



УНИВЕРЗИТЕТ СИНГИДУНУМ
ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Цурење информација преко бочних канала и њихов утицај на безбедност криптографских механизма

- Дипломски рад -

Ментор:

Доц. др Саша Адамовић

Студент:

Алиса Деспић

Бр. Индекса: 2013201609

Београд, 2014.



ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

УНИВЕРЗИТЕТ СИНГИДУМУ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Београд, Данијелова 32

Кандидат: Алиса Деспих

Број индекса: 2013/201609

Смер: Информатика и рачунарство

Тема: Цурење информација преко бочних канала и њихов утицај на безбедност криптографских механизма

Датум одобрења рада:
Београд, _____._____._____.

МЕНТОР:

Доц. др Саша Адамовић

ДЕКАН:

Проф. др Драган Цветковић

Цурење информација преко бочних канала и њихов утицај на безбедност криптографских механизма

Сажетак: У раду истражујемо област која се бави бочним каналима комуникације, у рачунарским комуникационим системима познатијим као КЕМЗ (компромитијућа електромагнетна зрачења). Бочни комуникациони канали у рачунарским системима представљају канале преко којих долази до цурења информација на невербалан начин и поред постојања протокола који подразумевано обезбеђују сервисе за заштиту података. У овом случају, бочни канал за комуникацију настаје преко електромагнетних поља, која настају у раду свих електро уређаја. Иако се данас за заштиту података највише користе софтверска крипто решења, сваки софтвер се извршава на рачунару и тај рачунар ствара своје електромагнетно поље које је компромитијуће. Показало се да су електромагнетна поља у неким фреквенцијским опсезима специфична за сваки уређај, садрже модулацију која се може детектовати са веће удаљености и трансформисати у информацију. Електронско прислушкивање путем оваквих компромитијућих електромагнетских зрачења, представља пасивну инфилтрацију нападача коју је тешко открити, као и један од стварних типова напада преко којих је безбедност озбиљно угрожена. Све ово посебно представља опасност за компактне и физички изоловане рачунарске и информационе системе. Главни циљ рада је да се студиозно сагледа ова врста проблематике, да се истакну најактуелнији проблеми у овој области и да се сагледају све могућности заштите у виду процедура и препорука које нас могу довољно заштитити од постојања бочних комуникационих канала.

Кључне речи: компромитијућа електромагнетна зрачења, електромагнетно поље, бочни канали

Abstract: In this paper, we investigate an area that deals with the side channels of communication in computer communication systems known as CER (compromising electromagnetic radiation). The side channels of communication in computer systems are channels through which there is a leak in a non-verbal way, despite the existence of protocols that provide default services for data protection. In this case, the side channel formed for communication over the electromagnetic field, which is generated in the operation of electrical devices. Though the current data protection most used software encryption solutions, each software runs on a computer and the computer creates its own magnetic field that is compromising. It has been shown that the electromagnetic fields in certain frequency bands specific to each device, comprising modulation that can be detected with greater distances and transformed into information. Electronic eavesdropping by such compromising electromagnetic radiation, represents a passive attacker infiltration that is hard to detect, and one of the real attack types over which security is seriously threatened. All this is especially a danger for compact and physically isolated computer and information systems. The main objective of this paper is to meticulously examine these types of issues, to highlight the most current issues in this area and to look at all the possibilities of protection in the form of procedures and recommendations that we can sufficiently protect the existence of lateral communication channels.

Keywords: compromising electromagnetic radiation, electromagnetic field, side channels

Садржај

1. Увод	- 2 -
1.1 Предмет истраживања	- 2 -
1.2 Невербална комуникација	- 3 -
1.3 Доприноси рада	- 4 -
1.4 Структура рада	- 5 -
2. Преглед у области истраживања	- 6 -
2.1 Историја напада бочним каналима	- 6 -
2.2 Модели напада преко бочних канала	- 8 -
2.3 Класификација напада преко бочних канала	- 10 -
2.3.1 Конторола над процесом израчунавања	- 10 -
2.3.2 Начини којима се приступа модулу	- 10 -
2.3.2.1 Инвазивни напади	- 10 -
2.3.2.2 Полуинвазивни напади	- 11 -
2.3.2.3 Неинвазивни напади	- 11 -
2.3.3 Коришћене методе у процесу анализе	- 11 -
3. Теоријске основе истраживања	- 13 -
3.1 Електромагнетска компатибилност	- 13 -
3.2 Извори сметњи	- 13 -
3.3 Простирање сметњи	- 15 -
3.4 Дејство сметњи	- 16 -
3.5 Мере за испуњење електромагнетске компатибилности	- 17 -
3.6 ФИПС 140 стандард и слични проблеми	- 19 -
4. Напади преко бочних канала и против мере	- 21 -
4.1 Познати напади преко бочних канала	- 21 -
4.1.1 Временски напад	- 22 -
4.1.2 Напади увођењем грешке	- 24 -
4.1.3 Напад анализом потрошње снаге	- 26 -
4.1.4 Електромагнетни напад	- 28 -
4.1.5 Акустични напад	- 29 -
4.1.6 Напад видљивим светлом	- 29 -
4.1.7 Напад поруком о грешци	- 29 -
4.1.8 Кеш-базирани напад	- 30 -
4.1.9 Напад на бази фреквенције	- 31 -
4.1.10 Напад скенирањем	- 31 -
4.1.11 Комбинација напада	- 31 -
4.1.12 Комбинација напада бочних канала и математичких напада	- 32 -
4.1.13 Оптимизација напада	- 32 -
4.2 Методе за спречавање цурења информација преко бочних канала	- 33 -
4.2.1 Рандомизација	- 34 -
4.2.2 Заслепљивање	- 34 -
4.2.3 Маскирање	- 35 -
5. Утицаји на евалуацију безбедности криптографских модула	- 36 -
6. Закључак	- 38 -
Литература	- 39 -

1. Увод

1.1 Предмет истраживања

Безбедност је дуго била главна брига у рачунарима и комуникационим системима и велики истраживачки напори су јој били посвећени. Криптографски алгоритми, укључујући симетричне алгоритме за шифровање, алгоритме за шифровањем са јавним кључем и хеш функције заједно чине сет примитива које могу бити коришћене као блокови за конструисање безбедносних механизма за специфичне задатке. На пример, мрежни безбедносни протоколи, као ССХ и ТЛС, комбинују ове примитиве да омогуће аутентификацију између комуникационих ентитета и обезбеде тајност и интегритет преношених података. У пракси, ови сигурносни механизми само специфицирају које функције треба извести без назнака како су имплементирани. На пример, спецификације безбедносних протокола су углавном независне од тога да ли су алгоритми за шифровање имплементирани у софтверу, на конвенционалном процесору или користе посебне хардверске јединице и да ли је меморија коришћена да чува податке током израчунавања у истом чипу као процесорска јединица или у посебном чипу.

Овај начин раздвајања брига између безбедносних механизма и њихових имплементација је омогућио ригорозну теоријску анализу, као и дизајн криптосистема и безбедносних протокола. Мада су у процесу различите претпоставке учињене у вези са имплементацијом безбедносних механизма. Претпостављено је да се криптографски прорачуни идеалне црне кутије не могу надгледати изнутра и да се на њих не може утицати од стране малициозних ентитета. Помоћу ових претпоставки ниво безбедности је широко квантификован према математичким могућностима криптографских алгоритама и дужини њихових кључева.

У пракси ови безбедносни механизми далеко су од комплетних безбедносних решења. Потпуно је нереално претпоставити да ће нападач покушати директно да нападне на комплексност израчунавања и разбијања криптографских алгоритама употребљених у безбедносном механизму.

На основу овога може бити повучена занимљива аналогија између јаких криптографских алгоритама и нпр., веома сигурне браве на кућним вратима. Провалници који покушавају да провале у кућу ретко ће покушати све комбинације да обију браву; они ће ући кроз прозоре, разбиће врата или ће украсти кључеве од власника.

Слично, скоро сви познати безбедносни напади на криптографске системе нападају слабости у имплементацији и примени механизма и криптографских алгоритама. Ове слабости дозвољавају нападачу да комплетно заобиђе или веома ослаби теоретску снагу безбедносних решења.

Како би криптографски систем остао безбедан битно је да тајни кључеви који се користе за захтеване безбедносне задатке не буду ни у ком случају откривени. Међутим, хакери ће данас пре покушати да нападну хардвер и систем у којем се налази криптографска јединица.

Нова класа напада развијена је у последњих неколико година од стране Пол Кочера (енгл. Paul Kocher-a) [5,6]. Ови напади функционишу зато што постоји корелација између физичких мерења узетих на различитим местима током израчунавања и унутрашњих стања уређаја за процесирање, која су повезана са тајним кључем. Више речи о овоме биће у наставку рада.

У стварности криптографски алгоритми су увек имплементирани у софтверу или хардверу на физичким уређајима који су у интеракцији са или под утицајем окружења. Ове физичке интеракције могу бити примећене од стране трећег лица и искоришћене за криптоанализу.

Овакав тип информација назива се бочни канал информација и напади који користе такве информације називају се напади бочних канала. Идеја напада бочним каналом је да открије начин имплементације криптографских алгоритама пре него саме алгоритме.

Није тешко приметити да конвенционална криптоанализа третира криптографске алгоритме као чисте математичке објекте, док криптоанализа бочних канала такође узима у обзир имплементације алгоритма. Дакле, напади бочним каналима се још називају нападима на имплементацију. Чак иако сваки криптографски алгоритам мора бити шифрован како би функционисао правилно, такви шифровани алгоритми не смеју да откривају информације о коришћењу приватних кључева и поред могућности трећег лица које може да надгледа и манипулише алгоритмом.

Овим каналима, битне информације (информације које требају бити заштићене) на невербалан начин могу да исцуре тј., нападачу могу бити доступне а да при томе корисник није ни свестан тога.

1.2 Невербална комуникација

Битно је напоменути да је 93% људске комуникације невербално. Чињеница је да људи осим говором комуницирају и својим изразима лица, бојом гласа па чак и начином облачења. Невербалан начин комуникације је јако користан у свакодневним интеракцијама али би већина нас волела да има потпуну контролу над овим невидљивим сигнаlima како не би неприметно открили неку од својих најдубље чуваних тајни.

Међутим, испоставило се да осим људи и рачунарске системи такође имају методе комуникације које су аналогне изразима „вербални“ и „невербални“. На пример, за мрежну компоненту, као што је кућни рутер кажемо да „говори“ када шаље поруке путем мреже. Уколико би неко хтео да се пријави на наш рутер са погрешном лозинком, наш рутер би то морао да препозна и да врати неку поруку типа: „Ваша лозинка је погрешна“. Рутер би био вербалан начин комуникације код рачунарске система.

Напоменули смо како у рачунарске системима постоје и невербални начини комуникације а у њих спадају: брзина којом одговарају, потрошња енергије која је потребна док не дођу до одговора на упит, па чак и бука коју емитују. Иако делује невероватно, нападачи су успели да искористе ове невербалне сигнале како би дошли до неовлашћених приступа или информација.

Један од најчешћих примера јесте програм логовања, где се у временском интервалу проверава лозинка карактер по карактер. Уколико је тачна лозинка „Лозинка“, програм би проверио да ли се унос првог карактера поклапа и у том случају би издвојио сам први карактер а то је „Л“, затим следи провера другог карактера па се издваја карактер „о“ и тако редом. У сваком кораку, уколико се деси да се неки од карактера не поклопи, програм враћа поруку да је лозинка нетачна.

