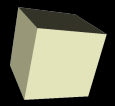
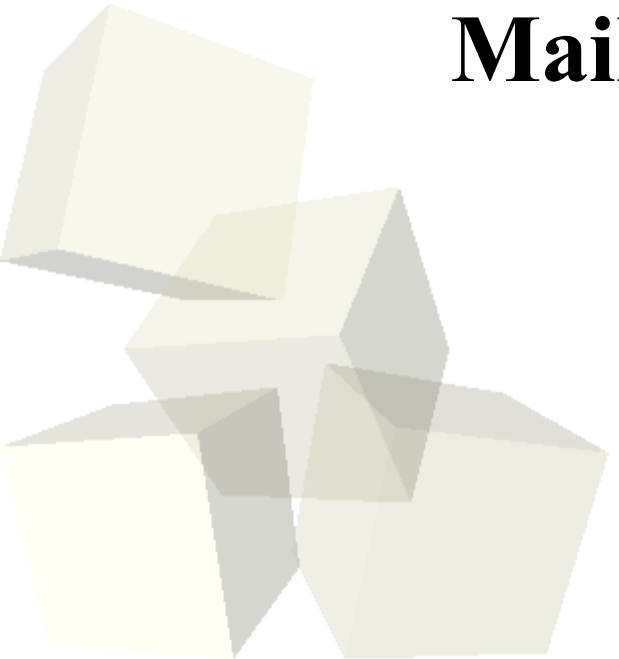


Sicurezza di protocolli P2P

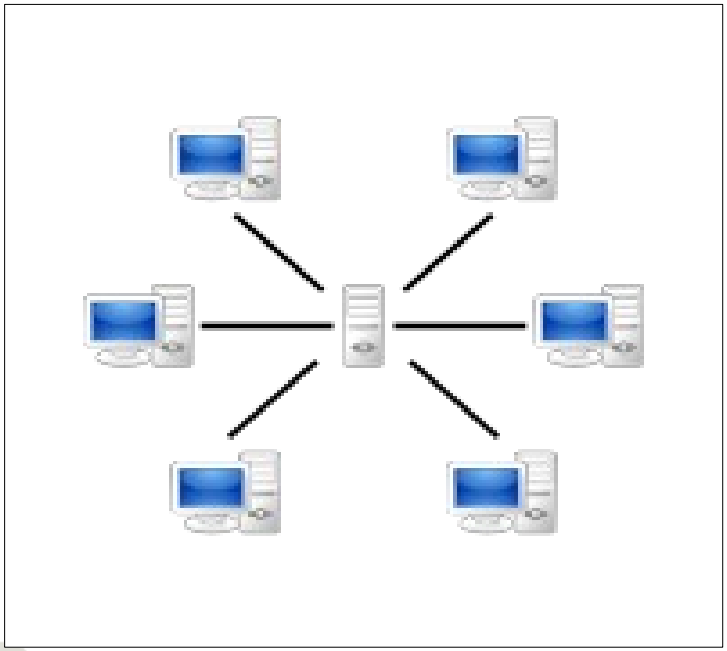
Marco Bagnaresi – Matr. 236050

Mail : frostland @ gmail . com

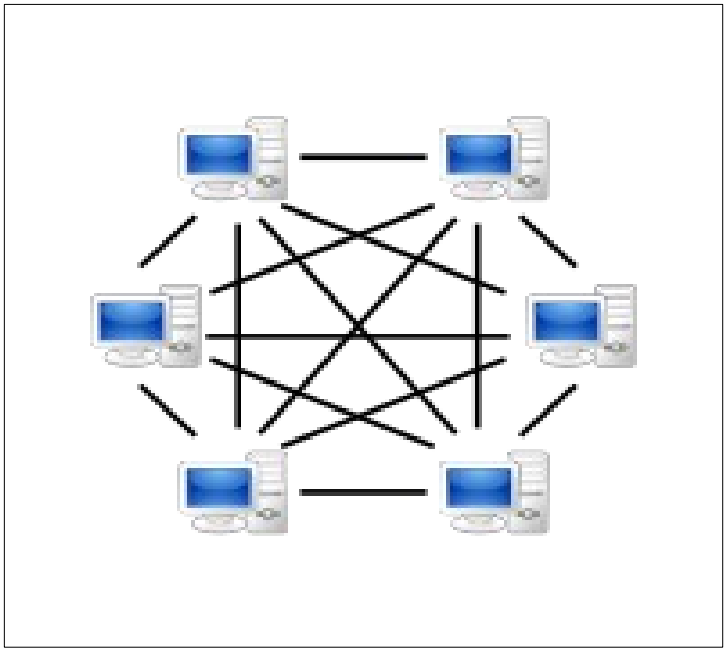


Introduzione

- Peer-to-Peer : un tipo di rete in cui ogni workstation ha equivalenti capacità e responsabilità.
- Contrapposto al modello client-server



