Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Tesi triennale in Ingegneria Informatica

Sicurezza Elettromagnetica: analisi dei dispositivi TEMPEST

Candidato Tesista

Alessandro Girlanda

Matricola 2032457

Supervisore

Prof. Roberto Corvaja

Università di Padova

Anno Accademico
2023/2024

Sommario

Le apparentemente innocue emissioni di energia legate al normale funzionamento dei dispositivi elettronici possono, in realtà, portare con sè importanti informazioni sui dati elaborati, portando a gravi problemi di sicurezza e privacy.

Questa tesi analizza in dettaglio i dispositivi TEMPEST e il loro fondamentale ruolo nel campo della sicurezza elettromagnetica. Partendo dalle origini storiche e dai principi fisici delle emissioni compromettenti, l'analisi si concentra sulle strategie offensive che sfruttano tali emissioni per rubare informazioni sensibili e sulle tecnologie difensive per attenuare l'intensità delle emanazioni o per schermare elettromagneticamente i dispositivi sotto attacco prevenendo possibili furti di informazioni.

Per concretizzare i concetti spiegati, questo documento mostra un semplice esperimento chiamato Tempest for Eliza, che permette di dimostrare l'esistenza delle cosiddette "emanazioni compromettenti" e il loro legame con il dispositivo che le ha generate.

I risultati di questa tesi mostrano che il furto di informazioni sensibili secondo il metodo TEMPEST è facilmente attuabile e, per questo motivo, richiede delle misure di prevenzione importanti per evitare conseguenze significative nel campo della sicurezza elettromagnetica.

Indice

Lista delle figure **i**

Lista delle tabelle **iii**

Lista degli acronimi **v**

1 Introduzione **1**

1.1 Importanza della protezione delle informazioni sensibili e motivazioni 2

1.2 Definizione e contesto dei dispositivi TEMPEST 2

1.3 Applicazioni 3

1.4 Struttura 4

2 Storia e Sviluppo **5**

2.1 Storia degli standard TEMPEST 5

2.2 Evoluzione di TEMPEST 7

2.3 Principali tappe storiche e normative 8

3 Segnali intercettabili - le emanazioni compromettenti **9**

3.1 Principi di funzionamento delle emanazioni elettromagnetiche . . 10

3.2 Sorgenti di segnali TEMPEST 11

3.3 Tipi di emanazioni e vulnerabilità associate 11

4 Tecnologie e Tecniche di Protezione TEMPEST **15**

4.1 Schermature elettromagnetiche 16

4.1.1 Zonizzazione 16

4.1.2 Hardening 19

4.1.3 Materiali 19

4.2 Filtraggio 20

4.3 Progettazione e layout dei circuiti per la mitigazione e la soppressione delle emissioni 21
4.4 Tecniche avanzate di protezione 22
4.4.1 Sistema Honeypot 23

5 Aspetti Offensivi: Attacchi TEMPEST 25
5.1 Definizione e principi degli attacchi TEMPEST 26
5.1.1 Esempi e casi di studio 27
5.2 Una vista più profonda: Van Eck Phreaking 28
5.2.1 Principi della televisione 28
5.2.2 Emissioni elettromagnetiche di un monitor CRT 30
5.2.3 Sistema di misurazione: le antenne 30
5.2.4 Decodifica del segnale: il sistema di recupero 31
5.2.5 Contromisure 32
5.2.6 TempestSDR 33

6 Tempest for Eliza 37
6.1 Descrizione dell'esperimento 37
6.2 Strumentazione 38
6.3 Fasi del progetto e realizzazione pratica 38
6.4 Discussione ed analisi dei risultati 40
6.5 Conclusioni 41

7 Conclusioni 43

Bibliografia 45

Lista delle figure

3.1 Composizione del campo elettromagnetico 10
3.2 Dominio del tempo e della frequenza di segnali a banda base RED 12
3.3 Dominio del tempo e della frequenza di segnali portanti modulati 12
3.4 Emanazioni impulsive correlate ad un segnale digitale RED . . . 13

4.1 Edificio schermato secondo le norme TEMPEST 17
4.2 Modello concettuale di zonizzazione TEMPEST 18
4.3 Efficienza di schermatura dei tre materiali a diverse frequenze di segnale schermato 20
4.4 Struttura complessiva del sistema Honeypot 23

5.1 Procedura di un attacco TEMPEST 26
5.2 Costruzione di un'immagine televisiva 28
5.3 Struttura generale di un tubo a raggi catodici 29
5.4 Rappresentazione del segnale line feed in un ricevitore TV 30
5.5 Van Eck Phreaking: esempio di set-up 32
5.6 Set-up usando TempestSDR 35
5.7 Immagine catturata dalle onde EM emanate dal monitor 35

6.1 Attrezzatura utilizzata in Tempest for Eliza 38
6.2 Schermo 1 39
6.3 Schermo 2 39
6.4 Schermo 3 39
6.5 Set up finale di Tempest for Eliza 40

Lista delle tabelle

2.1 Principali tappe storiche[21] 8

Lista degli acronimi

TEMPEST Transient ElectroMagnetic Pulse Emanation Standard

Comsec Communication security

NRL Naval Research Laboratory

CRT Cathode Ray Tube

GCHQ Government Communication Headquarters

CE Compromising Emanations

EUT Equipment Under Testing

EM ElectroMagnetic

DC Direct Current

PCB Printed Circuit Board

SE Shielding Effectiveness

KGB Komitet Gosudarstvennoj Bezopasnosti (Comitato per la sicurezza dello stato)

VDU Video Display Unit

TTL transistor-transistor logic

LF Line Feed

LCD Liquid Crystal Display

SDR Software Defined Radio

1

Introduzione

Le apparecchiature informatiche e di comunicazione generano e ricevono diverse forme di energia, tra cui correnti elettriche, calore, luce, onde elettromagnetiche condotte e irradiate, suoni e vibrazioni. La maggior parte dell'energia consumata viene rilasciata sotto forma di calore o utilizzata per l'elaborazione e per la creazione di messaggi di informazione sui canali di comunicazione. Le parti rimanenti possono essere correlate ai dati elaborati in modi diversi e trasformarsi in fughe di informazioni non intenzionali. Ciò offre opportunità non convenzionali a individui tecnicamente sofisticati che possono ottenere accesso non autorizzato a tali informazioni riservate[12]. Da questa preoccupazione, nascono multipli standard e tecnologie in grado di proteggere le macchine dal possibile furto di informazioni sensibili emesse durante il normale funzionamento dell'apparecchio.

In questa tesi, l'obiettivo è quello di studiare ed analizzare come è possibile proteggere i propri dispositivi dai furti appena introdotti e anche spiegare come funziona tale "furto". Per fare ciò verrà analizzato lo standard per eccellenza che ha studiato, in tutte le sue sfaccettature, il concetto di "emanazione compromettente" e che ha applicato questi studi su tecnologie avanzate di protezione e di attacco. Lo standard in questione è chiamato TEMPEST e verrà ampiamente spiegato nei prossimi paragrafi.

1.1 Importanza della protezione delle informazioni sensibili e motivazioni

Prima di parlare del funzionamento dei dispositivi TEMPEST, è importante capire la motivazione principale per la quale questi strumenti esistono.

La prorompente digitalizzazione del mondo ha portato a dover gestire un enorme quantità di dati che possono essere privati e personali dell'ente che li ha condivisi.

Si parla di informazioni sensibili: queste sono qualsiasi dato che, se divulgato, può danneggiare gli individui o le organizzazioni proprietarie di tali dati. Queste informazioni devono essere protette a causa della loro natura intima o riservata con la quale vengono registrate. Ad esempio, le informazioni sensibili possono includere dati di identificazione personale, dati finanziari e cartelle cliniche, e tante altre[8]. Proteggere questo tipo di informazioni diventa essenziale; in questo modo, infatti, è possibile tutelare la privacy personale, la sicurezza finanziaria ma anche la proprietà intelletuale di aziende e organizzazioni.

Dunque, capire lo spettro delle informazioni sensibili è cruciale in un mondo digitale sempre più in evoluzione, dove le minacce informatiche sono sempre più incombenti[8].

1.2 Definizione e contesto dei dispositivi TEMPEST

Nel contesto appena introdotto, essere in grado di proteggere le informazioni sensibili è fondamentale. Ma in che modo queste informazioni possono essere rubate se viaggiano in una comunicazione sicura? Come è possibile che informazioni di questo tipo possano essere intercettate?

Ogni qualvolta una macchina è usata per elaborare informazioni elettricamente, i vari switch, contatti, relè e altri componenti della stessa macchina possono emettere dell'energia acustica o in radio frequenza. Queste emissioni possono irradiare attraverso il vuoto per distanze consideravoli come mezzo miglio o più. Inoltre, queste emissioni possono essere indotte su conduttori vicini come linee di segnale, linee elettriche, linee telefoniche o tubature dell'acqua e condotte lungo quei percorsi per una certa distanza, e qui possiamo parlare di un miglio o più. Tali emissioni possono essere intercettate e registrate, ed è spesso possibile analizzarle e recuperare le informazioni che venivano elaborate

dall'apparecchiatura sorgente. Questo fenomeno non riguarda solo le macchine cifranti, ma qualsiasi apparecchiatura di elaborazione delle informazioni: telescriventi, apparecchiature per duplicazione, intercom, fax, computer, e così via. Tuttavia, ha un significato speciale per le macchine cifranti perché potrebbe rivelare non solo i testi in chiaro dei singoli messaggi elaborati, ma anche quelle informazioni accuratamente protette sui processi interni della macchina. Quindi, è concepibile che la macchina potrebbe emettere informazioni che potrebbero portare alla ricostruzione delle nostre variabili di chiave che cambiano quotidianamente, e dal punto di vista della sicurezza delle comunicazioni (Comsec), questo è assolutamente la cosa peggiore che possa capitarci[14].

In questo contesto nasce TEMPEST (Transient ElectroMagnetic Pulse Emanations Standard): un acronimo che si riferisce agli studi sulle emanazioni non intenzionali dei dispositivi elettronici, come computer, monitor, cavi di rete, etc, le quali possono compromettere la sicurezza dei dati trattati.

1.3 Applicazioni

I dispositivi TEMPEST hanno molteplici applicazioni, principalmente focalizzate sulla protezione delle informazioni sensibili e sulla sicurezza nazionale. Le principali aree di utilizzo sono:

- Protezione delle comunicazioni militari: TEMPEST permette di garantire che le comunicazioni militari siano al sicuro da intercettazioni elettromagnetiche. Questo è essenziale per evitare che informazioni militari cruciali vengano intercettate.
- Sicurezza delle infrastrutture governative: Uffici governativi e ambasciate usano tecnologie TEMPEST per proteggere informazioni sensibili e riservate da potenziali spie.
- Protezione dei dati aziendali: Aziende dedicate alla gestione di informazioni altamente riservate, come dati finanziari o segreti industriali, possono adottare dispositivi TEMPEST per prevenire e difendersi da fughe di informazioni.
- Laboratori di ricerca e sviluppo: Misure TEMPEST possono essere adottate anche da laboratori che lavorano su tecnologie avanzate o innovazioni industriali per evitare che le loro scoperte vengano intercettate e, quindi, rubate.
- Riduzione delle interferenze elettromagnetiche: E' possibile utilizzare dispositivi TEMPEST anche per ridurre al minimo le interferenze elettromagnetiche emesse dall'attrezzatura elettronica in quanto potrebbe compromettere il normale funzionamento di dispositivi elettronici sensibili.

- Operazioni di spionaggio: I dispositivi TEMPEST possono essere utilizzati anche in operazioni di spionaggio allo scopo di captare e rubare informazioni sensibili al nemico.

Dunque, le applicazioni si possono dividere in due rami: difesa e attacco. Per garantire la sicurezza elettromagnetica a dispositivi che producono emissioni di energia compromettenti, l'utilizzo di dispositivi TEMPEST diventa cruciale.

