Wrocław 01.10.2020

C Y B E R B E Z P I E C Z E Ń S T W O

L A B 5

1. Wstęp

Celem laboratorium jest zapoznanie się z elementami kryptoanalizy dla algorytmów symetrycznych i asymetrycznych. Poniżej znajduje się lista terminów zawierających teoretyczne modele ataków i ich praktyczne zastosowanie.

Bruteforce

Ten typ ataku polega na sprawdzeniu każdej możliwej kombinacji w kluczu w celu znalezienia „klucza" do prawidłowego rozszyfrowania wiadomości. Ataki Bruteforce mogą zająć mniej czasu w przypadku mniejszych przestrzeni kluczy, ale w przypadku większych przestrzeni kluczy zajmują wyjątkowo dużo czasu. Ataki Bruteforce są nie-praktyczne w przypadku nowoczesnych algorytmów szyfrowania.

Atak ze znanym szyfrogramem

W przypadku tego typu ataku napastnik zna szyfrogramy różnych wiadomości, które zostały zaszyfrowane przy użyciu tego samego algorytmu szyfrowania. Atakujący musi znaleźć klucz, którego można następnie użyć do odszyfrowania wszystkich wiadomości. Jest to jeden z najłatwiejszych do przeprowadzenia ataków, ponieważ łatwo jest przechwycić zaszyfrowany tekst (poprzez podsłuch), ale jest trudny do wykonania, ponieważ wiedza na temat procesu szyfrowania jest ograniczona.

Atak z wybranym tekstem jawnym

Atak z wybranym tekstem jawnym jest podobny do ataku na „znany tekst jawny", ale w tym przypadku atakujący wybiera własne teksty, aby znaleźć klucz. Odpowiednio dobrana sekwencja znaków z wygenerowanym szyfrem może przywrócić klucz. Znaleziony klucz może posłużyć do uzyskania informacji o całym procesie szyfrowania i zrozumienia, jak jest on wykonywany. Atakujący analizuje zachowanie systemu i wyprowadza zaszyfrowany tekst na podstawie dowolnego rodzaju danych wejściowych.

Atak ze znanym tekstem jawnym

W przypadku ataku ze znanym tekstem jawnym osoba atakująca zna niektóre z nich i szyfruje je. Następnie do znalezienia klucza używana jest inżynieria odwrotna. Ataki tego typu były używane tylko do łamania prostych szyfrów.

Analiza różnicowa

Atakujący obserwuje zmiany w dwóch tekstach do postaci zaszyfrowanej. Na podstawie zachodzących zmian atakujący próbuje znaleźć klucz. Jest to rodzaj ataku typu „wybrany tekst jawny", ponieważ atakujący wybiera zwykły tekst, aby obserwować zmiany. Atak został wykorzystany do złamania algorytmów symetrycznych, takich jak DES, ale z czasem kolejne algorytmy stały się odporne.

Analiza liniowych zależności

Osoba atakująca przeprowadza atak ze znanym tekstem jawnym na kilka wiadomości zaszyfrowanych tym samym kluczem. Daje to atakującemu wgląd w prawdopodobieństwo wystąpienia określonego klucza na podstawie odkrytych zależności pomiędzy wartością klucza, tekstu jawnego i kryptogramu.

Analiza częstości

Analiza częstości jest podobna do ataku na znany szyfrogram. Atak polega na analizie liter i grup liter pod kątem określonego języka. Znajomość języka jest ważna, ponieważ każdy język ma swoją częstotliwość występowania danych liter. Popularne znaki w zaszyfrowanym tekście są wyszukiwane i konwertowane na popularne znaki w danym języku.

Atak powtórzenia

Intruz wysyła do ofiary tę samą wiadomość, co we wcześniej zaobserwowanej komunikacji ofiary. Pozwala to na uwierzytelnienie intruza przez jedną ze stron i traktowanie go jako zaufanego podmiotu w komunikacji. Intruz może uzyskać nieautoryzowany dostęp i może wydobyć żądane informacje. Ten typ ataku jest podobny do ataku typu Man-in-the-Middle.