Client-Server



Peer-to-Peer

Vantaggi delle reti P2P

- Ogni client condivide risorse
  - Banda
  - Spazio su disco
  - Potenza computazionale
- La capacità della rete aumenta all'aumentare del numero dei client, cosa non sempre vera nel modello client-server
- La rete diventa più robusta tramite possibile replicazione dei dati
- Nel caso di reti P2P 'pure' non esistono punti deboli nell'architettura della rete.

Un po' di storia ...

- La prima rete P2P è Usenet, che nasce come rete di distribuzione delle news.
- I client distribuiscono le notizie ad altri client.
- La popolarità delle reti P2P esplode con l'avvento di Napster (giugno '99) e delle controversie legali ad esso legate.
- Tuttora esistono decine e decine di tipologie differenti di reti P2P.

Tipologie di reti P2P

- Esistono varie categorie di P2P :
  - Collaborative Computing
    - Conosciute anche come Distributed Computing, queste reti sfruttano la potenza di cpu e lo spazio su disco non utilizzato per eseguire complessi calcoli matematici.
      - Esempio : United Devices, effettua ricerca sul cancro con circa 2 milioni di pc connessi fra loro.
  - Instant Messaging e Telefonia
    - Un utilizzo comune è quello di reti di instant messaging o telefonia in cui le applicazioni consentono di chattare o videochiamarsi in real-time. Sta diventando lo strumento di comunicazione standard in ambienti Enterprise.
      - Esempi : MSN Messenger, AOL Instant Messenger, Skype
  - Affinity Communities
    - Scambio e condivisione file
      - Esempi : Bittorrent, Kazaa, ...
  - ...

Evoluzione di reti P2P (1)

- Prima generazione : Napster
  - Server centralizzato con l'indice dei contenuti
  - Controllo sui file condivisi
  - Single point of failure
  - Fallita per controversie legali legate alla distribuzione della musica
- Seconda generazione : Gnutella
  - Nata per eludere i problemi di Napster
  - Nessun server centralizzato
  - Peer della rete rintracciati tramite liste o web cache
  - Ricerche tramite “query flooding”
  - Successive evoluzioni e miglioramenti della rete tramite introduzione di ultrapeers e leaves.
  - Miglioramenti con QRP e DQ

Evoluzione di reti P2P (2)

- Terza generazione : Freenet
  - Nata per garantire libertà di parola e anonimato
  - Nessun server centralizzato
  - Ricerche effettuate con euristica di routing basata sulla chiave
  - Dati distribuiti e replicati
  - Una volta inseriti i dati rimangono nella rete (anche se il client si disconnette)
- Quarta generazione : DHT
  - Ricerche basate su Distributed Hash Table
  - Efficienza di Napster nelle ricerche, decentralizzazione di Gnutella
  - Esempi : eDonkey, Bittorrent, ecc ...

Evoluzione di reti P2P (3)

