UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica

Tesi di Laurea Magistrale

TITOLO ITALIANO

TITOLO INGLESE

MARCO BURACCHI

Relatore: Prof. *Michele Boreale*

Anno Accademico 2017-2018

INDICE

1 Introduzione 9
2 Side-channel attacks 11
2.1 Background 12
2.1.1 Tipi di canali 12
2.1.2 Tipi di attacco 12
2.1.3 Grandezza fisica osservata 13
2.1.4 Hardware attaccato 13
2.1.5 Algoritmo attaccato 13
2.2 Attacchi basati sul suono 14
2.3 Attacchi basati sulla luce 14
2.4 Attacchi basati sul tempo 14
2.5 Attacchi basati sul consumo elettrico 14
2.6 Attacchi basati sul campo elettromagnetico 14
2.7 Attacchi basati sui risultati delle computazioni 14

ELENCO DELLE FIGURE

Figura 1 Esempio di side-channel attack 11

ELENCO DELLE TABELLE

Tabella 1 Classificazione dei principali attacchi analizzati 14

"citazione prima riga.
citazione seconda riga."
— autore

1

INTRODUZIONE

Il mondo moderno è ormai pervaso dalla *crittografia*. Quotidianamente e spesso inconsapevolmente utilizziamo funzioni crittografiche per le normali operazioni della vita quotidiana. Controllare il conto sull'home-banking, scambiarsi messaggi tramite servizi di messaggistica o anche navigare in internet utilizzando il protocollo *HTTPS* sono azioni che svolgiamo ormai con naturalezza. I sistemi moderni rendono trasparente all'utente l'utilizzo di tali tecnologie ma ciò non vuol dire che non ci siano.

Una *funzione crittografica* è un oggetto matematico astratto che trasforma con l'utilizzo di una chiave, un dato in input (plaintext) in una sua rappresentazione diversa (ciphertext) il più possibile non riconducibile al dato originale. Questa funzione deve poi essere implementata in un programma che girerà su un *dispositivo crittografico* in un certo ambiente, presentando perciò caratteristiche fisiche peculiari. Esempi di dispositivi crittografici potrebbero essere smartcard, chiavette USB, chip dedicati montati su dispositivi general purpose (smartphone, notebook) o periferiche progettate e costruite apposta per effettuare questo unico compito.

In passato si guardava ad un dispositivo crittografico semplicemente come una black-box che riceveva un plaintext e restituiva un ciphertext (encryption) e viceversa (decryption). Gli attacchi erano basati sulla conoscenza del ciphertext (ciphertext-only attacks) o di alcune coppie di entrambi (known plaintext attacks). Con l'accesso al meccanismo di encryption o di decryption, anche solo temporaneo, si possono attuare anche altri due tipi di attacchi (rispettivamente chosen-plaintext e chosen-ciphertext)[1].

Al giorno d'oggi si è consapevoli del fatto che un dispositivo crittografico ha spesso altri input oltre al plaintext e altri output oltre al ciphertext. Gli input differenti dal plaintext possono essere interazioni col mondo esterno come modifiche al voltaggio della corrente, condizioni atmosfe-

riche particolari o sollecitazioni fisiche. L'interesse sarà però focalizzato sulle informazioni (facilmente misurabili) che vengono lasciate trapelare dai dispositivi stessi oltre al ciphertext come ad esempio il tempo di esecuzione di un programma, le radiazioni emesse, suoni, luci e quant'altro chiamate *side-channel informations*.

Il resto della tesi è organizzata nel seguente modo. Nel capitolo 1 verrà definita una classificazione dei side-channel attacks e verrà presentata una panoramica dello stato dell'arte. Il capitolo 2 approfondirà i *cache attacks* e in particolar modo quelli basati sul tempo. Nel capitolo 3 verrà presentato approfonditamente il recente attacco *SPECTRE* che ha afflitto tutti i recenti processori AMD, ARM e Intel. Nel capitolo 4 verrà affrontato il problema della generalizzazione di questi attacchi utilizzando la Quantitative information-flow analysis (QIF) una nuova tecnica che permette di stabilire proprietà di confidenzialità delle informazioni.

2

SIDE-CHANNEL ATTACKS

I *side-channel attacks* sono metodi di criptanalisi che sfruttano le side-channels informations insieme ad altre tecniche di analisi per recuperare la chiave utilizzata da un dispositivo crittografico [2].

