Studio di reti di sensori con comportamento ciclico con il simulatore Castalia

Corso di Laurea in Informatica

Candidato
Andrea Di Saverio

Relatori
Maria Cristina Pinotti
Alfredo Navarra

Anno accademico 2009/2010

Sommario

Sommario

Sommario

Sommario

Sommario

Introduzione

Sicurezza informatica:

- Non esiste una soluzione unica e definitiva
- Approccio a cipolla
- Servizi offerti dal server
- Aggiornamenti costanti

Per la maggior parte dei servizi non si può fare di meglio. Per il resto?

Introduzione

Sicurezza informatica:

- Non esiste una soluzione unica e definitiva
- Approccio a cipolla
- Servizi offerti dal server
- Aggiornamenti costanti

Per la maggior parte dei servizi non si può fare di meglio. Per il resto?

Port knocking

Cos'è?

Definizione

Il **Port Knocking** *è una tecnica che permette di comunicare con una macchina attraverso porte filtrate dal firewall.*
La sequenza di knock rappresenta la chiave di autenticazione.

Cos'è?

Definizione

Il **Port Knocking** *è una tecnica che permette di comunicare con una macchina attraverso porte filtrate dal firewall.*
La sequenza di knock rappresenta la chiave di autenticazione.

A chi è destinata:

- servizi sensibili
- servizi con una base di utenti limitata
- servizi che non hanno bisogno di essere costantemente esposti al pubblico

Cos'è?

Definizione

Il **Port Knocking** *è una tecnica che permette di comunicare con una macchina attraverso porte filtrate dal firewall.*
La sequenza di knock rappresenta la chiave di autenticazione.

A chi è destinata:

- servizi sensibili
- servizi con una base di utenti limitata
- servizi che non hanno bisogno di essere costantemente esposti al pubblico

Obiettivo:

- nascondere al mondo esterno quali sono i servizi che girano sulla macchina
- difendere il server in quel lasso di tempo che intercorre tra la scoperta di un nuovo *bug* e il rilascio della relativa *patch*

In teoria

Il Port Knocking aggiunge un nuovo strato al modello "a cipolla":

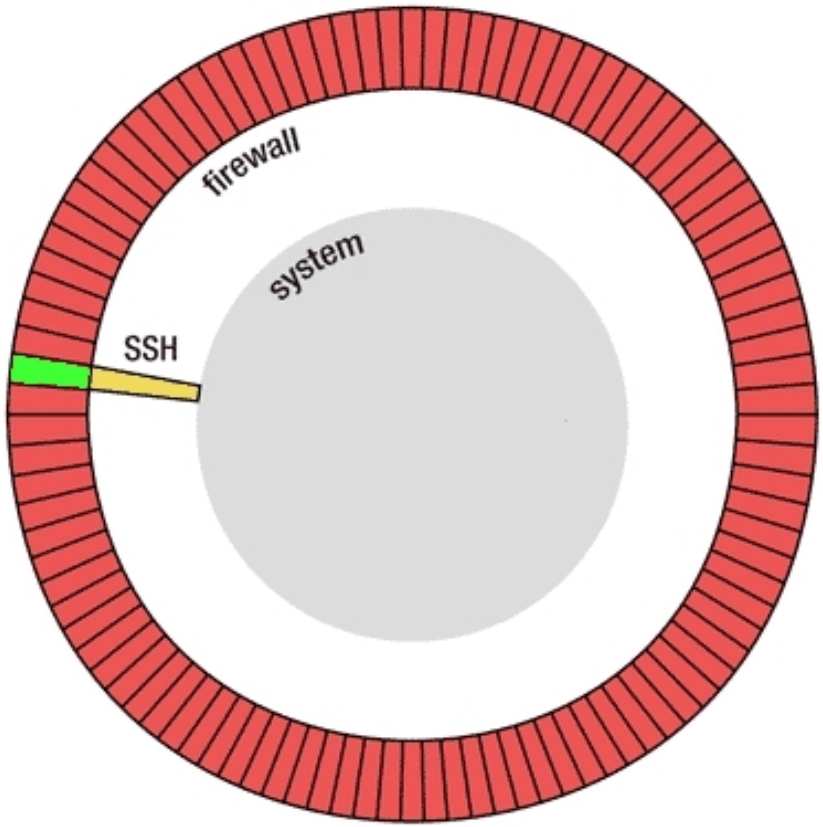


Figura: Modello classico

In teoria

Il Port Knocking aggiunge un nuovo strato al modello "a cipolla":