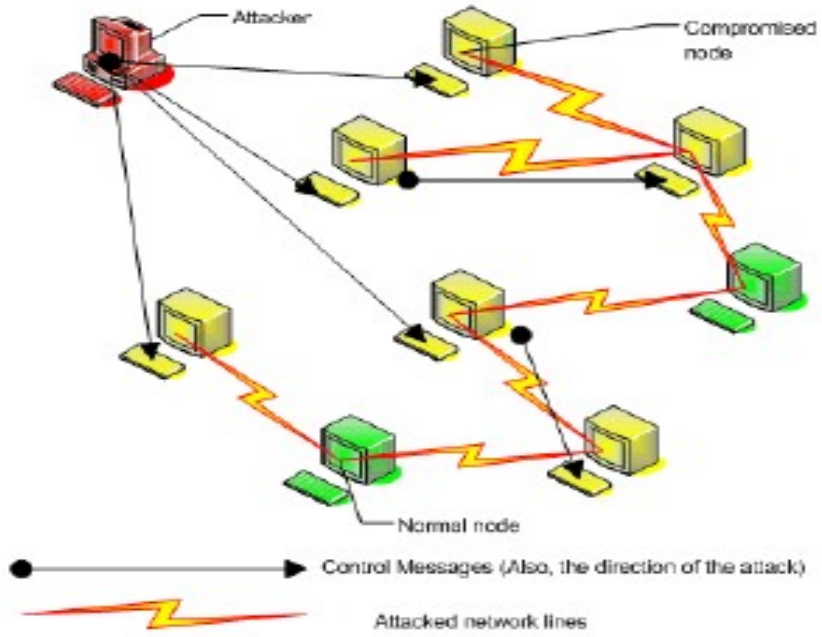
- Quinta generazione : utilizzo di CDN
  - Viene utilizzata una mappa della rete (Content Distribution Network) per aumentare la banda complessiva.
  - Si selezionano host “vicini” (separati da pochi “hops”)
  - Attualmente disponibile soltanto col client Azureus della rete Bittorrent
  - Plugin sperimentale
  - Aumenti dichiarati tra il 31% e 207%
  - Fonte : Punto Informatico (5/5/08)

P2P : alcuni concetti importanti

- Overlay Network
  - Rete costruita sopra un'altra rete.
  - Esempi : Dial-up su rete telefonica, P2P sopra IP
  - Il routing avviene in maniera differente da una rete all'altra.
- DHT : Distributed Hash Table
  - E' una struttura dati
  - Proprietà principali : Decentralizzazione, Scalabilità, Fault tolerance
  - Ogni nodo si coordina con pochi altri nodi
  - Concetti chiave : Keyspace, Keyspace partitioning
  - Operazioni chiave : PING, STORE, FIND_NODE, FIND_VALUE
  - Molte implementazioni differenti (KAD,Chord, CAN ...)

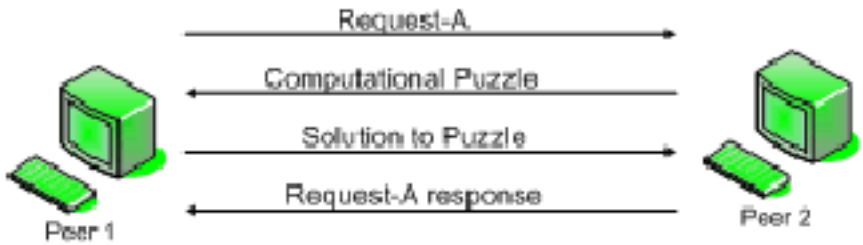
Attacchi a reti P2P : DDoS

- Scopo : inondare (flood) di richieste non valide la rete in modo che le richieste valide non vengano ricevute.
- In particolare il DDoS utilizza diversi host per generare un numero maggiore di richieste.
- Il vero attaccante è nascosto.



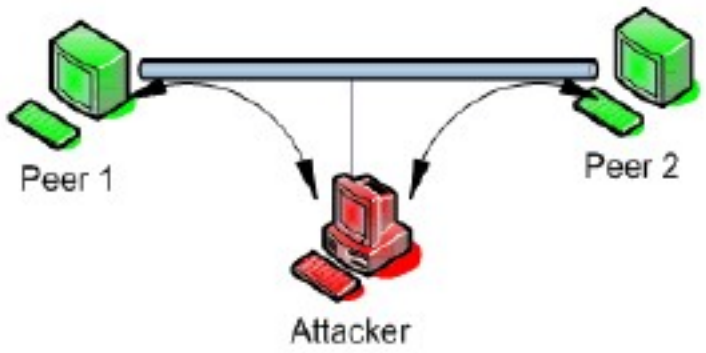
Attacchi a reti P2P : DDoS (2)

- Soluzione : prima di rispondere alla richiesta l'host si aspetta la soluzione di un puzzle computazionale. (tecnica del “pricing”)
- In questo modo si rallentano le richieste e si evita il flood.
- Esempio di Puzzle : calcoli di digest su stringhe casuali.



