



# Sicurezza dei sistemi e delle reti<sup>1</sup>

Mattia Monga

Dip. di Informatica  
Università degli Studi di Milano, Italia  
[mattia.monga@unimi.it](mailto:mattia.monga@unimi.it)

a.a. 2014/15



# Lezione XVI: L'assegnazione automatica di IP



Il Dynamic Host Configuration Protocol è un elemento critico nelle reti in cui i numeri IP sono **assegnati dinamicamente**.

- Permette configurazioni dinamiche (quindi aggiornate)
- Ma non prevede forme di autenticazione (ipotesi trusted LAN)



- Assegna i numeri IP
- Default gateway
- DNS server

Particolarmente adatto nelle reti la cui topologia cambia continuamente (es. ISP)



- 1 L'amministratore della rete mantiene un pool di configurazioni sul DHCP server
- 2 Quando un client si connette alla rete (spesso al boot) fa broadcast di una richiesta di configurazione
- 3 Il server assegna una configurazione del pool, comunicandola al client



- 1 Il client fa broadcast DHCPDISCOVER
- 2 Il server risponde con DHCPOFFER
- 3 Se accetta, il client fa broadcast di DHCPREQUEST (il broadcast serve a rispondere anche ad eventuali altri server)
- 4 Il server manda un DHCPACK



Il protocollo lavora a livello di rete locale in cui i nodi

- condividono il mezzo trasmissivo
- sono “identificati” dal MAC



Non essendo prevista nessuna forma di autenticazione, un attaccante:

- manda molte richieste, con MAC differenti
- il pool si esaurisce
- client legittimi non riescono a ottenere una configurazione





Una parziale contromisura già presente nel protocollo è il concetto di **leasing**: una configurazione viene “noleggiata” solo per un certo tempo, poi ritorna disponibile nel pool.



Una parziale contromisura già presente nel protocollo è il concetto di **leasing**: una configurazione viene “noleggiata” solo per un certo tempo, poi ritorna disponibile nel pool.



Molti switch permettono di **limitare il numero di MAC** utilizzabili da una determinata borchia: se questo limite è minore della disponibilità del pool, l'attaccante deve controllare più borchie per essere efficace.



I client che entrano nella rete non conoscono l'indirizzo del DHCP server (infatti fanno broadcast)

- Un attaccante può allestire un **rogue server**
- Deve raggiungere il client **prima** del server legittimo

# Rogue Server: sostituire il gw



Sicurezza delle  
reti

Monga

DHCP

DNS

Un rogue server può comunicare un configurazione scorretta.

Sostituirsi al gateway In questo modo intercetta tutto il traffico (senza agire in modalità promiscua)

# Rogue Server: sostituire il DNS



Sicurezza delle  
reti

Monga

DHCP

DNS

Un rogue server può comunicare un configurazione scorretta.

**Sostituirsi al DNS** In questo modo può manipolare tutte le destinazioni espresse con nome simbolico



- L'amministratore di rete può monitorare i nodi che fanno da DHCP server o anche forzare che ciò avvenga solo da un borchia determinata
- Esistono estensioni di DHCP con varie forme di autenticazione



## Il protocollo DHCP

- Lavora a livello LAN, con mezzo trasmissivo condiviso e identificazione affidata ai MAC
- Generalmente non sono previste forme di autenticazione sicura
  - Address starvation
  - Rogue server





Il DNS è un servizio fondamentale per il buon funzionamento delle reti.

- È un elemento molto importante nella catena di trust delle transazioni iniziate da un utente umano, che raramente usa direttamente i numeri IP
- È un servizio generalmente **pubblico** e ottenuto in maniera decentralizzata, quindi nessuno ne ha il completo controllo



- Può essere utilizzato anche come strumento di “intelligence” prima di ulteriori attacchi
- Esistono moltissime implementazioni, non tutte curate dal punto di vista della sicurezza
- Per questi motivi è un bersaglio particolarmente attraente



Spesso si allestiscono due server DNS

**DNS Esterno** Riceve query da utenti **esterni** per informazioni riguardo host pubblicamente accessibili della rete aziendale, incluso l'MX server (il Mail Relay)



Spesso si allestiscono due server DNS

**DNS Interno** Riceve query da utenti **interni** per informazioni su host sia della intranet aziendale che di Internet. Per le query che il DNS Interno non è in grado di risolvere contatta altri DNS (query ricorsive).



Sicurezza delle  
reti

Monga

DHCP

DNS

I due DNS mantengono informazioni differenti (solo quelle pubbliche l'esterno, tutte quelle della intranet l'interno) e hanno connessioni con zone a diverso grado di sicurezza.



- Separazione fisica delle informazioni riguardante servizi pubblici da quelle riguardanti servizi della intranet
- Assegnazione a diverse zone di sicurezza per la protezione delle informazioni
- Isolamento del DNS pubblico dalla rete interna nel caso di compromissione

# Separazione DNS

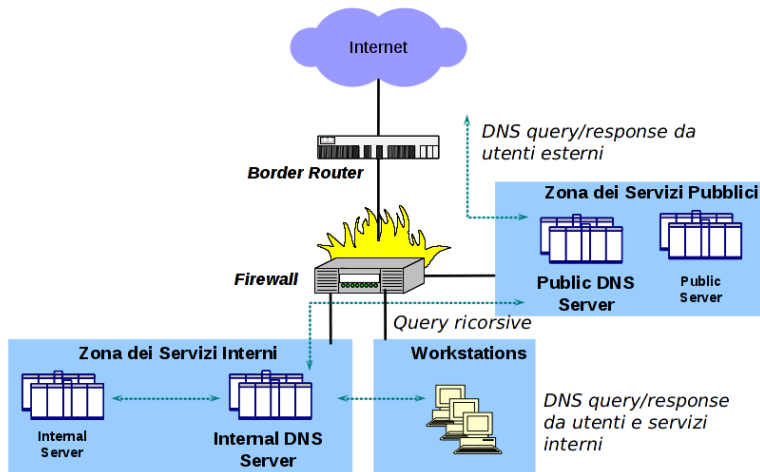


Sicurezza delle  
reti

Monga

DHCP

DNS





Il DNS è un servizio altamente critico in una rete

- Il protocollo è privo di feature di sicurezza
- È opportuno strutturarne la difesa in più livelli