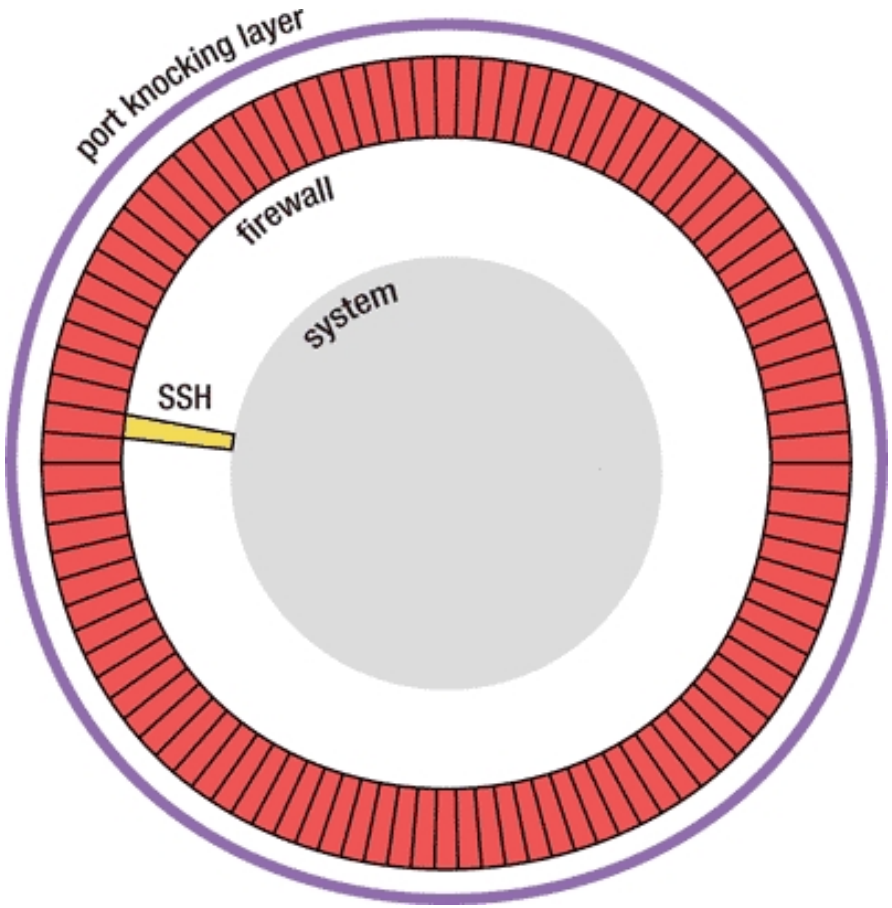


Figura: Modello con Port Knocking

Esempio

Hardening di un server SSH

Soluzione comune: fornire una lista di indirizzi IP *trusted*.

Esempio

Hardening di un server SSH

Soluzione comune: fornire una lista di indirizzi IP *trusted*.

Limiti:

- gli indirizzi IP spesso non sono statici
- dietro un indirizzo IP *trusted* non è detto operi un utente fidato

Esempio

Hardening di un server SSH

Soluzione comune: fornire una lista di indirizzi IP *trusted*.

Limiti:

- gli indirizzi IP spesso non sono statici
- dietro un indirizzo IP *trusted* non è detto operi un utente fidato

Il Port Knocking ribalta il punto di vista:

- permette a uno specifico utente di collegarsi da qualsiasi indirizzo IP, piuttosto che permettere a qualsiasi utente di collegarsi da uno specifico indirizzo IP.

