HOGYAN MITM-ELJÜNK MITM-ELÉS NÉLKÜL

SOME PEOPLE, WHEN CONFRONTED WITH TLS DECRYPTION, THINK "I KNOW, I'LL USE MITM." NOW THEY HAVE TWO PROBLEMS.

silent signal

Veres-Szentkirályi András 2020-05-29

$ whoami

Veres-Szentkirályi András

- OSCP, GWAPT, SISE
- Silent Signal társalapító (2009-)
- IT biztonsági szakértő, pentester, toolmaker

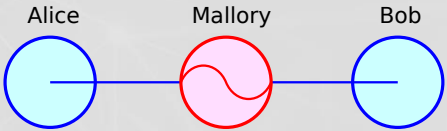
Bevezetés

silent signal

- https://blog.silentsignal.eu/2020/05/04/decrypting-and-analyzing-https-traffic-without-mitm/
- hálózati forgalmat sniffelni hasznos
- nem új támadás, inkább felderítési technika
- TLS: titkosítás, integritásvédelem és autentikáció
- MITM: a legtöbb ember első eszköze

MITM

- Alice és Bob kommunikálnának
- és köztük áll Mallory
  - aktív támadó (vö. Eve passzív)
  - képes módosítani üzeneteket
  - képes kicserélni üzeneteket
  - képes újraküldeni régi üzeneteket



MITM demo

silent signal

- Burp Suite tanúsítványát elfogadja a kliens
- Burp: TLS kliens és szerver egyszerre
- plain text triviálisan megszerezhető

MITM problémák

silent signal

- key/cert pinning
- kliens tanúsítvány
- nem-HTTP forgalom
- ezek tetszőleges kombinációja

MITM-en túl

silent signal

- mindkét végpont kompromittálható
- szerver: RSA vs. PFS
- kliens: (Pre-)Master Secret
  - Pre: ami ma DH/ECDH kulcscsere, régen RSA feloldás eredménye
  - Master Secret: 48 bájtos hosszú magas entrópiájú tömb
  - ebből lesz: $\{client, server\} \times \{write, MAC\}$
  - `https://www.cryptologie.net/article/340/tls-pre-master-secrets-and-master-secrets/`

Frida demo

silent signal

- „belemászunk” a processbe
  - futásidőben *(server)*
  - előre csomagolva *(gadget)*
- meghookoljuk a megfelelő OpenSSL függvényeket
  - `https://github.com/saleemrashid/frida-sslkeylog`
- kiolvassuk a (Pre-)Master Secretet
- Wireshark feloldja a titkosítást

Absztrakt összefoglalás

- nem mindig egyértelmű, mi a legjobb út
- ahogy előrébb haladunk egy úton, kiderülhet, hogy az mégsem olyan jó, `GOTO 10`
- a hackelés akkor az igazi, ha rájövünk, hogy a járt és a(z éppen) járatlan utat is érdemes megnézni

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t

silent signal