3. Zapoznanie się ze środowiskiem pracy - program CrypTool, FineCrypt, inne.

- Na tych zajęciach laboratoryjnych będą wykorzystywane głównie narzędzia dostępne z zakładki z programu CrypTool:
    - *Kryptoanaliza/Algorytmy symetryczne*
    - *Kryptoanaliza/Algorytmy asymetryczne*

4. Ocena możliwości kryptoanalizy algorytmów symetrycznych.

Zadania:

1. Proszę ocenić czas potrzebny do odnalezienia pełnego klucza o długości 64, 128, 192, 256 bitów.
2. Proszę porównać czasy poszukiwania kluczy o tej samej długości (np. 128 bitów) dla różnych algorytmów.
3. Proszę określić czas poszukiwania klucza przy 4,8,12,16,20,24, ... nieznanych bitach. (Jedna gwiazdka w kluczu = 4 bity)
4. Proszę sprawdzić czy pozycja nieznanych bitów w kluczy wpływa na czas poszukiwania klucza.
5. Proszę ocenić jakość działania algorytmu łamiącego.
   Czy każdorazowo otrzymujemy poprawny klucz?
   Czy liczba szukanych bitów wpływa na jakość odtwarzanego klucza?
   Czy pozycja nieznanych bitów wpływa na jakość odtwarzanego klucza?

Wnioski/Pytania:

1. Czy współczesne algorytmy blokowe możemy uznać za bezpieczne (w świetle przeprowadzonych eksperymentów)?
2. Jaka długość klucza oferuje nam wystarczający poziom bezpieczeństwa? (Dlaczego?)
3. Czy wielkość kryptogramu ma wpływ na możliwość jego złamania?
4. Czy format i wcześniejsze przetwarzanie dokumentu (kompresja, zmiana formatu dokumentu,...) wpływa na możliwość jego kryptoanalizy?
5. Ile możliwych haseł możemy sprawdzić przez rok nieustannej pracy na jednym komputerze, który sprawdza milion haseł w ciągu sekundy (~2^{20})?
   Co ten wynik mówi o bezpieczeństwie współczesnych algorytmów?

5. Ocena możliwości kryptoanalizy algorytmów asymetrycznych.

Zadania:

1. Proszę rozłożyć na czynniki pierwsze liczbę powstałą z połączenia wartości oznaczających:
   - Numer indeksu
   - Bieżący rok
   - Miesiąc
   - Dzień
   - Godzinę
   - Minutę

   Zakładka: *Algorytmy/Kryptosystem RSA/test pierwszości*
2. Proszę sprawdzić jak rośnie czas poszukiwania liczb pierwszych wraz ze wzrostem wartości przeglądanego przedziału.

   Zakładka: *Algorytmy/Kryptosystem RSA/Generowanie liczb pierwszych*
3. Proszę sprawdzić jak zależy skuteczność oraz czas potrzeby na realizację ataku faktoryzacji modułu N algorytmu RSA dla różnych wartości parametrów: Długość N, Długość p, Długość znanego ciągu bitów P.

   Zakładka: *Kryptoanaliza/Algorytmy asymetryczne/ Ataki oparte na kracie /faktoryzacja z podpowiedzią*

   (skorzystać z przykładów generowanych przez program)
4. Proszę zapoznać się z metodą ataku dostępną w zakładce:

   Kryptoanaliza/Algorytmy asymetryczne/ Ataki oparte na kracie /Ataki na wiadomości stereotypowe

   i spróbować odnaleźć brakujący fragment tekstu z załączonego pliku lab_5_number.txt
5. Proszę zapoznać się z metodą ataku dostępną pod zakładką:

   Kryptoanaliza/Algorytmy asymetryczne/ Ataki oparte na kracie /Atak na mały tajny klucz

   i spróbować dokonać faktoryzacji modułów z załączonego pliku lab_5_number.txt

Wnioski/Pytania:

1. Jaka jest minimalna długość modułu (liczba N) algorytmu RSA, która gwarantuje, że jej rozkład (znalezienie jej czynników pierwszych) będzie dostatecznie trudne.
2. Czy dla przyjętej we wcześniejszym punkcie jako bezpiecznej długości modułu, można przeprowadzić skuteczny atak faktoryzacji w oparciu o częściową znajomość wartości jednego parametru? (zadanie 3)
3. W jakich przypadkach szyfrowanie algorytmem RSA może być zagrożone przez atak realizowany w punkcie 4?
4. W jakich przypadkach szyfrowanie algorytmem RSA może być zagrożone przez atak realizowany w punkcie 5?

6. Raport z przeprowadzonych eksperymentów.

Raport powinien mieć postać dokumentu elektronicznego, w którym zostanie zapisany przebieg realizowanych w trakcie zajęć eksperymentów (np. fragment treści tekstu jawnego, parametry algorytmu szyfrowania, fragment kryptogramu) oraz wnioski, spostrzeżenia, odpowiedzi na pytania umieszczone w instrukcji laboratoryjnej, itp.