

# Tesi Magistrale

## Analisi dei Covert Channel applicati al protocollo ICMP

*Francesco Santini*

*Marco Mecarelli*

Università degli Studi di Perugia

26 febbraio 2025

# Indice

<b>1</b>	<b>Introduzione ai Covert Channel</b>	<b>5</b>
1.1	Cos'è un Covert Channel? . . . . .	5
1.2	Principali categorie di Covert Channel . . . . .	5
1.2.1	Covert Channel Timing (temporizzazione) . . . . .	6
1.2.2	Covert Channel Storage (Archiviazione) . . . . .	6
1.2.3	Covert Channel Behavioral (Comportamentali) . . . . .	6
1.3	Struttura/Caratteristiche dei Covert Channel . . . . .	6
1.4	Vulnerabilità Utilizzate . . . . .	9
1.5	Applicazione dei Covert Channel . . . . .	10
1.6	Covert Channel Attacks . . . . .	11
1.7	Protezione contro i Covert Channel . . . . .	14
1.8	Strategie di mitigazione . . . . .	15
1.9	Aree di ricerca sui covert Channel . . . . .	17
<b>2</b>	<b>Introduzione al protocollo ICMP</b>	<b>18</b>
2.1	Characteristics of ICMP . . . . .	18
2.2	Functions of ICMP . . . . .	19
2.3	ICMP in Networking Tools . . . . .	21
2.4	Security Risks of ICMP . . . . .	21
2.5	How ICMP is Used in Networking . . . . .	22
2.6	ICMP Security Risks and Mitigations . . . . .	23
2.7	Differences Between ICMP, TCP, and UDP . . . . .	24
2.8	Attacks on ICMP . . . . .	24
2.9	Security Best Practices for ICMP . . . . .	27
<b>3</b>	<b>Covert Channel Attacks on ICMP</b>	<b>29</b>
3.1	How ICMP Covert Channels Work . . . . .	29
3.1.1	ICMP Tunneling . . . . .	29
3.1.2	ICMP Data Exfiltration . . . . .	30
3.1.3	ICMP-Based Botnet Command & Control (C2) . . . . .	30
3.2	How to Detect and Mitigate ICMP Covert Channels . . . . .	30
3.2.1	Detection Techniques . . . . .	30
3.2.2	Prevention and Mitigation Strategies . . . . .	31
3.3	Real-World Example of an ICMP Covert Channel Attack . . . . .	31
3.4	Summary: How to Secure Against ICMP Covert Channels . . . . .	32
3.5	Covert Channel Attacks on ICMP: Mitigation and Detection Strategies . . . . .	32
3.6	What Are ICMP Covert Channel Attacks? . . . . .	32
3.7	Detection Strategies for ICMP Covert Channels . . . . .	33

3.7.1	Network Traffic Monitoring . . . . .	33
3.7.2	Deep Packet Inspection (DPI) . . . . .	33
3.7.3	Intrusion Detection and Prevention Systems (IDS/IPS)	33
3.7.4	Anomaly-Based Detection . . . . .	33
3.8	Mitigation Strategies for ICMP Covert Channels . . . . .	34
3.8.1	Restrict ICMP Traffic . . . . .	34
3.8.2	Use Encryption to Prevent Data Leakage . . . . .	34
3.8.3	Block ICMP on External Interfaces . . . . .	34
3.8.4	Endpoint Security & Antivirus . . . . .	34
3.8.5	Implement ICMP Proxy Filtering . . . . .	34
3.9	Summary: Detection & Mitigation Techniques . . . . .	35

## Listings

python . . . . .	31
shell . . . . .	33

## Elenco delle figure

# 1 Introduzione ai Covert Channel

## 1.1 Cos'è un Covert Channel?

Un **Covert Channel** è un attacco che permette (in ambienti ritenuti sicuri) la capacità di comunicare/trasferire dati, in maniera non autorizzata e non voluta, fra processi/entità comunicanti spesso senza essere rivelati e spesso evitando (se non violando) le normali politiche di sicurezza.

Solitamente operano al di fuori dei soliti meccanismi di comunicazioni. Quindi non usando i normali protocolli/canali di comunicazione (es network sockets, emails) non generano segnali di un uso improprio del sistema. Ciò li rende difficili da rilevare usando i tipici strumenti di monitoraggio. Inoltre questi canali sfruttano le vulnerabilità o comportamenti non previsti nei sistemi.

In un Covert Channel, qualsiasi risorsa condivisa può essere utilizzata come canale nascosto ed è per questo che possono esistere in qualunque sistema (che abbia delle risorse condivise). Lo sfruttamento di queste risorse porta alla fuoriuscita/scambio di dati.

L'attacco è un problema siccome sono estremamente difficili da identificare e controllare. La loro esistenza spesso rimane non notata dagli amministratori (di sistema) siccome si nascondono all'interno dei normali processi del sistema. Sono inoltre un problema significativo in tutti quegli ambienti altamente sicuri (es ambienti militari, governativi, . . . ) dove una fuoriuscita di informazioni può avere conseguenze gravi.

## 1.2 Principali categorie di Covert Channel

Le principali categorie di canali nascosti sono:

- Covert Channel Timing (Temporizzazione): coinvolgono la scrittura di dati a un'area di memoria condivisa in cui entrambi i processi possono accedere

**Esempio 1.1.** *Modificare i permessi dei file o i metadati per codificare informazioni. Oppure modificare variabili condivise o buffer*

- Covert Channel Storage (Archiviazione): manipolano la temporalizzazione o l'ordine di eventi per codificare informazioni.

**Esempio 1.2.** *Variare deliberatamente il tempo fra delle azioni (es trasmissione di network packet, patter di uso della CPU) oppure codificando dati nella temporalizzazione dell'esecuzione dei processi o delay di risposta.*

- Covert Channel Behavioral (Comportamentali)

### 1.2.1 Covert Channel Timing (temporizzazione)

I canali nascosti di temporizzazione sono metodi di comunicazione che permettono ad un osservatore (umano o processo) di acquisire informazioni attraverso il cambiamento nel tempo di risposta di una risorsa. Essenzialmente qualsiasi metodo che utilizza un orologio o una misurazione del tempo per segnalare il valore inviato sul canale. Esempio

### 1.2.2 Covert Channel Storage (Archiviazione)

Nei canali nascosti di archiviazione un processo scrive su una risorsa condivisa, mentre un altro processo legge da essa. I canali di archiviazione possono essere utilizzati tra processi all'interno di un singolo computer o tra più computer in una rete.