1.4 Struttura

Il progetto di tesi in questo documento è strutturato considerando sia le tecnologie di difesa che quelle di attacco secondo gli standard TEMPEST.

Nel secondo capitolo, l'obiettivo è quello di spiegare il contesto storico che sta dietro a TEMPEST, in modo da comprendere le tappe storiche che hanno portato allo sviluppo di tali tecnologie.

Nel terzo capitolo, invece, viene fatta una panoramica sulle cosiddette "emanazioni compromettenti", spiegandone struttura, tipologie e sorgenti. Questo serve per comprendere a livello fisico cosa sono queste emissioni di energia che un apparecchio elettronico emana.

Nel quarto capitolo, vengono introdotte le maggiori tecniche TEMPEST per la protezione dei dispositivi da questi furti "a distanza". Le principali strategie prevedono l'attenuazioni delle stesse emanazioni che causano il problema. Si approfondiranno i concetti di schermatura, filtraggio e soppressione.

Nel quinto capitolo, invece, verrà definito l'attacco TEMPEST. Più in particolare, viene dettagliatamente spiegato il più famoso di questi attacchi: Van Eck Phreaking. Questo attacco permette la ricostruzione delle informazioni mostrate su un monitor a partire dalle sole onde elettromagnetiche emanate dallo schermo stesso.

Nel sesto capitolo, a scopo dimostrativo, mostreremo un facile attacco TEMPEST che può essere eseguito anche in casa: Tempest for Eliza. Questo ci permetterà di provare l'esistenza delle "emanazioni compromettenti" e di dimostrare la facilità pratica di un banale attacco TEMPEST.

Nel settimo capitolo, infine, verranno tratte le conclusioni sui dispositivi TEMPEST introdotti provando la necessità di prevenire questo tipo di attacchi.

2

Storia e Sviluppo

Per comprendere appieno le motivazioni dietro la comparsa degli standard TEMPEST, è importante conoscerne la storia. Grazie a questa, infatti, è possibile ricostruire il pensiero umano che ha accompagnato la creazione delle tecnologie per l'intercettazione e la protezione di informazioni sensibili emanate dalle componenti elettriche di qualsiasi apparecchiatura per l'elaborazione di dati.

In questo capitolo viene raccontata la storia degli standard TEMPEST e i cambiamenti che questo progetto ha subito nel tempo.

2.1 Storia degli standard TEMPEST

Durante la seconda guerra mondiale, Bell Telephone, la prima compagnia telefonica del mondo fondata il 9 luglio 1877 da Alexander Graham Bell, fornì all'esercito americano il "mixer 131-B2", un sistema di comunicazione innovativo con capacità senza precedenti per la crittografia di segnali telescriventi. Utilizzava la porta logica XOR, fondamento di tutti i circuiti digitali, e una combinazione del SIGTOT, una macchina a nastro, e il SIGCUM (Converter M-228), una macchina cifratrice a rotore. Tutte queste macchine utilizzavano relè elettromeccanici durante il funzionamento.

Bell in seguito scoprì e informò il governo che il mixer 131-B2 emetteva radiazioni elettromagnetiche che potevano essere rilevate, catturate e decifrate a distanza, recuperando così le informazioni trasmesse. Egli identificò tre aree problematiche: segnali irradiati, segnali condotti su fili che escono dalla struttura

e campi magnetici, e ha suggerito la schermatura, il filtraggio e il mascheramento come possibili soluzioni.

Il risultato della rivelazione di Bell fu l'invenzione di un nuovo dispositivo chiamato "131-A1", un mixer modificato con capacità di schermatura e filtraggio il quale, però, era troppo difficile da mantenere e troppo costoso da distribuire. Bell, quindi, consigliò alle forze armate statunitensi di mantenere e controllare sempre un perimetro di 100 piedi attorno al loro centro di comunicazione al fine di prevenire e controllare l'intercettazione di messaggi nascosti. Dopo la morte di Bell nel 1951, la CIA scoprì che potevano recuperare il testo normale dalla linea che trasportava il segnale crittografato a un quarto di miglio di distanza dal mixer 131-B2. Ciò ha portato allo sviluppo di filtri di segnale e linee elettriche e all'espansione del perimetro di controllo da 100 a 200 piedi.

Nel 1956, il Naval Research Laboratory (NRL), un laboratorio di ricerca statle statunitense, creò un miscelatore migliore che funzionava a tensioni e correnti molto più basse, e quindi le emissioni che perdevano erano molto inferiori. Questo dispositivo fu presto approvato dalla NSA, ma dovette includere l'opzione per aumentare il segnale trasmesso al fine di consegnare messaggi alle telescriventi a distanze molto maggiori. Poco dopo, la NSA ha iniziato a ideare metodi, linee guida e specifiche per filtrare, schermare, mettere a terra e separare i conduttori che trasportavano informazioni sensibili da linee che non lo facevano, che è attualmente noto come separazione ROSSO/NERO. Nel 1958, il NAG-1, una normativa degli Stati Uniti, stabilì standard di radiazione per apparecchiature e installazioni basati su un limite di controllo di 50 piedi. Inoltre, il NAG-1 stabilisce i livelli di classificazione per quasi tutte le variabili TEMPEST .

Tuttavia, nuove sfide hanno accompagnato lo spostamento verso NAG-1. È stato rivelato che la Friden Flexowriter, una macchina da scrivere I/O molto comune utilizzata negli anni '50 e '60, era tra gli emettitori più forti, leggibile fino a 3.200 piedi nei test sul campo. Successivamente, la NSA ha riscontrato problemi simili con l'introduzione di display a tubo catodico (CRT), che erano anche forti emettitori elettromagnetici. Soprattutto, stavano emergendo computer più potenti che erano in grado di memorizzare e trasmettere una quantità di dati di intelligence che cresceva esponenzialmente, spostando il paradigma TEMPEST dalla semplice raccomandazione delle necessarie misure preventive all'applicazione, garantendo così la conformità tra i militari che a sua volta avrebbe migliorato la sicurezza delle informazioni sensibili. Allo stesso tempo, il problema dello spionaggio acustico divenne più diffuso. Oltre 900 microfoni

sono stati scoperti in basi, campi o guarnigioni statunitensi all'estero, la maggior parte dietro la cortina di ferro. Gli Stati Uniti risposero costruendo recinzioni o unità che schermavano completamente le loro emanazioni elettroniche.

Gli standard TEMPEST hanno continuato ad evolversi nel 1970 e oltre, sono emersi nuovi metodi di test e sono state stabilite linee guida più precise.[20]

2.2 Evoluzione di TEMPEST

Lo standard originale degli anni '50 si chiamava NAG1A. Negli anni '60 fu revisionato e ripubblicato come FS222 e successivamente FS222A. Nel 1970, lo standard fu significativamente rivisto e pubblicato come National Communications Security Information Memorandum 5100 (Direttiva sulla sicurezza TEMPEST), noto anche come 'NACSIM 5100'. Fu nuovamente revisionato nel 1974, e l'attuale politica nazionale 'TEMPEST' degli Stati Uniti è stabilita nella National Communications Security Directive 4, datata 16 gennaio 1981. Essa istruisce le agenzie federali a proteggere le informazioni classificate contro le emanazioni compromettenti. Questo documento è noto come 'NACSIM 5100A'.

La NATO ha uno standard simile chiamato AMSG 720B Compromising Emanations Laboratory Test Standard.

In Germania, il programma TEMPEST è amministrato dal Consiglio Nazionale delle Telecomunicazioni.

Nel Regno Unito, il Government Communication Headquarters (GCHQ), l'equivalente della NSA, ha il proprio programma.[6]

2.3 Principali tappe storiche e normative

Nella seguente tabella 2.1 vengono riassunte le principali tappe dello sviluppo storico e normativo di TEMPEST.

Anno	Evento
1943	Bell telephone rilascia il modello 131-B2 non sicuro
1944 in poi	Si inizia a formulare strategie per evitare l'intercettazione di informazioni
1950	La NATO scopre che le intercettazioni del tunnel di Berlino sulle comunicazioni cifrate del telescrivente comunista contengono segnale testuale (primo attacco HIJACK).
1953	Sicurezza delle comunicazioni diventa responsabilità nazione: viene formato il consiglio COMSEC
1958	definito il primo standard TEMPEST: NAG-1A
1960	Gli standard Federali FS222/FS222A rimpiazzano NAG-1A
1960	Si espande la missione COMSEC per includere TEMPEST
1962	Il progetto TEMPEST di NSA inzia (metodi difensivi)
Fine 1960	NVL inizia lavora su TEMPEST, portando a standard nazionali
1967	TEMPEST viene discusso pubblicamente prima volta alla Spring joint computer conference
1970	Viene pubblicato NACSIM 5100
1974	NACSIM 5100A rimpiazza NACSIM 5100
1977	La Germania scopre TEMPEST durante l'esercitazione con NATO
1980	Programma di sicurezza TEMPEST interno: NACSIM 5002
1984	Wang Corporation vende prodotti TEMPEST per un guadagno di 75 milioni di dollari
1984	Vengono pubblicati NACSI 5004, NACSI 5005 e i requisiti di sicurezza TEMPEST da NSA
1986	I guadagni dati dalla vendita di sistemi di sicurezza TEMPEST raggiungono 874 milioni di dollari
1987	Zenith fornisce 12,000 Pc tempest al Pentagono
1988	Oltre 2,9 miliardi di dollari guadagnati tramite i sistemi di sicurezza TEMPEST
1996	Prodotti dei testing systems TEMPEST di nuova generazione usando l'elaborazione di segnale digitale

Tabella 2.1: Principali tappe storiche[21]

3

Segnali intercettabili - le emanazioni compromettenti

I meccanismi di attacco e difesa dei dispositivi TEMPEST sono basati sull'esistenza delle cosiddette emanazioni compromettenti: queste segnali non intenzionali che trasportano informazioni che, se intercettati e analizzati, rivelano le informazioni sensibili trasmesse, ricevute, gestite o elaborate in altro modo da qualsiasi apparecchiatura di elaborazione delle informazioni. Le emanazioni compromettenti possono essere emesse involontariamente da una grande varietà di componenti elettriche all'interno di apparecchiature/sistemi che elaborano informazioni sensibili. Test di laboratorio e sul campo hanno stabilito che tali emanazioni compromettenti possono propagarsi attraverso lo spazio e lungo conduttori vicini. Gli intervalli di intercettazione/propagazione e l'analisi di tali emanazioni sono influenzati da una varietà di fattori, come il design funzionale dell'apparecchiatura di elaborazione delle informazioni; l'installazione del sistema/apparecchiatura; e le condizioni ambientali legate alla sicurezza fisica e al rumore ambientale. Il termine "emanazioni compromettenti" piuttosto che "radiazioni" è utilizzato perché i segnali compromettenti possono esistere in diverse forme come radiazioni di campi magnetici e/o elettrici, conduzione lungo le linee (segnale e potenza) o emissioni acustiche.[13]

In questo capitolo, viene data una breve ma completa spiegazione di queste emanazioni, perchè utile per una maggiore comprensione del funzionamento dei dispositivi TEMPEST.

3.1 Principi di funzionamento delle emanazioni elettromagnetiche

Per un migliore approfondimento delle emanazioni compromettenti, è utile spiegare brevemente il campo elettromagnetico in quanto la maggior parte delle emissioni si trovano in forma di onda EM.

I campi EM vengono prodotti quando la corrente scorre attraverso un conduttore e sono composti da una componente di campo elettrico (E) e una componente di campo magnetico (H). Le due componenti sono reciprocamente dipendenti: nessun campo elettrico in movimento può esistere senza un campo magnetico associato. Essi si irradiano da un conduttore viaggiando perpendicolarmente tra di essi.