Attacchi a reti P2P : MitM

- Scopo : controllare e modificare il traffico fra due nodi.
- Facilmente realizzabile se ci si controlla il layer di rete.
- Altrettanto facilmente realizzabile nelle reti P2P : genero un'ID che in base alla metrica della rete mi posiziona fra i due nodi interessati.

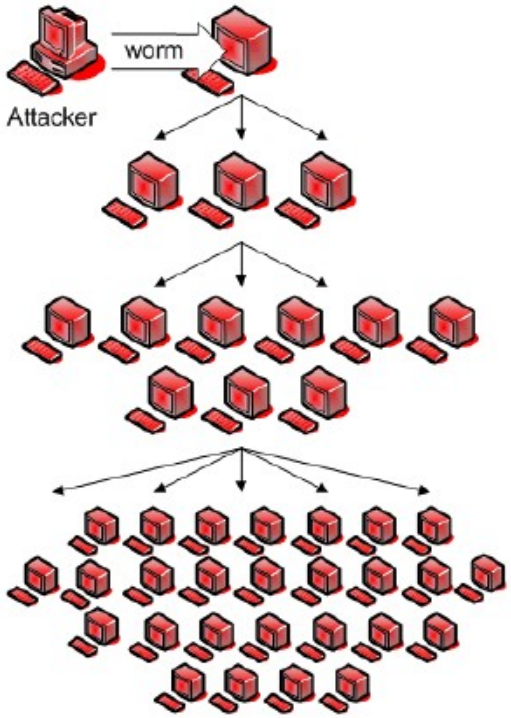


Attacchi a reti P2P : MitM (2)

- Soluzione : è necessaria un'autorità centrale per stabilire l'identità dei nodi.
- Esempi : Super Node, Indexing Server, CA.
- Digital Signatures per impedire la modifica/generazione dei dati.
- Crittografia a chiave pubblica/privata per impedire la lettura dei messaggi.

Attacchi a reti P2P : Worms

- Worm : Programma auto-replicante che si propaga sfruttando vulnerabilità software.
- Estremamente pericoloso per P2P : molti client utilizzano lo stesso software
- Attacco i nodi adiacenti.



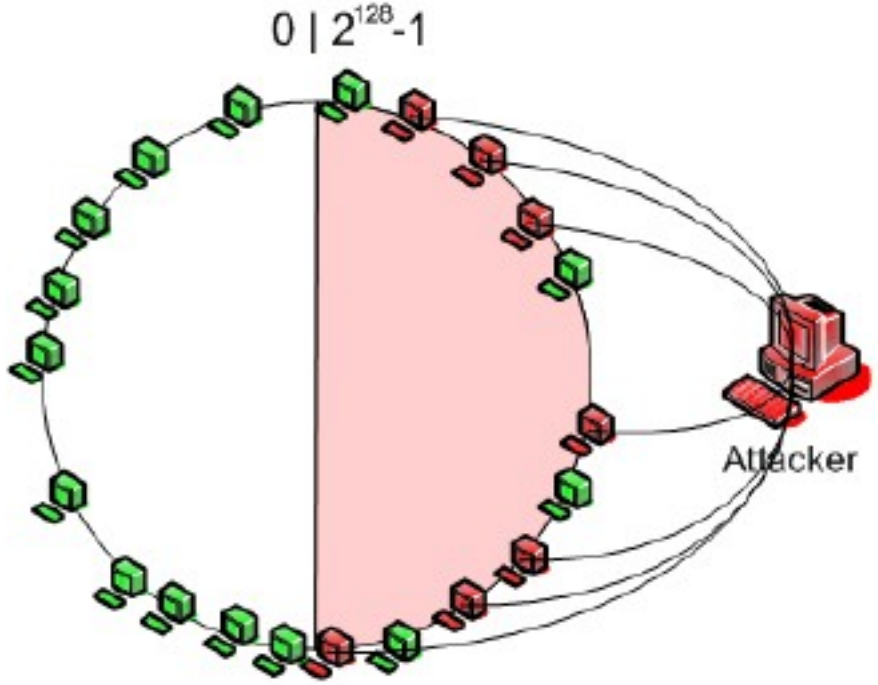
Attacchi a reti P2P : Worms (2)

- Soluzione : Scrivere applicazioni sicure.