I veicoli dell'attacco sono tutte quelle risorse che consentono la scrittura, diretta o indiretta, di una risorsa da parte di un processo e la sua lettura, diretta o indiretta, da parte di un altro.

**Esempio 1.3.** *Un esempio di canale di archiviazione è la condivisione di un file. Supponiamo che l'utente A con privilegi di autorizzazione elevati voglia trasmettere in segreto, dati riservati all'utente B con un livello di sicurezza inferiore. Per farlo, utilizzerà un file word apparentemente contenente informazioni non classificate, dove invece occulterà l'informazione riservata.*

### 1.2.3 Covert Channel Behavioral (Comportamentali)

I canali nascosti comportamentali operano trasmettendo dati in base all'assegnazione di diversi eventi di processi, sistemi e applicazioni, generalmente suddividendo e trasmettendo i dati in pacchetti più piccoli.

## 1.3 Struttura/Caratteristiche dei Covert Channel

Tipicamente è costituito da due principali componenti:

- **Mittente** (Covert Transmitter): è l'entità che codifica e trasmette le informazioni nascoste usando una risorsa di sistema condivisa.

- **Destinatario** (Covert Listener): è l'entità che rileva e decifra l'informazione segreta dalla risorsa condivisa.

### Come funzionano i Covert Channel?

Il mittente inserisce informazioni segrete in un componente del sistema che è osservabile da un destinatario. Il destinatario decifra i dati trasmessi di nascosto monitorando i cambiamenti nel comportamento del sistema.

Le informazioni vengono inserite sfruttando gli effetti collaterali delle normali operazioni del sistema senza un esplicito intento di comunicare.

Un Covert Channel quindi opera cifrando dati nascosti nei comportamenti del sistema che i controlli di sicurezza tipicamente non monitorano così da permettere la comunicazione segreta fra due entità.

### Caratteristiche Chiave dei covert Channel

Le principali caratteristiche di un Covert Channel sono:

- **Stealthiness** (furtività):

si devono poter aggirare i controlli in maniera nascosta

- **Bandwidth** (capacità di trasmissione):

la capacità di trasmissione dei dati che è generalmente bassa in termini di dati/tempo (throughput). Un eccessivo carico di informazioni, potrebbe rendere anomalo il funzionamento di quelle risorse o delle normali strutture dati. Nei canali nascosti generalmente il throughput è inversamente correlato alla segretezza di un canale.

Più dati un canale trasmette in un determinato periodo di tempo, maggiore è il rischio che il canale venga scoperto

- **Indistinguishability** (Indistinguibilità):

di solito si sfruttano servizi e/o risorse già presenti e quindi non sospette.

Uno dei maggiori problemi nell'implementazione di un canale nascosto è il "rumore" (es. sfruttando eccessivamente le risorse alterando e/o danneggiando il corretto funzionamento delle stesse) che potrebbe attirare l'attenzione da parte degli amministratori di sistema. La necessità è quella di riuscire a trasmettere attraverso un canale nascosto mantenendo conforme e inalterato il funzionamento della risorsa utilizzata così da rendersi "indistinguibili" dalla risorsa autorizzata e quindi invisibili ai sistemi di monitoraggio.

Ulteriori caratteristiche sono:



- **Unintended Use of Resources:** Covert channels exploit system resources (e.g. shared memory, CPU usage, or file attributes) in ways that were not intended for communication.

- **Hidden Communication:** They are designed to avoid detection, often leveraging legitimate system operations to mask the transmission of data.

- **Violation of Security Policies:** They allow unauthorized exchange of information, potentially breaching confidentiality, integrity, or availability requirements.

- **Hidden Communication Medium:**

The channel is embedded within legitimate system operations, such as CPU load, memory access, network traffic, or file system metadata. Examples: CPU cache, TCP/IP headers, power consumption, packet timing.

- **Encoding Mechanism:**

The sender manipulates a shared system resource to encode data. Common techniques:

- **Timing-Based Encoding:** Using time intervals (e.g., delays between network packets).
- **Storage-Based Encoding:** Modifying file attributes, memory bits, or cache states.
- **Protocol Abuse:** Altering TCP flags, sequence numbers, or unused bits in packet headers.

- **Transmission Mechanism:**

The sender continuously alters system behavior to transmit bits of information. This can be done by introducing delays, changing CPU load, or modifying memory states in a controlled manner.

- **Decoding Mechanism:**

The receiver monitors the shared resource to detect and reconstruct the transmitted data. Example: Measuring execution time variations to infer secret data.

- **Synchronization and Error Correction:**

The sender and receiver must synchronize (e.g., using pre-agreed timing signals). Error detection mechanisms (such as parity bits or checksums) ensure accurate data retrieval.

**Esempio 1.4.** *Esempio di un Covert channel in una rete*

- *Sender: Modifies the Time-to-Live (TTL) field in IP packets to represent*

*binary data (e.g.,  $TTL=64 \rightarrow \text{bit } 1$ ,  $TTL=128 \rightarrow \text{bit } 0$ ).*

- *Receiver: Observes incoming packet TTL values to reconstruct the hidden message.*

## 1.4 Vulnerabilità Utilizzate

I Covert Channel sfruttano le vulnerabilità nel design del sistema, nelle politiche di sicurezza e nei protocolli di comunicazione per trasferire informazioni segretamente. Sfruttando queste vulnerabilità, gli attaccanti possono stabilire Covert Channel che evitano il controllo degli standard sicurezza, permettendo esfiltrazione non autorizzata di dati o comunicazione fra processi interni (inter-process communication).

La loro mitigazione richiede controllo degli accessi, randomizzazione dei tempi, iniezione di rumore e una sicurezza hardware migliore.

