DROWN: Breaking TLS using SSLv2

Student: Pipis Raul-Alex
Grupa:341C4

TLS fiind cel mai utilizat protocol de securitate din Internet, acesta transportand cele mai multe date criptate, multi rau voitori doresc sa profite de eventuale brese de securitate in structura acestuia. Multe brese de securitate exista in versiunile mai vechi, mai precis in precursorul acestuia, SSLv2.

Atacul DROWN se bazeaza pe o astfel de bresa de securitate in SSLv2, mai precis raspunsul la un padding incorect de tip PKCS1v1.5 la o criptare RSA. In sine acesta nu ar trebui sa mai fie o problema, SSLv2 fiind deprecat, dar atunci care este problema? Problema majora este ca destul de multe servere(33% in 2016) inca au un server SSLv2 care ruleaza in paralel cu cel TLS. In mod normal sunt entitati separate, dar datorita impartirii a aceleiasi cheie RSA, date trimise sau primite de server-ul TLS put fi sparte cu ajutorul server-ului SSLv2.

Metoda de atac este un atac Bleichenbacher modificat, un atac de tipul Chosen Ciphertext, care cu un efort mediu computational si folosindu-se de informatia data de catre server-ul SSLv2, mai precis corectitudinea padding-ului, reuseste sa decripteze integral mesajul.

Ca si etape ale atacului se disting urmatoarele:

1. Acumularea a peste 1000 de mesaje de tipul ClientKeyExchange primite de server-ul TLS
2. Gasirea unui mesaj care, modelat prin inmultire cu o fractie ridicata la puterea exponentului de criptare sa genereze un mesaj SSLv2 cu padding valid.
3. Efectuarea a 3 rotatii prin inmultirea cu 3 numere care trebuie identificate
4. Aplicarea atacului Bleichenbacher
5. Revenirea la mesajul initial

Personal am facut o implementare completa a atacului, doar partial functionala in timp util(prima etapa gata in aproximativ 10s), atacul optimizat consumand aproximativ 2^50 calcule, implementarea in Python rulata pe un laptop neavand sperante sa reuseasca ceva.