Come suggerisce la figura 3.1, il campo elettrico è legato alle differenze di potenziale lungo il conduttore (qui indicato dai segni più e meno alle estremità del segmento di conduttore illustrato). Questo campo elettrico è quindi più forte nei circuiti in cui la tensione, in relazione alla corrente, è alta (maggiore è la tensione, maggiore è l'ampiezza della componente del campo elettrico). Il campo magnetico, invece, emerge come un cerchio in espansione attorno al conduttore ed è più dipendente dal flusso di corrente che dalle differenze di potenziale. Pertanto, in circuiti con corrente relativamente alta, questa componente del campo magnetico è dominante.[13]

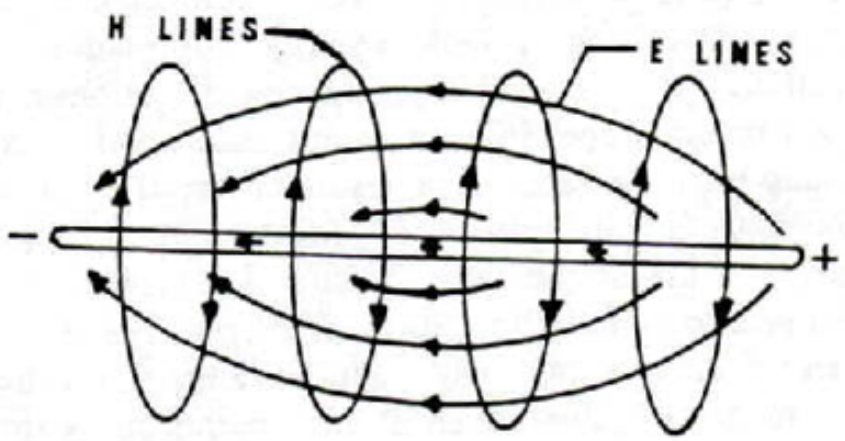

Figura 3.1: Composizione del campo elettromagnetico

3.2 Sorgenti di segnali TEMPEST

Come è stato già detto, emanazioni compromettenti possono essere generate da qualsiasi tipo di componente elettronico di un apparecchiatura di elaborazione di informazioni. In termini fisici, i campi elettromagnetici abbastanza potenti da essere intercettati a distanza sono rilasciati da conduttori quando avvengono cambiamenti rapidi di corrente o tensione all'interno di esso. Il processo di produzione di informazioni sensibili include proprio questi segnali con variazioni rapide. Pertanto, questi campi possono compromettere l'operazione di occultamento che il sistema stesso sta cercando di eseguire.

Più in particolare, si sono due principali sorgenti di emanazioni compromettenti (CE) o, meglio dette, segnali TEMPEST:

- Sorgenti funzionali: Le fonti funzionali sono quelle progettate per lo scopo specifico di generare energia elettromagnetica. Esempi includono transistor di commutazione, oscillatori, generatori di segnali, sincronizzatori, driver di linea e relè di linea.
- Sorgenti incidentali: Le fonti incidentali sono quelle che non sono progettate per lo scopo specifico di generare energia elettromagnetica. Esempi includono interruttori elettromeccanici e motori a spazzole. Più in particolare, le fonti di emanazioni compromettenti possono includere tutti gli apparecchi e i sistemi elettromeccanici ed elettronici utilizzati per elaborare informazioni sensibili.
  La generazione di alcuni tipi di emanazioni compromettenti è aumentata a causa della tendenza a creare apparecchi compatti favorendo l'accoppiamento tra elementi sicuri e non sicuri. Inoltre, i segnali non devono essere di grande ampiezza per essere compromettenti perché gli strumenti di ricezione con cui possono essere intercettati possono rilevare anche una piccola quantità di energia.[13]

3.3 Tipi di emanazioni e vulnerabilità associate

Le emanazioni compromettenti sono divise in 3 classi principali:

- Segnale a banda base RED: una delle emanazioni compromettenti più comunemente identificata. È il segnale originale trasmesso da un dispositivo di comunicazione o di elaborazione prima che venga applicata qualsiasi forma di protezione o crittografia. Esso trasporta informazioni sensibili e richiede protezione attiva.

  Un esempio comune di segnale a banda base RED è il segnale emanato dal monitor di un computer. Infatti, i segnali emessi dal monitor del computer possono essere catturati e visualizzati su un altro monitor.[17]

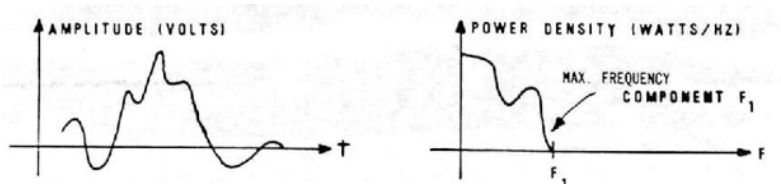

Figura 3.2: Dominio del tempo e della frequenza di segnali a banda base RED

- Segnale spurio modulato: è creato quando un segnale portante è modulato. è un segnale non desiderato che ha subito una modulazione (di fase o di ampiezza) involontaria, risultando in interferenze che possono degradare la qualità e l'affidabilità delle comunicazioni o del funzionamento dei dispositivi elettronici.[16]

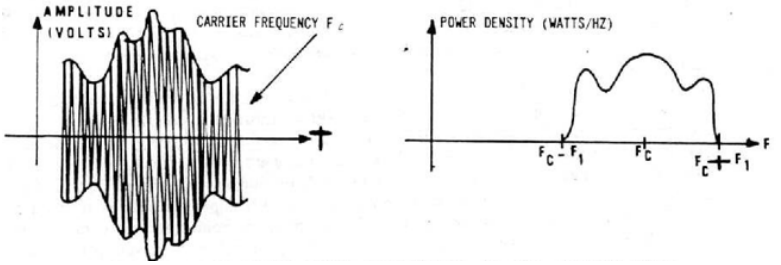

Figura 3.3: Dominio del tempo e della frequenza di segnali portanti modulati

- Emanazioni impulsive: sono formate dalle apparecchiature elettriche in fase di test. In particolare, le emanazioni impulsive sono causate quando l'apparecchiatura in prova (EUT) elabora rapidamente i segnali digitali[15]. (Vedi figura 3.4)

- Altri tipi di emanazioni: La maggior parte delle CE rientrano tra i tipi menzionati finora. Tuttavia, ci sono altre possibili categorie di emanazioni compromettenti causate da operazioni lineari e non lineari che si verificano nelle apparecchiature e nei sistemi di elaborazione delle informazioni. Queste CE non possono essere facilmente categorizzate[13].

I vari tipi di emanazioni si possono propagare in diverse forme:

- Radiazione elettromagnetica: E' il tipo di emanazione più studiato. Le radiazioni elettromagnetiche danno informazioni essenziali sul segnale/apparecchio che l'hanno generate. Dunque, a seconda del nostro atteggiamento nei confronti della segretezza, le radiazioni EM possono essere sia interferenti che informative o compromettenti[6].

- Conduzione accidentale: emanazioni sotto forma di segnali che si propagano lungo conduttori non intenzionali come tubi, travi, fili, cavi, condotti, e condutture[13].

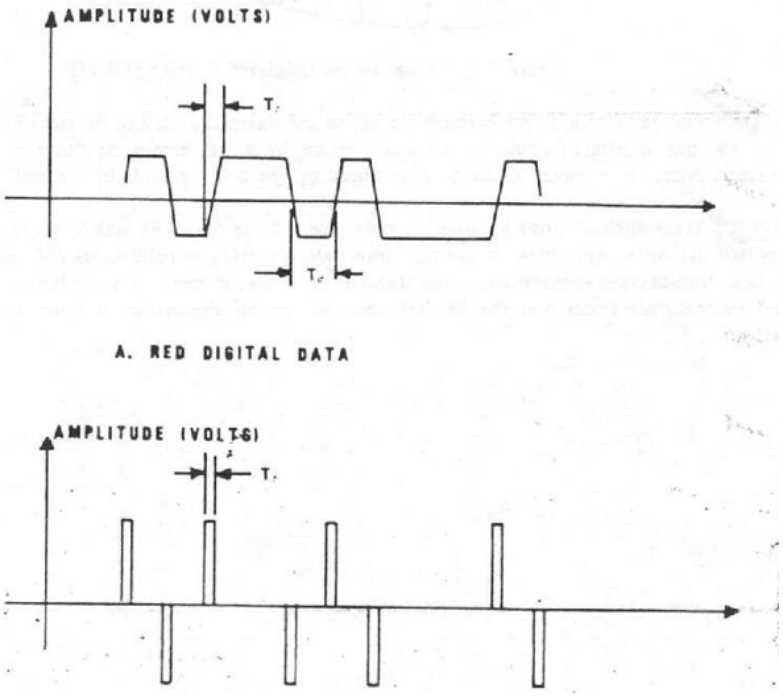

Figura 3.4: Emanazioni impulsive correlate ad un segnale digitale RED

- Emanazioni acustiche: Le emanazioni acustiche si sono rivelate essere eccellenti fonti di informazioni camuffate. Queste diventano compromettenti perchè, se ricostruite, danno informazioni sui componenti meccanici che hanno causato tali emanazioni[6]. Più in particolare, le onde sonore causano vibrazioni che possono essere analizzate per ricostruire il segnale acustico di partenza. I principali componenti vulnerabili a questo tipo di intercettazione sono: tastiere, stampanti e relè[13].

- Emanazioni ottiche: Questo tipo di CE non sono tradizionalmente trattate dai dispositivi TEMPEST ma in contesti di alta sicurezza anche emissioni di luce visibile, infrarosse e laser possono trapelare informazioni sensibili.

4

Tecnologie e Tecniche di Protezione TEMPEST

Dopo questa breve panoramica sulle emissioni compromettenti, siamo finalmente pronti ad addentrarci nel vivo del discorso: Come possiamo proteggere un qualsiasi dispositivo di elaborazione di informazioni da attacchi TEMPEST?

Le tecniche di protezione TEMPEST prevedono la progettazione di circuiti e reti per minimizzare la quantità di emanazioni compromettenti (CE), principalmente attraverso l'applicazione di schermature, messa a terra e collegamenti appropriati. Nella fase di progettazione dei sistemi, le metodologie di sicurezza principalmente applicate includono metodi di schermatura delle radiazioni e tipicamente comportano l'eliminazione o la riduzione dei transitori causati da un segnale di comunicazione, utilizzando tecniche di modulazione e modellazione del segnale.

Una progettazione adeguata minimizza i segnali non intenzionali emessi da un dispositivo, ma l'eradicazione totale non può essere raggiunta.

Nel caso di un trasmettitore di comunicazione, le varie fonti di emissioni spurie sono i componenti del circuito negli stadi di ingresso/uscita, a causa di disallineamenti, giunzioni del circuito inadeguate, radiazioni dai cavi locali che collegano il centro di comunicazione/centro di segnale alla stazione di trasmissione a diversi chilometri di distanza, i cavi di collegamento interni ed esterni, ecc.

In questo contesto, la protezione TEMPEST può essere fornita a livello di apparecchiatura, a livello di sistema, o entrambi[6].

In questo capitolo, vengono presentate le principali tecniche TEMPEST utilizzate per ridurre la quantità e l'intensità delle emanazioni compromettenti.

4.1 Schermature elettromagnetiche

La prima strategia protettiva TEMPEST è la schermatura: un sistema in grado di ridurre in una determinata zona dello spazio il campo elettromagnetico generato da una sorgente[2]. Questo metodo è di gran lunga il più comune per la protezione di alto livello TEMPEST. Massimizza la flessibilità poiché qualsiasi apparecchiatura standard può essere utilizzata all'interno della struttura schermata[6].

Come suggerisce il nome, la schermatura introduce uno "schermo" che mette una discontinuità di impedenza nel percorso di un'onda elettromagnetica irradiata che si propaga, riflettendola e/o assorbendola. Questo è concettualmente molto simile al modo in cui funzionano i filtri: mettono una discontinuità di impedenza nel percorso di un segnale condotto indesiderato. Maggiore è il rapporto di impedenza, maggiore è l'efficacia dello schermo o, meglio detta, shielding effectiveness (SE).