### Principali vulnerabilità usate dai covert Channel

#### • Shared Resource Exploitation

- CPU Scheduling: l'attaccante può modulare l'uso della CPU per diffondere informazioni.
- Cache Memory: gli attacchi side-channel alla cache sfruttano le differenze nei tempi di accesso per dedurre i dati.
- File System Access: i processi possono dedurre informazioni in base ai lock dei file, timestamp o sull'attività del disco

#### • Timing-Based Vulnerabilities

- **Response Time Variability:** l'attaccante misura i tempi di risposta del sistema per estrarre segreti.
- **Instruction Execution Delays:** le differenze del tempo di esecuzione tra le operazioni privilegiate e non possono causare la fuoriuscita di dati.

#### • Timing-Based Vulnerabilities

- **Packet Timing:** le informazioni possono essere codificate negli intervalli durante la trasmissione dei pacchetti

- **Header Manipulation:** campi come TTL, sequenza dei numeri o bit non utilizzati possono essere utilizzati per codificare i dati
- **Traffic Patterns:** le variazioni nel flusso del traffico (es burst size) si possono comportare come un Covert Channel.
- **Memory and CPU State Manipulation**
  - Branch Prediction and Speculative Execution: Exploited in attacks like Spectre and Meltdown.
  - Power Consumption Analysis: Side channels can reveal cryptographic keys
- **Operating System and Virtualization Flaws**
  - Inter-Process Communication (IPC) Abuse: Processes can infer data through shared memory or message passing.
  - Hypervisor Weaknesses: Virtual machines can leak information across guest instances.
- **Hardware Vulnerabilities**
  - Electromagnetic Emissions: Sensitive data can be leaked via EM signals (TEMPEST attacks).
  - Acoustic Side-Channels: Keyboard sounds, fan speed variations, or power supply noise can be analyzed.

## 1.5 Applicazione dei Covert Channel

I Covert Channel sono spesso applicati in:

- Malware and Espionage: usati per esfiltrare dati sensibili.
- Security Testing: identificare e mitigare i Covert Channel è una parte fondamentale nel stabilire la sicurezza del sistema.
- Ricerca: espolare i Covert Channel aiuta a capire potenziali vulnerabilità in sistemi complessi.

## 1.6 Covert Channel Attacks

Gli attacchi tramite Covert Channel sfruttano vulnerabilità nel design del sistema, nelle risorse condivise e nelle politiche di sicurezza per trasmettere segretamente dati fra processi o sistemi aggirando i tradizionali controlli di sicurezza. Questi attacchi sono spesso usati per l'esfiltrazione dei dati, privilege escalation o comunicazioni silenziose tra delle componenti malware.

### Types of Covert Channel Attacks

1. **Storage-Based Covert Channels:** These attacks manipulate shared system resources to store and retrieve hidden information.

#### **Esempio 1.5.** 1

*File Attribute Manipulation:* Malware alters file metadata (e.g., timestamps, permissions) to encode messages.

*Shared Memory Exploitation:* Processes communicate by modifying shared memory regions.

*Disk Usage Signaling:* One process writes or deletes data, and another process detects changes.

*TCP/IP Header Fields:* Attackers encode data in unused or optional fields of network packets (e.g., IP ID, sequence numbers, or TTL values).

2. **Timing-Based Covert Channels:** These attacks manipulate system timing or performance to transmit hidden information.

#### **Esempio 1.6.**

*CPU Load Fluctuation:* Malware alters CPU usage patterns, which another process measures to decode information.

*Network Packet Timing:* The sender transmits packets at specific time intervals to encode binary data.

*Cache-Based Attacks:* Attackers use cache access times (e.g., Flush+Reload, Prime+Probe) to leak secrets

*Power Consumption Analysis:* Sensitive data is extracted by analyzing power usage variations (used in side-channel cryptographic attacks).

### Notable Covert Channel Attacks

#### Real-World Examples of Covert Channel Attacks

- **Malware-Based Attacks:**  
Duqu 2.0 (2015): Used covert TCP/IP channels to exfiltrate data while

Attack Name	Type	Description
Spectre and Meltdown	Timing (Cache)	Exploit speculative execution to leak memory contents
Flush+Reload	Timing (Cache)	Attacker flushes shared memory and reloads it to observe access patterns.
Prime+Probe	Timing (Cache)	Attacker fills cache and monitors eviction patterns to infer secret data.
TCP Covert Channel	Storage (Network)	Encodes data in TCP packet fields (e.g., sequence numbers, flags).
File Lock Covert Channel	Storage (Filesystem)	Uses file locking/unlocking as a signaling mechanism.
Packet Timing Attack	Timing (Network)	Varies packet transmission timing to send hidden messages.
Keystroke Timing Attack	Timing (Human Interaction)	Infers typed keys based on timing variations between keystrokes.

avoiding detection. DNS Tunneling Attacks: Malware hides data inside DNS queries (e.g., C2 communication for botnets).

- Cloud & Virtualization-Based Covert Channels:  
Hypervisor Covert Channels: Virtual machines (VMs) on the same physical host leak data via shared CPU cache or memory. Cloud Timing Attacks: Cloud tenants use execution timing differences to infer co-resident VM activities.

## Mitigation Strategies

Gli attacchi tramite Covert Channel sfruttano le debolezze, del timing del sistema, delle risorse condivise e dei protocolli di rete, per trasmettere dati nascosti. Pongono una seria minaccia nella comunicazione fra malware, esfiltrazione dei dati e il cyber-spionaggio. Difese efficaci implicano l'isolamento delle risorse, iniezione di rumore e rilevamento delle anomalie così da disturbare questi attacchi. **System-Level Defenses**

- Enforce strong access control (MAC, RBAC) to prevent unauthorized process interactions.
- Use mandatory data flow control models (Bell-LaPadula, Biba) to prevent information leaks.
- Disable unnecessary shared resources (e.g., inter-process communication, shared memory).

## Network Defenses

- Deploy deep packet inspection (DPI) and anomaly detection to identify hidden data in network traffic.
- Enforce network segmentation to limit unauthorized data flows.

