досліджуються способи підвищити ефективність та безпеку цієї порівняно нової комунікаційної технології. На жаль, у той час, коли загальноприйнятим є факт, що пакети VoIP повинні бути зашифровані, аби гарантувати конфіденційність [3], було показано, що просто їх шифрування може бути не достатнім з точки зору забезпечення приватності.

Наукова робота деталізує доказові методи відновлення інформації із голосового спілкування, що здійснюється з використанням зашифрованих потоків даних VoIP.

У цій роботі ми показуємо, що інформація, отримана з комбінації використання VBR та шифрування зі збереження довжини, дійсно може бути використана для викриття вимовлених фраз.

З високою точністю успіх цієї технології базується на експлуатації кореляції між основними стандартними блоками мови - а саме, фонемами,- та довжинами пакетів, які продукує VoIP-кодек, у відповідь на ці фонеми. Інтуїтивно, що для пошуку слова чи фрази ми спочатку будуємо модель, поділяючи цільову фразу на її фонеми, а потім розкладаємо ці фонеми в найбільш ймовірні довжини пакетів.

Далі, враховуючи послідовність довжин пакетів, які відповідають зашифрованій VoIP-розмові, ми просто перевіряємо потік трафіку на наявність підпослідовності довжин пакетів, що відповідають нашій моделі.

Природно, мовлення змінюється залежно від значної кількості факторів впливу і, таким чином, дві вимови того ж самого слова будуть не обов'язково закодовані однаковим шляхом. Враховуючи це, ми використовуємо профільні приховані марківські моделі [1], щоб побудувати незалежну від мовця модель фрази, яку ми б хотіли розпізнати. Використовуючи таку модель маємо змогу визначити, коли серія пакетів подібна тій, що очікується для бажаної послідовності фонем. Таким чином, підхід, який ми досліджуємо, точний навіть для дуже невеликого об’єму інформації.

У цій роботі ми припускаємо, що у нападника є доступ тільки до зашифрованого тексту, який він хоче шукати, знання мови розмови та статистичні дані співвідношення фонем та довжин пакетів у випадку використання конкретного VoIP-кодека.

Досліджено можливість атаки на VoIP-системи, базуючись на довжинах мережевих пакетів, а також розроблено програмне забезпечення для реалізації даної атаки. У якості середовища програмування Java було обране середовище NetBeans IDE. Воно є безкоштовним для використання у будь-яких цілях (особистих або комерційних), а також володіє усіма корисними засобами, що пришвидшують розробку, як і інші популярні середовища (Eclipse, IntelliJ IDEA).

Для роботи із прихованими марківськими моделями було використано бібліотеку BioJava.

Що ж до тієї частини нашого програмного продукту, яке розроблялося за допомогою Python, який є скриптовою мовою програмування, як середовище його розробки, було обрано термінальний редактор ОС Unix Vim. Для зручного аналізу трафіку використовувався пакет dpkt.

Висновок

1. Показано залежність кількості необхідних тренувань атакуючої системи від особливостей цільової фрази, зокрема різновидів та співвідношення фонем, що в ній використовуються.
2. Доведено, що наразі єдиним 100%-ковим способом захисту слід вважати використання для кодування голосової інформації кодеків із постійним бітрейтом.

Список використаних джерел

1. Benoît Dupasquier. Analysis of information leakage from encrypted Skype conversations /Benoît Dupasquier, Stefan Burschka, Kieran McLaughlin, Sakir Sezer – International Journal of Information Security, October 2010, Vol. 9, Issue 5, pages 313-325.
2. Hidden Markov Models, Theory and Applications /Hidden Markov. Edited by Przemyslaw Dymarski, ISBN 978-953-307-208-1, Hard cover, 314 pages, Publisher: InTech, Published: April 19, 2011 under CC BY-NC-SA 3.0 license.
3. N. Provos. Voice over misconfigured internet telephones. http://vomit.xtdnet.nl.