Vi sono diversi metodi per applicare una schermatura, ma il metodo tradizionale TEMPEST prevede una combinazione di isolamento della fonte di alimentazione circondando la macchina, a rischio di monitoraggio indesiderato, con una gabbia di Faraday che blocca i campi elettromagnetici e non consente alcuna emanazione vagante. In particolare, la schermatura TEMPEST (50 decibel, protezione media) consiste in pareti, pavimenti e soffitti di acciaio di spessore tra 22 e 26 gauge, con giunzioni serrate.[6] Altri metodi di schermatura TEMPEST includono l'isolamento della stanza e delle pareti e il posizionamento preciso delle apparecchiature, che possono ulteriormente garantire che nessun onda EM possa sfuggire[3].

4.1.1 Zonizzazione

Motivazioni

La zonizzazione è un metodo di controllo utilizzato quando sono richiesti diversi livelli di protezione. Ad esempio, un generatore di energia può funzionare senza problemi in un'area di attenuazione molto bassa, magari solo sotto una

Figura 4.1: Edificio schermato secondo le norme TEMPEST

struttura di armatura in ferro. Una sala di alimentazione e di comunicazione più sensibile potrebbe richiedere un livello di protezione da basso a medio di 60 decibel, mentre una sala di controllo e computer molto sensibile potrebbe richiedere un'area con un alto livello di protezione (100 decibel)[6].

Livelli e Zone

Le procedure di zonizzazione definiscono e classificano diversi ambienti in "zone", ognuna delle quali con un certo livello di attenuazione. Ogni porzione di spazio più o meno grande può essere classificata in Zona 0, Zona 1, Zona 2 o Zona 3 a seconda del livello di protezione richiesto, come mostrato nella figura 4.2.

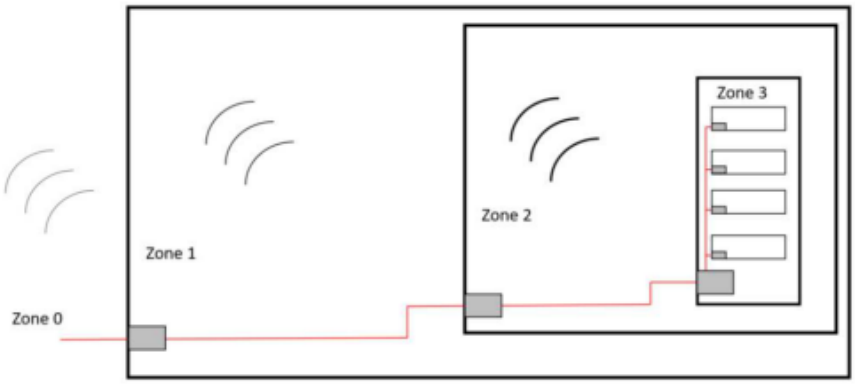

Figura 4.2: Modello concettuale di zonizzazione TEMPEST

Gli attuali standard di schermatura Tempest degli Stati Uniti e della NATO sono segmentati in tre livelli di requisiti di protezione, applicati alla gamma di frequenze da 100 kHZ a 1 GHz:

- NATO SDIP-27 Level A (ex AMSG 720B) e USA NSTISSAM Level I "Compromise Emanations Laboratory Test Standard" Questo è lo standard più severo per i dispositivi che operano in ambienti NATO Zona 0, dove si presume che un utente malintenzionato abbia accesso quasi immediato (ad esempio stanza vicina, 1 m di distanza). In questa zona, infatti, vi è un attenuazione tipicamente superiore ai 60 dB;

- NATO SDIP-27 Level B (ex AMSG 788A) e USA NSTISSAM Level II "Laboratory Test Standard for Protected Facility Equipment" Questo standard è per i dispositivi che operano in ambienti NATO Zona 1, dove si presume che un attaccante non possa avvicinarsi a circa 20 m (o dove i materiali da costruzione assicurano un'attenuazione tra i 40 dB e i 60 db);

- NATO SDIP-27 Level C (ex AMSG 784) e USA NSTISSAM Level III "Laboratory Test Standard for Tactical Mobile Equipment/Systems" Lo standard più permissivo che si concentra sui dispositivi che operano in ambienti NATO Zona 2, dove gli aggressori devono affrontare l'equivalente di 100 m di attenuazione dello spazio libero tipicamente inferiore ai 40 dB[3].

4.1.2 Hardening

la procedura di hardening (rafforzare, in italiano) consiste nel definire un sottoinsieme di apparecchiature da schermare e nel rafforzare (ossia contenere le CE) solo tali attrezzature e i relativi ausiliari necessari. Questo metodo viene utilizzato in due circostanze principali:

- Ampia distanza: le apparecchiature sono fisicamente separate da larghe distanze e non è realistico provare a schermare l'intera area;

- Schermatura di componente: Le apparecchiature da schermare si trovano in una struttura in cui rappresentano solo una piccola parte di tutte le attrezzature presenti, e quindi non è consigliabile schermare l'intera struttura. In particolare, vengono utilizzate piccole stanze o apparecchiature schermate con filtri elettrici, pannelli di accesso e porte RF. Rispetto alla schermatura di un'intera struttura, questo tipo di protezione presenta diversi svantaggi: totalmente inflessibile, molto costosa e molto difficile da mantenere. Inoltre, il sistema risulta essere vulnerabile durante la manutenzione, quando i pannelli di accesso sono aperti[6].

4.1.3 Materiali

Finora, sono stati trattati il principio e il funzionamento della schermatura elettromagnetica, ma quali sono i materiali più usati per questo tipo di operazione?

Si parla in questo caso di reti di metallo: materiali fondamentali utilizzati per schermare le onde elettromagnetiche. Offrono facilità d'uso grazie al loro peso ridotto rispetto alle piastre metalliche standard. Le reti metalliche sono strutture flessibili. Per questo motivo, possono essere facilmente utilizzate anche come materiale di schermatura nella fase di progettazione dei dispositivi elettronici[7].

Per dimostrare che la scelta del materiale è importante, è utile vedere come l'attenuazione del segnale varia a seconda del metallo scelto. Prendendo, per esempio, una piastra in alluminio, una rete in rame e un'altra rete in zinco l'efficienza di schermatura (SE) cambia come mostrato nella figura 4.3 al variare della frequenza del segnale da schermare (tra 10 MHz e 6 GHz).

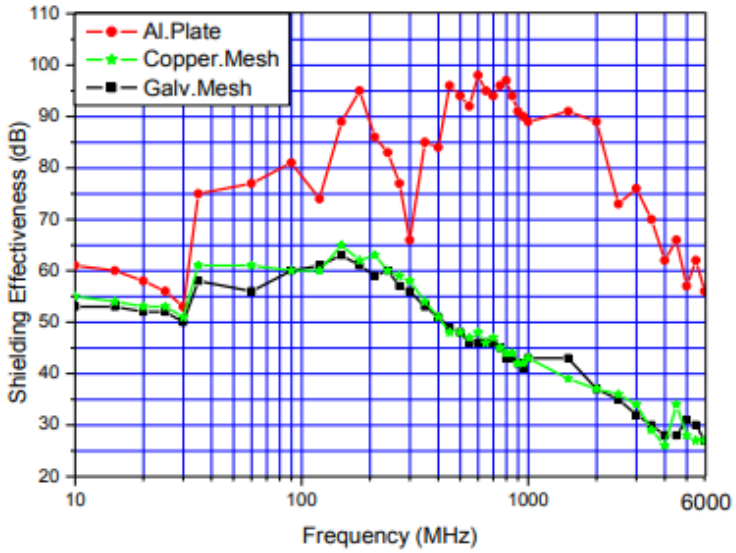

Figura 4.3: Efficienza di schermatura dei tre materiali a diverse frequenze di segnale schermato

Come si può vedere, Il valore di attenuazione (SE) della lastra di alluminio è piuttosto elevato. Tuttavia, la lastra di alluminio è pesante, più costosa delle reti metalliche e non è abbastanza flessibile per l'assemblaggio. I valori di SE delle reti metalliche in rame e zincate sono approssimativamente uguali. Tuttavia, ci sono alcuni svantaggi della rete in rame, come il costo maggiore rispetto alla rete zincata con le stesse proprietà geometriche, la suscettibilità alla corrosione e la difficoltà di reperibilità sul mercato. A seguito di questi confronti, se una schermatura di livello moderato o basso è sufficiente per gli scopi TEMPEST, la rete zincata è la soluzione più ottimale da utilizzare per la schermatura delle pareti di uffici o case, poiché è economica, flessibile e leggera. Inoltre, ha valori SE sufficienti ed è facilmente reperibile sul mercato[7].

4.2 Filtraggio

Un'altra tecnica TEMPEST per l'attenuazione delle emanazioni compromettenti di un dispositivo è il filtraggio. In particolare, un filtro elettrico è una rete di resistori, induttori e condensatori o loro equivalenti, o una qualsiasi combinazione di questi, che offre una resistenza relativamente bassa a determinate

frequenze o alla corrente continua (DC), bloccando totalmente il passaggio di altre frequenze.

La caratteristica più significativa di un filtro è la perdita di inserzione (ossia la perdita di potenza di un segnale dovuta all'inserimento del filtro[4]) che offre in funzione della frequenza. Infatti, questa relazione viene spesso chiamata caratteristica in frequenza del filtro.

Per le applicazioni TEMPEST, i filtri possono essere progettati utilizzando componenti reattivi che impediscono il passaggio delle frequenze indesiderate riflettendole verso la sorgente, o utilizzando componenti dissipativi, che assorbono le frequenze indesiderate[18].

Posizione dei filtri

Tali filtri sono installati in punti critici allinterno dei sistemi che vengono protetti. Ciò include:

- Filtri dingresso e di uscita dalla stanza o dellapparecchiatura: tutti i cavi che entrano o escono dalla stanza schermata o dall'apparecchiatura, come i cavi di alimentazione, di segnale, e di rete;
- Punti di penetrazione: Qualsiasi punto in cui i cavi o i condotti attraversano le pareti della schermatura elettromagnetica;
- Apparecchiature elettroniche interne: I filtri possono essere integrati anche all'interno delle stesse apparecchiature elettroniche per ridurre le emissioni direttamente alla fonte;
- Sistemi di alimentazione: Gli ingressi dell'alimentazione elettrica.

In generale, la disposizione dei filtri è studiata per garantire che non vi siano percorsi non schermati o non filtrati attraverso i quali le emissioni compromettenti possano fuoriuscire, assicurando così che l'informazione sensibile rimanga protetta.

4.3 Progettazione e layout dei circuiti per la mitigazione e la soppressione delle emissioni

Per la gran parte dei sistemi elettronici, la maggiore fonte di emanazioni compromettenti è rappresentata dalle schede a circuito stampato (PCB) contenute all'interno del sistema stesso, a causa delle lunghe tracce che trasportano correnti

transitorie con un consistente contenuto spettrale ad alta frequenza[18]. In questo contesto, si introduce il concetto di soppressione: tecnica che mira a ridurre le emissioni spurie indesiderate prodotte dai singoli componenti del circuito in diverse fasi. Questo si basa semplicemente su buone pratiche di progettazione dei circuiti supportate dai principi fondamentali di messa a terra, collegamento, schermatura, filtraggio e tecniche di isolamento.

Infatti, i progetti conformi alle specifiche 'TEMPEST' includono dettagli come la disposizione dei componenti sulla PCB, il layout delle tracce, le dimensioni, ecc.; tutto ciò, però, porta a una maggiore complessità nella progettazione di un PCB multistrato[6].

I principali passaggi per una buona progettazione di un PCB sono: determinare lo schema di alimentazione e messa a terra, disporre le aree di alimentazione e di massa, e disporre le aree del clock. In genere, il rumore di massa è un problema maggiore rispetto al rumore dell'alimentazione.