## Hardware & OS Defenses

- Randomize execution times and inject noise into system responses (to disrupt timing-based attacks).
- Implement constant-time cryptographic operations to prevent timing side channels.
- Flush and partition CPU caches to prevent cross-process cache attacks.

## 1.7 Protezione contro i Covert Channel

Il loro rilevamento e la loro mitigazione richiede un rigoroso monitoraggio, l'isolamento delle risorse e tecniche per introdurre rumore. I Covert channel sfruttano le vulnerabilità del sistema per trasmettere segretamente dei dati. Proteggersi da loro, richiede una combinazione di rinforzo delle politiche, gestione delle risorse e tecniche di monitoraggio. Mitigare i Covert channel richiede una sicurezza multi livello fra hardware, OS, applicazioni e reti. Siccome la completa eliminazione è difficile, strategie di rilevazione e minimizzazione sono essenziali (es randomizzazione, rigoroso controllo degli accessi delle risorse, rilevamento delle anomalie). Le effettive strategie per la mitigazione sono:

### System and Policy-Based Protections

1. **Strict Access Control Policies:**

Implement least privilege and mandatory access control (MAC) to restrict unauthorized communication between processes. Use sandboxing and compartmentalization to isolate processes.

2. **Information Flow Control:**

Enforce data flow policies to prevent high-security processes from leaking data to lower-security processes (Bell-LaPadula, Biba model).

3. **Process Separation and Isolation:**

Use virtualization and containerization to separate processes. Apply air-gapping for highly sensitive systems

### Timing and Resource Management Protections

- **Randomization Techniques**

Introduce noise in system responses (e.g., randomizing execution times, adding delays) to disrupt timing-based covert channels. Use cache randomization or flush techniques to prevent cache-based side-channel attacks.

- **Rate Limiting and Bandwidth Control**

Restrict CPU, memory, or network bandwidth to limit the capacity of a covert channel. Implement throttling mechanisms for shared resources.

## Network Security Protections

- **Packet Inspection and Filtering:**  
Use Deep Packet Inspection (DPI) to detect anomalous patterns in network traffic. Block or sanitize unused fields in protocols (e.g., TCP/IP headers).
- **Traffic Analysis and Anomaly Detection:**  
Employ AI-based monitoring to detect unusual communication patterns. Use intrusion detection systems (IDS) and log analysis to identify suspicious activities.

## Hardware and Software Security Enhancements

- **Secure Hardware Design**  
Implement constant-time cryptographic operations to prevent timing-based attacks. Use secure enclaves (e.g., Intel SGX, ARM TrustZone) to protect sensitive computations.
- **OS-Level Protections**  
Enforce memory isolation and disable shared memory where unnecessary. Implement secure scheduling algorithms to prevent process-based timing leaks.

## Covert Channel Auditing and Testing

- Regularly perform covert channel analysis in penetration tests.
- Use covert channel detection tools (e.g., network flow analysis, system behavior monitoring).

## 1.8 Strategie di mitigazione

### Strategie di Mitigazione

Controllo sugli Accessi: limitare i permessi per prevenire scambio di informazioni non autorizzato  
Monitoraggio del Traffico: analizzare i comportamenti del sistema per rilevare anomalie  
Aggiunta di Rumore (Noise Injection): introdurre casualità nei pattern temporali o di accesso alla memoria per rendere il prelevamento dei dati difficile. Strategie di mitigazione:

- **System Design:** Minimize shared resources and unnecessary communication paths.
- **Monitoring:** Detect unusual patterns in resource usage or timing.



- Access Controls: Restrict access to critical resources.
- Noise Introduction: Add random delays or variations to disrupt timing-based channels.

I Covert Channel possono passare attraverso sistemi operativi sicuri a richiedono misure speciali per poterli controllare; in particolare l'analisi dei Covert Channel è l'unico modo provato per poterli gestire. Al contrario, sistemi operativi sicuri possono facilmente identificare e/o prevenire l'uso improprio di canali legittimi.

## Identifying Covert Channels

PASS

## Eliminating Covert Channels

Le possibilità di un Covert Channel non possono essere eliminate sebbene possano essere significativamente ridotte da un design e analisi attenti. La rilevazione di un Covert Channel può essere resa maggiormente difficile usando caratteristiche del medium di comunicazione per il canale legittimo che non sono mai controllati o esaminati da utenti legittimi.

**Esempio 1.7.** *Un file può essere aperto e chiuso da un programma in modo specifico pattern temporale così che possa essere rilevato da un altro programma; lo schema potrà essere poi interpretato come una stringa di bit formando così un Covert Channel. Di conseguenza, siccome è improbabile che l'utente legittimo controlli i pattern relativi alla chiusura/apertura dei file; questo tipo di Covert Channel può rimanere non identificato per un lungo periodo.*

## Data hiding in OSI model

PASS

## DATA hiding in LAN environment by covert channels

PASS

## Data hiding in TCP/IP Protocols suite

PASS

### 1.9 Aree di ricerca sui covert Channel

One significant area of research involves the development of covert communication mechanisms in wireless environments. For instance, a study introduced a covert wireless unidirectional communication method that utilizes the beacon intervals of access points in IEEE 802.11 networks. This method, known as the ping-pong covert timing channel (PPCTC), aims to minimize the chances of detection while ensuring reliable data transmission, even in the presence of errors[1]. This innovation demonstrates the potential for covert channels to be effectively integrated into existing network protocols with minimal modifications.