1.3 Доприноси рада

Наведена тема рада је у потпуности обрађена на теоријској основи. Дат је квалитетан преглед различитих најактуелнијих напада из овог домена и све то на различитим платформама, како софтверским тако и хардверским.

Поред добро обрађених типова напада, дат је детаљан преглед против мера или ефикасних метода које је могуће употребити за спречавање или онемогућавање напада који се односе на нападе преко бочних канала.

Овај рад има изузетну теоријску вредност, која је неопходна за примену знања из ове области у пракси.

1.4 Структура рада

У наставку текста, биће кратко описана комплетна структура рада.

У другом поглављу, биће представљена историја свих проблема који се јављају као последица цурења информација. Затим модели напада бочних канала, њихова класификација и прича о свакој од подела.

У трећем поглављу, дат је целокупан теоријски приступ електромагнетних зрачења, као и сви термини који се провлаче у овој области. Биће детаљно објашњено шта су електромагнетна зрачења, како настају, шта је електромагнетска компатибилност, како се простиру, како настају сметње и сл.

У четвртом поглављу, које је уједно и суштина овог рада, биће размотрени конкретни напади бочних канала, до сада откривени напади и мере против тих напада.

У петом поглављу се објашњавају могући утицаји на евалуацију безбедносних модула и све што се до сада појавило као проблем, као и могућа решења.

У шестом поглављу се анализира све о нападима бочних канала, како се од њих одбранити и савети за будуће инжењере криптографских модула.

2. Преглед у области истраживања

2.1 Историја напада бочним каналима

Прва званична информација у вези са нападима бочних канала датира још од 1965., када је један научник објавио да је МИ5 (енгл. MI5-Military Intelligence, Section 5) покушала да разбије криптографски алгоритам коришћен у египатској амбасадџи у Лондону, али безуспешно због ограничења њихових рачунарских моћи. Овај напад је изведен постављањем микрофона близу криптографске машине како би се ослушкивао њен звук. Помоћу кликтања ротора током њиховог ресетовања сваког јутра, МИ5 је успешно открио позицију језгра за два од три ротора. Ова додатна информација умањила је захтеве за прорачуном потребним за разбијање алгоритма и МИ5 је могао да прислушкује комуникације у амбасадџи годинама.

Са друге стране оригинални радови као и велики број основних идеја о нападима бочних канала, јавности су приказани од стране већ поменутог Пол Кочера. Основни принципи ових напада су једноставни. Напади бочним каналима функционишу зато што постоји веза између физичких мерења током израчунавања и унутрашњег стања уређаја, која је зависна од тајног кључа. То је корелација између информације у бочним каналима и операције над тајним кључем који напад бочним каналом треба да открије.

Ови напади су се доказали као вишеструко ефектинији од конвенционалних напада заснованих на математичкој анализи и много су практичнији за примену. У области дизајна протокола или конструкције софтвера могуће је применити низ формалних техника за моделовање уређаја како би се моделовао спектар могућих акција од стране трећег лица и на крају је могуће резонovati могућности које уређај треба да омогући. Дакле, могуће је да ће бар у оквиру апстрактности модела уређај бити отпоран на нападе од стране трећег лица.

Међутим, када се из апстрактног погледа на безбедност пређе у реалан процес у физичком свету ствари постају компликованије. Све разлике са спољним светом које апстаракија прикрила постају важне. Која је граница овог криптографског уређаја у стварном свету? Које излазе треће лице може да надгледа, а којим улазима да манипулише? Тешко је наћи одговор на ова питања али важно је изградити бар неку одбрану против оваквих напада.

Физички акт прорачуна често резултира у физичким ефектима које треће лице може да надгледа; ове обезбавације често издају осетљиве унутрашње податке које би требало да прикрива архитектура криптографског модела. Ова врста напада се назива још и анализа бочног канала, јер уређај одаје информације преко канала који за то нису намењени.

Физички нападајући криптографски уређај, треће лице покушава да заобиђе његове безбедносне мере углавном извлачећи неку тајну коју уређај не би требало да открије. На први поглед, природни начин да се ово постигне је директан приступ, некако заобићи заштиту криптографског модула и прочитати податке. Срећом у пракси овакав директан напад може бити лако одбијен такозваним техникама забране приступа уређају.

Иако овај директан приступ може бити успешан, настао је и велики број софистицираних индиректних приступа где треће лице покушава да изазове грешку у модулу и ако модул настави да функционише може открити довољно информација за реконструкцију тајни.

Истраживачи у Белкор лабораторијама (енгл. Bellcore-Bell Communications Research) су први описали овај напад изазивањем грешака на криптографском хардверу који је користио ЦРТ имплементацију RSA. Овај резултат генерисао је велики број радова који су постали познати као диференцијална анализа грешке. Ови теоретски напади су постали практични и названи су Белкор напади.

Један од најпопуларнијих израза у безбедносном систему данас је ТПМ (енгл. TPM - Trusted Platform Module). ТПМ је углавном у облику криптографски сигурног модула и представља срж сигурне платформе за израчунавање. Главна компонента тих криптографских модула је да чувају и користе тајне упркос покушајима од стране трећег лица са физичким приступом да би их извукао.

Уређаји на једном чипу, конкретно паметне картице, привукле су доста пажње хакерске заједнице, вероватно услед широке примене у пракси и ниске цене (експериментисање и деструктивна анализа су омогућене широкој популацији). Андерсон и Кун [7,8] су сумирали различите технике које су ефективне у пракси.

Претња од стране напада бочним каналима привукла је пажњу и водећој научној заједници. Геботис и остали су презентовали оквир за безбедност научне заједнице путем криптографије засноване на симетричном кључу, на мрежном нивоу и на основном нивоу илустровањем софтверских модификација са веома малим додацима за безбедност од стране напада бочним каналима.

Дакле, криптографски алгоритам који је отпоран на конвенционалне нападе засноване на криптоанализи је непрактичан уколико га није могуће имплементирати на широком спектру платформи. Већ током АЕС и НЕССИЕ (енгл. NESSIE-New European Schemes for Signatures, Integrity and Encryption) процеса криптографска заједница је дошла до тог закључка.

Мотивација овог рада је да се разуме историја ових напада, да се препознају озбиљне претње од стране ових напада, да се процене различите контрамере и утицај напада на безбедносно тестирање криптографских модула.

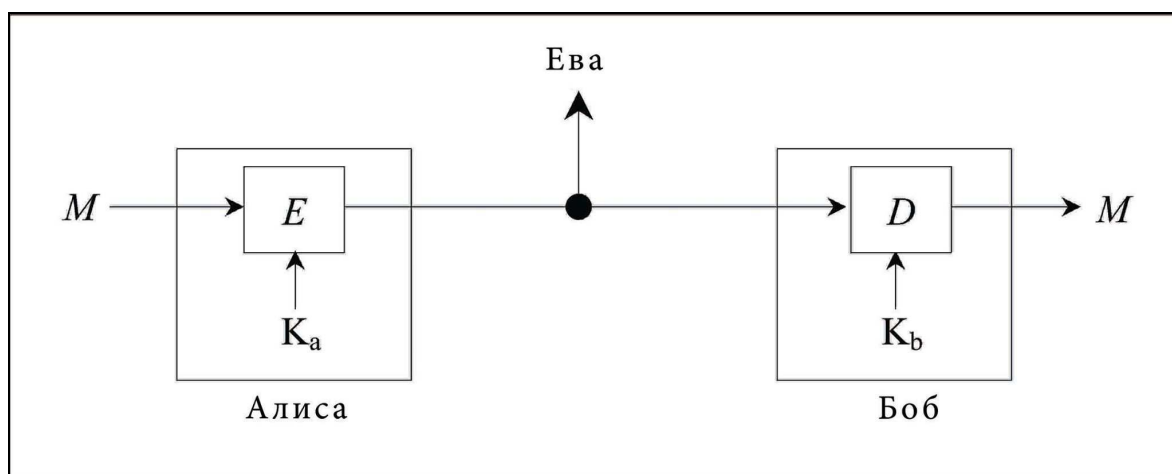
2.2 Модели напада преко бочних канала

Криптографске примитиве могу бити разматране на два начина: као апстрактни математички објекти (трансформације које задати улаз претварају у одређени излаз) или као имплементација програма на одређеном процесору, у одређеном окружењу, са специфичним карактеристикама. Први начин представља класичну криптоанализу, док други представља криптоанализу бочних канала. Криптоанализа бочних канала користи предности карактеристика специфичних за имплементацију како би извукла тајне параметре укључене у израчунавање. Дакле, пружа много више него класична криптоанализа и зато је веома озбиљно разматрана у индустрији криптографских уређаја.

У традиционалној криптоанализи, када се разматра безбедност криптографског протокола, сматра се да треће лице има комплетну спецификацију протокола, има приступ свим јавним кључевима и једино нема приступ тајним кључевима. Треће лице чак може бити у поседу података размењених између корисника или чак утицати на те податке. Дакле, треће лице покушава да пронађе начин да открије тајну проналазећи грешку у дизајну протокола.

У овом процесу, математичка апстракција може бити користан алат у проучавању криптографских примитива. Криптографи често могу да процене безбедност алгоритама разматрајући их као математичке функције као у сценарију приказаном на слици 2.2.1.

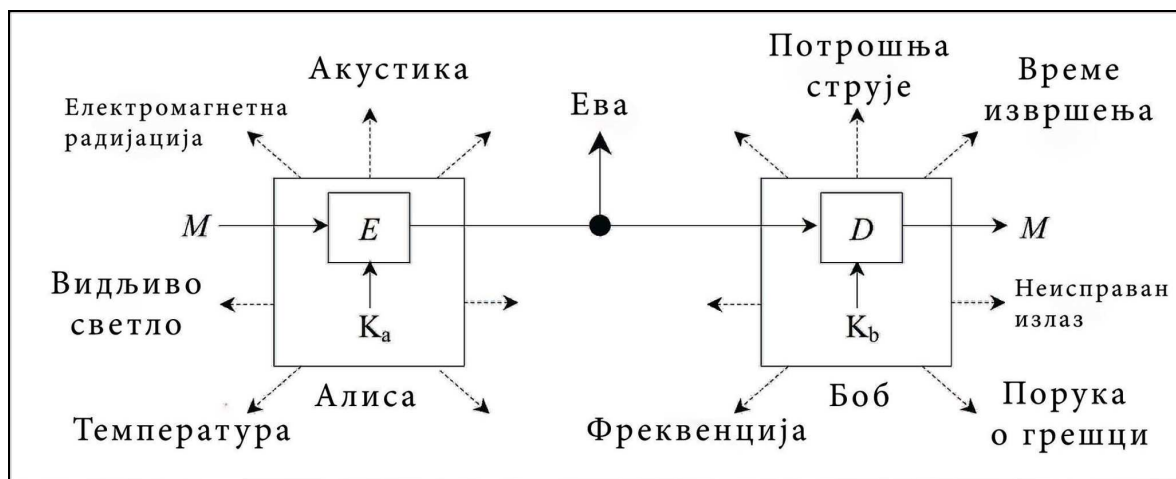
Традиционално, сигурни криптографски алгоритми омогућавају безбедност против трећег лица који има искључиво приступ тајним информацијама као према тзв. црној кутији. Међутим, такви модели нису увек адекватни. Заправо, безбедност таквих алгоритама може бити комплетно разбијена под нападима који покушавају да манипулишу тајним кључем.



Слика 2.2.1: Традиционалан криптографски модел

Напади разматрани у овом традиционалном безбедносном моделу експолатишу математичке спецификације протокола. У последњим годинама, истраживачи су све више свесни могућности напада који искоришћавају специфичне особине имплементације и оперативног окружења.