Il rumore di massa è prodotto da due tipi di correnti: quella transitoria dell'alimentazione e quella di ritorno del segnale. La prima può essere controllata mediante l'uso corretto di condensatori di disaccoppiamento, ma le correnti della seconda tipologia non possono essere disaccoppiate o bypassate.

Le correnti transitorie di massa sono una delle principali fonti di rumore di tensione intra-sistema e di emissioni condotte e irradiate. Per ridurre al minimo il rumore derivante da questa tipologia di correnti, l'impedenza della massa deve essere minimizzata. In questo contesto, vengono ideati diversi metodi per ridurre l'induttanza di un circuito come: minimizzare la lunghezza dei conduttori critici che trasportano grandi correnti transitorie oppure fornire percorsi alternativi per il flusso di corrente. Questi percorsi devono essere elettricamente, ma non necessariamente fisicamente, paralleli[18].

4.4 Tecniche avanzate di protezione

Le tecniche di protezione appena mostrate sono quelle più comuni e maggiormente utilizzate. Esistono, però, ulteriori strategie avanzate che permettono di proteggere dispositivi da attacchi TEMPEST.

Di seguito, viene riportato un esempio di una possibile strategia avanzata per la protezione dal furto di informazioni: il sistema Honeypot.

4.4.1 Sistema Honeypot

Il sistema honeypot (vaso di miele, in italiano) consiste in una piattaforma SDR (Software Defined Radio) che, tramite due apposite antenne multibanda, cattura le CE emesse dal dispositivo attaccato e produce i cosiddetti "honey baits": segnali in grado di coprire la banda in frequenza dell'emanazione compromettente che si sta proteggendo e di ingannare il ladro che, captando questi segnali, non riceverà alcuna informazione sensibile.

Più in particolare, la piattaforma SDR può rilevare le radiazioni elettromagnetiche e catturare i segnali trapelati in base alla frequenza specificata e alla risoluzione, e inoltre risolvere e regolare automaticamente la frequenza di aggiornamento[24].

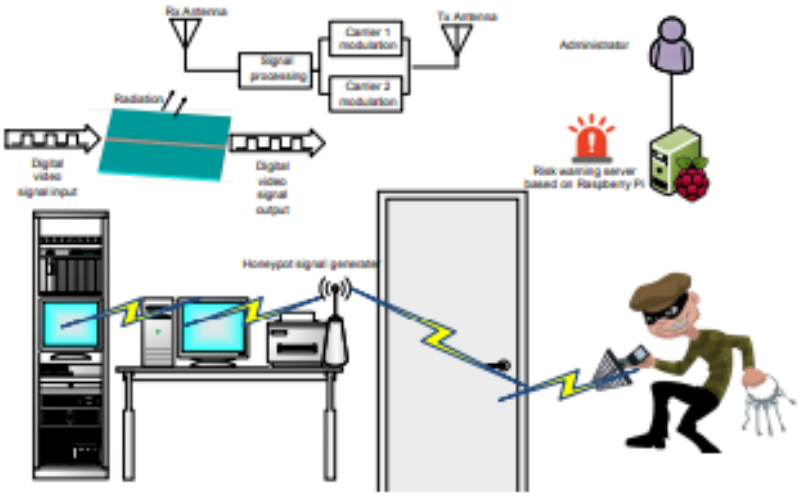

Figura 4.4: Struttura complessiva del sistema Honeypot

5

Aspetti Offensivi: Attacchi TEMPEST

Nel precedente capitolo sono state presentate tecnologie e strategie per la prevenzione e la protezione di dispositivi elettronici da ladri di informazioni. E' giusto ora chiedersi quali siano le metodologie utilizzate da questi "ladri" per l'intercettazione e la ricostruzione di emanazioni compromettenti.

Come è già stato anticipato, in alcuni casi è possibile ottenere informazioni sui segnali utilizzati all'interno dell'apparecchiatura quando le radiazioni vengono captate e i segnali ricevuti vengono decodificati. Specialmente nel caso delle apparecchiature digitali, questa possibilità costituisce un problema, poiché la ricostruzione remota dei segnali all'interno dell'apparecchiatura potrebbe permettere la ricostruzione dei dati che l'apparecchiatura sta elaborando.

Questo problema non è nuovo; gli specialisti della difesa ne sono a conoscenza da oltre cento anni ma le informazioni su come prevenire questo tipo di "spionaggio" non sono liberamente disponibili e le apparecchiature progettate per proteggere le informazioni militari saranno probabilmente tre o quattro volte più costose rispetto a quelle che verosimilmente verranno utilizzate per l'elaborazione di informazioni non militari.

Fino a poco tempo fa, si considerava molto difficile il furto di dati a partire dal segnale elettromagnetico e si credeva quindi che lo spionaggio delle apparecchiature digitali potesse essere effettuato solo da professionisti con accesso a strumenti di rilevamento e decodifica molto sofisticati[11]. In realtà non è così: gli strumenti necessari per effettuare un cosiddetto attacco TEMPEST non sono così costosi come si crede.

In questo capitolo, verranno analizzati i principi e le tecnologie dietro gli attacchi TEMPEST mostrando il pericolo e le preoccupazioni che ne derivano.

5.1 Definizione e principi degli attacchi TEMPEST

Come già anticipato, TEMPEST appartiene alla categoria degli attacchi passivi che utilizzano onde elettromagnetiche irradiate da dispositivi elettronici per recuperare o intercettare informazioni dal bersaglio[9]. Tra i vari dispositivi maggiormente soggetti a questo tipo di attacco abbiamo computer, monitor, tastiere, stampanti e persino cavi di rete[22].

I metodi impiegati in TEMPEST per intercettare le emissioni compromettenti possono essere classificati in una procedura a tre step, come mostrato nella Figura 5.1. I tre passi della procedura prevedono la selezione di un sistema target, una strategia di misurazione adatta e un sistema di recupero delle informazioni.

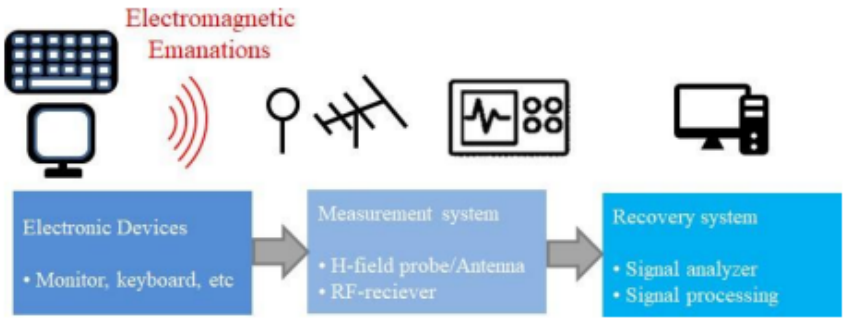

Figura 5.1: Procedura di un attacco TEMPEST

La procedura può essere descritta come segue:

- Selezione di un sistema target: In questa fase l'obiettivo principale è identificare le informazioni sui segnali digitali desiderati. Le caratteristiche di dispersione di tali segnali sono la chiave per capire come eseguire l'intercettazione con meno errori possibili.

- Individuazione di un sistema di misurazione adatto: Una configurazione tipica di un sistema TEMPEST comprende una sonda H o un'antenna, e, se necessario, un ricevitore RF con amplificatori a bassa rumorosità ed eventuali filtri. Le onde elettromagnetiche di dispersione contengono vari componenti di frequenza a seconda delle caratteristiche spettrali del segnale del bersaglio. Pertanto, per analizzare e ricostruire le informazioni di dispersione dai dispositivi elettronici bersaglio, è necessario considerare varie bande di frequenza e, di conseguenza, utilizzare più ricevitori RF per coprire le varie bande.

- Selezione di un sistema di recupero informazioni: La terza procedura del metodo TEMPEST comprende il sistema di recupero delle informazioni e gli algoritmi che analizzano la dispersione delle onde elettromagnetiche misurate e che ricostruiscono le informazioni appropriate attraverso varie tecniche di elaborazione dei segnali. Come già anticipato, le onde elettromagnetiche di dispersione provenienti da apparecchiature elettroniche, che possono essere raccolte con un sistema di misurazione ad alta sensibilità, possono contenere informazioni critiche sul funzionamento dei sistemi elettronici. Tuttavia, la potenza della dispersione è tendenzialmente estremamente debole e distorta per un riconoscimento immediato. Pertanto, deve essere ripristinata in informazioni utilizzabili attraverso l'applicazione di numerose tecniche di elaborazione dei segnali, comprese l'intelligenza artificiale (AI) o il deep learning. In generale, il recupero delle informazioni è possibile quando i meccanismi operativi e i protocolli dell'apparecchiatura elettronica target sono conosciuti. Ad esempio, per ricevere e recuperare informazioni dalle onde elettromagnetiche disperse da un monitor, è necessario sapere come le informazioni dello schermo sono rappresentate su tale monitor[9].

5.1.1 Esempi e casi di studio

Prima di approfondire gli aspetti tecnici degli attacchi TEMPEST, è utile mostrare qualche esempio, in modo da comprendere quanto può essere minaccioso e pericoloso un attacco TEMPEST.

- Van Eck Phreaking: è uno dei più noti attacchi TEMPEST, prende il nome dall'ingegnere olandese Wim van Eck che nel 1985 dimostrò come le emissioni elettromagnetiche di un monitor CRT potessero essere intercettate e ricostruite a distanza.

- KGB attack: Durante la guerra fredda, il Comitato per la sicurezza dello stato Russo utilizzò spesso i principi TEMPEST per intercettare le comunicazioni delle ambasciate e delle strutture governative occidentali.

- Kuhn attack: Nel 1998 gli studiosi Markus G. Kuhn e Ross J. Anderson pubblicarono un documento in cui definivano il Kuhn attack. Si tratta di un'ulteriore minaccia TEMPEST che permette di recuperare informazioni riguardo ai tasti premuti su una tastiera fino a 20 metri di distanza, anche attraverso un muro[10].

Questi sono pochi di tutti i gli esempi che potrebbero essere fatti di attacchi TEMPEST. La varietà e il pericolo di questi attacchi destano preoccupazioni non banali in campo di sicurezza elettromagnetica.

5.2 Una vista più profonda: Van Eck Phreaking

Data la vasta gamma di attacchi TEMPEST che possono essere attuati, risulta difficile e dispersivo riportare in un unico report tutte le tecniche di intercettazione e ricostruzione utilizzate in questo ambito. Quindi, per una migliore compresione del tema trattato conviene prendere uno degli esempi soprariportati e approfondirlo con lo scopo di fornire un'idea più concisa e precisa del funzionamento di questi attacchi.

Il caso di studio scelto è quello di Van Eck Phreaking: esso consiste nell'intercettare e riprodurre le informazioni di un monitor CRT semplicemente tracciando le emissioni elettromagnetiche del display stesso.

5.2.1 Principi della televisione

Al fine di comprendere a fondo il funzionamento dell'attacco Van Eck Phreaking è giusto dare una breve descrizione di come funziona una televisione a tubo a raggi catodici (CRT).

La costruzione di un'immagine

L'immagine su uno schermo televisivo viene costruita in modo sequenziale. Ogni immagine è composta da un certo numero di linee orizzontali così vicine tra loro che non possono essere riconosciute singolarmente da una distanza ragionevole dallo schermo della tv. Queste linee orizzontali vengono scritte sullo schermo TV in una sequenza predeterminata: da sinistra a destra e partendo dall'alto dello schermo.