Another critical aspect of covert channels is their detection. As covert communications become more advanced and harder to identify, researchers are exploring machine learning (ML) techniques to enhance detection capabilities. A review highlighted various types of covert channels and the effectiveness of different ML approaches in identifying these hidden threats. The study emphasized the need for ongoing research to improve detection methods, as traditional security measures often fail to recognize covert communications[2]. Additionally, the use of Internet of Things (IoT) protocols for data exfiltration has garnered attention. Research has shown that protocols like MQTT and AMQP are particularly effective for covert data transfers due to their design for low bandwidth and power consumption, making them suitable for IoT environments. A software tool developed for this purpose demonstrated how these protocols could be exploited for unauthorized data transfers, underscoring the need for robust detection mechanisms in IoT networks[3]. Furthermore, a long-term analysis of the Internet's susceptibility to covert channels revealed that the evolution of network protocols has influenced the effectiveness of information hiding techniques. This study suggested that continuous monitoring and quantification of covert channel capabilities should be integral to cybersecurity strategies[4]. Lastly, a specific threat analysis focused on using port scans as a cover for covert command and control channels. This research proposed a novel method for hiding information within TCP port scans and syslog messages, providing insights into potential indicators of compromise and mitigation strategies[5].

## 2 Introduzione al protocollo ICMP

ICMP (Internet Control Message Protocol) is a network layer protocol used for diagnostics, error reporting, and network troubleshooting in IP-based networks. It helps devices (such as routers and hosts) communicate about network issues, but it is not used for data transmission like TCP or UDP.

ICMP is essential for network diagnostics and error reporting but can be misused for attacks. Proper firewall rules and rate limiting help balance usability and security.

ICMP (Internet Control Message Protocol) is a network layer protocol used for sending error messages, diagnostics, and control information in IP-based networks. Unlike TCP or UDP, ICMP is not used for data transport but instead helps manage and troubleshoot network communication.

### 2.1 Characteristics of ICMP

- Operates at Layer 3 (Network Layer) in the OSI model.
- Works with IP to provide feedback about network issues.
- Stateless and Connectionless, meaning it does not establish a session.
- No Port Numbers, unlike TCP and UDP.
- Used for Network Troubleshooting (e.g., ping, traceroute).
- Supports IPv4 (ICMPv4) and IPv6 (ICMPv6) with enhanced features in ICMPv6.

Un messaggio ICMP è strutturato in questo modo. Each ICMP message consists of:

- Type - Identifies the message type (e.g., Echo Request, Destination Unreachable).
- Code - Provides additional details about the message type.
- Checksum - Ensures data integrity.
- Data - Optional, may contain part of the original IP packet that caused the error.

## ICMP Header Format

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
— Type — Code — Checksum —
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
— Additional Data (if required) —
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

## 2.2 Functions of ICMP

ICMP is primarily used for:

- Error Reporting: Informs the sender about network issues (e.g., destination unreachable, packet loss).
- Network Diagnostics: Helps in network troubleshooting using tools like ping and traceroute.
- Control Messaging: Manages network congestion and routing updates in some cases.

ICMP messages are categorized as error messages or informational messages, identified by their Type and Code values.

ICMP messages fall into two categories:

- Error Messages - Report problems in network communication.
- Informational Messages - Used for diagnostic and control purposes.

## Error Messages

Type	Code	Meaning
3	0-15	Destination Unreachable (e.g., no route to host, port unreachable)
4	0	Source Quench (deprecated, used to indicate congestion)
5	0-3	Redirect Message (suggesting a better route)
11	0-1	Time Exceeded (TTL expired, used in trace-route)
12	0-1	Parameter Problem (invalid IP header)

## Error Messages

Type	Code	Message Name	Description
3	0	Network Unreachable	No route to destination network.
3	1	Host Unreachable	No route to specific host.
3	3	Port Unreachable	Destination port is closed.
3	4	Fragmentation Needed	Packet needs fragmentation, but DF bit is set.
4	0	Source Quench (Deprecated)	Indicates network congestion.
5	0-3	Redirect Message	Suggests a better route for packets.
11	0	Time Exceeded	TTL expired before reaching the destination (used in traceroute).
12	0-1	Parameter Problem	Invalid IP header field.

### Informational Messages

Type	Code	Meaning
0	0	Echo Reply (response to ping)
8	0	Echo Request (used by ping command)
9	0	Router Advertisement (announces routers on a network)
10	0	Router Solicitation (asks routers for advertisements)

### Informational Messages

Type	Code	Message Name	Description
0	0	Echo Reply	Response to a ping request.
8	0	Echo Request	Used by ping to test connectivity.
9	0	Router Advertisement	Routers announce themselves to hosts.
10	0	Router Solicitation	Hosts request router advertisements.

## 2.3 ICMP in Networking Tools

ICMP is widely used in network diagnostic tools:

- ping - Sends ICMP Echo Request packets to test connectivity.
- traceroute - Uses ICMP Time Exceeded messages to map the path of packets.
- MTU Path Discovery - Uses ICMP Fragmentation Needed messages to optimize packet size.

## 2.4 Security Risks of ICMP

Although useful, ICMP can be abused for network reconnaissance and attacks, such as:

- Ping Flood (ICMP Flood) - Overwhelming a target with Echo Requests (DDoS attack).
- Smurf Attack - Spoofed ICMP requests amplify traffic against a victim.
- ICMP Tunneling - Covert channels using ICMP packets to bypass firewalls.
- Ping of Death - Sending oversized ICMP packets to crash systems (historical).

Mitigation Strategies:

- Limit or block unnecessary ICMP traffic on firewalls.
- Rate-limit ICMP requests to prevent floods.
- Allow only necessary ICMP messages (e.g., Echo Reply but not Redirect).

## 2.5 How ICMP is Used in Networking

### Network Diagnostics and Troubleshooting

#### 1) Ping Command (ICMP Echo Request & Echo Reply)

- Sends ICMP Echo Requests to a destination to check connectivity.
- If the host is reachable, it replies with an ICMP Echo Reply.

#### 2) Traceroute (tracert in Windows, traceroute in Linux/macOS)

- Uses ICMP Time Exceeded messages to track the path packets take through a network
- TTL (Time-To-Live) value is incremented to determine each router along the path.

#### 3) Path MTU Discovery (PMTUD)

- Uses ICMP Fragmentation Needed messages to find the optimal packet size for a network path.

## 2.6 ICMP Security Risks and Mitigations

ICMP is a crucial protocol for network diagnostics, error reporting, and communication control in both IPv4 and IPv6. However, it can be exploited for attacks, so security measures like firewall filtering, rate limiting, and anomaly detection should be implemented.

