Universitat de Girona
Escola Politècnica Superior

Treball Final de Màster

Estudi: Màster en Ciència de Dades

Títol: Side channel attack against the Mbed TLS implementation of the RSA algorithm.

Document: Resum

Alumne: Victor Micó Biosca

Tutor: David Juher Barrot
Departament: Departament d'Informàtica, Matemàtica Aplicada i Estadística
Àrea: Matemàtica Aplicada

Convocatòria (mes/any): Juny 2023

Universitat de Girona
Escola Politècnica Superior

TREBALL FINAL DE MÀSTER

Side channel attack against the Mbed TLS implementation of the RSA algorithm.

Autor:
Victor MICÓ BIOSCA

Juny 2023

Màster en Ciència de Dades

Tutor:
David JUHER BARROT

Índex

CAPÍTOL 1

Introducció

Els dispositius criptogràfics són capaços de rebre un missatge a través d'una interfície, xifrar el contingut del missatge i transmetre el missatge xifrat. Generalment, també són capaços de fer l'operació a l'inversa: rebre un missatge xifrat, desxifrar-lo i transmetre el missatge en text pla.

La seguretat d'aquests dispositius no només es basa en la robustesa dels seus algoritmes sinó en la impossibilitat teòrica d'extraure'n les claus criptogràfiques que contenen. L'acció d'intentar obtenir les claus d'un dispositiu criptogràfic sense autorització s'anomena atac.

Els atacs a dispositius criptogràfics es poden dividir en dues grans categories:

- Atacs actius: Un atac actiu consisteix a manipular els *inputs* o l'entorn del dispositiu amb l'objectiu que funcioni de manera errònia o diferent de les condicions normals. Amb la injecció de faltes (*fault injection*) és possible fer passar un PIN dolent per bo o extreure claus criptogràfiques, entre d'altres.

- Atacs passius: En un atac passiu, l'atacant extreu informació del dispositiu a través de canals laterals (*side-channel*) mentre que el dispositiu funciona en condicions normals. Aquests canals laterals poden ser el consum elèctric, la radiació electromagnètica o, fins i tot, el so o la temperatura.

Obtenir les claus dels dispositius mencionats anteriorment pot suposar aconseguir l'accés al compte bancari d'una persona, poder interceptar les seves comunicacions o suplantar-ne la identitat. És per això que aquests tipus d'atacs tenen un gran interès entre la comunitat acadèmica i contínuament se'n publiquen de nous i contramesures per a evitar-los.

L'objectiu d'aquest treball és realitzar un atac de canal lateral a una implementació de codi obert de l'algoritme RSA.

Tot i que a l'estat de l'art es mencionen moltes publicacions sobre com realitzar atacs de canal lateral, la majoria es centren en els algoritmes de clau simètrica. Entre les publicacions de clau asimètrica, en són poques les que publiquen de manera oberta les dades i el codi per reproduir l'atac.

CAPÍTOL 2

Objectius

En aquest treball s'ha dut a terme un atac a la versió 2.5.1 de la llibreria Mbed TLS, que implementa un algoritme d'exponenciació RSA-CRT utilitzant el mètode de *Sliding windows*.

Les motivacions del treball són les següents:

1. Enrobustir la llibreria de codi lliure Mbed TLS.
2. Fer difusió dels mètodes de captura, processament i atac d'un algoritme de clau asimètrica.
3. Publicar de manera oberta l'anàlisi i les traces.

CAPÍTOL 3

Procés de desenvolupament del TFM

La idea inicial del projecte es va presentar al *NewAE ChipWhisperer Contest 2021*. L'objectiu era generar *datasets* per a analitzar la viabilitat de realitzar atacs de *clustering* sobre algoritmes de finestra com el k-ary utilitzant tres mides de k diferents (2, 3 i 4) .

La proposta va estar guardonada amb:

- ChipWhisperer-Husky
- CW305 Artix FPGA 7A35 Target Board
- Una còpia signada del llibre *The Hardware Hacking Handbook*

La primera tasca va consistir a buscar implementacions públiques d'RSA o ECC per a una FPGA. Tot i trobar-ne, la dificultat de programar una FPGA per adaptar-ne el codi va fer que desestimés aquesta proposta.

Després de parlar-ho amb Jean-Pierre Thibault *(Senior Security Engineer)* i Colin O'Flynn(*CEO)* a *NewAE Technology Inc.* vaig decidir encaminar el treball a atacar una llibreria pública i presentar-ne els resultats en aquest treball.

Aquest és el mètode proposat per a l'anàlisi:

1. Analitzar les diferents llibreries públiques d'RSA i seleccionar-ne una que utilitzi un algoritme d'exponenciació de finestra per a realitzar l'atac
2. Capturar una traça
3. Realitzar una anàlisi visual de la traça de potència, identificar les regions de l'RSA i les operacions modulars
4. Desenvolupar un mètode per a distingir quadrats de multiplicacions
5. Desenvolupar un mètode per a distingir els diferents valors precalculats
6. En cas d'obtenir resultats satisfactoris, informar als desenvolupadors de la llibreria de la vulnerabilitat.

CAPÍTOL 4

Resultats

L'atac es basa en la captura d'una traça de l'operació RSA i s'ha realitzat un SPA per identificar les dues exponenciacions. A través de l'anàlisi de correspondència de patrons, s'ha aconseguit inferir la seqüència d'operacions modulars, distingint entre quadrats i multiplicacions.

A partir d'aquesta fase, s'ha obtingut aproximadament el 30% dels bits de cada exponent. Identificant l'inici de cada finestra, s'ha pogut localitzar la regió on es carreguen els bits. Emprant la tècnica de correspondència de patrons, s'ha determinat la totalitat dels bits de tots dos exponents.

La següent taula mostra un resum dels resultats obtinguts per a les dues exponenciacions durant les dues fases de l'atac.

	1ª exponenciació	2ª exponenciació
Distingir quadrats de multiplicacions	33,98%	30,91%
Distingir bits de cada finestra	99,80%	100%

Taula 4.1: Resum de resultats

CAPÍTOL 5

Conclusions

Aquest treball demostra que els atacs de canal lateral són factibles, es poden realitzar amb un pressupost ajustat i amb mètodes relativament senzills de processat de senyal.

Com a treball futur es proposa:

1. Actualitzar el codi de la llibreria Mbed TLS a l'última versió per comprovar si és possible explotar aquesta vulnerabilitat.

2. Provar altres dispositius *target* alternatius a l'STM32F3.

3. Utilitzar altres tècniques per extreure els valors de l'exponent, com algoritmes de *clustering*.

Aquestes iniciatives permetran ampliar el coneixement sobre la vulnerabilitat detectada i buscar solucions més efectives per protegir les implementacions criptogràfiques basades en la llibreria Mbed TLS.