Odhalení klíče AES sledováním běhu programu

Diplomová práce vypracovaná Jonatanem Matějkou pod vedením Ing. Josefa Kokeše

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

AUTOMATICKÉ ROZPOZNÁNÍ ŠIFRY AES

Šifra AES je nejpoužívanější symetrická bloková šifra. Denně se s ní setkáváme v zabezpečených komunikačních protokolech a při skladování dat. V jedné oblasti nás ale použití této šifry netěší – v nevyžádaném software. Může to být ransomware, který proti naší vůli šifruje naše cenná data a požaduje výkupné za jejich dešifrování, nebo klient botnetu, který se šifrovaně domlouvá na dalším cíli útoku. V takových situacích by bylo vhodné mít k dispozici nástroj, který by šifrovaná data odhalil.

V této práci jsme pro tento účel navrhli algoritmus. Sledováním přístupů do S-Boxu při běhu programu jsme schopni odhalit klíče a data použitá při šifrování. Algoritmus jsme následně implementovali pro systém Microsoft Windows a architekturu Intel x86. Výsledný program nalezne použité klíče a data v programech provádějících AES šifrování pomocí kryptografických knihoven a v běžných uživatelských aplikacích.

Program jsme úspěšně otestovali na knihovnách OpenSSL, CryptoPP, Botan a na šifrovacím rozhraní pro Microsoft Windows. Dále jsme automaticky odhalili data ukládaná do šifrovaného ZIP archivu a data přenášená protokoly HTTPS a SSH.

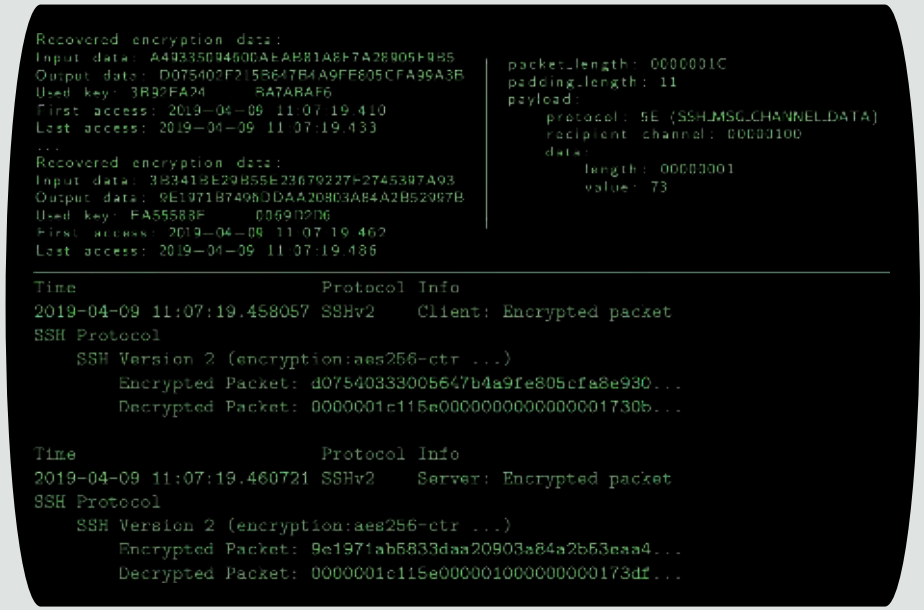
OD S-BOXU K POUŽITÉMU KLÍČI

Jako klíčovou součást implementace šifry AES jsme určili substituční tabulku. Většina programů a knihoven využívající AES obsahuje tuto strukturu ať už ve formě standardního S-Boxu, nebo v podobě T-Tabulek předpočítaných pro urychlení výpočtu. Tuto posloupnost bajtů můžeme v paměti sledovaného procesu jednoduše automaticky identifikovat.

Nastavením přístupových práv paměťové stránce obsahující S-Boxu můžeme sledovaný program zastavit v okamžiku provádění substitučního kroku šifry. Tímto postupem získáme posloupnost substituovaných bajtů. Uspořádání jednotlivých bajtů je závislé na konkrétní implementaci. Po zjištění pořadí přístupů do S-Boxu aplikujeme inverzní kroky a získáme šifrovací klíč (v případě substituce při expanzi klíče) nebo šifrovaná data (v případě substituce při výpočtu rundy). Pro určení pořadí jsme navrhli robustní algoritmus, který využívá aritmetických závislostí mezi jednotlivými bajty posloupnosti.

UKÁZKA ODHALENÍ SSH SPOJENÍ

Jedním z programů, na kterém jsme náš nástroj vyzkoušeli, je SSH klient PuTTy. V kombinaci s nástrojem Wireshark jsme byli schopni číst přenášená data v nezašifrované podobě.



UŽITEČNÝ NÁSTROJ PRO KAŽDÉHO

Výsledkem této práce je nástroj, který výrazně ulehčuje analýzu programů využívajících šifru AES, ať už pro účely bezpečné komunikace nebo skladovaní dat. Díky tomu si jistě najde cestu do sbírek nástrojů mnoha reverzních inženýrů a zvídavých uživatelů.