### ICMP-Based Attacks

1. Ping Flood (ICMP Flood Attack)
  - Attacker overwhelms a target with excessive ICMP Echo Requests, consuming bandwidth.
  - Mitigation: Rate-limit ICMP requests at the firewall.
2. Smurf Attack
  - Attacker sends ICMP Echo Requests with a spoofed source IP, causing multiple responses to flood a victim
  - Mitigation: Block ICMP requests to broadcast addresses
3. ICMP Tunneling (Covert Channel Attack)
  - Data is embedded inside ICMP packets to evade firewalls and exfiltrate information
  - Mitigation: Inspect and filter ICMP traffic using Deep Packet Inspection (DPI)
4. Ping of Death (Historical)
  - Oversized ICMP packets cause buffer overflow crashes on vulnerable systems.
  - Mitigation: Modern systems reject oversized ICMP packets.
5. ICMP Redirect Attack
  - Rogue ICMP Redirect messages reroute traffic to a malicious gateway.
  - Mitigation: Disable ICMP Redirect on secure systems



## Security Best Practices for ICMP

Block unnecessary ICMP types on firewalls (e.g., Redirect, Timestamp, Source Quench).

Rate-limit ICMP requests to prevent flooding.

Allow only essential ICMP messages (e.g., Echo Reply, Destination Unreachable).

Use Intrusion Detection Systems (IDS) to monitor suspicious ICMP activity.

## 2.7 Differences Between ICMP, TCP, and UDP

Feature	ICMP	TCP	UDP
Purpose	Error reporting and diagnostics	Reliable data transfer	Fast, connectionless data transfer
Connection-Oriented?	No	Yes	No
Port Numbers?	No	Yes	Yes
Reliability	No	Yes (Acknowledgments)	No
Used By	Ping, Traceroute, PMTUD	HTTP, FTP, Email	DNS, VoIP, Streaming

## 2.8 Attacks on ICMP

ICMP is a crucial protocol for network diagnostics and error reporting, but it can also be exploited for various cyberattacks. Attackers use ICMP for DDoS attacks, reconnaissance, data exfiltration, and covert channels.

### ICMP-Based Denial-of-Service (DoS/DDoS) Attacks

#### ICMP Flood (Ping Flood)

- **Attack:**  
The attacker sends a large number of ICMP Echo Requests (ping requests) to a target system. If the system responds with ICMP Echo Replies, it consumes processing power and bandwidth. If multiple machines attack at once, it's called a Distributed DoS (DDoS) ICMP Flood.
- **Mitigation:**  
Rate-limit ICMP traffic on firewalls and routers. Disable ICMP Echo

Requests from external networks if not needed. Use Intrusion Detection Systems (IDS) to monitor excessive ping requests.

### **Smurf Attack**

- **Attack:**  
The attacker sends ICMP Echo Requests with a spoofed source IP (the victim's IP). The requests are sent to a broadcast address, causing all hosts on the network to reply. The victim is overwhelmed with ICMP Echo Replies, leading to a DoS condition.
- **Mitigation:**  
Disable ICMP broadcast requests on routers (no ip directed-broadcast)  
Implement ingress filtering to block packets with spoofed source addresses. Use firewall rules to block unnecessary ICMP traffic.

### **Ping of Death (Historical Attack)**

- **Attack:** The attacker sends an oversized ICMP packet (≥ 65,535 bytes). Older operating systems could crash, freeze, or reboot when handling such packets.
- **Mitigation:** Modern systems reject oversized packets. Apply system updates and patches to prevent this vulnerability.

### **ICMP Unreachable Flood**

- **Attack:**  
The attacker sends a massive number of ICMP Destination Unreachable messages. Can overwhelm network devices and cause denial of service.
- **Mitigation:**  
Configure rate limits for ICMP error messages. Implement firewall rules to drop excessive ICMP traffic

## **ICMP-Based Reconnaissance Attacks**

### **ICMP Ping Sweep**

- **Attack:**  
The attacker sends ICMP Echo Requests to multiple hosts on a network. Based on the ICMP Echo Replies, the attacker identifies live hosts for further attacks.

- Mitigation:  
Block ICMP Echo Requests from external sources. Use Intrusion Prevention Systems (IPS) to detect and block suspicious scanning activity.

### **ICMP Timestamp Attack**

- Attack:  
ICMP Timestamp Requests (Type 13) allow attackers to determine system uptime. This information helps attackers find vulnerable or recently rebooted systems.
- Mitigation:  
Disable ICMP Timestamp Requests on firewalls and routers. Use time synchronization protocols (NTP) with authentication instead of ICMP-based time queries.

### **ICMP Address Mask Attack**

- Attack:  
The attacker sends an ICMP Address Mask Request (Type 17) to a target. If the target responds with its subnet mask, it reveals network details to the attacker.
- Mitigation:  
Disable ICMP Address Mask Replies unless required for network operations. Use firewalls to filter ICMP traffic from untrusted sources.

## **ICMP Tunneling and Covert Channel Attacks**

### **ICMP Tunneling**

- Attack:  
Attackers encapsulate malicious data inside ICMP Echo Requests and Replies. Used to bypass firewalls that allow ICMP traffic but block TCP/UDP connections. Often used for covert communication in malware and C2 (Command & Control) channels.
- Example Tools:  
Icmpsh – Creates a reverse shell using ICMP. PingTunnel – Tunnels TCP traffic through ICMP packets.
- Mitigation:  
Deep Packet Inspection (DPI) to detect ICMP tunnels. Block ICMP

Echo Requests/Replies from untrusted networks. Monitor network traffic for unusual ICMP patterns.

### **ICMP Exfiltration (Data Theft via ICMP)**

- **Attack:**  
Attackers embed sensitive data (passwords, files, commands) inside ICMP packets. The data is sent to an external server controlled by the attacker.
- **Mitigation:**  
Monitor and log ICMP traffic for abnormal activity. Use firewalls to restrict ICMP traffic to only necessary devices. Employ DLP (Data Loss Prevention) solutions to detect exfiltration attempts

### **ICMP Covert Channels**

- **Attack:**  
Malware or attackers use ICMP packets to establish a hidden communication channel. Often used in C2 communication for botnets or stealthy malware operations.
- **Mitigation:**  
Monitor ICMP traffic for unusual usage patterns. Use Network Intrusion Detection Systems (NIDS) to detect covert channels. Restrict ICMP communication between internal and external networks.