Такви напади бочних канала, користе информације процедуре током извршавања протокола и нису разматране у традиционалном безбедносном моделу. На пример треће лице може да надзире потрошњу струје или електромагнетну радијацију емитовану од стране паметне картице док изводи операције са приватним кључем као што су декрипција и генерисање потписа. Треће лице такође може да измери време потребно за криптографску операцију или анализира како се криптографски уређај понаша при одређеним грешкама. Информације бочних канала се лако добијају у пракси и зато је веома важно да се опасност од напада бочним каналима квантификује при процењивању укупне безбедности система као на слици 2.2.2.



Слика 2.2.2: Криптографски модел који укључује бочне нападе

Спољни канали су по дефиницији ненамерни излазни канали система. Пол Кочер је 1996. године, објавио рад “Временски напади на имплементације Дифи-Хелман, RSA, ДСС и осталих система” у којем је приказао да променљиво време извршавања алгоритама за шифровање може да садржи информације о кључу. Када имплементације користе предности оптимизације проблем постаје израженији.

Треба назначити да одређени напади бочних канала не могу представљати реалну претњу у неким окружењима. На пример, напади који мере потрошњу струје криптографског уређаја сматрају се изводљивим ако је уређај паметна картица која вуче струју са спољног неповерљивог извора. Са друге стране ако је уређај радна станица лоцирана у сигурној канцеларији, тада напади на основу потрошње струје не представљају озбиљну претњу.

2.3 Класификација напада преко бочних канала

Напади бочних канала се углавном класификују у наредне три ортогоналне осе:

- у зависности од контроле над процесом израчунавања,
- у зависности од начина приступа модулу,
- у зависности од метода коришћеног у процесу анализе.

2.3.1 Контрола над процесом израчунавања

У зависности од контроле над процесом израчунавања, напади бочних канала могу бити пасивни или активни.

Пасивни напади су они који се неприметно мешају у операције у циљаном систему; нападач добија неку информацију о циљаном систему али систем се понаша као да није дошло до напада.

Активни, напад са друге, стране трећем лицу омогућава одређени утицај на понашање циљаног система, док активно нападнут систем може а и не мора детектовати такав утицај; спољни посматрач може да примети разлику у операцији система. Важно је напоменути да подела између активних и пасивних система више има везе са суштинском природом напада него са физичком имплементацијом.

2.3.2 Начини којима се приступа модулу

Када се анализира безбедност криптографских хардверских модула, корисно је извршити систематски преглед површине напада- сет физичких, електричних и логичких интерфејса који су изложени потенцијалном противнику. Према овоме напади се деле на: инвазивне, полу инвазивне и неинвазивне.

2.3.2.1 Инвазивни напади

Инвазивни напад укључује распакивање како би се добио директан приступ унутрашњим компонентама криптографских модула или уређаја. Типичан пример је да нападач направи рупу кућишту криптографског модула и да спусти електроду на магистралу података како би надзирао пренос података.

Заштитни механизми имплементирани у хардверу углавном ефикасно одбијају инвазивне нападе. На пример, неки криптографски модули вишег нивоа заштите могу избрисати сву меморију када региструју такав напад.

2.3.2.2 Полуинвазивни напади

Концепт полуинвазивних напада подразумева приступ уређају без оштећивања кућишта или електричног контакта осим са дозвољеним површинама. На пример, нападач може користити ласерски зрак како би јонизовао уређај да промени неку од својих меморија и самим тим мења се излаз уређаја.

2.3.2.3 Неинвазивни напади

Неинвазивни напади представљају блиско посматрање или манипулацију рада уређаја. Ови напади искључиво искоришћавају информације које ненамерно цуре ван уређаја. Типичан пример таквог напада је временска анализа: мерењем времена потребног уређају да изврши операцију и његова корелација са израчунавањем уређаја како би се сазнала вредност тајних кључева.

Битна карактеристика неинвазивног напада је та да је потпуно неприметан. Не постоји начин да паметна картица сазна да се њено време извршавања тренутно мери. Са друге стране у поређењу са инвазивним нападима, неинвазивни су много јефтинији и економичнији. У том смислу неинвазивни напади представљају већу опасност индустрији паметних картица.

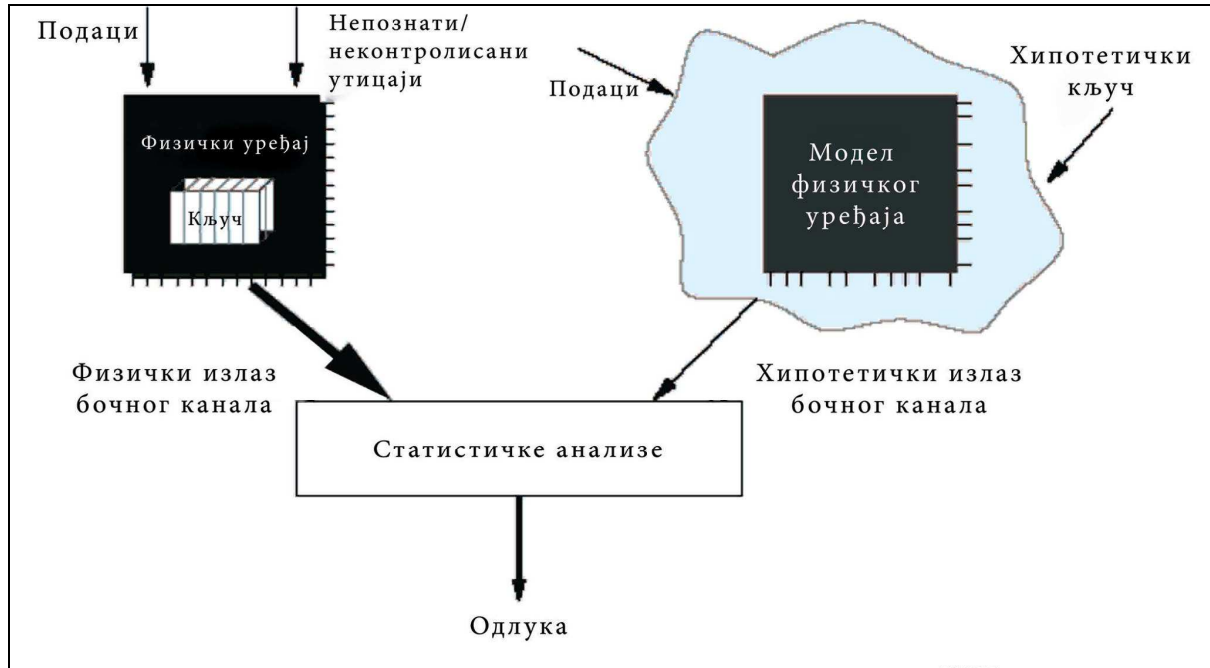
2.3.3 Коришћене методе у процесу анализе

У зависности од метода коришћених у процесу анализе података, напади бочних канала могу бити подељени на: једноставне и диференцијалне.

Једноставни напад користи спољни канал у зависности од операција које се извршавају. Типично, један траг се користи у анализи и тајни кључ може бити директно прочитан из трага бочног канала. Информација бочног канала у вези са нападнутом инструкцијом мора да буде већа него информација са непотребном инструкцијом. Оно што једноставни напади искоришћавају је заправо однос између извршених инструкција и излаза бочног канала.

Кад једноставни напад није могућ, због претераног шума у мерењима, користи се диференцијални напад. Диференцијални напад искоришћава корелацију између процесираних података и излаза бочних канала. Како је та корелација углавном мала статистичке методе морају бити коришћене. Нападач користи хипотетички модел уређаја који напада, а квалитет тог модела зависи искључиво од способности нападача. Типично, многи трагови се користе у диференцијалној анализи и статистичким методама се сведе на могуће тајне кључеве. Стога се може тврдити да је диференцијални напад моћнији од једноставног.

Хипотетички модел се користи да предвиди излаз бочног канала уређаја који може имати више вредности. То могу бити вредности које описују један начин цурења информација током времена или вредности које предвиђају цурење различитих бочних канала. У случају само једне излазне вредности напад се назива нападом првог реда, а ако се користе две или више излазних вредности истог бочног канала напад се назива нападом другог или нападима вишег реда.



Слика 2.3.3.1: Генерална идеја иза диференцијалних напада бочним каналом

3. Теоријске основе истраживања

3.1 Електромагнетска компатибилност

Да бисмо објаснили појам електромагнетске компатибилности, потребно је рећи да сваки електрични уређај приликом свог рада ствара неку врсту сметњи. Кажемо да су електрични уређаји електромагнетски компатибилни ако електромагнетне сметње које ти уређаји стварају не ометају њихов нормалан рад. Битно је напоменути да се под ометањем нормалног рада подразумева да један уређај не омета остале уређаје, али да при томе не омета ни самог себе. Електромагнетска компатибилност (енгл. EMC-electromagnetic compatibility) је способност уређаја да раде без међусобног ометања.

Приликом рада сваког уређаја под дејством нежељених напона и струја тј. електромагнетног поља, долази до појаве електромагнетске интерференције (енгл. EMI-electromagnetic interference). Сметње генерално могу настати у самом уређају или могу потицати из његове околине. Неки од примера појаве сметњи су: приликом проласка аутомобила са „неблокираним“ свећицама долази до непријатног пуккетања код радио пријемника или појаве снега на ТВ екранима; ако се два дисплеја са катодним цевима поставе близу један друге, долази до таласања њихових слика; радио апарати брује у близини рачунара; исто тако ове сметње могу бити опасне по живот, рецимо код пејсмејкера.

Мобилни телефон изазива у аудио појачавачу карактеристичне сметње и ремети слику на монитору. Рад рачунара може бити блокиран у мрежном напајању због јаких сметњи. Пејсмејкери отказују приликом проласка особе која их носи кроз детекторе метала, рецимо на аеродрому. Пријем жељеног радио или телевизијског сигнала може бити ометен сигналом неко другог предајника. Радар може пореметити рад околних рачунара и слично.

3.2 Извори сметњи

Електромагнетски гледано, извори сметњи су јаке струје и велика наелектрисања, посебно у случају када се брзо мењају. Нивои сметњи могу бити различити. На пример у околини снажних предајника постоји електрично поље реда величине неколико десетина па и стотина V/m. Ово поље може индуковати јаке сметње. Између осталог, долази до блокирања улазних степена радио пријемника који се налазе у околини или до нелинеарних изобличења других сигнала које пријемник треба да прими. Штавише овако јака поља могу бити штетна по здравље човека, јер изазивају загревање ткива.

Мрежни напон (230 V) може садржати импулсне и друге сметње од рада мотора, прекидача и другог, амплитуде неколико стотина волти и врло широког спектра. У електромагнетским постројењима могу се јавити поворке импулса (трајање импулса неколико десетина нано секунди и амплитуде неколико кило волта). Електрично поље које у својој околини стварају дигитални уређаји је реда величине mV/m, што може угрозити рад радио пријемника.

Поред сметњи које стварају електрични и електронски уређаји, постоје и други извори. Близак удар грома може довести до поремећаја рада уређаја, а директан удар до њиховог трајног оштећења. Приликом удара грома јављају се импулсне струје јачине реда кА, стварајући јако електромагнетно поље у својој околини.