- Utilizzo di linguaggi Strongly Typed.
- Utilizzo di librerie di gestione della memoria testate e sicure.
- Scrivere applicazioni open-source
- Utilizzare standard aperti
- Utilizzare sistemi operativi hardened (Esempio OpenBSD >=3.8 utilizza indirizzi di memoria pseudo-casuali).

Attacchi a reti P2P : Sybil

- Lo scopo di questo attacco è guadagnare il controllo di una parte della rete inserendo in essa molti nodi fittizi.
- I network più vulnerabili sono quelli a una dimensione in cui l'attaccante può scegliere l'ID
- Usato come gateway per attacchi più grandi

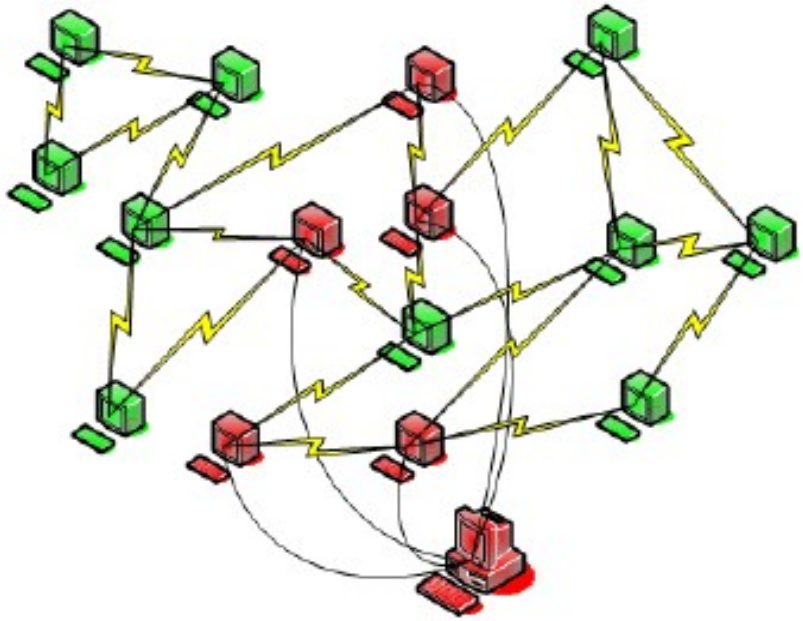


Attacchi a reti P2P : Sybil (2)

- Impossibile fermarlo completamente in un network senza autorità centrale
- E' possibile rallentarlo con tecniche di pricing per entrare a far parte del network
- Una ulteriore contromisura è quella di far scadere l'ID dopo un certo tempo

Attacchi a reti P2P : Eclipse

- Scopo : separare la rete in due o più partizioni per controllare tutti i messaggi che passano da una partizione all'altra
- MitM su larga scala
- Creando nodi fake è possibile contaminare le tabelle di routing e rendere inutilizzabile l'intera rete



Attacchi a reti P2P : Eclipse (2)

- Soluzione : le stesse di MitM, ovvero crittografia.
- Come per Sybil è importante che l'attaccante non possa scegliere l'ID dei nodi
- E' da notare comunque che da Sybil è sempre possibile passare a un Eclipse

Conclusioni

- Per aver maggior sicurezza è necessario :
  - Impedire che i nodi possano scegliere il loro ID
  - Limitare il rate col quale i nodi possono far parte del network P2P
  - Usare crittografia a chiave pubblica/certificati digitali
  - Sviluppare su standard aperti
- La maggior parte degli attacchi possono essere sventati tramite un accurato design del network e l'uso di crittografia

Bibliografia

- [1] http://en.wikipedia.org/wiki/Peer-to-peer
- [2] Atul Singh, Miguel Castro, Peter Drushel, Anthony Rowstron : “Defending against Eclipse attacks on overlay networks”
- [3] Baptiste Peter, Roger Wattenhofer : “Attacks on Peer-to-Peer Networks”
- [4] John R. Douceur : “The Sybil Attack”
- [5] Emil Sit, Robert Morris : “Security Considerations for Peer-to-Peer Distributed Hash Tables”
- [6] Mudhakar Srivatsa, Ling Liu : “Vulnerabilities and Security Threats in Structured Peer-to-Peer Systems : A Quantitative Analysis”

FINE

Marco Bagnaresi

Mail : frostland @ gmail . com