## **2.9 Security Best Practices for ICMP**

ICMP is essential for network diagnostics, but it is also a target for DDoS, reconnaissance, covert channels, and data exfiltration attacks. By limiting ICMP usage, implementing firewalls, monitoring traffic, and using security tools, organizations can protect their networks from ICMP-based threats.

To prevent ICMP-based attacks, implement the following security measures:

### **Firewall Rules**

- Block ICMP Echo Requests from external networks unless needed.
- Disable ICMP Timestamp and Address Mask Replies to prevent reconnaissance.

- Allow only necessary ICMP error messages (e.g., Destination Unreachable).
- Drop ICMP Redirect messages to prevent routing manipulation.

### **Rate Limiting**

- Limit the number of ICMP packets per second to prevent flooding.
- Configure ICMP rate-limiting policies on routers and firewalls.

### **Network Monitoring & Detection**

- Use Intrusion Detection Systems (IDS/IPS) to detect ICMP abuse.
- Analyze network logs for unusual ICMP activity (e.g., large ICMP packets, frequent pings).
- Employ Deep Packet Inspection (DPI) to identify ICMP tunneling.

### **System Hardening**

- Keep systems and firmware updated to patch known ICMP vulnerabilities.
- Disable ICMP services on critical systems if not required.
- Use endpoint security solutions to detect malware using ICMP for communication

## 3 Covert Channel Attacks on ICMP

A covert channel is a hidden communication method that allows attackers to transfer data in a way that bypasses security policies. ICMP covert channels use ICMP packets (typically Echo Requests and Replies) to hide data inside fields that are normally ignored or not monitored.

Attackers exploit ICMP because:

- Many firewalls and security devices allow ICMP traffic for network diagnostics.
- ICMP packets can carry hidden payloads without raising suspicion.
- Traditional security systems focus on TCP/UDP traffic, neglecting ICMP.

### 3.1 How ICMP Covert Channels Work

#### 3.1.1 ICMP Tunneling

ICMP tunneling allows attackers to encapsulate data inside ICMP packets, creating a hidden communication channel.

1. The attacker embeds command and control (C2) instructions inside ICMP packets.
2. These packets are sent to a compromised system behind a firewall.
3. The system extracts the hidden instructions and executes them.
4. Responses are sent back using ICMP Echo Replies

#### **Esempio 3.1.** *Example Use Case*

*Malware (e.g., botnets) uses ICMP to bypass firewalls and receive commands from remote attackers. Attackers establish a reverse shell over ICMP, controlling a compromised machine.*

#### **Esempio 3.2.** *Example Tools for ICMP Tunneling*

*Icmpsh – Creates a reverse shell over ICMP. PingTunnel – Tunnels TCP traffic through ICMP Echo Requests and Replies. Ptunnel-NG – Advanced version of PingTunnel for bypassing firewalls*

### 3.1.2 ICMP Data Exfiltration

Attackers can steal data (passwords, files, sensitive information) by embedding it inside ICMP packets and sending it to an external server.

1. The attacker encodes sensitive data (e.g., credit card numbers, encryption keys) into ICMP packets.
2. The packets are sent to an external server controlled by the attacker.
3. The attacker extracts and decodes the stolen data from the ICMP traffic.

**Esempio 3.3.** *Example Use Case*

*An insider threat exfiltrates classified data using ICMP Echo Requests. A malware infection transmits keylogs or screenshots via ICMP packets*

**Esempio 3.4.** *Example Tools for ICMP Data Exfiltration*

*icmptx – Encodes and transfers data via ICMP packets. LOKI – Hides data in ICMP Echo Replies. Hans – Uses ICMP for encrypted data transfer*

### 3.1.3 ICMP-Based Botnet Command & Control (C2)

Some botnets and malware use ICMP to communicate with their command-and-control servers (C2)

1. The attacker embeds C2 commands in ICMP packets.
2. The infected bot reads the command and executes it.
3. The bot sends execution results back via ICMP replies

**Esempio 3.5.** *Example Malware Using ICMP for C2 Communication*

*Duqu – Used ICMP to send encrypted data. Pingback – A malware that receives commands via ICMP. Trojan.Medo – Used ICMP as a backdoor channel*

## 3.2 How to Detect and Mitigate ICMP Covert Channels

### 3.2.1 Detection Techniques

1. Monitor ICMP Traffic  
Analyze ICMP packet size (e.g., unusually large payloads). Detect high-frequency ICMP traffic to unknown external hosts. Check for ICMP packets with irregular patterns (e.g., varying TTL values).

2. Use Deep Packet Inspection (DPI)  
Inspect ICMP payloads for unusual embedded data. Flag ICMP packets that contain non-standard responses.
3. Anomaly Detection with IDS/IPS  
Use Snort, Suricata, or Zeek to detect abnormal ICMP activity.

**Esempio 3.6.** *Snort rule to detect ICMP tunneling*

```
alert icmp any any -> any any (msg:"ICMP tunnel detected";
```

### 3.2.2 Prevention and Mitigation Strategies

1. Restrict ICMP Traffic  
Block ICMP traffic from untrusted sources at the firewall. Allow only necessary ICMP messages (e.g., Destination Unreachable). Disable ICMP Echo Requests/Replies on critical systems.
2. Rate-Limit ICMP Packets  
Limit ICMP packet size to prevent hidden data transfer. Configure firewalls to allow only a specific number of ICMP packets per second.
3. Use Encryption for Data Transfer  
Prevent attackers from intercepting sensitive data by encrypting all legitimate communication (e.g., using VPNs, TLS).
4. Deploy Endpoint Security Solutions  
Use host-based firewalls to block suspicious ICMP communication. Install antivirus and EDR (Endpoint Detection and Response) tools to detect malware using ICMP covert channels

## 3.3 Real-World Example of an ICMP Covert Channel Attack

Case Study: Duqu Malware (2011)

- What Happened? Duqu, a sophisticated malware, used ICMP packets to exfiltrate data from infected systems
- How It Worked: It embedded stolen data inside ICMP Echo Requests sent to a remote server. Security tools failed to detect it because ICMP was considered harmless



- Mitigation: Organizations learned to monitor ICMP traffic and block unnecessary ICMP messages to prevent future attacks

### 3.4 Summary: How to Secure Against ICMP Covert Channels

ICMP covert channels pose a serious security risk because they bypass firewalls, evade detection, and allow hidden data transmission. Organizations must monitor ICMP traffic, restrict its use, and employ security tools to detect and block covert channels effectively.

