УДК 621.326
Бреус В.
Одеський національний університет ім. І. І. Мечникова
Одеський національний морський університет

РОЗПОДІЛЕНА СИСТЕМА ЗАХИЩЕНОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ

Науковий керівник: д.ф-м.н., професор Андронов І.Л.

При обміні даними через комп'ютерні мережі існує небезпека того, що їх можуть отримати сторонні особи і використати з недобрими намірами. Для звичайного користувача це можуть бути паролі та інші конфіденційні дані, для компаній і підприємств – інформація, що може становити комерційну таємницю. Отримати їх можуть як за допомогою програм-сніферів, що перехоплюють інформацію при її передачі мережами загального користування, так і за допомогою шпигунських програм, несанкціоновано встановлених на комп'ютер.

З метою вирішення цієї проблеми ведеться розробка програмного забезпечення для захисту передачі даних в локальних комп'ютерних мережах та через мережу Інтернет. Основна ціль даного програмного продукту – забезпечити цілісність та безпеку інформації криптографічними засобами, зробити неможливим розшифрування перехоплених даних, та здійснити інтеграцію з іншим програмним забезпеченням.

Розроблена динамічно – підключаєма бібліотека, що може використовуватись при будь-якому програмному забезпеченні, що потребує захисту передачі даних. Із бібліотеки експортовані функції задання параметрів (ключі, метод шифрування, стиснення даних та ін.), шифрування та дешифрування даних. Зашифрований блок даних може бути розділений на частини заданого розміру. Опціонально вони можуть бути конвертовані з бінарного в ASCII формат (Base64). Таким чином, бібліотека може використовуватись для передачі даних як протоколами TCP/IP, де максимальний розмір пакету становить 64 Кбайта, так і протоколами ICQ, Jabber та інших систем миттєвої передачі повідомлень, де максимальний розмір пакету значно менший, але вирішена проблема відсутності зовнішньої ір–адреси.

На основі цієї бібліотеки йде розробка розподіленої системи захищеної передачі даних. Система складається з ряду вузлів (програм – сервісів, запущених на декількох комп'ютерах). Під час ініціалізації сеансу передачі даних вказується або обирається випадковий вихідний вузол, вибірка вузлів, що будуть брати участь у поточному сеансі. Проводиться опитування вузлів, під час якого встановлюється їх працездатність та генеруються ключі для шифрування. Використовуються ключі декількох типів: ті, що передаються від клієнта всім вузлам в зашифрованому вигляді (задані користувачем або випадкові); ті, що взагалі не передаються, а генеруютья вузлами на основі деяких параметрів комп'ютерів та ін.; ті, що генеруються на основі поточних даних (час та ін.). Після цього програма-клієнт розбиває зашифровану інформацію на блоки, обирає поточний вузол, шифрує блок за допомогою ключів і відправляє на цей вузол. Далі (згідно налаштувань) цей блок направляється на вихідний вузол або на інший випадковий. Блоки даних збираються і дешифруються тільки на вихідному вузлі.

Планується розробка локального шифруючого проксі-сервера, що дозволить використовувати можливості даної бібліотеки та розподіленої системи для анонімної роботи в WWW за допомогою звичайного web-браузера.

Дане програмне забезпечення може бути корисним як для індивідуальних користувачів, так і для корпоративних клієнтів.