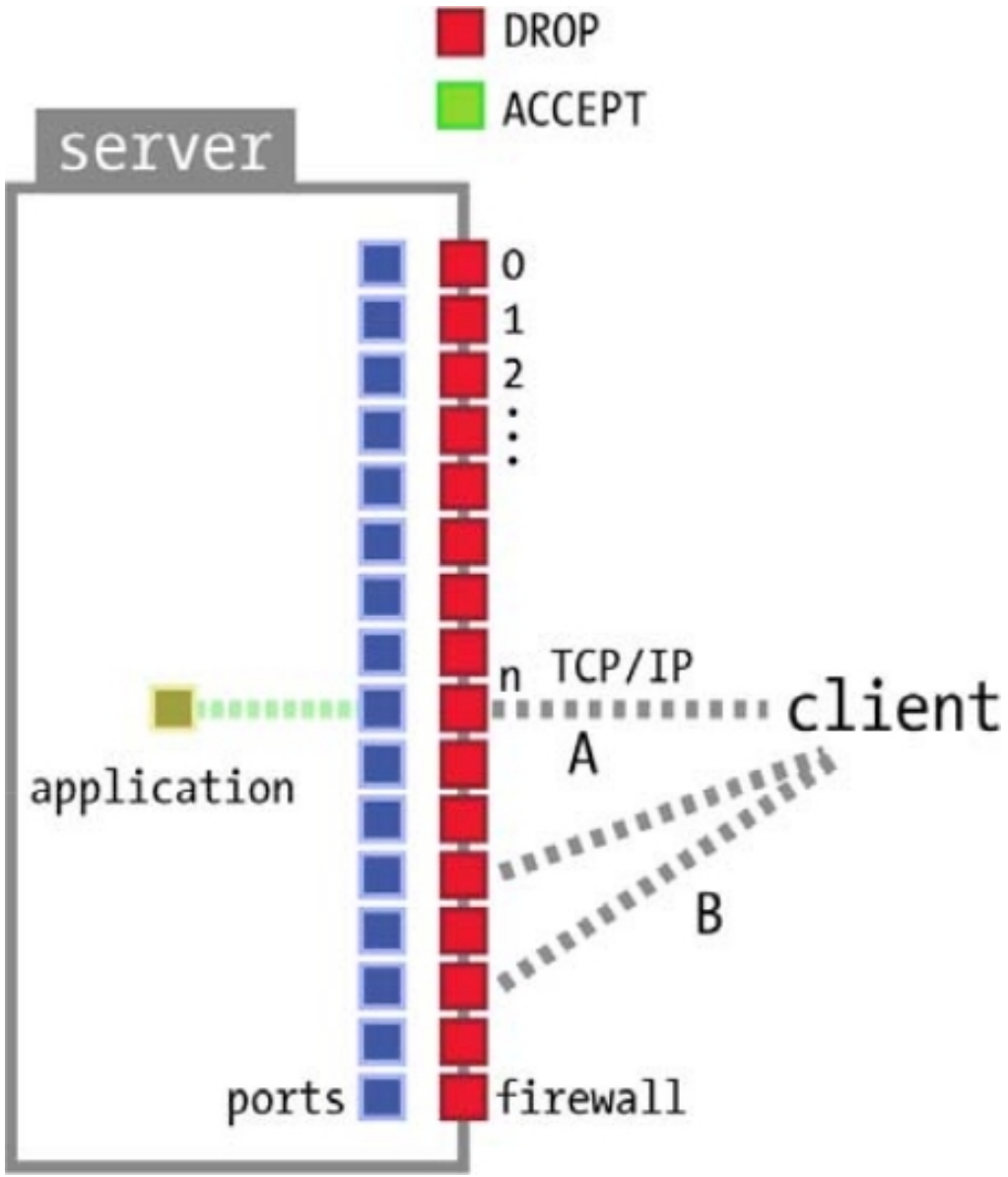
Se sulla macchina il firewall è configurato per monitorare l'arrivo di pacchetti a porte predefinite allora essa sarà in grado di riconoscere la sequenza ed aprirci il servizio.

Security Through Obscurity?