Mitigation Method	Effectiveness
Disable ICMP if not needed Limit ICMP to necessary types Monitor ICMP traffic patterns	Prevents most ICMP-based attacks. Blocks unnecessary attack vectors. Detects anomalies and data exfiltration.
Use Deep Packet Inspection (DPI)	Identifies hidden data in ICMP packets.
Implement IDS/IPS rules for ICMP Block outgoing ICMP at firewalls	Alerts on suspicious ICMP activity. Prevents data leaks via ICMP.

### 3.5 Covert Channel Attacks on ICMP: Mitigation and Detection Strategies

### 3.6 What Are ICMP Covert Channel Attacks?

ICMP (Internet Control Message Protocol) is primarily used for network diagnostics and error reporting, but attackers can exploit it to create covert channels—hidden communication pathways used for data exfiltration, command and control (C2), and bypassing security policies.

#### How ICMP Covert Channels Work

- Data Encoding: Attackers embed hidden messages inside ICMP packets, such as Echo Requests (ping) or Echo Replies.
- Firewall Evasion: Since ICMP is often allowed in firewalls, attackers use it to bypass security policies.
- Stealth Communication: Malware and botnets use ICMP to secretly communicate with a remote attacker

Example ICMP Covert Channel Attacks:

Attack Type	Description
ICMP Tunneling	Encapsulating TCP/IP traffic inside ICMP packets to evade firewall restrictions.
ICMP Data Exfiltration	Sending stolen data hidden inside ICMP payloads to an external server.
ICMP-Based Command & Control (C2)	Malware receiving commands from an attacker via ICMP.
ICMP Reverse Shell	A backdoor that allows an attacker to control a machine remotely using ICMP.

### 3.7 Detection Strategies for ICMP Covert Channels

#### 3.7.1 Network Traffic Monitoring

Monitor ICMP packet volume and packet sizes for anomalies. Detect ICMP packets with unusually large payloads (e.g., data exfiltration attempts) Identify ICMP packets with constant payload changes, which could indicate hidden data transfer

#### 3.7.2 Deep Packet Inspection (DPI)

Analyze ICMP payload content for encoded messages, encryption, or anomalies. Look for non-standard ICMP responses (e.g., an Echo Reply containing unexpected data). Identify patterns of communication with external IP addresses over ICMP

#### 3.7.3 Intrusion Detection and Prevention Systems (IDS/IPS)

Use Snort, Suricata, or Zeek to detect and alert on suspicious ICMP activity

**Esempio 3.7.** *Snort Rule for ICMP Tunneling Detection*

```
alert icmp any any -> any any (msg:"ICMP tunnel detected"; co
```

Implement behavioral analysis to detect abnormal ICMP usage

#### 3.7.4 Anomaly-Based Detection

Use Machine Learning or SIEM (Security Information and Event Management) tools to flag deviations in ICMP usage. Detect high-frequency ICMP traffic that could indicate C2 communication

## 3.8 Mitigation Strategies for ICMP Covert Channels

### 3.8.1 Restrict ICMP Traffic

Disable ICMP on servers and endpoints unless explicitly needed. Configure firewalls and routers to allow only essential ICMP messages (e.g., "Destination Unreachable," "Time Exceeded").

**Esempio 3.8.** *Firewall Rule to Block ICMP Traffic*

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

### Rate-Limiting ICMP Traffic

Limit the frequency and size of ICMP packets to prevent tunneling. Example: Configure firewalls to allow only a certain number of ICMP requests per second

**Esempio 3.9.**

```
iptables -A INPUT -p icmp -m limit --limit 1/second
```

### 3.8.2 Use Encryption to Prevent Data Leakage

Implement TLS/SSL encryption for legitimate communications to prevent attackers from using ICMP for exfiltration. Block unauthorized plaintext transmissions over ICMP.

### 3.8.3 Block ICMP on External Interfaces

Prevent outbound ICMP traffic from internal networks to stop exfiltration. Allow ICMP only for internal diagnostic purposes.

### 3.8.4 Endpoint Security & Antivirus

Deploy EDR (Endpoint Detection & Response) solutions to detect malware using ICMP for communication. Regularly update antivirus software to identify and block known threats.

### 3.8.5 Implement ICMP Proxy Filtering

Use ICMP proxies to inspect, sanitize, and block unexpected ICMP payloads. Allow only legitimate diagnostic ICMP traffic to pass through.

### 3.9 Summary: Detection & Mitigation Techniques

ICMP covert channels pose serious security risks, allowing stealthy data exfiltration, tunneling, and malware communication. By implementing strict ICMP restrictions, deep packet inspection, firewall rules, and anomaly detection, organizations can effectively detect and mitigate these threats.

Technique	Detection	Mitigation
Network Traffic Analysis	Identifies anomalies in ICMP volume and patterns	Restricts unnecessary ICMP types
Deep Packet Inspection (DPI)	Detects data exfiltration and tunneling	Blocks ICMP packets with unexpected payloads
IDS/IPS (Snort, Zeek)	Alerts on unusual ICMP behavior	Blocks suspicious ICMP requests
Rate Limiting	Detects excessive ICMP requests	Prevents ICMP flooding and tunneling
Firewall Rules	Flags unauthorized ICMP requests	Blocks outbound ICMP from critical systems
Endpoint Security (EDR)	Detects malware using ICMP covert channels	Prevents malicious ICMP execution