Cold boot attack

Karolina Stanko
11.04.2019r.

Idea : Szyfrowanie nie chroni

- Atakujący ma fizyczny dostęp do komputera pozostającego w uśpieniu
- Podłącza do wyłączonego komputera urządzenie, np. klips USB, z własnym systemem operacyjnym, ponownie włącza maszynę i odczytuje zawartość jej pamięci RAM, w której znajdują się klucze kryptograficzne
- Możliwość uzyskania dostępu do dysków chronionych popularnymi programami, takimi jak BitLocker, FileVault, dm-crypt i TrueCrypt

Rozwiązania techniczne

- zawartość pamięci RAM nie znika natychmiast po odłączeniu zasilania
- dane mogą pozostawać w niej nawet przez kilkadziesiąt sekund, co daje atakującemu czas na ich odczytanie
- możliwe jest przedłużenie czasu przechowywania informacji przez RAM (atakujący musi jedynie schłodzić układy pamięci.W tym celu można wykorzystać sprężone powietrze w puszkach, dostępne w większości sklepów komputerowych)
- przeprowadzone eksperymenty wykazały, że dobrze schłodzony układ pamięci można nawet wyjąć z komputera bez utraty zawartych w nim danych
- liczba błędów w danych przechowywanych w układach RAM po odłączeniu zasilania na od 60 do 600 sekund wahała się od 41 do 50 procent wówczas, gdy kości były przechowywane w temperaturze pokojowej. Natomiast gdy układy schłodzono do temperatury -50 stopni Celsjusza, liczba błędów wahała się od 0% do 0,18%

Zastosowanie:

1. Cyfrowe dochodzenia sądowe

2. Nadużycia techniki przez złodziei

3. Odzwyskiwanie danych

Możliwość obejścia szyfrowania dysku

1. **Bitlocker**

- Bitlocker w swojej domyślnej konfiguracji korzysta z zaufanego modułu platformy, który nie wymaga szpilki ani klucza zewnętrznego do deszyfrowania dysku
- Po uruchomieniu systemu operacyjnego funkcja BitLocker pobiera klucz z modułu TPM bez interakcji użytkownika
- atakujący może włączyć komputer, poczekać, aż system operacyjny rozpocznie uruchamianie, a następnie wykonać atak na komputer, aby pobrać klucz
- Z tego powodu uwierzytelnianie dwuskładnikowe, takie jak PIN przed uruchomieniem lub wymienne urządzenie USB zawierające klucz startowy wraz z modułem TPM, powinno być używane do obejścia tej luki w domyślnej implementacji Bitlockera

Przechowywanie kluczy szyfrowania

1**. Register-based key storage (pamięć kluczy oparta na rejestrze)**

- Przechowywanie kluczy w oparciu o rejestr (Implementacje tego rozwiązania to TRESOR i Loop-Amnesia)
- Implementacje te modyfikują jądro systemu operacyjnego, dzięki czemu rejestry procesora (w przypadku TRESOR-a rejestry debugowania x86 oraz w przypadku Loop-Amnesia rejestry profilowania AMD64 lub EMT64) mogą być używane do przechowywania kluczy szyfrowania, a nie w pamięci RAM
- Klucze przechowywane na tym poziomie nie mogą być łatwo odczytane z przestrzeni użytkownika i są tracone, gdy komputer uruchamia się ponownie z jakiegokolwiek powodu

2. Cache-based key storage (Pamięć kluczy oparta na pamięci podręcznej)

- Działa poprzez wyłączenie pamięci podręcznej procesora L1 procesora i używa go do przechowywania kluczy, jednak może to znacznie obniżyć ogólną wydajność systemu do tego stopnia, że jest zbyt wolny dla większości celów

Demontaż zaszyfrowanych dysków

Najlepsza praktyka zaleca demontaż wszystkich zaszyfrowanych, niesystemowych dysków, gdy nie są używane, ponieważ większość oprogramowania do szyfrowania dysków jest przeznaczona do bezpiecznego kasowania kluczy buforowanych w pamięci po użyciu. Zmniejsza to ryzyko, że atakujący będzie mógł odzyskać klucze szyfrowania z pamięci, wykonując atak. Aby zminimalizować dostęp do zaszyfrowanych informacji na dysku twardym systemu operacyjnego, urządzenie powinno zostać całkowicie wyłączone, gdy nie jest używane, aby zmniejszyć prawdopodobieństwo udanego ataku przy zimnym rozruchu. Skonfigurowanie systemu operacyjnego do wyłączenia lub hibernacji, gdy nie jest używany, zamiast korzystania z trybu uśpienia, może pomóc zmniejszyć ryzyko udanego ataku.

Zapobieganie atakom

1. Dostęp fizyczny

- Lutowanie lub przyklejanie modułów pamięci do płyty głównej, przez co nie można ich łatwo usunąć z gniazd i włożyć do innej maszyny pod kontrolą atakującego
- Nie uniemożliwia to jednak atakującemu uruchomienia komputera ofiary i wykonania zrzutu pamięci za pomocą wymiennego dysku flash USB
- Ograniczenie, takie jak UEFI Secure Boot lub podobne metody weryfikacji rozruchu, może skutecznie uniemożliwić osobie atakującej uruchomienie niestandardowego środowiska oprogramowania w celu zrzucenia zawartości wlutowanej pamięci głównej

2. Pełne szyfrowanie pamięci

- Szyfrowanie oparte na oprogramowaniu, podobne do przechowywania klucza opartego na CPU
- Kluczowy materiał nigdy nie jest wystawiony na działanie pamięci, ale jest bardziej wszechstronny - cała zawartość pamięci jest szyfrowana

3. Bezpieczne usuwanie pamięci

- ataki są wymierzone w niezaszyfrowaną pamięć o dostępie swobodnym, więc jednym z rozwiązań jest wymazanie poufnych danych z pamięci, gdy nie jest już używana

4. System Tails

- dane w pamięci RAM są zastępowane losowymi danymi podczas zamykania Tails, co powoduje usunięcie wszystkich śladów z sesji na tym komputerze

Dziekuję za uwagę! :)