За војне примере је значајан електромагнетни импулс нуклеарне експлозије, који настаје приликом експлозије хидрогенске бомбе у јоносфери (на висини од неколико стотина километара изнад земље). Гама зраци који при томе настају сударају се са слободним електронима који постоје у јоносфери и покрећу их (комптонов ефекат). При томе је важан и утицај земљиног магнетског поља, који мења облик путање електрона тако да се добија веома јак струјни импулс који се понаша као огромна антена. Последица је изузетно јако поље на површи земље које у подручју пречника неколико стотина километара и има облик импулсног електромагнетског таласа успонске ивице око 5 ns, трајања око 100 ns и амплитуде електричног поља око 50 kV/m. Ово поље може уништити многе уређаје или им пореметити рад.

Приликом електростатичких пражњења из намештаја или из човека (нпр човек се може наелектрисати до потенцијала реда десетак киловолти) може доћи до оштећења електронских компоненти (нпр ако се додирне интегрисано коли или друга компонента), а јаке струје које се при томе јављају (реда десетак ампера) могу пореметити рад уређаја. Још већи електростатички потенцијали и јаче струје пражњења се јављају код возила (нпр авиона). Код радио уређаја сметње могу проузроковати и други извори уколико се спектар сметњи преклапа са спектром корисног сигнала. Тако су атмосферска пражњења у екваторијалном појасу земље јак извор сметњи чији се спектар протеже до краткоталасног подручја. Те сметње се простиру на целој Земљи, вођене таласоводом који образују површ Земље и јоносфера.

3.3 Простирање сметњи

Простирање сметњи може бити двојако: претежно вођеним таласом (дуж проводника), што представља кондукционе сметње, и претежно слободним таласом, што представља радијационе сметње. У пракси је често мешовито простирање.

Пример кондукционог простирања сметњи је преко мреже за напајање (импулсне сметње настале приликом прекидања јаких струја продиру у рачунар и блокирају му рад).

Пример радијационог простирања су сметње од аутомобилских мотора на кућни радио или телевизијски пријемник. Међутим сметње од аутомобилских мотора ометају радио апарат у том истом аутомобилу и кондукционо (преко нисконапонске инсталације), и радијационо (сметње стижу до антене радио апарата).

Удар грома близу далековода ствара радијационе сметње које индукују сметње у далеководу. Те сметње се даље преносе кондукционим путем. Међутим директан удар грома у далековод изазива кондукционе сметње.

Водови и други проводници који су везани за уређај спрегнути су са самим уређајем (функционално или због паразитних спрега). Осим тога електромагнетски су спрегнути са околним простором и понашају се као антене. Струје које уређај побуђује у свим тим проводницима стварају радијационе сметње (као предајне антене). Реципрочно, у тим проводницима се индукују сигнали када се налазе у пољу сметњи (понашају се као пријемне антене), што утиче на уређај.

3.4 Дејство сметњи

Различити уређаји различито реагују на сметње. Електроенергетски уређаји су врло имуни на њих и обично само удари грома (или по интензитету слични електромагнетски импулси нуклеарне експлозије) могу изазвати проблеме, као што су поремећаји у раду (прекид услед деловања заштитних склопова или распад електроенергетског система) или прегоривање инсталација и машина.

Електронски уређаји су много осетљивији. Сметње у напону напајања могу довести до пада рачунарских система, сметње индуковане у телекомуникационим водовима могу довести до прекида везе, електростатичка пражњења чак и на кућишту уређаја могу довести до прегоривања електронских компоненти (диода, транзистора, интегрисаних кола, пасивних елемената, па и штампаних плоча.), радијационе сметње могу онемогућити пријем радио, телевизијских и радарских сигнала а јаке радијационе сметње могу чак оштетити осетљиве улазне степене пријемника. Оштећења настају због пробоја компоненти услед јаког електричног поља (нпр у кондензаторима или код инверзно поларизованих пн спојева) или термичких ефеката (нпр прегоривање отпорника услед великог загревања или поремећај у структури полупроводничких компоненти).

Електронски уређаји са цевима издржавају много веће сметње од транзисторских, а биополарни транзистори су обично отпорнији од транзистора са ефектом поља. Компоненте које су пројектоване за мање снаге или напоне осетљивије су од јачих компоненти.

Приликом оцене дејства сметњи на уређај (електромагнетске суцептибилности) разликују се следећи случајеви: (а) уређај издржава сметњу без икаквог поремећаја у раду, (б) сметња изазива поремећај после кога уређај сам наставља да ради (нпр сам се ресетује или се поново успостави као синхронизација), (в) уређај остаје блокиран, па је потребна ручна интервенција да би уређај наставио рад и (г) долази до трајног оштећења уређаја које захтева оправку.

Сигнали који кондукционим или радијационим путем цуре из неког уређаја могу представљати и опасност не у смислу ометања других уређаја , већ у смислу компромитовања самог уређаја и информација у њему. Нпр електронски млаз катодне цеви ствара у својој околини поље на основу кога се може реконструисати слика са екрана и тако шпијунирати са растојања од неколико метара (нпр из суседне просторије). Други пример је цурење сигнала из локалног осцилатора телевизијског пријемника. Овај осцилатор се налази близу улазних антенских прикључака пријемника, па делић тог сигнала израчи антена. Осетљивим пријемником подешеним на учестаност локалног осцилатора то поље се може детектовати, што је један од начина откривања непријављених телевизијских пријемника. Слична опасност постоји и од откривања рачунарских уређаја у војним постројењима.

3.5 Мере за испуњење електромагнетске компатибилности

Путеви продирања сметњи у уређај у принципу су исти као и путеви којима сметње излазе из уређаја (јер су путеви обично линеарни, па важи реципроцитет). Стога су и многе методе повећања имуности уређаја на сметње исте као и методие смањења сметњи који неки уређај ствара.

Један од начина смањења сметњи је правилан избор веза између компоненти и уређаја. Замислимо коло које се састоји од импулсног генератора и пријемника. Нека је трајање импулса 10ns, време успона (и пада) 1ns и нека је растојање између генератора и пријемника 0,1 m. Ово су типични подаци за дигитално коло средње брзине. Веза између генератора и пријемника може се остварити помоћу два проводника. Нека ти проводници образују петљу (нпр. иду ободом штампане плоче). Спектар импулса је шири од 1 GHz. Оваква контура се понаша као ефикасна антена. У било којој другој контури која се налази у њеној близини индуковаће се јаке сметње, које могу пореметити рад самог уређаја, а у околини се јавља довољно јако поље да поремети ради радио и телевизијских апарата.

Осим тога сигнал који стиже до пријемника, биће веома изобличен. Уколико се генератор и пријемник повежу микротракастим водом, не само да ће сметње бити далеко мање (преслушавање ће се јавити само у врло блиско постављеним водовима), него ће и интегритет сигнала бити очуван, односно сигнал стиже до пријемника са малим изобличењима. Још боље је повезивање тракастим водом или коаксијалним водом, али је ово последње решење скуп (мада се понекад примењује за дистрибуцију тактова у брзим рачунарима).

Због могућности индуковања јаких струја треба избегавати све везе (укључујући штампане везе, проводнике за уземљење и енергетске каблове) у којима се јављају галвански затворене петље. Развођење напајања, уземљења или сигнала обично се ради по звездастој шеми. За галванско раздвајање могу се употребити трансформатори. Код широкопојасних и високофреквентних трансформатора морају се предузети посебне мере у циљу смањивања капацитивног преслушавања између примарног и секундарног намотаја. Галванско раздвајање преноса сигнала може се остварити и оптичким спрежњацима (оптокаплерима). Посебно квалитетна веза у погледу готово идеалног галванског раздвајања, веома велике имуности на сметње и практично занемарљивих сметњи које ствара у својој околини је веза помоћу оптичких влакана. Оптичке везе имају и врло широк пропусни опсег. Међутим још увек постоји проблем релативно високе цене оптичких система.

Једна од мера је и правилан избор компоненти и склопова. У условима јаких сметњи цеви су погодније од транзистора. Асинхрони мотор ствара много мање сметње од мотора са комутатором. Стабилизатор напона који ради у линеарном режиму ствара много мање сметње од прекидачког стабилизатора.

Између свих водова и околног простора постоји спрега. Код обичног двожишног вода поље које ствара вод протеже се, теоријски у бесконачност. Ако се такав вод налази у магнетском пољу, кроз вод постоји магнетски флуks, па се у њему индукује електромоторна сила. Спрега са околним простором може се смањити упредањем вода (као код телефонске и рачунарске парице), јер се електромоторне силе индуковане у две суседне секције практично поништавају, а поништавају се и наелектрисања индукована на сваком проводнику.

Главна мера заштите од радијационих сметњи (и емитовања радијационих сметњи) је оклапање. Теоријски оклоп је шупље метално тело у коме се налази штићена компонента или уређај. Практично, оклопи се праве од лимова (бакарних, гвоздених или алуминијумских). Лимови се на саставима морају добро спојити (заварити, зашрафити или залемити). Оклопи се праве и од мрежица и метализоване пластике. Делови оклопа се могу направити тако да се могу скидати. Растављива веза се остварује завртњима, који морају бити постављени довољно густо да се обезбеди добро налегање или се на месту налегања постављају контактна пера или друге еластичне проводне траке.

Оклопи неминовно имају отворе кроз које пролазе разни водови (за напајање, комуникације, контролу и сл.), отворе за разне прекидаче и индикаторе, као и отворе за вентилацију.

Данас се постављају врло строги услови у погледу електромагнетске компатибилности. Постоје разни прописи који ограничавају нивое кондукционих и радијационих сметњи које емитују уређаји. Ти прописи дефинишу и поступке мерења, мада се различити прописи и поступци не могу увек лако међусобно упоредити. Неки од њих захтевају контролу сметњи чак и до неколико десетина GHz. Другим прописима дефинише се потребна имуност уређаја на електромагнетске сметње. Потврде о испуњењу ових услова обавезни су код продаје практично свих електричних и електронских уређаја.

Добар дизајн електричних и електронских уређаја захтева да се о електромагнетској компатибилности води рачуна од самог почетка. Много је једноставније и ефикасније предвидети мере заштите када се почне пројектовање уређаја, него примењивати мере заштите на готовом уређају. Често накнадне измене на уређају нису ни изводљиве. Основни приступ је да се извори сметњи блокирају (оклопе или филтрирају) на самом месту где се налази извор. Уколико се сметња пусти у већи простор, заштита је обично тежа и скупља. Пошто су мере за смањење сметњи исте као мере за повећања имуности, потребно је на исти начин (оклапањем или филтрирањем) заштитити сва осетљива места у уређају као и уређај у целини.

3.6 ФИПС 140 стандард и слични проблеми

ФИПС 140 стандард је стандард намењен за коришћење у федералним организацијама САД-а, када се специфицирају криптографски безбедносни системи који омогућавају заштиту осетљивих или вредних података. ФИПС 140 стандард прецизира безбедносне захтеве који треба да буду задовољени од стране криптографских модула на четири квалитативна нивоа безбедности (нивои иду од најнижег до највишег):

- Безбедносни ниво 1 даје најнижи ниво безбедности и прецизира основне безбедносне захтеве за криптографски модул (само за софтверску имплементацију),
- Безбедносни ниво 2 побољшава физичку безбедност нивоа 1 криптографског модула додајући захтев за физичку заштиту или печат или непробојну браву,
- Безбедносни ниво 3 захтева побољшану физичку сигурност покушавајући да спречи уљезе да добију приступ критичним безбедносним параметрима у модулу,
- Безбедносни ниво 4 обезбеђује највиши ниво сигурности ниво 4 физичког обезбеђења омогућава заштиту око криптографског модула ради детекције упада у уређај из свих праваца

Ови нивои су намењени да покрију широк спектар потенцијалних апликација и окружења у којима се могу користити криптографски модули. Безбедносни захтеви покривају једанаест области у вези са безбедносним дизајном и имплементацијом криптографских модула. Ове области укључују следеће: спецификација криптографских модула; портови и интерфејси криптографских модула; улоге; сервиси и аутентификација; модел коначног стања; физичка безбедност; операционо окружење; управљање криптографским кључевима; електромагнетно ометање/електромагнетна компатибилност; сопствено тестирање; осигурање дизајна; и ублажавање других напада.

