Список використаних джерел

1. Ложкін Г. Інфомаційна безпека. Методи психологічного впливу [Електронний ресурс] / Г. Ложкін // Персонал. – 2003.
2. Толубко В. Б. Інфомаційна безпека. Методи психологічного впливу [Електронний ресурс] / В. Б. Толубко // Навчальний посібник. К. :НАОУ. – 2002..
3. Юдін О. К. Інфомаційна безпека. Методи психологічного впливу [Електронний ресурс] / О. К. Юдін // Навчальний посібник. Х.: Консум. – 2005..

УДК 004.056.55

СУЧАСНА КРИПТОГРАФІЯ. СИМЕТРИЧНЕ ТА АСИМЕТРИЧНЕ ШИФРУВАННЯ

Сич К. В., здобувач вищої освіти гр. КБ-181
Науковий керівник: **Семедяй С. М.,** викладач
Національний університет «Чернігівська політехніка»

До алгоритмів симетричного шифрування належать методи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або, що менш поширено, ключі різні, але споріднені та легко обчислюються). Ці алгоритми шифрування були єдиними загально відомими до липня 1976.

Сучасні дослідження симетричних алгоритмів шифрування зосереджено, в основному, навколо блочних та потокових алгоритмів шифрування та їхнього застосування. Блочний шифр подібний до поліалфавітного шифру Альберті: блочні шифри отримують фрагмент відкритого тексту та ключ, і видають на виході шифротекст такого самого розміру. Оскільки повідомлення зазвичай довші за один блок, потрібен деякий метод склеювання послідовних блоків. Було розроблено декілька методів, що відрізняються в різних аспектах. Вони є режимами дії блочних шифрів та мають обережно обиратись під час застосування блочного шифру в криптосистемі [1].

Шифри Data Encryption Standard (DES) та Advanced Encryption Standard (AES) є стандартами блочних шифрів, затверджених урядом США (однак, стандартизацію DES було скасовано після прийняття стандарту AES). Не зважаючи на те, що стандарт DES було визнано застарілим, він (та особливо його все ще дійсний варіант triple DES) залишається досить популярним; він використовується в багатьох випадках, від шифрування в банкоматах до забезпечення приватності електронного листування та безпечного доступу до віддалених терміналів. Було також розроблено багато інших шифрів різної якості. Багато з них було зламано.

Потокові шифри, на відміну від блочних, створюють ключ довільної довжини, що накладається на відкритий текст побітово або політерно, в дечому подібно до одноразової дошки. В потокових шифрах, потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем, та, в деяких алгоритмах, ще і потоком відкритого тексту. RC4 є прикладом добре відомого, та широко розповсюдженого потокового шифру.

Криптографічні гешувальні функції (англ. cryptographic hash functions, або англ. message digest functions) не обов'язково використовують ключі, але часто використовуються і є важливим класом криптографічних алгоритмів. Ці функції отримують дані (часто, ціле повідомлення), та обчислюють коротке, фіксованого розміру число (хеш). Якісні хешувальні функції створені таким чином, що дуже важко знайти колізії (два відкритих тексти, що мають однакове значення хешу).

Коди автентифікації повідомлень (англ. Message authentication code, MAC) подібні до криптографічних хешувальних функцій, за винятком того, що вони використовують секретний

ключ для автентифікації значення хешу при отриманні повідомлення. Ці функції пропонують захист проти атак на прості хешувальні функції [2].

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим. В асиметричних криптосистемах, відкритий ключ може вільно розповсюджуватись, в той час як приватний ключ має зберігатись в таємниці. Зазвичай, відкритий ключ використовується для шифрування, в той час як приватний (секретний) ключ використовується для дешифрування. Діффі та Хелман показали, що криптографія з відкритим ключем можлива за умови використання протоколу обміну ключами Діффі-Хелмана [3].

Отже, сучасні дослідження симетричних алгоритмів шифрування зосереджено, в основному, навколо блочних та потокових алгоритмів шифрування та їхнього застосування. Асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний.

Список використаних джерел

1. https://uk.wikipedia.org/wiki/Криптографія#cite_note-dh2-7
2. https://uk.wikipedia.org/wiki/Шифрування_з_симетричними_ключами
3. https://uk.wikipedia.org/wiki/Асиметричні_алгоритми_шифрування

УДК: 004.056.5

АНАЛІЗ СУЧАСНИХ SIEM ТЕХНОЛОГІЙ

Соколовська А. А., здобувачка вищої освіти гр. КБ-171
Науковий керівник: **Мехед Д. Б**., к.п.н., доцент
Національний університет «Чернігівська політехніка»

Технологія SIEM (Security information and event management) має на увазі аналіз в реальному часі подій безпеки в мережевих пристроях і додатках. У лінійку рішень SIEM входять різні додатки, прилади та послуги, які застосовуються для збору та аналізу інцидентів інформаційної безпеки.

Число атак за 2020 рік зросло на 59% в порівнянні з аналогічним періодом 2019 року. За моїми спостереженнями, гучні світові події неминуче супроводжуються зростанням числа кібератак, оскільки створюють сприятливий грунт для застосування зловмисниками методів соціальної інженерії. Так, квітень і травень 2020 року стали рекордними за кількістю успішних кібератак. Це можна пов'язати зі складною епідеміологічною та економічною ситуацією в світі, яка припала на ці місяці.

Зловмисники все частіше заражають жертв не одним типом шкідливого ПО, а відразу цілим «букетом» троянів. Так, в ході однієї з масових шкідливих кампаній кіберзлочинці доставляли на скомпрометовані комп'ютери шпигунське програмне забезпечення, ворующее збережені облікові дані з різних додатків.

Проаналізувавши найактуальніші атаки ІБ за 2020 рік можна виділити наступні:

Атаки на 5G. Адже перехід на технології 5G погіршує ситуацію з погрозами для телекомунікаційної галузі, оскільки архітектурні особливості 5G відкривають можливості для нових типів атак на мережі операторів.

Розвиток deep fake. З розвитком технологій штучного інтелекту і нейромереж зловмисники можуть створювати різноманітні інформаційні підробки - deep fake, які можуть використовуватися як для обходу біометричної ідентифікації, так і для обману громадськості та інших цілей.