4.Sandip Modha, Thomas Mandl, Prasenjit Majumder, Daksh Patel, DA-IICT,Gandhinagar, India sjmodha@gmail.com , Overview of the HASOC track at FIRE 2019: *Hate Speech and Offensive Content Identification in Indo-European Languages*, FIRE 2019, 12–15 December 2019, Kolkata, India.

5. Shervin Malmasi, Marcos Zampieri. *Detecting Hate Speech in Social Media*, 26 Dec 2017, doi:arXiv:1712.06427v2 [cs.CL].

6. Arup Baruah, Ferdous Ahmed Barbhuiya, Kuntal Dey: IITG-ADBU at HASOC 2019: *Automated Hate Speech and Offensive Content Detection in English and Code Mixed Hindi Text*, 2019, pp. 12–15, doi: http://ceur-ws.org/Vol-2517/T3-7.pdf

7. Vijayasaradhi Indurthi1,3, Bakhtiyar Syed1, Manish Shrivastava1 Manish Gupta1,2, Vasudeva Varma11 IIIT Hyderabad, 2 Microsoft, 3 Teradata Fermi at SemEval-2019 Task 6: *Identifying and Categorizing Offensive Language in Social Media using Sentence Embeddings*

8. John Pavlopoulos, Ion Androutsopoulos, Nithum Thain, Lucas Dixon ConvAI at SemEval-2019 Task 6: *Offensive Language Identification and Categorization with Perspective and BERT*

УДК 004.056.55

АТАКИ НА СТЕГАНОСИСТЕМИ. КРИПТОГРАФІЧНІ АТАКИ

П. В. Римар, В. В. Крохмалюк

Захист інформації від несанкціонованого доступу вирішуються в усі часи історії людства. Вже в стародавньому світі виділилося два основні напрямки вирішення цієї задачі, що існують і до сьогоднішнього дня: криптографія і стеганографія. Метою криптографії є приховання вмісту повідомлень за рахунок шифрування. На відміну від цього, при стеганографії приховується сам факт існування таємного повідомлення.

Серед можливих методів (заходів) захисту конфіденційної інформації найпоширенішим на сьогодні є метод криптографічного захисту, під яким розуміється приховання змісту повідомлення за рахунок його шифрування (кодування) за певним алгоритмом, що має на меті зробити повідомлення незрозумілим для непосвячених в цей алгоритм або у зміст ключа, який використовувався при шифруванні. Але зазначений метод захисту є неефективним щонайменше з двох причин.

По-перше, зашифрована за допомогою більш-менш стійкої криптосистеми інформація є недоступною (протягом часу, що визначається стійкістю криптосистеми) для ознайомлення без знання алгоритму і ключа.

По-друге, слід звернути увагу на те, що криптографічний захист захищає лише зміст конфіденційної інформації. У цьому випадку проблема інформаційної безпеки повертається до стійкості криптографічного коду.

На противагу вище зазначеному, стеганографічний захист забезпечує приховання самого факту існування конфіденційних відомостей при їх передачі, зберіганні чи обробці. Під приховуванням факту існування розуміється не тільки унеможливлення виявлення в перехопленому повідомленні наявності іншого (прихованого) повідомлення, але й взагалі зробити неможливим викликання на цей рахунок будь-яких підозр. Загальною рисою стеганографічних методів є те, що приховуване повідомлення вбудовується в деякий не приваблюючий увагу об’єкт (контейнер), який згодом відкрито транспортується (пересилається) адресату.

Завданням пропонованої роботи є розробка програмного комплексу для демонстрації принципів, закладених в основу поширених на сьогодні методів стеганографічного приховування з можливістю обчислення основних показників спотворення контейнера при вбудовуванні до нього приховуваних даних.

Дана задача вирішується попереднім опрацюванням наступних питань:

– розгляд особливостей побудови стеганографічних систем та основних типів атак на зазначені системи;

– аналіз сучасних досліджень і публікацій з приводу існуючих методів стеганографії та заходів підвищення їх стійкості до стеганоаналізу і пропускної здатності;

– формулювання практичних рекомендацій стосовно вбудовування даних.

Стеганосистема вважається зламаною, якщо порушникові вдалося, принаймні, довести існування прихованого повідомлення в перехопленому контейнері. Передбачається, що порушник здатний проводити будь-які види атак і має необмежені обчислювальні можливості. Якщо йому не вдається підтвердити гіпотезу про те, що в контейнері приховано секретне повідомлення, то стеганографічна система вважається стійкою.

У більшості випадків виділяють декілька етапів зламу стеганографічної системи:

– виявлення факту присутності прихованої інформації;

– видобування прихованого повідомлення;

– видозміна (модифікація) прихованої інформації;

– заборона на здійснення будь-якого пересилання інформації, у тому числі і прихованої.