ФИПС 140 стандард се преиспитује на сваких пет година. ФИПС 140-1 специфицира сигурносне услове које треба да задовоље криптографски модул коришћен у сигурносном систему штитећи неklasификоване информације унутар рачунара и телекомуникационог система (укључујући и гласовне системе). ФИПС 140-2 је наследио ФИПС 140-1, 2001. године са техничким модификацијама за решавање напретка технологије од објављивања ФИПС 140-1.

Постоје одређени проблеми са тренутном верзијом ФИПС 140-2. Прво ова верзија стандарда је углавном фокусирана на хардверске модуле, а није добро адаптирана софтверским модулима, али очекује се да ће се променити у верзији ФИПС 140-3. Друго ова верзија стандарда покрива преуски опсег система који се тестира. Захтева се боље усаглашавање са заједничким критеријумима и безбедносни пропусти функционалних протокола треба да буду боље решени. Коначно функционални захтеви за ову верзију стандарда су већ застарели. Захтеви наведени у ФИПС 140-2 далеко заостају иза актуелних потреба информационе безбедности како у теорији тако и у пракси.

Истовремено, сложен процес валидације ФИПС 140 показује да је савршенство у креирању јаких криптографских алгоритама и модула тешко достићи. Од једанаест области ове четири су најтеже: физичко обезбеђење, сопствени тестови, генератори случајних бројева и управљање кључевима.

Конкретно што се тиче напада бочним каналима ФИПС 140-1 не спомиње експлицитну безбедност криптографских модула против ових напада, док је ФИПС 140-2 само накратко споменуо спецификацију за ублажавање напада за који тренутно не постоје захтеви које је могуће тестирати.

4. Напади преко бочних канала и против мере

Ово поглавље је срж рада. У овом поглављу, биће прегледане познате методе и технике у нападима бочних канала, деструктивни ефекти таквих напада, контра мере и процена њихове изводљивости и примене.

До сада, ови напади су успешно коришћени за разбијање хардверских и софтверских имплементација многих криптосистема укључујући: блок алгоритме за шифровање, стрим алгоритме за шифровање, алгоритме за шифровање помоћу јавног кључа, за разбијање имплементација шема потписа, за разбијање кодних шема за аутентикацију порука, за разбијање имплементације криптографских протокола, за разбијање имплементација криптосистема и чак за разбијање мрежних система.

Као што многи безбедносни експерти назначавају безбедност није једнака криптографији и добри криптографски алгоритми аутоматски не гарантују безбедност система. Иако је свака компонента безбедна то не мора да значи да је комплетан систем безбедан. За комплексне системе безбедност треба бити посматрана из различитих углова веома пажљиво.

4.1 Познати напади преко бочних канала

Напади бочних канала против криптографских модула искоришћавају карактеристичне информације извучене из имплементација криптографских примитива и протокола. Ове карактеристичне информације могу бити извучене из временских, струјних или електромагнетних особина. Други облици цурења информација могу бити резултат хардверских, софтверских и грешака у израчунавању и промене у фреквенцији или температуре. Ови напади користе карактеристике хардверских и софтверских елемената као и структуре имплементације криптографске примитиве. Према томе, насупрот анализи математичких структура и криптографских примитива, анализа бочних канала укључује имплементацију.

Све ове чињенице се сумирају у једну да је конкретна имплементација веома важна за безбедност и да мале разлике у имплементацији могу учинити велику разлику у безбедности. Дакле, инжењери који имплементирају безбедносне шеме морају пажљиво да прате сваки њихов корак. Нападаци ће највероватније тражити најслабију карику у безбедносном ланцу. Када се користе проверени криптографски алгоритми и протоколи, криптоанализа сигурно није најслабија карика. Дизајнери система морају тежити да буду свесни о ненамерним “задњим вратима” која нису безбедна против напада.

4.1.1 Временски напад

Имплементација криптографских алгоритама често обавља прорачуне у различитим временским интервалима, због оптимизације перформанси. Ако свака од операција укључује тајне параметре, ове временске варијације могу проузроковати цурење неких информација и под условом да нападач има довољно знања примене при руци, пажљивом статистичком анализаом може чак да доведе до укупног опоравка тих тајних параметара. Ову идеју је увео Кочер, иако је развијена од стране једне друге компаније, где је спроведен и практичан временски напад против стварне примене паметне картице на РСА.

Временски напад је, у суштини, начин добијања неке корисникове приватне информације пажљивим мерењем времена које је потребно да корисник изврши криптографске операције. Принцип овог напада је врло једноставан: да искористи временску варијансу у операцији.

Основне претпоставке временске анализе биле би:

- Време извршења криптографских операција зависи донекле од кључа. Са хардвером ће ово вероватно бити случај, али требало би имати на уму да постоје разни ефикаснији хардвери базирани на предлозима да се временски напади мање изводе „инјекцијом буке“.
- Довољно велики број шифровања може да се изведе а да се за то време кључ не мења. Протокол изазов-одговор је идеалан за временске нападе.
- Време се може мерити са познатом грешком. Ако је грешка мања, мање време мерења је потребно.

Временски напади су уведени 1996. године, када је нападнуто модуларно степеновање РСА. Шиндлер је представио временске нападе на имплементацији РСА. Експериментални резултати за реализацију једног РСА на паметне картице су пријавили са Дем-а (лабораторије која се бави дизајном ефикасног јавног кључа).

Временски напади на ДЕС-а који може да поврати Хемингову тежину од тајног кључа, описао је професор Хевиа [9], са универзитета из Чилеа.

Отворен ССЛ је добро позната бесплатна (отвореног кода) крипто библиотека, која се често користи на Апач веб серверима да обезбеди ССЛ функције. Два научника, Брумли и Бон, [10] показали су да временски напади могу да открију РСА приватне кључеве од отвореног ССЛ-а, базираног на локалној мрежи једног веб сервера. Они су још показали да се модификована Кочерова верзија напада може вршити даљински, помоћу сервера који раде са отвореним ССЛ-ом.

Правећи приближно трећину милиона упита (за око два сата времена), фактори 1024-битних модула се могу наћи. Канвел [11] је осмислио временске нападе на шеме ЦБЦ режима за шифровање, које се користе у ССЛ-у и ТЛС-у. Њихови напади могу да дешифрују најчешће коришћени шифрат попут шифровања лозинке.

На једном симпозијуму безбедности, представљена је временска анализа притисака на тастере и временски напади на ССХ протокол. Они примењују технике праћења и анализирања интеракције ССХ веза у циљу закључивања информација о шифрованим садржајима прикључака. Закључено је да се на тастатури временски подаци могу посматрати кроз ССХ имплементације, које откривају веома значајну количину информација о корисничким терминалним сесијама - довољних да пронађе откуцане лозинке на сесији протока података и да смањи компјутерски рад укључен у погађање лозинки чак и оне са фактором 50.

Временски напад на идентификационе шеме предложен је на такозваном НЕССИЕ (енгл. *NESSIE-New European Schemes for Signatures, Integrity and Encryption*) пројекту у Европи. Показано је да само 800 временских мерења дозвољава нападачу да пронађе приватни кључ у неколико секунди на рачунару, са успехом и вероватноћом од 80%. Занимљиво је рећи да овим методама напада могу одолети неке класичне противмере.

Посматрањем временски одбачених знакова из дешифрата, један јапански научник представио је временски напад на јавни кључ криптосистема који је показао да се шифрат разликовања може обезбедити под претпоставком чињенице случајности.

Недавно је представљен временски напад на системе слабих кашњења који су базирани на комуникационим изасланицима, који покушавају да сакрију преписку између својих долазних и одлазних порука. Тврди се да је монтажа овог напада преко мреже, мале успешане вероватноће јер је мерење времена сувише нетачно. Ипак, верује се да у дистрибуираном систему са радом у реалном времену, временски напад на безбедносне протоколе оваквог система може постати реална претња.

Један једноставан приступ одбрани је да су оперативни параметри независни од улазних података. Изводљивост овог приступа зависи од операције. На пример, у РСА, једанпут се могу користити насумични подаци за спровођење процеса треперења (убризгавања шума) на параметре пре операције, а затим обрнути процес не-треперења после операције. Међутим, овај приступ извођења на поузданој рачунарској платформи која нема добар извор случајности или добар начин да се случајност добије, може бити онемогућен.

И још једна против мера нападима овог типа је да се елиминише грана обраде у алгоритму имплементације, тако да шифровање времена буде еквивалентно (огранак уједначавања). Заправо, противмере за временске нападе морају бити моделиране ригорозније, тако да можемо да проучавамо које су најефикасније предложене мере.

Две уобичајене појаве противмера које су тренутно у употреби, (убризгавање буке и грана изједначавања) се фундаментално разликују, у смислу да ињекција буке слаби моћ временског напада али га не поражава, док га грана изједначавања напада поражава, али у виду трошкова.

Још један лакши приступ одбрана, новија генерација модуларних степеновања, као и РСА мотори, почели су да се уграђују у дизајн хардвера, како би се одржало константно време за сваку операцију, без обзира са којим подацима се барата.

Када је Пол Кочер по први пут објавио свој временски напад 1995. године, бар један староседеоц је тврдио да је неколицина њих из комерцијалног света такође успела да одржи време константним, што нам говори да су људи још тада имали нека сазнања о овом нападу.

Вредно је напоменути да чак и временски напад искоришћава временске варијације у свакој операцији алгоритма и појединачно време сваке операције се не може мерити у пракси.

4.1.2 Напади увођењем грешке

За већину уређаја који обављају разне криптографске операције се обично претпоставља да поуздано раде када их користимо, тако да никоме од нас не пада на памет питање да ли безбедност таквих операција зависи од поузданости уређаја који их спроводе. Упркос овој претпоставци, хардверске грешке и грешке које се дешавају у току рада криптографских модула, у ствари су показали да озбиљно утичу на безбедност.

Неисправна понашања излаза такође могу постати важни бочни канали, па понекад чак могу довести и до знатног повећања рањивости шифрата на криптоанализу. Напади грешком представљају практичне и ефикасне нападе против криптографских хардверских уређаја као што су смарт картице. Дакле, у овом делу фокус ће углавном бити на нападе грешке хардверских уређаја.

Напади грешке на криптографске алгоритае се проучавају од 1996. године и од тада скоро сви криптографски алгоритми су пуцали коришћењем ове врсте напада. Напади грешком, нападачу нуде обиље могућности да нападне криптосистем. Начини да се искористе неисправани резултати су веома различити и варирају од алгоритма до алгоритма. Изводљивост ових напада (или бар његова ефикасност) зависи од прецизних способности нападача и врсти кварова које он може изазвати.

Генерално речено, модел грешке треба да садржи бар следеће наведене аспекте:

- Прецизност нападача, како би он могао да достигне време и локацију на којој се јавља грешка током извршавања криптографских модула.
- Дужину података погођених грешком, на пример само један бит или један бајт.
- Упорност квара, тј. да ли је грешка пролазног карактера или не.
- Врсту квара, као што је рецимо један погрешан бит и то са правилом у једном смеру (где јединице прелазе у нуле), или бајт промењен у случајну (непознату) вредност и тако даље.