Nella figura 1 si può vedere una configurazione tipo di side-channel attack. Da una parte c'è il dispositivo che implementa la funzione crittografica e accanto c'è lo strumento utilizzato per rilevare le grandezze fisiche prodotte dal dispositivo attaccato. La cosa fondamentale è che questo tipo di attacchi non vanno a colpire direttamente la funzione crittografica ma sfruttano le informazioni fisiche dell'ambiente intorno al dispositivo.

L'analisi di questi metodi ha acquisito notevole interesse dato che questo tipo di attacchi possono essere montati velocemente e molto spesso non richiedono hardware particolare e costoso. Con pochi euro si possono ad esempio acquistare in comuni negozi di bricolage o elettronica apparecchi in grado di analizzare il consumo elettrico di un dispositivo. Con tali apparecchi è possibile montare in pochi secondi un attacco di tipo *Simple Power Analysis*[3] che verrà spiegato più avanti.

Il governo degli USA, nel suo "Orange book"[4] indica dei requisiti di

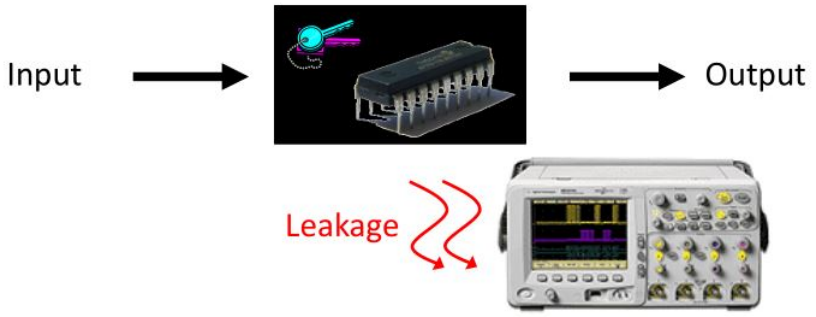

Figura 1: Esempio di side-channel attack

sicurezza per i sistemi operativi. Questo documento introduce i primi standard per l'*information leakage*. Purtroppo la letteratura specializzata è però molto variegata e disomogenea quindi, come prima cosa, cerchiamo di trovare un modo per classificare i vari tipi di attacchi in maniera tale da avere una visione più sistemistica del settore.

2.1 BACKGROUND

In questa sezione verranno stabiliti dei parametri per classificare i vari tipi di attacchi side-channel.

2.1.1 *Tipi di canali*

Nel lavoro di *Ge, Yarom, Cock e Heiser*[5] vengono fornite alcune definizioni che utilizzeremo nel prosieguo di questa tesi. La prima distinzione che è necessario fare è quella tra side-channel e *covert-channel*. Con i primi ci si riferisce ai canali che lasciano *accidentalmente* filtrare informazioni sensibili (ad esempio una chiave crittografica) in una comunicazione tra due partecipanti fidati. I secondi sono quelli creati e sfruttati dall'attaccante ad esempio tramite l'utilizzo di Trojan e che *deliberatamente* lasciano filtrare le informazioni. In questo lavoro verranno trattati solamente i primi.

L'altra differenza fondamentale per quello che riguarda i canali è quella tra canali di tipo *storage* e canali di tipo *timing*. I canali di tipo storage vengono sfruttati per ottenere qualcosa di direttamente visibile nel sistema (valore dei registri, valore di ritorno di una system call, ecc.). Quelli di tipo timing vengono sfruttati andando ad osservare variazioni del tempo di esecuzione di un programma (o di parti di esso).

2.1.2 *Tipi di attacco*

Standaert nel suo lavoro [2] utilizza altre due dimensioni interessanti per classificare questi attacchi; l'*invasività* e l'*attività*.

Si definisce invasivo un attacco che richiede un disassemblamento del dispositivo attaccato per avere accesso diretto ai suoi componenti interni (wiretapping o sensori collegati direttamente all'hardware). Un attacco non invasivo, al contrario, sfrutta solamente le informazioni disponibili esternamente (quasi sempre involontarie) come il tempo d'esecuzione o l'energia consumata.

Si definisce attivo un attacco che cerca di interferire con il corretto funzionamento del dispositivo (fault-injection) mentre un attacco passivo si limita ad osservare il comportamento del dispositivo durante il suo lavoro senza disturbarlo.

2.1.3 *Grandezza fisica osservata*

Una caratteristica principale di questi attacchi è sicuramente la grandezza fisica che viene osservata per montare l'attacco. Teoricamente, qualunque grandezza fisica misurabile può essere sfruttata ma alcune si prestano maggiormente rispetto ad altre.