Перші два етапи відносяться до пасивних атак на стеганосистему, а останні – до активних (або зловмисних) атак. Виділяють такі види атак на стеганосистеми (за аналогією з криптоаналізом):

– атака на основі відомого заповненого контейнера. У цьому випадку порушник має у своєму розпорядженні один або декілька заповнених контейнерів (в останньому випадку передбачається, що вбудовування прихованої інформації здійснювалося тим самим способом). Завдання порушника може складатися у виявленні факту наявності стеганоканалу (основне завдання), а також у видобуванні даних чи визначенні ключа. Знаючи ключ, порушник матиме можливість аналізу інших стеганоповідомлень;

– атака на основі відомого вбудованого повідомлення. Цей тип атаки більшою мірою характерний для систем захисту інтелектуальної власності, коли в якості ЦВЗ, наприклад, використовується відомий логотип фірми. Завданням аналізу є одержання ключа. Якщо відповідний прихованому повідомленню заповнений контейнер невідомий, то завдання є вкрай важко розв’язуваним;

– атака на основі обраного прихованого повідомлення. У цьому випадку порушник може пропонувати для передачі свої повідомлення й аналізувати отримувані при цьому контейнери-результати;

– адаптивна атака на основі обраного прихованого повідомлення. Ця атака є окремим випадком попередньої. При цьому порушник має можливість обирати повідомлення для нав’язування їх адаптивно, в залежності від результатів аналізу попередніх контейнерів-результатів – атака на основі обраного заповненого контейнера.

Крім того, в порушника може існувати можливість застосувати ще три атаки, які не мають прямих аналогій в криптоаналізі:

– атака на основі відомого порожнього контейнера. Якщо останній є відомим порушнику, то шляхом порівняння його з підозрюваним на присутність прихованих даних контейнером, той завжди може встановити факт наявності стеганоканалу. У цьому випадку існує можливість побудови стійкої стеганосистеми;

– атака на основі обраного порожнього контейнера. У цьому випадку порушник здатний змусити користуватися запропонованим ним контейнером. Останній, наприклад, може мати більші однорідні області (однотонні зображення), і тоді буде важко забезпечити таємність вбудовування;

– атака на основі відомої математичної моделі контейнера або його частини. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі.

Основна мета атаки на стеганографічну систему аналогічна атакам на криптосистему з тією лише різницею, що різко зростає значимість активних (зловмисних) атак.

Однозначно стверджувати про факт існування прихованої інформації можна лише після її виділення в явному вигляді. Іноді метою стеганографічного аналізу є не алгоритм взагалі, а пошук, наприклад, конкретного стеганоключа, що використовується для вибору бітів контейнера в стеганоперетворенні.

Література

1. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. К.: «Центр навчальної літератури», 2018. 558 с.

2. Конахович Г. Ф., Пузиренко О. Ю. Комп'ютерна стеганографія. Теорія і практика. К.: «МК-Пресс», 2006. 288 с., іл.

УДК 004.9

ОНОВЛЕННЯ ДИЗАЙНУ І РОЗРОБКА FRONT-END ЧАСТИНИ САЙТУ НАУКОВОЇ БІБЛІОТЕКИ

П. К. Ніколюк, А. А. Ємельянова

Із розвитком технологій у сучасному світі люди все більше жадають знаходити всю потрібну їм інформацію тут і зараз за допомогою мережі Інтернет. Для того, щоб відвідувач залишився на веб-сайті, інформацію на ньому потрібно подавати лаконічно, у максимально привабливому та зручному для перегляду вигляді. Веб-сайт у наш час – це обличчя підприємства, компанії, навчального закладу тощо [1].

Веб-сайт університетської бібліотеки дещо відрізняється від загальної атмосфери головного сайту університету своїм зовнішнім виглядом, зручністю та стилем подання інформації. Тому метою цієї роботи є повний редизайн сайту із дотриманням кольорів та інших вимог, які зазначені в офіційному брендбуці університету, а також адаптування під різні мобільні пристрої, такі як планшет та смартфон.

Перш ніж почати роботу, потрібно ознайомитись із сайтом, який потрібно оновити, вивчити його структуру, дізнатись вимоги, визначити дані, які мають обов'язково бути у новому дизайні та сформувати технічне завдання, за яким відбуватиметься подальше моделювання і розробка.

Далі, після затвердження вимог, першим етапом є оновлення логотипу, оскільки це візитна картка бібліотеки, яка впливає на перше враження і впізнаваність у соціумі [2].

Рис. 1. Оновлений логотип бібліотеки (справа)

Наступним етапом є розробка макету дизайну сайту з урахуванням визначених вимог до зовнішнього вигляду і функціоналу. Здебільшого вся увага приділяється