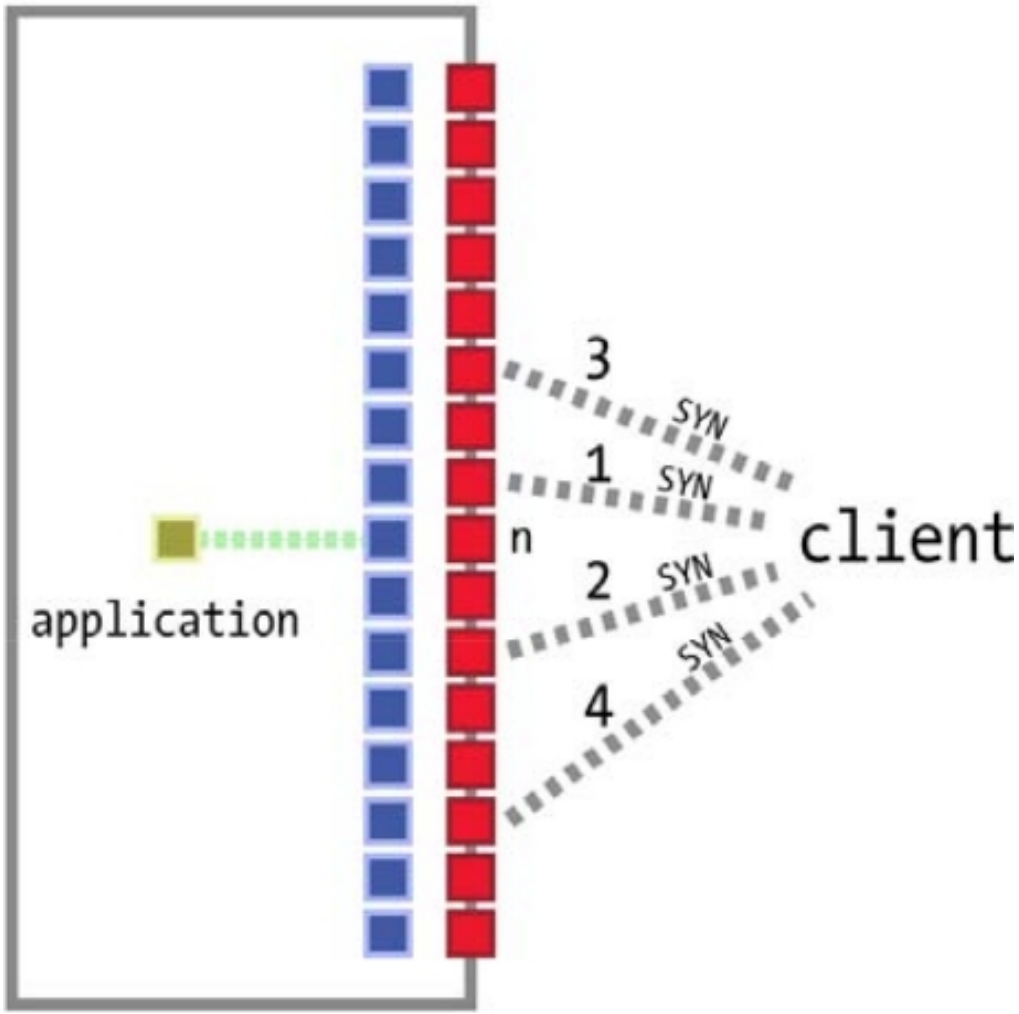
Port knocking come forma di sicurezza attraverso la segretezza.
In realtà non è così:

- l'integrità del sistema non è garantita dal fatto che l'avversario non conosce il sistema
- la sicurezza dipende dalla conoscenza della sequenza di knock, paragonabile ad una *shared-key*
- la segretezza che garantisce questa tecnica riguarda i servizi attivi sulla macchina