Постоје две главне врсте грешке бочних канала. Прво, бочни канали који су изазвали рачунске грешке, спровели су их током криптографског рачунања у модулу напада. Ове грешке могу бити насумично или намерно изазване, на пример прецизном манипулацијом напона. Имајући у виду могућност да нападачи могу да уводе рачунарске грешке, ова врста напада може да се користи на скоро свакој врсти криптографског механизма и то се сматра једним од најефикаснијих напада бочним каналима уопште. Друга врста грешака бочних канала су оне које су изазване слањем намерно оштећених улазних података на нападнути модул. За модул, то значи нестандартна ситуација којом мора да се рукује на посебан начин. Обично модул мора да користи поруку о грешци да обавести корисника (модул тешко може да зна да ли је у питању обичан корисник или нападач) да је прорачун заустављен из неких разлога.

Уопштено говорећи, успешност напада грешке на криптографске модуле и уређаје захтева два корака: убризгавање грешке и кораке искоришћења те грешке. Први корак се састоји од убризгавања грешке у одговарајућем временском тренутку током процеса. Убризгавање грешке је веома зависно од хардверског уређаја. Грешке могу бити индуковане у паметне картице, где би својим деловањем стварале у окружењу нерегуларне услове. Неки од тих нерегуларних услова су: нагли пад или пораст напона, време, температура, зрачење, осветљење, и тако даље. Други корак се састоји у коришћењу погрешних резултата или неочекиваног понашања. Искористивост грешака зависи и од дизајна и имплементације софтвера. У случају алгорита то ће такође зависити од његове спецификације и искористивост грешке ће се комбиновати са криптоанализом већи део времена. У зависности од типа извршене анализе, убризгавање грешке ће морати да се уради у прецизном тренутку или отприлике у датом временском периоду.

Анализе нападима грешком прво је размотрио професор Бонех [10], 1997. године, и он је описао такве нападе на шеме РСА потписа. Анализу напада грешком на елиптичне криве шифровања јавног кључа представио је Бил [12]. Њихови напади су успели ако грешке током процеса дешифровања производе тачку која није на одговарајућем месту елиптичне криве. Напади се могу спречити уколико су тачке, које су резултат криптографских обрачуна, заиста на правој елиптичне криве. Бихам и Шамир [13], представили су анализу напада грешком на симетрични кључ за шифровање ДЕС шеме. Андерсон и Кун су пронашли неке реалне начине изазивања пролазних сметњи, које су назвали кваровима. Они су показали да може да се користи јефтина опрема за индукцију грешке у паметне картице, која осветљава одређене транзисторе. Такође су предложили противмере ових оптички индукционих напада грешком. Овај напад може изнова да убеди сваког читаоца да је убризгавање грешке дефинитивно проблем вредан разматрања у дизајну и тестирању сигурног система или уређаја.

Диференцијална анализа грешке обично изазива неку врсту физички погрешног рада криптографског уређаја, а затим мери резултате тих феномена. Они се углавном састоје у анализирању резултата алгоритма (шифрата) у регуларним и нерегуларним условима, за исти улаз (отворени текст). Нерегуларно стање се обично добија убризгавањем грешке током процеса (пролазна грешка), или пре процеса (стална грешка). Диференцијална анализа грешке је нашироко студирана са теоријског становишта и изгледа могуће применити је у готово свим симетричним криптосистемима.

Ако претпоставимо да нападач не може изазвати исту грешку два пута, једна од најбољих мера заштите симетричних алгоритама, као што су ДЕС и АЕС, је да се израчуна цела или део рунди два пута (укључујући и заказивање кључа). Наравно, ово ће ослабити све перформансе. У случају алгоритама јавних кључева, један приступ одбране је да се провери потпис (излаз из операција приватног кључа) помоћу јавног кључа пре слања потписа. Још је интересантније што је показано да провера исправности обрачунатих резултата, пре него што се предају даље, може бити недовољна да се заштити хардвер од грешака заснованих на криптоанализи. Још једна предложена мера заштите алгоритама јавних кључева, из неких специфичних напада грешком, је да се провери интегритет тајног кључа на крају израчунавања потписа. Други општи трикови независни од конкретних алгоритама, који су такође предложени, укључују контролне суме, насумично извршавање, поновљена освежења.

Да резимирамо, напади грешком су стварни и представљају велику претњу за било који сигурни токен (без обзира на његов облик) и то се мора узети у обзир у свим корацима дизајна производа као и његове спецификације. Против мере и заштита од напада грешаком може бити дизајнирана у хардвер и софтвер. Осмишљавање и анализирање напада грешком је неопходно, јер нам омогућава процену снага мера заштите и да ли су добро распоређене.

4.1.3 Напад анализом потрошње снаге

Поред сопствене потрошње времена извршавања и сопственог неисправног понашања, потрошња енергије код криптографских уређаја може да пружи много информација о операцијама које се одвијају, као и параметара које укључују. Ово је сама идеја напада анализом снаге. Наравно, напад анализом снаге важи само за хардверске имплементације на криптосистем. Напад анализе снаге је посебно ефикасан и доказано успешан у нападима на паметне картице или друге наменски уграђене системе складиштења тајног кључа.

Од свих врста напада бочним каналима познатих данас, највећи је број забележених напада анализом снаге који садржи релевантне противмере. Грубим рачунањем, тренутно постоји најмање преко 200 радова објављених у овој области. Напад анализом снаге је заправо фокус истраживања напада бочним каналима.

Напад анализе снаге се показао као веома моћан напад за најједноставније имплементације симетричних и шифрама јавних кључева. Због једноставности, највише се користе криптосистеми елиптичне криве (енгл. ECC-Elliptic Curve Cryptosystems) да илуструју нападе анализе снаге у овом одељку. Ипак, многе релевантне методе напада и разне контра мере примењују се и на друге криптосистеме.

У суштини, напад анализе снаге се може поделити на једноставану (енгл. SPA - Simple Power Analysis) и диференцијалну анализу снаге (енгл. DPA - Differential Power Analysis). Код једноставних, СПА напада, циљ је у суштини да се погоди траг из напајања којим се утврђује која се тачно инструкција извршава у одређено време и које вредности улаза и излаза има. Дакле, противник мора строго да познаје све о спровођењу и монтирању таквих напада. С друге стране, диференцијални, ДПА је напад код кога нам не треба знање о детаљима имплементације и искористивости алтернативних статистичких метода у процесу анализе. ДПА је један од најмоћнијих напада бочних канала, иако се може поставити помоћу веома мало ресурса.

Више напредна диференцијална анализа снаге гледа суптилне статистичке корелације између тајних бита и потрошње енергије. ДПА је јак напад, али ради само у одређеним случајевима као на пример код паметних картица. У овом класичном примеру, противник прикупља велики скуп парова траг-шифрат. Противник такође бира функцију селекције који узима шифрат и претпостављени део кључа и излаз једног бита. Идеја је да ако је претпоставка тачна, овај бит одражава нешто што се заправо приказује у обрачуна, али ако је претпоставка погрешна, онда ће се шифрат насумично претраживати.

Противник онда прави претпоставку кључа, користи ту претпоставку и функцијом селекције дели скуп трагова у два сета. Затим прави просеке трагова у сваком сету, а онда гледа разлику између ових просечних трагова. Уколико није био у праву, ове две групе нису у корелацији, и диференцијални траг постаје фиксан како се величина узорка повећава. Међутим, уколико је у претпоставка кључа тачна, диференцијални приступ сужава корелацију дешифрата и снаге потрошње.

СПА и ДПА нападе, као и многе друге увео је Кочер 1999. године. Они практично извршавају напад анализом снаге на имплементацију ДЕС-а у хардверу. Корон [14], је први применио ове нападе на елиптичне криве криптографских шема, и предложио је СПА отпоран метод за тачке множење, и ДПА отпоран метод случајно пројективних координата.

Предлози за хардверски-засноване одбране против напада анализом снаге укључују интерни извор напајања, случајни редослед којим се извршавају инструкције, случајан списак преименовања, и користе два кондензатора, од којих је један напуњен спољним напајањем, а други извором напајања уређаја.

Један ефикасан метод за одбрану од напада бочним каналима јесте да се на тачке умножавања примене адиционе формуле елиптичних кривих које могу да се користе за удвостручавање.

Друга стратегија за одбрану од ових напада је да се користе тачке множења алгоритама, као што су методе, где је образац допуне и двоструких операција независан од мултипликатора. Још један приступ донешен је са Геботис-а [15], а циљ је осмишљавање формуле за сабирање и двоструке операције које имају исти шаблон операција као што су сабирање, одузимање, множење и степеновање.

4.1.4 Електромагнетни напад

Као и електрични уређаји, компјутерске компоненте често генеришу електромагнетну радијацију током рада. Треће лице може да надзире ове промене и да разуме њихов однос са израчунавањем и ти подаци могу да садрже изненађујућу количину информација о том израчунавању. Ова могућност може бити кобна уколико је рачунар поуздана рачунарска платформа намењена да сакрије ове информације од трећег лица.

Слично нападима анализе струјне потрошње, напади електромагнетном анализом могу бити подељени у две групе: једноставни електромагнетни напади и диференцијални електромагнетни напади.

Потенцијал експлоатисања електромагнетне радијације је познат већ дуго времена у војним круговима. Један такав пример је TEMPIEST документ написан од стране националне агенције безбедности НСА (енгл. NSA-National Security Agency) који истражује различите компромитујуће сигнале укључујући електромагнетну радијацију, проводљивост жице, и акустичке емисије. Некласификована литература о техникама напада и контрамерама је такође бројна. На пример, дискутабилне су софтверске технике за покретање и превенцију напада заснованих на дедукцији информација на видео екранима услед емитоване електромагнетне радијације.

Експериментални резултати ових напада на криптографске уређаје као нпр., паметне картице и поређење са нападима анализе потрошње струје су први пут презентовани од стране криптографа *Quisquater-a* и *Gandolfi-a*. Најсадржанија неклаификована студија о електромагнетним нападима до данас, је рад професора компјутерске науке *Divyakant Agrawal*. Показао је да не само што се електромагнетна радијација може користити за напад на криптографске уређаје где струјни спољни канал није приступачан, већ могу бити коришћене за разбијање контрамера струјне анализе.

Контра мере против електромагнетних напада на специфичне имплементације делимо у две категорије: редукција снаге сигнала и редукција информација сигнала. Технике за редукцију снаге сигнала укључују редизајн електричних кола како би се умањила нежељена радијација. Још користе кућишта и физички осигуране зоне како би смањили снагу компромитујућих сигнала. Технике за редукцију информације сигнала се ослањају на коришћење рандомизације или учесталог освежавања кључа како би се смањила ефективност статистичких напада помоћу емитованих сигнала.

4.1.5 Акустични напад

Већина истраживања напада на бочне канале је усмерена на електромагнетне еманиације (Темпест), потрошњу енергије и дифузну видљиву светлост на ЦРТ екранима. Међутим, један од најстаријих напада је прислушкивање канала тј., акустичне еманиације, којима је пружено мало пажње. Врло недавно, је показано да постоји корелација између звука процесора и његовог рачунања. Међутим, ово је релативно ново поље, а много тога треба да се уради.