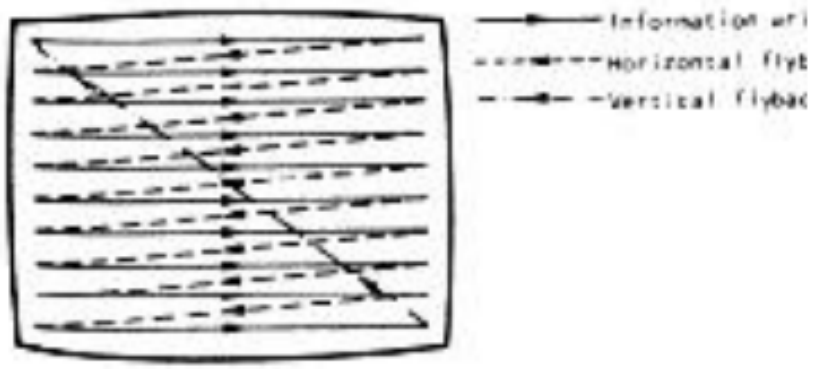

Figura 5.2: Costruzione di un'immagine televisiva

Il dispositivo utilizzato per costruire l'immagine viene chiamato tubo a raggi catodici (CRT). Esso è formato da un catodo e un anodo e, di conseguenza all'applicazione di un campo magnetico attorno al "piede" del CRT, è possibile creare un fascio di elettroni. Se la tensione è sufficientemente alta, l'energia cinetica degli elettroni sarà abbastanza elevata da eccitare il fosforo sullo schermo rendendolo luminoso (ossia emette fotoni). Pertanto, controllando la tensione applicata tra il catodo e l'anodo, è possibile controllare l'intensità luminosa di un determinato punto sullo schermo. Inoltre, essendo gli elettroni particelle cariche, è possibile applicare un campo magnetico o elettrico perpendicolare alla direzione del flusso per cambiare la posizione del punto luminoso sullo schermo[11].

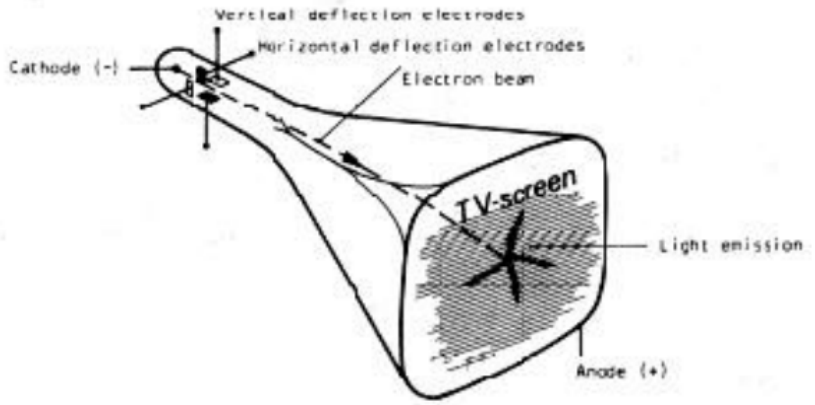

Figura 5.3: Struttura generale di un tubo a raggi catodici

Il segnale video

Per modulare l'intensità (in termini di luce) del punto luminoso sullo schermo è necessario un segnale chiamato segnale video. In genere, un ricevitore televisivo riceve questo specifico segnale video dal trasmettitore. Come detto nel sottoparagrafo precedente, l'immagine è costruita da diverse linee orizzontali e, per far sì che il ricevitore TV riesca a decodificare il segnale video ricevuto in un'immagine leggibile, deve conoscere in quale momento del segnale ricevuto inizia l'informazione su ogni linea. Per questo motivo, anche l'informazione sull'istante di inizio di ogni linea di un'immagine viene trasmessa. Il segnale utilizzato per fornire queste informazioni al ricevitore TV è chiamato segnale di sincronizzazione. In particolare, il segnale video e il segnale di sincronizzazione sono combinati in un unico segnale, chiamato segnale line feed (LF)[11].

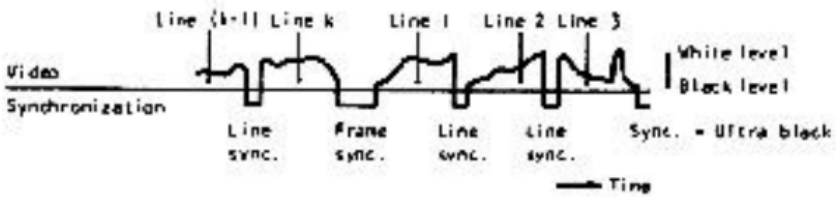

Figura 5.4: Rappresentazione del segnale line feed in un ricevitore TV

5.2.2 Emissioni elettromagnetiche di un monitor CRT

Il campo irradiato da un VDU (Video Display Unit) può essere diviso in due parti:

- Radiazioni dei segnali digitali di clock;
- Radiazioni dei segnali digitali "casuali" come il segnale video.

In particolare, il segnale video viene amplificato dall'unità di logica transistor-transistor (TTL) diverse centinaia di volte prima di essere inviato al CRT. Pertanto, la radiazione derivante dal segnale video è tendenzialmente la componente dominante del campo generato dal VDU.

I principi fisici dell'attacco Van Eck Phreaking si basano sul fatto che ogni radiazione proveniente dal segnale video mostra una notevole somiglianza con il segnale televisivo stesso. Quindi, risulta possibile ricostruire l'immagine visualizzata su un monitor CRT solo dalle emissioni irradiate da esso[11].

5.2.3 Sistema di misurazione: le antenne

Seguendo la procedura indicata nel paragrafo 5.1, sono stati già analizzati il dispositivo target (ossia un VDU) e il segnale da intercettare che porta informazione (segnale video).

Ora si passa al secondo step: il sistema di misurazione. Come già accennato, l'apparecchitura TEMPEST utilizzata per intercettare e ricevere segnali consiste in un antenna a dipolo e in un semplice ricevitore TV. Tendenzialmente, è anche necessario un amplificatore di antenna per aumentare la potenza del segnale ricevuto (solitamente debole o instabile). Con questo semplice equipaggiamento, è possibile intercettare segnale anche a distanza di centinaia di metri se non viene presa nessuna misura preventiva. Con attrezzi notevolmente sofisticati, è possibile prelevare informazioni a più di un kilometro di distanza.

Wim van Eck condusse diversi esperimenti al riguardo. In uno di questi viene posizionata tutta l'attrezzatura necessaria in una macchina posta nel parcheggio di un edificio in cui viene utilizzato uno strumento di elaborazione di testo (word processor). L'esperimento fu un successo: le informazioni mostrate sullo schermo del dispositivo furono facilmente captate e rappresentate sul ricevitore TV.

Un altro esperimento condotto da Wim van Eck è stato eseguito nel febbraio del 1985 dove un piccolo van fu equipaggiato con un'antenna VHF (Very High frequency, 10 dB di guadagno[5]) alta 10 metri e il segnale venne amplificato fino a 18 dB e mostrato su uno schermo televisivo nel van. La riuscita dell'esperimento dimostrò che anche con dell'attrezzatura relativamente semplice ed economica è possibile rubare informazioni sensibili a grandi distanze.

Con questi esperimenti le persone si sono rese conto della minaccia incombente nel campo della sicurezza informatica[11].

5.2.4 Decodifica del segnale: il sistema di recupero

Dopo aver captato e intercettato il segnale video, l'ultimo passaggio della procedura TEMPEST prevede la selezione di un sistema di recupero delle informazioni attraverso la decodifica delle onde elettromagnetiche.

Il problema della sincronizzazione

Il problema maggiore riguardo l'attacco Van Eck Phreaking riguarda il fatto che il ricevitore TV capta solamente il segnale video e non quello di sincronizzazione. Questo significa che l'immagine visualizzata sullo schermo della TV si costruirà sul ricevitore sia in direzione orizzontale che verticale, a meno che le frequenze di sincronizzazione del VDU e del ricevitore siano le stesse. Anche se questo è vero per molti tipi di unità video, l'immagine non sarà molto stabile e quindi difficile da leggere. Per questo motivo, bisogna cercare di sincronizzare i due schermi o altrimenti l'immagine mostrata non sarà fedele a quella originale[11].

Possibili soluzioni

Se il problema della sincronizzazione non viene risolto, l'attacco non funziona. Per questo motivo, sono state ideate due principali soluzioni:

- Oscillatore esterno: Il modo più semplice ed economico per gestire il problema della sincronizzazione è l'uso di un dispositivo con due oscillatori regolabili: il primo con frequenza di 15-20 kHz per gestire la sincronizzazione orizzontale e il secondo con frequenza di 40-80 Hz per quella verticale. Questi segnali sono poi combinati e inviati al separatore di sincronizzazione del ricevitore TV che ricostruisce il segnale di sincronizzazione e, quindi, il segnale LF. Poiché le frequenze di sincronizzazione verticale e orizzontale sono correlate secondo l'equazione $f_{hor} = kf_{vert}$, è possibile generare solo la frequenza di sincronizzazione orizzontale e ottenere quella verticale dividendo la prima per il numero di linee dello schermo k.
- Recupero dal segnale ricevuto: E' possibile recuperare le frequenze di sincronizzazione orizzontale e verticale nello spettro del segnale video, poiché il segnale video viene azzerato durante il flyback orizzontale e verticale del fascio di elettroni nel CRT. L'estrazione delle frequenze in questione prevede l'utilizzo di un circuito recupero della sincronizzazione che utilizza un filtro passa banda per prelevare la frequenza di sincronizzazione orizzontale dal segnale LF. Il segnale risultante è un'onda sinusoidale di 15-20 kHz con un certo rumore di fase, che può essere eliminato con un phase-locked loop. Infine, tramite un circuito di manipolazione dell'impulso viene trasformata l'onda sinusoidale in un'onda quadra (segnale di sincronizzazione) e la frequenza di sincronizzazione verticale è facilmente ottenuta dividendo quella orizzontale per il numero di linee dello schermo k[11].

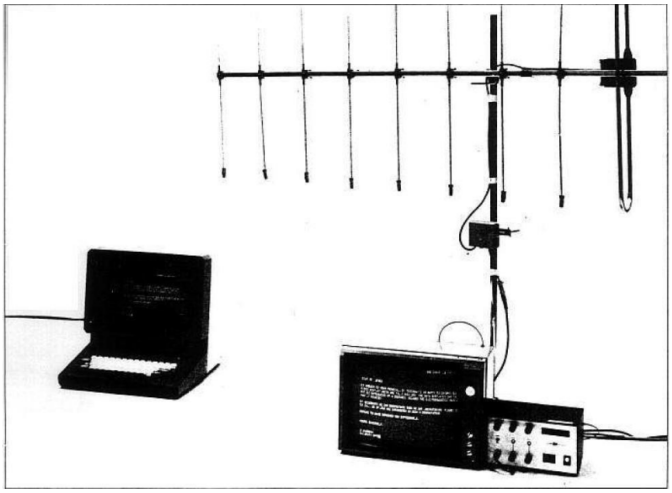

Figura 5.5: Van Eck Phreaking: esempio di set-up

5.2.5 Contromisure

Riprendendo ciò che è stato detto nel capitolo 4, è importante conoscere le contromisure pensate per evitare questo tipo di attacchi.

Le soluzioni adottate sono le seguenti:

- Attenuare la potenza delle emissioni compromettenti: la migliore misura preventiva per evitare attacchi TEMPEST di qualsiasi tipo (non solo Van Eck Phreaking) è quella di ridurre le CE. A quest scopo le strategie principali prevedono la proibizione di componenti che commutano più velocemente di quello che serve, la riduzione dell'area del circuito che produce tali emissioni, mantenere i collegamenti più corti possibile e schermare elettromagneticamente la zona;

- Aumentare la potenza del rumore: Dal punto di vista di una radio, più rumore è presente peggiore è il segnale ricevuto. A questo scopo, si può pensare di posizionare molto equipaggiamento in un'unica stanza (come un grande numero di terminali).

  Questa soluzione, però, è tendenzialmente scartata. Infatti, il pattern di radiazione di un terminale è determinato in gran parte dalle risonanze a determinate frequenze. Queste risonanze si verificano a frequenze diverse, anche se vengono scelti due terminali dello stesso tipo. Ciò significa che è possibile intercettare anche un solo VDU individuale in mezzo a tanti terminali, poiché ogni unità ha frequenze di risonanza diverse in cui la radiazione è dominante.

