Реєстраційна картка НДДКР

Державний реєстраційний номер: 0124U004134

Відкрита

Дата реєстрації: 25-09-2024

Статус виконавця: 17 - головний виконавець

1. Загальні відомості

Підстава для проведення робіт: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

КПКВК: 0111010

Напрям фінансування: 2.7 - інше (Стипендіальна робота в рамках іменної стипендії Верховної Ради України для молодих учених - докторів наук (Постанова Верховної Ради України від 22.08.2024 № 3925-IX))

Джерела фінансування

7713 - кошти держбюджету

Загальний обсяг фінансування (тис. грн.): 181.680

У тому числі по роках (тис. грн.):

Рік	Фінансування
2024	181.680

2. Замовник

Назва організації: Управління справами Апарату Верховної Ради України

Код ЄДРПОУ/ІПН: 44276271

Адреса: вул. М. Грушевського, 5, м. Київ, 01008, Україна

Підпорядкованість: Верховна Рада України

Телефон: 380442552847

Телефон: 380442552081

3. Виконавець

Назва організації: Чернящук Наталія Леонідівна

Код ЄДРПОУ/ІПН: 3109314886

Підпорядкованість:

Адреса: Чорновола, 44\51, м. Луцьк, Луцький р-н., Волинська обл., 43000, Україна

Телефон: 380958787095

4. Співвиконавець

5. Науково-технічна робота

Назва роботи (укр)

Детектування атак на основі міток компрометації

Назва роботи (англ)

Detection of attacks based on compromise marks

Мета роботи (укр)

Будь-яке відхилення статистики контрольованого зловмисником у каналі зв'язку повідомлення від середньостатистичних характеристик порожніх контейнерів кваліфікується як факт виявлення стеганоканалу. Така ідеальна модель не цілком адекватна реаліям інформаційно-приховуючих систем. По-перше, зловмисник знає характеристики не дійсно використаного відправником контейнера, а усереднені характеристики множини повідомлень деяких джерел, які потенційно можуть бути використані в якості контейнера. По-друге, всі відомі джерела можливих контейнерів у силу їх природи є нестаціонарними, тобто їх точних оцінок не існує. По-третє, приховувати інформацію для вбудовування приховуваної інформації вільні вибирати з усієї множини такі контейнери, характеристики яких відрізняються від відомих зловмиснику характеристик цієї множини. Більш того, відправник може підбирати такі контейнери або спеціально їх генерувати, щоб при вбудовуванні в них приховуваних повідомлень характеристики сформованого стега були б невідмінні від середньостатистичних характеристик порожніх контейнерів. По-четверте, у сучасних, комунікаційних системах передаються надлишкові повідомлення, як правило, стискуються з внесенням деяких допустимих для їх одержувачів спотворень, що змінюють їх характеристики. Наприклад, мовленнєвий сигнал кодується методами лінійного передбачення мови, зображення стискуються алгоритмами JPEG, MPEG або H.263. І, по-п'яте, канал зв'язку може вносити перешкоди в інформаційні потоки, що передаються. А якщо канал досконалий, то відправник для маскування може сам зашумляти передавані стеги та порожні контейнери такими перешкодами, які в допустимих межах передачі повідомлення, в достатній для приховування мірі модифікують статистику стегів та контейнерів.

Мета роботи (англ)

Any deviation of the statistics controlled by the attacker in the communication channel of the message from the average statistical characteristics of empty containers qualifies as the fact of detecting a steganochannel. Such an ideal model is not fully adequate to the realities of information-hiding systems. First, the attacker does not know the characteristics of the container actually used by the sender, but the averaged characteristics of a set of messages from some sources that can potentially be used as a container. Secondly, all known sources of possible containers are by their nature non-stationary, that is, their exact estimates do not exist. Third, to hide information for embedding hidden information, it is free to choose from the entire set such containers whose characteristics differ from the characteristics of this set known to the attacker. Moreover, the sender can select such containers or specially generate them so that when hidden messages are embedded in them, the characteristics of the formed stack would be no different from the average statistical characteristics of empty containers. Fourth, in modern communication systems, redundant messages are transmitted, as a rule, they are compressed with the introduction of some distortions acceptable for their recipients, which change their characteristics. For example, a speech signal is encoded using linear speech prediction methods, images are compressed using JPEG, MPEG or H.263 algorithms. And, fifthly, the communication channel can interfere with the transmitted information flows. And if the channel is perfect, then the sender for masking can make noise on transmitted tags and empty containers with such interference that, within the permissible limits of message transmission, modify the statistics of tags and containers to a sufficient extent for concealment.

Пріоритетний напрям науково-технічної діяльності: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності:

Вид роботи: 57 - науково-технічна розробка

Очікувані результати: Технології, Програмні продукти

Галузь застосування: Інформаційні технології

Експерти

6. Етапи виконання

Номер	Початок	Закінчення	Звітний документ	Назва етапу
1	01.2024	06.2025	Остаточний звіт	Детектування атак на основі міток компрометації

7. Індекс УДК тематичних рубрик НТІ

Коди тематичних рубрик НТІ: 20.56.03

Індекс УДК: , 33:659

8. Заключні відомості

Керівник організації:

Цьось Анатолій Васильович (д.фіз.вих., професор)

Керівники роботи:

Чернящук Наталія Леонідівна (д.пед.н., професор)

Відповідальний за подання документів: Чернящук Наталія Леонідівна (Тел.: +38 (095) 878-70-95)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.