Il tempo e il consumo energetico sono le più sfruttate ma non sono di certo le uniche. *Genkin, Shamir e Tromer* nel loro lavoro [6] vanno ad ascoltare i rumori prodotti dal processore. *Ferrigno e Hlavac*[7] osservano la luce (qualche fotone) emessa dai transistor nel passaggio di stato da 0 a 1. *Martinasek, Zeman e Trasy* sfruttano i campi elettromagnetici creati dai chip. *Giraud*[8] sfrutta la tecnica della fault-injection e analizza i risultati delle computazioni.

Questo elenco assolutamente non esaustivo delle tecniche utilizzate può far capire quanto variegato ed eterogeneo (nonché in continua evoluzione) sia questo settore.

Tutti questi attacchi (e anche altri) verranno approfonditi più avanti.

2.1.4 *Hardware attaccato*

Gli attacchi possono essere suddivisi anche in base alla componente hardware che viene attaccata. Anche in questo caso ci sono componenti più attaccati di altri (cache e processori) ma non mancano esempi di attacchi a monitor[9], tastiere[10] o stampanti[11].

2.1.5 *Algoritmo attaccato*

Un'ultima classificazione può essere effettuata andando a discriminare gli attacchi secondo l'algoritmo crittografico attaccato. In questo caso i due maggiori algoritmi attaccati sono senza dubbio AES ed RSA.

Nella tabella 1 si è provato a classificare con i criteri sopra definiti i 6 attacchi che verranno approfonditi in questo lavoro.

Tabella 1: Classificazione dei principali attacchi analizzati

Articolo	Grandezza	Hardware	Algoritmo	Invasivo	Attivo
[6]	Suono	CPU	RSA	No	No
[7]	Luce	Transistor	AES	Sì	No
[12]	Tempo	Cache	RSA	No	No
[3]	Consumo elettrico	Smartcard	AES	No	No
[13]	Campo elettromagnetico	Chip	AES	No	No
[8]	Risultato della computazione	Smartcard	AES	Sì	Sì

2.2 ATTACCHI BASATI SUL SUONO

2.3 ATTACCHI BASATI SULLA LUCE

2.4 ATTACCHI BASATI SUL TEMPO

2.5 ATTACCHI BASATI SUL CONSUMO ELETTRICO

2.6 ATTACCHI BASATI SUL CAMPO ELETTROMAGNETICO

2.7 ATTACCHI BASATI SUI RISULTATI DELLE COMPUTAZIONI

BIBLIOGRAFIA

[1] Michele Boreale. *Note per il corso di CODICI E SICUREZZA*. 2013. (Cited on page 9.)

[2] François-Xavier Standaert. Introduction to side-channel attacks. In *Secure Integrated Circuits and Systems*, pages 27–42. Springer, 2010. (Cited on pages 11 and 12.)

[3] Stefan Mangard. A simple power-analysis (spa) attack on implementations of the aes key expansion. In *International Conference on Information Security and Cryptology*, pages 343–358. Springer, 2002. (Cited on pages 11 and 14.)

[4] Donald C Latham. Department of defense trusted computer system evaluation criteria. *Department of Defense*, 1986. (Cited on page 11.)

[5] Qian Ge, Yuval Yarom, David Cock, and Gernot Heiser. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. *Journal of Cryptographic Engineering*, pages 1–27, 2016. (Cited on page 12.)

[6] Daniel Genkin, Adi Shamir, and Eran Tromer. Rsa key extraction via low-bandwidth acoustic cryptanalysis. In *International Cryptology Conference*, pages 444–461. Springer, 2014. (Cited on pages 13 and 14.)

[7] Julie Ferrigno and M Hlaváč. When aes blinks: introducing optical side channel. *IET Information Security*, 2(3):94–98, 2008. (Cited on pages 13 and 14.)

[8] Christophe Giraud. Dfa on aes. In *International Conference on Advanced Encryption Standard*, pages 27–41. Springer, 2004. (Cited on pages 13 and 14.)

[9] Wim Van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985. (Cited on page 13.)

[10] Dmitri Asonov and Rakesh Agrawal. Keyboard acoustic emanations. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 3–11. IEEE, 2004. (Cited on page 13.)

[11] Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, and Caroline Sporleder. Acoustic side-channel attacks on printers. In *USENIX Security symposium*, pages 307–322, 2010. (Cited on page 13.)

[12] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. *arXiv preprint arXiv:1801.01203*, 2018. (Cited on page 14.)

[13] Zdenek Martinasek, Vaclav Zeman, and Krisztina Trasy. Simple electromagnetic analysis in cryptography. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, 1(1):13–19, 2012. (Cited on page 14.)