- Cambio della costruzione di un'immagine: Il fattore principale che consente la rilevazione delle informazioni visualizzate su un VDU tramite un normale ricevitore TV è la somiglianza tra i due sistemi per quanto riguarda la costruzione dell'immagine, come visto prima. Pertanto, una soluzione semplice ed efficace a questo problema è cambiare la sequenza con cui le linee successive vengono scritte sullo schermo. In questo caso, infatti, il segnale video ricevuto dall'antenna diventa illeggibile e risulta molto complicata la ricostruzione dell'immagine a partire dal segnale ricevuto se non si ha a disposizione un equipaggiamento di decodifica piuttosto sofisticato. In particolare, la sequenza di costruzione delle linee nello schermo può essere resa dipendente da una chiave inserita nelle unità circuitali che definisce l'ordine di build-up dell'immagine.

  Questo metodo è efficace ma può essere aggirato tramite una strategia di decodifica "a tentativi", ossia si provano tutte le combinazioni possibili fino a trovare quella giusta. Per questo motivo, si può fare in modo di cambiare la chiave di costruzione dopo un intervallo di tempo predeterminato[11].

5.2.6 TempestSDR

Il set-up presentato fino ad ora è quello del 1985, ossia quasi quaranta anni fa. E ora? Come si è evoluta la tecnologia TEMPEST per gli attacchi come Van Eck Phreaking?

L'attrezzatura utilizzata per effettuare un attacco TEMPEST è cambiata e, in particolare, si è ridotta. Infatti, sono state sviluppate idee software per eseguire Van Eck Phreaking con ancora meno equipaggiamento.

Lo strumento in questione si chiama TempestSDR: è un toolkit software open-source per l'intercettazione e l'elaborazione dei segnali video provenienti da un monitor utilizzando un ricevitore Software Defined Radio (SDR). TempestSDR presenta diversi vantagi:

- Costo minore e mobilità maggiore: viene utilizzato un semplice hardware commerciale non modificato, riducendo i costi e aumentando la mobilità rispetto alle soluzioni esistenti.
- Qualità aumentata: il software prevede un'ulteriore post-elaborazione che migliora il rapporto segnale-rumore.
- Requisiti minori: L'attaccante non ha bisogno di avere conoscenze preliminari sul monitor video bersaglio. Tutti i parametri, come la risoluzione e la frequenza di aggiornamento, sono stimati con l'aiuto del software.

In particolare, il software è composto da una libreria scritta in C, una raccolta di plug-in per vari front-end SDR e un'interfaccia grafica utente (GUI) basata su Java. È un'applicazione multipiattaforma, con tutte le librerie native precompilate e integrate in un singolo file jar Java[19].

Il set-up completo, prevede anche un hardware di supporto (come RTL-SDR, Airspy, SDRplay, HackRF) che riceve le radiazioni non intenzionali dal monitor. Inoltre, è possibile aggiungere un'antenna direzionale per aumentare la massima distanza di ricezione del segnale. Le figure 5.6 5.7 mostrano un esempio di set-up tramite TempestSDR[1].

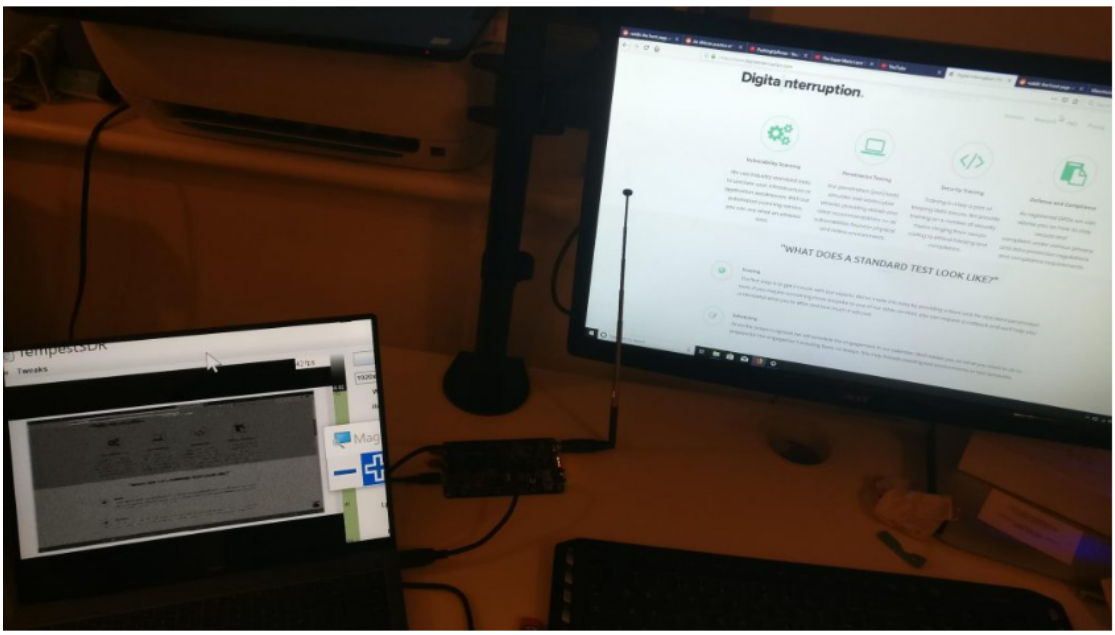

Figura 5.6: Set-up usando TempestSDR

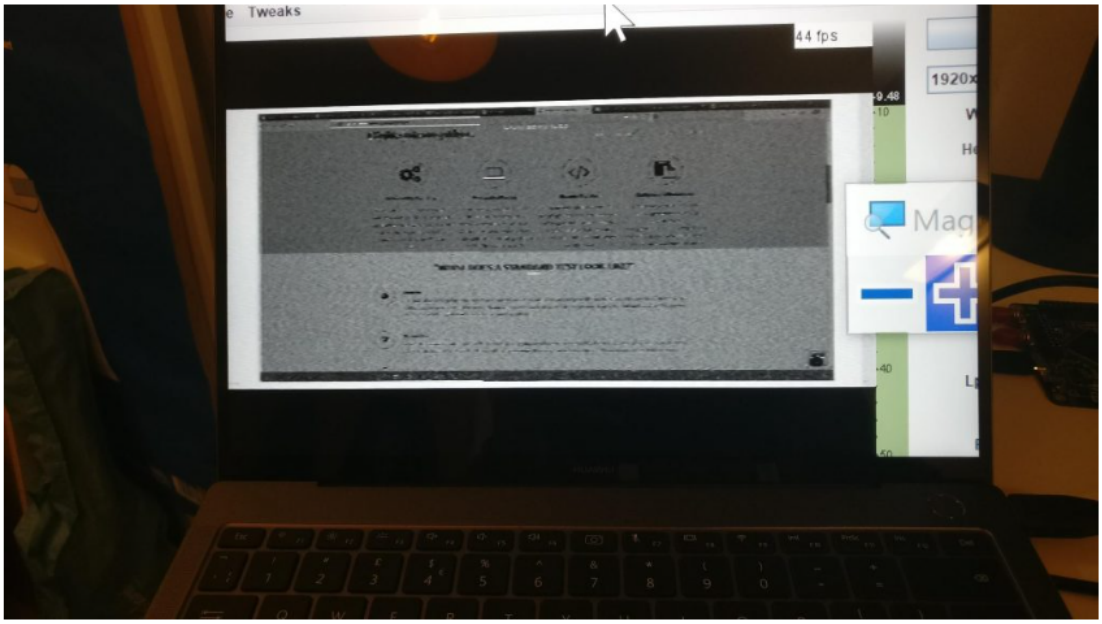

Figura 5.7: Immagine catturata dalle onde EM emanate dal monitor

6

Tempest for Eliza

A seguito di questa trattazione altamente teorica dei dispositivi TEMPEST, è utile dare un piccola dimostrazione pratica di come è facilmente possibile intercettare emissioni elettromagnetiche anche in casa.

In particolare, in questa sezione verrà mostrato l'esperimento dal nome "Tempest for eliza" che permette, attraverso l'uso di semplice apparecchiatura, di intercettare e trasformare le onde EM emesse da un monitor di un banale PC.

6.1 Descrizione dell'esperimento

L'esperimento prevede l'utilizzo di un pc a monitor CRT o LCD e una semplice radiolina AM. Nel pc viene installato il programma Tempest_for_eliza in C++ che permette al monitor del computer di emanare onde radio. In particolare, una volta eseguito il programma verranno riprodotte delle sequenze di immagini sul monitor dove ogni frame, tramite un'opportuna disposizione di pixel bianchi e neri alla giusta frequenza, emana un certo tipo di onda radio. La radiolina AM, impostata su una specifica frequenza, riuscirà a intercettare tali onde e a riprodurre in maniera semplificata il brano Für Elise di Beethoven.

L'obiettivo di tale esperimento è quello di mostrare, anche con apparecchiatura assolutamente semplice, poco costosa e facilmente reperibile, la veridicità della teoria TEMPEST: è possibile ricostruire informazioni gestite da un appa-

recchio elettronico intercettando le emissioni di energia (elettromagnetiche, in questo caso) provenienti dal dispositivo stesso.

L'esperimento in sè è molto semplice e non ha un effettiva utilità pratica, ma dimostra che un potenziale hacker con un equipaggiamento più sofisticato potrebbe facilmente rubare informazioni private senza fare molto: gli basta intercettare le naturali onde EM emesse dal dispositivo e decodificarle.

6.2 Strumentazione

Come anticipato, l'attrezzatura utilizzata in questo esperimento è molto semplice: un pc e una radio AM.

Nel caso di questo elaborato viene usato un PC di modello Notebook HP 340S G7 e una semplice radio portatile XHDATA D219.

Figura 6.1: Attrezzatura utilizzata in Tempest for Eliza

6.3 Fasi del progetto e realizzazione pratica

Il semplice programma tempest_for_eliza è fatto per Linux. In particolare, il sistema operativo utilizzato durante la realizzazione di questo esperimento è Ubuntu 22.04.1 LTS.

Successivamente, è stato installato il programma dal sito segnato in bibliografia come [23] e estratta la cartella corrispondente. In seguito, da terminale nella cartella estratta, sono stati usati i comandi *./configure* e *make* per la compilazione del software e la generazione dei file necessari alla costruzione del programma.

Per far funzionare tempest_for_eliza è necessario avere SDL installato. SDL sta per Simple DirectMedia Layer ed è una libreria multipiattaforma progettata per facilitare la scrittura di software multimediali, come giochi ed emulatori. Il pacchetto SDL è stato scaricato tramite il comando *sudo apt-get install libsdl1.2 -dev*.

Infine, per la corretta esecuzione del programma è necessario dare in input da terminale dei parametri specifici del proprio monitor. I valori necessari sono il pixel clock, l'altezza e la larghezza della risoluzione del proprio monitor e il numero totale di pixel. Infine, viene arbitrariamente scelta una frequenza da tramettere. In questo esperimento, è stato scelto 1000 kHz = 1 MHz di frequenza.

Nel caso studiato, i valori sono 173000000 per il pixel clock, 1920 per l'altezza, 1080 per la larghezza, 2576 come numero di pixel e 10000000 è la frequenza scelta. Questi parametri sono stati ottenuti tramite il comando *xrandr –verbose* da terminale.

Infine, sempre da terminale nella cartella estratta, viene eseguito il comando *./tempest_for_eliza 173000000 1920 1080 2576 10000000 songs/forelise* dove l'ultimo parametro specifica la canzone scelta. Infatti, nella cartella scaricata sono presenti diverse canzoni da provare. In questo caso, è stata scelta la canzone di default Für Elise.