4.1.6 Напад видљивим светлом

Просечно осветљење ЦРТ дифузном рефлексijом о зид, може бити довољно да се реконструише сигнал приказан на ЦРТ екрану. Једна изузетна карактеристика овог напада је да физички приступ није потребан. Исте технике су једнако применљиве на лед сигнаlima. Чак и без видокруга, противник може бити у стању да прочита сигнал који поуздана компјутерска платформа ослобађа преко оптичких излазних канала. Индикатори статуса могу се анализирати и тако можемо закључити податке које обрађује уређај. За сада је само описан дизајн промене који би требало да успешно блокира ову врсту напада од угрожавања оптичких еманиација.

4.1.7 Напад поруком о грешци

У многим стандардима (ССЛ, ТЛС), поруке су прво унапред форматиране, онда кодиране у ЦБЦ режиму за блоковске шифре. Дешифровање треба да провери да ли је формат важећи. Важност формата лако процури из комуникационих протокола у изабраном нападу пошто пријемник обично шаље потврду или поруку о грешци. Ово може да постане користан бочни канал за криптоанализу и напад који користи овај бочни канал се често назива порука о нападу грешком.

Противник може да искористи споредне канале који дају довољно информација о шифрату како би га лако дешифровао. Нежељени канали често у пракси дају могућност противнику да изазове предвидиве промене у отвореном тексту кроз модификацију шифрата. Овде ће бити размотрене неке од ових напада на симетричне и асиметричне шеме за шифровање. Иако постоји приступ дешифровању предвиђање је понекад нереално у пракси. Овај напад функционише на следећи начин: модел оваквог понашања као што је предвиђање враћа важећу вредност ако је отворени текст правилно постављен (постављен без грешке), у супротном враћа не важећу вредност.

Порука о грешци описана је у анализи напада на симетричан кључ за шифровање, када поруке најпре треба форматирати, а затим кодовати са блоковским шифрама у ЦБЦ моду. У случају ЦБЦ режима у симетричним шемама, дужина поруке мора бити већа од дужине блока. Уколико то није случај, усклађивање је обавезно. Оно што пријемник треба да уради после дешифровања, ако је откривено да је грешка постављена и да је модел вратио не важећи резултат, зависи од протокола који се користи.

Ако је поставка после дешифровања неважећа, прецизира се да сесија буде срушена, или се само пријављује грешка и враћа се порука о грешци. Ако противник може да утврди уметнуту грешку, може и да је користи као споредни канал за монтирање напада одабраном шифром.

Неколико популарних шема уметања, које се данас користе у циљу трансформације блоковских шифара у шеме за шифровање променљиве улазне дужине, може да уведе важну безбедносну ману. Након објављивања резултата неких истраживања верује се да је од велике важности укључивање јаке провере интегритета у РСА шифровање. Фаза између дешифровање и провере интегритета је критична и уколико та информација лако исцури, може представљати безбедносни ризик. Циљ је да неисправна вредност (уметнута вредност), мора прекинути дешифровање.

4.1.8 Кеш-базирани напад

Раније предложени временски напади користе чињеницу да условна грана која се јавља током шифровања обрађује узрок варијација у времену шифровања. Процесорски кеш промашаји, такође могу да изазову такве варијације. Већина новијих рачунара користи процесорски кеш, између процесора и главне меморије, јер овај тип хијерархијске структуре може да убрза време покретања програма у просеку.

Ако, међутим, процесор приступа подацима који нису уписани у кеш меморију, односно уколико дође до промашаја кеша, кашњење ће бити генерисано, као што циљни подаци морају бити учитани из главне меморије у кеш меморију. Мерење овог кашњења може омогућити нападачима да утврде појаву и учесталост промашаја кеша.

Првобитну идеју да би кеш меморија могла да се користи као бочни канал преко кога информације цуре током рада криптографских алгорита предложио је професор Келси [16]. Идеја је проширена и испитана је теоријска употреба кеш меморије као бочног канала у криптоанализи.

Првобитна идеја даље је проширена на блоковске шифре са заменом и пермутацијом структуре мреже, као што је АЕС. Њихов поступак напада се може користити за криптоанализу криптографских примитива који користе зависне податке табеле.

Још важније, показан је изузетно јак тип напада, што не захтева познавање специфичног отвореног текста, нити шифрата. Радови се свode само на праћење ефекта криптографског процеса на кешу.

Противмере за ублажавање напада заснованих на кешу, јесу да се користе апликације алгоритамског маскирања у зависности од подршке оперативног система. Потврђено је да су примитиве које се обично примењују без табела претраживања, као што је то случај код СХА отпорне на нападе овог типа. Мада, до проналажења довољног ефикасног решења за ове нападе, сматра се да они и даље представљају велики проблем.

4.1.9 Напад на бази фреквенције

Нападе бочним каналима засноване на фреквенцији, против мобилних уређаја као што су ПДА уређаји, мобилни телефони и пејцери, предложио је Тио [17]. Његов метод је ефикасан чак и када су трагови непоравнани у експерименталним нападима, док раније истраживани диференцијални електромагнетни напади нису били у таквом стању.

Поред тога, предложен је напад фреквенцијом првог реда, који је у стању да победи противмеру десинхронизације која убацује кашњења. Међутим, то може бити штетно, јер друге мере против ове врсте напада заснованих на фреквенцији нису евидентирани.

4.1.10 Напад скенирањем

Ова врста напада, представља подједнако снажан напад на безбедност. Године 2004., први пут се помињу технике скенирања као напад бочног канала, како би се открили тајни кључеви из хардверски имплементираног ДЕС-а. Коришћењем једном уграђених шема за самоиспитивање, постиже се да интерни статус криптографских чипова више не буде скениран, чиме се оваква врста напада може избећи. На срећу, ова врста самотестирања је већ препоручена од стандарда ФИПС 140-2, као услов физичког обезбеђења криптографских чипова.

4.1.11 Комбинација напада

Комбинација временске анализе и анализе потрошње струје може бити коришћена за заобилажење појединих против мера код специфичних напада бочним каналима. Једноставан пример коришћења неколико бочних канала је мерење времена између важних карактеристика у струјном трагу. Не тако давно, научници су истражили потенцијал више каналних напада, који користе потрошњу струје и електромагнетну радијацију истовремено.

Комбинација нека друга два или више бочних канала такође може водити до напада, мада они нису били интезивно истражени.

4.1.12 Комбинација напада бочних канала и математичких напада

Традиционалне технике криптоанализа се такође могу комбиновати са нападима бочних канала, како би се открио тајни кључ или сломили детаљи имплементације шифрата. У представи овога, чак и мала количина информација бочних канала је довољна да се пробију шифре.

На пример, различите анализе грешке које користе намерно убачене захтеве грешака, од 50 до 200 шифрованих текстуалних блокова могу да опораве симетричан кључ ДЕС блоковске шифре, док најбољи традиционални напад захтева око 64 терабајта обичаног текста и шифрованог текста једним кључем.

Иако постоји неколико комбинација напада бочним каналима и традиционалним математичким нападима, са сигурношћу се може проценити да је ова комбинација постала једна од најразорнијих напада на криптосистем.

4.1.13 Оптимизација напада

У нападима бочних канала, нападач обично претпоставља тајни кључ део по део. Као последица тога, велики број мерења треба обезбедити за успешан напад. Међутим, у стварном свету неког напада бочним каналом, број мерења је често ограничен или је у најмању руку веома скупо извршити велики број мерења. Са становишта нападача је зато пожељно да се смањи вероватноћа грешке у нагађањима појединих делова кључа или да се смањи број мерења, до границе која је довољна за успешан напад.

Уколико исход претходних погађања има утицај на стратегију погађања, представљеног дела кључа, пожељно је имати критеријуме са којима би се исправност претходних погађања могла проверити са разумном вероватноћом. Да би се искористиле информације бочних канала на оптималан начин, развијен је општи приступ оптимизацији ових напада кроз коришћење метода стохастичких процеса и статистичке теорије одлучивања.

Показано је да је применом одговарајућих стохастичких метода било могуће значајно повећати ефикасност броја познатих напада до чак 50 посто.

4.2 Методе за спречавање цурења информација преко бочних канала

До сада су предложене бројне стратегије (у хардверу и софтверу) за борбу против напада бочним каналима. Међу њима су :

- Декорелација излазних трагова (увођењем случајних померања у времену и стања чекања, убацивање лажних инструкција, насумично извођење операција, итд.)
- Замена критичних асемблерских инструкција са онима чији је ”потпис потрошње” тежак за анализу или преправљање критичних кола које изводе аритметичке операције и меморијске трансфере,
- Алгоритамске промене на криптографским примитивима тако да напади буду доказано неефикасни на задатој имплементацији (маскирање података и кључева са случајном маском).

Доказано је да међу овим контрамерама алгоритамске технике су најразноврсније, најпрактичније и могу бити најмоћније. Такође, у много контекста су најјефтиније. Софтверске контрамере укључују лажне инструкције, случајно извођење секвенци инструкција, балансирање Хемингових тежина унутрашњих података и раздвајање битова. На хардверском нивоу контрамере углавном укључују случајне промене такта, случајне промене искоришћења струје, случајни редослед извођења сета инструкција и коришћења регистара. Мада ефекти ових контрамера могу бити редуковани коришћењем различитих техника обраде сигнала. Софтверске контрамере лоше утичу на перформансе криптографских алгоритама у смислу меморије и времена извођења. Један од изазова је постићи сигурну имплементацију са што мање трошкова.

Избор одговарајућег нивоа контрамера зависи од вредности података и моћи трећег лица (њиховог знања и ресурса). Процена нивоа отпорности треба бити сагледана из бар три угла : моћи трећег лица, моћи напада и ефективности контрамера. Чини се да комбинација хардверских и софтверских контрамера даје добар однос безбедности и трошкова.

Следеће дискусије могу се пронаћи у савременој литератури: напади, контрамере и теоретски модели. Заправо ова литература није довољна како би се извела комплетна процена напада и контрамера. На пример, у првој апроксимацији игноришемо ефекте спреге и креирамо линеарни модел у нападима анализе снаге, тј. предпостављамо да је функција потрошња струје чипа сума функција потрошње струје свих догађаја који се дешавају. Заправо чак и мали број спрега може да изазове велики извор компромитујућег цурења. Искоришћавање тих цурења може бити ефикасније од покушаја анализе тих цурења. Заправо пуно интезивног и конзистентног рада треба бити захтевано у овим основним истраживачким областима.

4.2.1 Рандомизација

Најопштија метода против напада бочних канала је рандомизација података који могу цурети кроз различите канале. Проблем је како гарантовати да ће нападач добити искључиво случајну информацију и да не може да добије никакво корисно знање о правим иницијалним или тренутним подацима израчунавања.

У случају криптосистема елиптичне криве, случајни метод пројективних координата је практична контрамера против ових напада у којој нападач не може да предвиди појаву специфичних вредности јер су координате случајне. На пример, код напада бочним каналима, отпорни метод множења скалара може узети било који број унапред израчунатих тачака. Предложена шема суштински тежи да се опире једноставној анализи снаге, а не диференцијалној анализи снаге.

Стандардни диференцијални напад анализом снаге користи корелациону функцију која разликује да ли је специфични бит у релацији са надгледаним израчунавањем. Како би се опирали диференцијалним нападима, потребно је рандомизирати параметре елиптичних крива. Постоје три стандарда рандомизације: основна тачка је маскирана случајном тачком; тајни скалар је рандомизован множителем реда криве; и основна тачка је рандомизована у пројектвну координату. Неки напади против сваке од наведених контрамера су предложени, међутим ако су ове рандомизационе методе коришћене истовремено, није познат напад који пробија такву шему. Другим речима, једностани напади анализом снаге отпорне шеме могу лако конвертовати у отпорне диференцијалне користећи ове рандомизације. Насупрот томе појављују се поједине шеме које покушавају да истовремено постигну једноставну и диференцијалну отпорност без коришћења комбинација (рандомизоване прозорске методе).

4.2.2 Заслепљивање

Заслепљивање је концепт у криптографији који омогућава клијенту да зада провајдеру да израчуна математичку функцију $y=f(x)$, где клијент задаје улаз x и добија одговарајући излаз y , а да провајдер не зна ни x ни y . Овај концепт је користан уколико клијент не може самостално да израчуна функцију f , нпр. зато што провајдер користи додатни приватни улаз како би израчунао f .

Прва техника заслепљивања је базирана на хомоморфним особинама RSA потписне функције. Технике заслепљивања су најефикаснија контрамера против даљинске временске анализе веб сервера и против анализе снаге и временске анализе хардверских безбедносних модула.

4.2.3 Маскирање

Технике маскирања података су најшире коришћене контрамере против анализе снаге и временских напада на софтверском нивоу. Маскирање алгорита значи маскирање тренутних вредности које су процесирани у израчунавању алгоритамих операција.

Маскирање података је такође једна од моћнијих софтверских контрамера напада бочних канала. Идеја је веома једноставна, порука и кључ су маскирани случајном маском на почетку израчунавања и одатле је све као и уобичајено. Наравно вредност маске на крају неког фиксног корака (нпр., на крају круга или на крају линеарног дела израчунавања) мора бити позната како би се поново успоставили очекивани подаци на крају израчунавања; то се зове корекција маске.

У случају АЕС-а, ова контрамера представља претварање тренутних бајтова у обрађене приликом израчунавања. Маскирање бајта непознате вредности значи изабрати случајну маскау и дефинисати функцију маскирања које узима обе вредности као улаз како би израчунала маскирани излаз $f(x,m) = x * m$. Оператор $*$ је дефинисан као битска ексклузивно-ИЛИ операција.

Оптимизована контрамера за АЕС блоковски алгорита састоји се из трансформисања булове маске у мултипликативну маску пре нелинеарне операције замене бајтова (дакле избегавање поновног израчунавања С-бокова за сваки пролаз или чување вишеструких С-бокс табела у РАМ-у) док се задржава логичка маска на осталим местима.

5. Утицаји на евалуацију безбедности криптографских модула

Из детаљне дискусије може се извући закључак да напади бочним каналима представљају озбиљну реалну претњу безбедности криптографских модула. Све ово за последицу треба да има опште разумевање не само дизајнера или имплементатора већ и корисника криптографског модула. У овој области дискутовали смо о могућим утицајима на тестирање безбедности криптографских модула.

Традиционална метода црне кутије широко коришћене у анализи и дизајну криптосистема има неколико ограничења, дакле не може бити у складу са савременим напретком и развојом информационе безбедности. Више других аспеката мора бити укључено у евалуацију система како би се проценила укупна безбедност прецизније и објективније. Захтевано је да минимална безбедна имплементација криптографских модула (протоколи и системи) буде озбиљно узета у разматрање при дизајнирању функционалних криптографских компоненти.

Избор одговарајућих криптографских модула или уређаја своди се на захтевани ниво безбедности. Дакле тајно тестирање и процена су не само практични већ и обавезни. Током овог комплексног и независног процеса тестирања захтеване су нове теорије моделовања безбедности и тестирања безбедности.

Нису сви делови система склони овим нападима али није тривијалан задатак специфицирати који делови треба да буду обезбеђени а који не. Како би се смањио ризик незаштићених делова скупе контрамере се често примењују на деловима који уопште нису склони нападима, дакле све контрамере треба да буду дизајниране и имплементирани са одговарајућом и квантитативном проценом њихових ефеката на укупну ефикасност. Праћењем ових опажања јавља се проблем да ли је могуће развити методологије које омогућавају нападима бочних канала симулације у раним фазама дизајна система или не.

Осим тренутних захтева тестирања безбедности, захтеви стандарда ФИПС 140 треба да буду проширени како би покрили следеће аспекте: анализа криптографских протокола, анализа ефикасности вођења кључева; анализа бочних канала или слични пропусти; анализа правилне употребе криптографских модула у већем уређају; сваки став о ФИПС дозвољеним и недозвољеним алгоритмима итд.

Када би се повећала величина кључа у неким случајевима то не мора да значи истовремено повећавање нивоа безбедности. Неки аутори тврде да што је дужи кључ лакши су напади. Повећање дужине кључа је стандардна контрамера у криптоанализи, међутим дужи кључ углавном значи веће цурење на бочном каналу. За уграђене РСА криптосистеме, повећање процурелих података назначавала повећање тајних података тако да насупрот напреднијој математичкој снази, дужи кључ води до слабије безбедности.

Напад и дизајн за безбедност није балансиран у складу са практичним сценаријима. По нашем мишљењу постоји јаз између процене или тестирања и напада. Може бити од помоћи постојање генерализованих напада али то није обавезно. Напади такође не захтевају ригорозну анализу, једноставна демонстрација ефикасности напада је довољна да се доведе у питање безбедност система чак и без постојања детаљног објашњења механизма напада. Дизајнирање за безбедност, са друге стране захтева и генералност и ригорозност. Осим предлагања конкретних метрика за процену можемо предложити неке од безбедносних захтева за тестирање криптографских модула:

- Сви критеријуми морају бити проверљиви
- Критеријум треба да омогући процену перформансе различитих имплементација и да пронађе најефикаснију
- критеријум мора да буде у стању да процени цену имплементација као и меморије и производње
- сваки критеријум мора бити лако изводљив

Већина бочних напада нису покривена са готово свим безбедносним моделима теоријске криптографије. Дакле, чак и доказиво безбедне имплементације криптографских алгоритама могу бити нападнуте услед могућих цурења информације. Заправо већ постоје доказане објављене безбедносне криптографске шеме пробијене преко метода ове врсте напада. Треба напоменути да су ови напади ефикасно изведени против сигурних криптосистема али то не умањује математичку базу тих система нити рефлектује њихове математичке слабости.

6. Закључак

Криптологија може бити виђена као непрекидна расправа између криптографа и криптоаналитичара. Напади на криптографију такође имају дугу историју. Безбедност криптографских модула омогућава практичан ниво заштите против напада на такозвану белу кутију (потпуни приступ) која може бити посматрана у тотално непоузданом окружењу.

Јака криптографија је веома моћна када се имплементира на прави начин али то не решава све проблеме. Фокусирање на криптографске алгоритме, игноришући остале аспекте безбедности је исто као и бранити кућу без ограда, али ослањати се искључиво на тло и надајући се да ће противник ићи управо преко тла. Данас ови аргументи треба да буду поново прегледани. Изградити ограду око куће је далеко од довољног, јер ко може да гарантује да нападач неће ископати тунел испод ограда? Могуће је направити и веома тврдо тло али ко може да гарантује да нападач неће пасти са неба? Треба имати у виду да ваш противник није ништа мање паметан од вас. Највероватније никад не можете бити сигурни у следећи потез вашег противника.

У овом раду су испитани напади преко бочних канала и релевантне контрамере. Широки спектар контрамера против ових напада је развијен од стране криптографа како би се омогућила заштита. Верујемо да ће чисто разумевање напада као и жртве повезане са уграђивањем контрамера омогућити архитекти система да развије заиста безбедан систем.

Сви проблеми у криптографији нису решени, остало је још много изазова пред истраживачком заједницом и индустријом, са безбедним и ефикасним имплементацијама криптографског система. Ширина спектра могућих напада компликује задатак њиховог решавања. До сада је откривено бар десет врста бочних напада. Предвиђа се да ће бити откривено и експлоатисано све више ових напада. Који ће бити следећи бочни канал и да ли ће бити последњи? Дакле, дизајн имплементација криптографских модула или система захтева јаку свест о потенцијалним слабостима у имплементацији који могу довести до безбедносних пропуста и пажљиво треба узети у разматрање безбедност током свих аспеката процеса дизајна архитектуре хардвера и софтвера. Сада је време да се правилно процени отпорност криптографских модула против ових напада у процедури тестирања безбедности таквих модула. Не треба заборавити да је велики број још неоткривених бочних канала.

Већина проблема у вези са нападима бочних канала и контрамера ће се појавити приликом проучавања међусобног утицаја системских параметара. Можемо се надати да ће се развити генерална теорија, методе и алати који ће помоћи инжењеру безбедности. Све у свему важно је уложити још доста теоретског и практичног рада како би се добиле нове идеје о овим нападима.

Коначно, најважнији закључак овог рада је да није само потребно, већ је и обавезно у наредној верзији ФИПС 140-3 стандарда проценити криптографске модуле на њихову отпорност на нападе преко бочних канала.

Литература

- [1] Kriptologija I, Mladen Veinović, Saša Adamović, Univerzitet Singidunum
- [2] Kriptologija II, Milan Milosavljević, Saša Adamović, Univerzitet Singidunum
- [3] Elektromagnetika, Antonije R. Đorđević, Akademski misao
- [4] Ispitivanje elektromagnetske kompatibilnosti, Antonije Đorđević, Dragan Olćan, Akademski misao
- [5] P. Kocher, J. Jaffe, B. Jun. Differential power analysis. CRYPTO'99, LNCS 1666, pp.388-397, 1999.
- [6] P. Kocher. Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems. CRYPTO'96, LNCS 1109, pp.104-113, 1996.
- [7] R. Anderson, M. Kuhn. Tamper resistance—a cautionary note. Proc of the 2nd USENIX Workshop on Electronic Commerce, pp.1-11, 1996.
- [8] R. Anderson, M. Kuhn. Low cost attacks on tamper resistant devices. Proc of the 1997 Security Protocols Workshop, pp.125-136, LNCS 1361, 1997.
- [9] A. Hevia, M. Kiwi. Strength of two data encryption standard implementations under timing attacks. ACM Transactions on Information and System Security, Vol.2, pp.416-437, 1999.
- [10] D. Brumley, D. Boneh. Remote Timing Attacks are Practical. Proc of 12th Usenix Security Symposium, 2003.
- [11] B. Canvel, A. Hiltgen, S. Vaudenay, M. Vuagnoux. Password Interception in a SSL/TLS Channel. CRYPTO 2003, LNCS 2729, pp.583-599, 2003.
- [12] I. Biehl, B. Meyer, V. Müller. Differential fault attacks on elliptic curve cryptosystems. CRYPTO 2000, LNCS 1880, pp.131-146, 2000.
- [13] E. Biham, A. Shamir. Differential fault analysis of secret key cryptosystems. CRYPTO '97, LNCS 1294, pp.513-525, 1997.
- [14] J.S. Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. CHES'99, LNCS 1717, pp.292-302, 1999.
- [15] C.H. Gebotys, R.J. Gebotys. Secure elliptic curve implementations: an analysis of resistance to power-attacks in a DSP processor. CHES 2002, LNCS 2523, pp.114-128, 2003.
- [16] J. Kelsey, B. Schneier, D. Wagner, C. Hall. Side channel cryptanalysis of product ciphers. Proc of 5th European Symposium on Research in Computer Security, LNCS 1485, pp.97-110, 1998.

[17] C.C. Tiu. A New Frequency-Based Side Channel Attack for Embedded Systems. Master degree thesis, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, 2005.

[18] Интернет старница:

<http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf>

[19] Интернет старница:

https://www.thecsiac.com/journal_article/software-protection-against-side-channel-analysis-through-hardware-level-power

[20] Интернет старница: <http://wikipedia.org/>