Una volta eseguito il programma venivano mostrate a schermo intero sequenze di immagini di questo tipo:

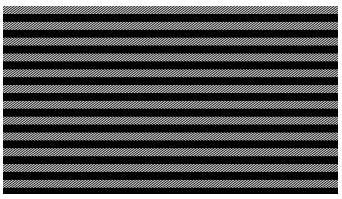

Figura 6.2: Schermo 1

Figura 6.3: Schermo 2

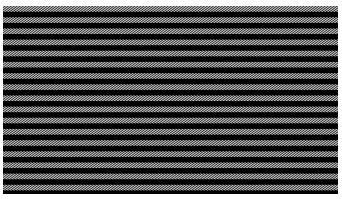

Figura 6.4: Schermo 3

Prima di far partire il programma, è stata accesa radio, messa in modalità AM e alzata l'antenna.

A questo punto, viene fatto eseguire il programma su PC e si avvicina la radio al monitor. La frequenza AM della radio va man mano modificata fino a quando la musica non si sente meglio. Nel caso di questo esperimento, la frequenza in cui la musica si sentiva meglio è tra i 600 e i 650 kHz.

Figura 6.5: Set up finale di Tempest for Eliza

6.4 Discussione ed analisi dei risultati

L'esperimento è stato un successo: la radio è riuscita a captare e trasformare le onde radio emesse dal monitor in musica.

Nonostante la semplicità dell'esperimento, vi sono alcune difficoltà da segnalare:

1. Installazione e configurazione del software: La difficoltà principale dell'esperimento è stata quella di capire quale software installare e come configurarlo. In particolare, data l'età dell'esperimento (2001) esso è stato

inizialmente programmato per computer a monitor CRT e non LCD. Sono state provate diverse alternative ma nessuna di queste funzionava, l'unica funzionante è stata trovata nella fonte di numero [23] in bibliografia. Le istruzioni nel sito sono poco chiare e sbrigative, soprattutto in merito all'installazione di SDL e di quale versione usare (1.2).

2. Posizione della radio: La radiolina AM non sente la musica in qualsiasi posizione la si metta. Anche in questo caso le indicazioni sono assenti e l'unico modo per scoprire la posizione giusta è quella di andare a tentativi. La locazione corretta è stata trovata appena davanti al monitor in basso a dx appena sopra la tastiera. Un altra posizione in cui la radio dava buoni risultati in termini di qualità audio della musica è direttamente dietro al monitor. Aumentando la distanza dal monitor la musica si affievolisce sempre di più. La posizione dell'antenna risulta irrilevante.

   In altre locazioni la radio emette solo rumore che sovrasta la debole musica.

3. Frequenza AM della radio: Anche per quanto riguarda la giusta frequenza AM della radio l'unica maniera è andare a tentativi spostando la manopola lentamente fino a sentire la musica. La frequenza trovata è tra i 600 kHz e i 650 kHz. In altre frequenze si sente solo rumore.

4. Rumore: Il segnale acustico si sente ma è fortemente circondato da rumore prodotto dalla radio. La posizione e la frequenza di ricezione della radio sono stati scelti per minimizzare tale rumore senza però eliminarlo. Anche nella condizione posizione-frequenza "migliore" il rumore è comunque presente e fastidioso.

Probabilmente une delle cause principali di questi problemi riscontrati risiede negli hardware non sofisticati utilizzati.

E' interessante notare che in alcune frequenze/posizioni della radio, essa intercettava anche segnali non target come il cambio immagine del monitor, la comparsa di lettere sul monitor a seguito di un click sulla tastiera e persino la pulsazione del cursore di testo quando non si sta scrivendo. In questi casi, però, al posto di emanare musica la radio emetteva un suono sordo simile a un colpo.

6.5 Conclusioni

Questo semplice esperimento soddisfa pienamente il suo obiettivo. Viene mostrato, infatti, che le onde elettromagnetiche del monitor possono essere facilmente captate, decodificate e trasformate in musica. Più in particolare, Tempest for Eliza conferma la teoria TEMPEST. Questo simpatico esperimento prova che dispositivi non protetti non sono per niente al sicuro da furti di informazioni. Infatti, se un eventuale hacker riuscisse a stabilire una relazione

tra le note emesse dalla radio e l'immagine mostrata a schermo allora sarebbe benissimo in grado di sapere quale frame è proiettato sul monitor semplicemente ascoltando le note prodotte dalla radiolina. Con un'attrezzatura abbastanza sofisticata, questo è possibile anche a distanza di decine di metri e l'hacker saprebbe (a questa distanza) cosa viene proiettato sul monitor.

7 Conclusioni

La protezione delle informazioni sensibili dalle intercettazioni elettromagnetiche rappresenta una sfida cruciale nell'attuale panorama tecnologico e di sicurezza. In questa tesi, è stato possibile esplorare fino a fondo le origini, l'evoluzione e i principi tecnici fondamentali di questa disciplina evidenziando come le emissioni di energia compromettenti di qualsiasi apparecchio elettronico possano rappresentare una minaccia importante non solo per i sistemi di comunicazione militari e governativi, ma anche per semplici infrastrutture civili e aziendali.

In questo documento, sono state presentate le principali differenze tra strategie offensive e difensive degli standard TEMPEST ovvero le tecniche di intercettazione e di schermatura delle emissioni compromettenti. Dunque, si tratta di due aspetti della stessa medaglia: da un lato, i "ladri" cercano di utilizzare le vulnerabilità elettromagnetiche a loro vantaggio, ottenendo illegalmente informazioni sensibili, mentre dall'altro, ingegneri e tecnici si impegnano a sviluppare metodologie sempre più raffinate per prevenire tali situazioni di intercettazione attraverso l'uso di schermature, filtri e pratiche di progettazione avanzate.

Per fortuna, gli standard e le normative che si sono susseguite negli anni dimostrano che i dispositivi TEMPEST sono fortemente regolamentati. Inoltre, le tecnologie per la protezione da queste minacce sono sempre più sviluppate: la combinazione di schermature, filtraggi e circuiti ben progettati riesce ad attenuare fortemente l'intensità delle emissioni di energia compromettenti. Questo assicura un livello di protezione adeguato, ma al contempo impone sfide

significative in termini di progettazione e implementazione.

Purtroppo però, anche le tecnologie di attacco sono sempre in crescita. In particolare, si è appurato che eseguire un attacco TEMPEST non è affatto complicato e costoso. Con un'antenna, un ricevitore e un decodificatore è facilmente implementabile un buon sistema di furto che sfrutti le vulnerabilità elettromagnetiche dei dispositivi e che rubi informazioni sensibili anche a distanza di centinaia di metri, in totale sicurezza. La situazione è maggiormente aggravata dal fatto che non esiste alcun dispositivi per l'elaborazione di informazioni che non emetta le cosiddette "emanazioni compromettenti". Computer, radio e persino stampanti possono essere soggetti a questi tipi di attacchi. E non si parla solo di interi apparecchi, ma anche di singole componenti come monitor, tastiere e mouse.

La minaccia per la sicurezza e la privacy è parecchio grave ma, con una giusta prevenzione è possibile diminuire di molto le probabilità di essere elettromagneticamente spiati.

In conclusione, i dispositivi TEMPEST sono un elemento fondamentale nel campo della sicurezza elettromagnetiche delle informazioni nel mondo moderno, richiedendo continui aggiornamenti tecnologici e adattamenti normativi per far fronte a nuove minacce. Inoltre, le tecnologie TEMPEST dimostrano che nessun dispositivo è veramente sicuro: è necessario prestare attenzione a ogni singola emanazione dei dispositivi che sia acustica, ottica o elettromagnetica. Ogni emissione di energia è una possibile fuga di informazioni e l'unica via d'uscita è un'attenta prevenzione a 360 gradi.

Bibliografia

[1] In: *TempestSDR: An SDR tool for Eavesdropping on Computer Screens via Unintentionally Radiated RF*. 2017. URL: https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/.

[2] In: *Schermatura Elettromagnetica*. URL: https://it.wikipedia.org/wiki/Schermatura_elettromagnetica.

[3] In: *Standard di Schermatura*. URL: https://www.interelectronix.com/it/standard-di-schermatura.html.

[4] In: *Insertion Loss*. URL: https://it.wikipedia.org/wiki/Insertion_loss.

[5] In: *Van Eck phreaking*. URL: https://en.wikipedia.org/wiki/Van_Eck_phreaking.

[6] Sapnesh Sahu Anindya Auddy. «TEMPEST: Magnitude of threat and mitigation techniques». In: *2008 10th International Conference on Electromagnetic Interference Compatibility*. 2008.

[7] Fatih BULUT et al. «Electromagnetic shielding behavior of different metallic wire-meshes and thin metal plate». In: *2017 IV International Electromagnetic Compatibility Conference (EMC Turkiye)*. 2017.

[8] «Che cosa sono le informazioni sensibili?» In: *Tipi di informazioni sensibili - una guida completa.* URL: https://www.sealpath.com/it/blog/guida-ai-tipi-di-informazioni-sensibili/.

[9] Dong-Hoon Choi, Taesik Nam Euibum Lee e Jong-Gwan Yook. «Recent Trends in Image Information Recovery Using Leaked Electromagnetic Wave from Electronic Equipment». In: *IEEE Electromagnetic Compatibility Magazine*. 2022.

[10] Thomas Claburn. «Computer Keyboards Betray Users' Keystrokes To Radio Eavesdroppers». In: *Vulnerabilities and Threats*. 2008. URL: https://www.darkreading.com/vulnerabilities-threats/computer-keyboards-betray-users-keystrokes-to-radio-eavesdroppers.

[11] Wim van Eck. «Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?» In: *On the electromagfields generated by video display units. Proc. symp. EMC.* 1985.

[12] Markus G. Kuhn. «Compromising emanations: eavesdropping risks of computer displays». In: *Technical Report, Number 577*. 2003.

[13] MARYLAND 20755 NATIONAL SECURITY AGENCY FORT GEORGE G. MEADE. «Tempest Fundamentals». In: *NACSIM 5000*. 1982.

[14] NSA. «The story of the discovery of various compromising radiations from communications and Comsec equipment.» In: *TEMPEST: A Signal Problem*. 2007.

[15] Margaret Rouse. «Techopedia Explains Impulsive Emanations». In: *Impulsive Emanations*. URL: https://www.techopedia.com/definition/25918/impulsive-emanations.

[16] Margaret Rouse. «Techopedia Explains Modulated Spurious Signal». In: *Modulated Spurious Signal*. URL: https://www.techopedia.com/definition/25917/modulated-spurious-signal.

[17] Margaret Rouse. «Techopedia Explains RED Baseband Signal». In: *RED Baseband Signal*. URL: https://www.techopedia.com/definition/25916/red-baseband-signal.

[18] Servilio Sebastiani. «Characterization to a TEMPEST testing laboratory and methodology for control to compromising emanation». In: *1998 IEEE EMC Symposium. International Symposium on Electromagnetic Compatibility. Symposium Record (Cat. No.98CH36253)*. 1998.

[19] HANDSON SECURITY. «TempestSDR: An SDR tool for Eavesdropping on Computer Screens via Unintentionally Radiated RF». In: *TempestSDR*. 2019. URL: https://s34s0n.github.io/2019/07/10/TempestSDR/.

[20] «Storia di codename: TEMPEST». In: *TEMPEST-Storia di codename: TEMPEST*. URL: https://www.interelectronix.com/it/storia-di-codename-tempest.html.

[21] «TEMPEST Timeline». In: *CRYPTOME*. 2002. URL: https://cryptome.org/tempest-time.htm.

[22] «TEMPEST: The Invisible Threat to Information Security». In: *TEMPEST explained*. 2023. URL: https://isecjobs.com/insights/tempest-explained/#how-tempest-works.

[23] Erik Thiele. In: *Tempest for Eliza*. 2001. URL: http://www.erikyyy.de/tempest/.

[24] Kai Yao et al. «Active Countermeasure using EMI Honeypot against TEMPEST Eavesdropping in High-Speed Signalling». In: *2018 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*. 2018.