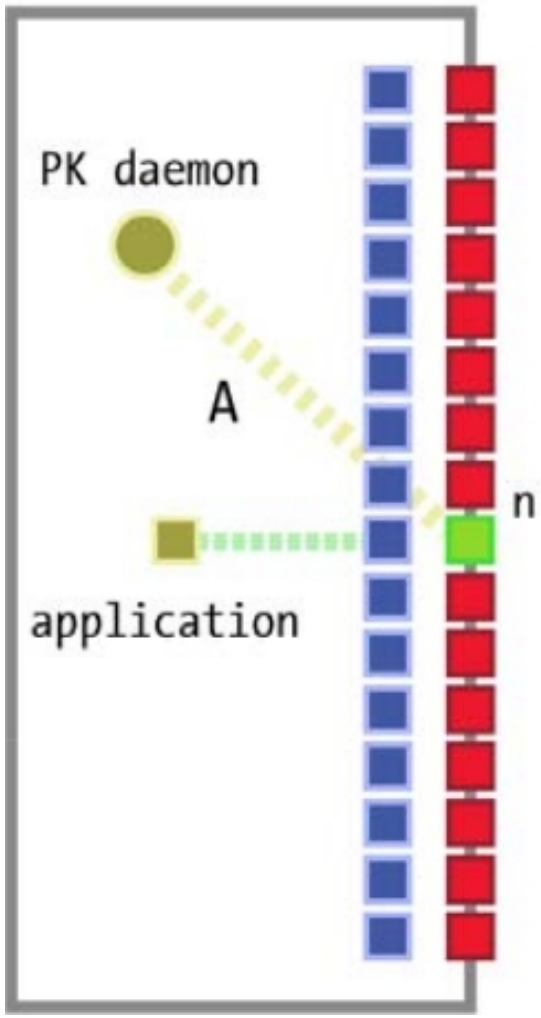
Funzionamento: situazione iniziale



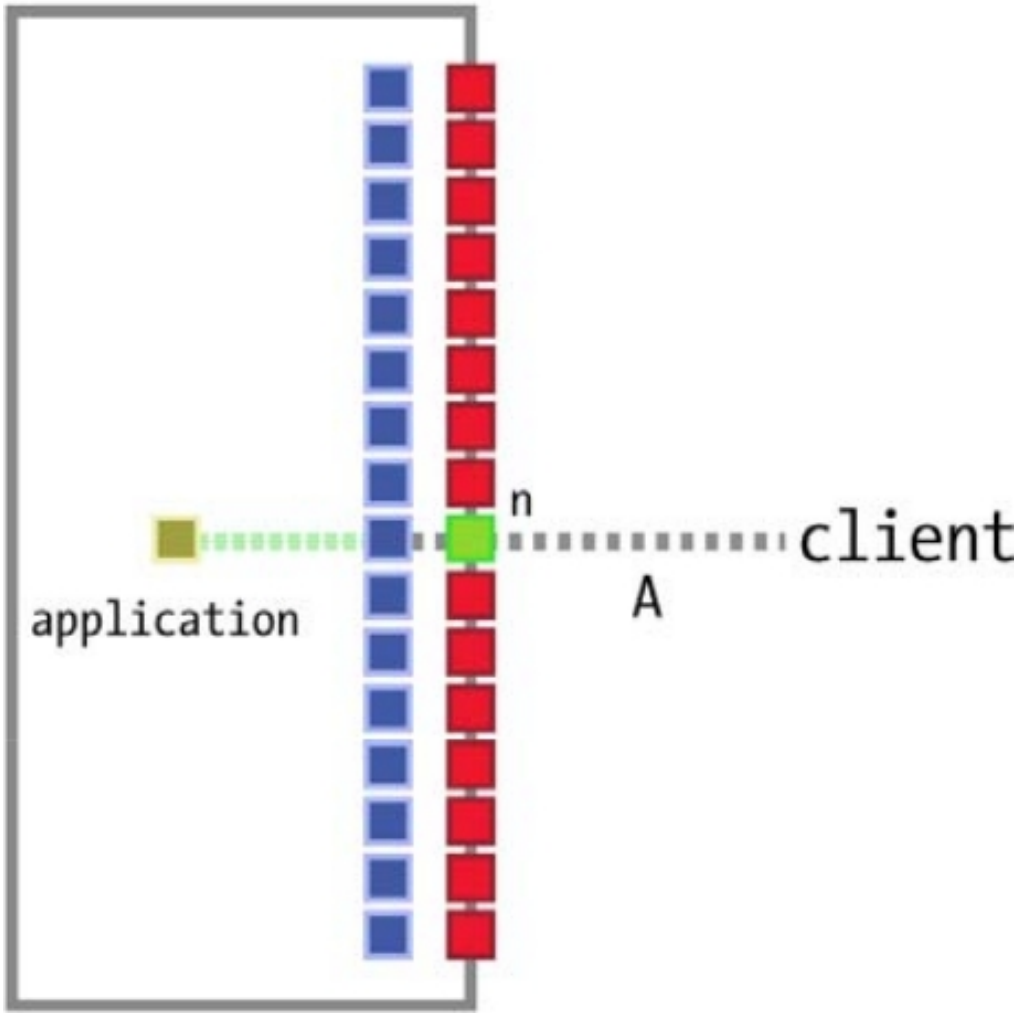
Funzionamento: la bussata



Funzionamento: il ruolo del pk-daeomn



Funzionamento: la connessione



Un'implementazione naive

Strumenti:

- iptables: lato server, si occupa della gestione delle porte e dei log
- sendip: lato client, è usato per forgiare e inviare i knock

Meccanismo pratico di funzionamento:

1. il firewall logga su file i tentativi falliti di connessione
2. uno script effettua il parsing del file di log alla ricerca di una sequenza valida
3. vengono modificate le regole di iptables per rendere possibile la connessione
4. al termine della connessione viene ripristinata la situazione iniziale

Obiettivi auspicabili:

- ruolo passivo del server: non deve fornire alcun feedback alle "bussate"
- chiusura automatica della porta aperta dal demone

Possibili attacchi:

Replay attack:

- se sottoposto a sniffing, il traffico è facilmente replicabile, a prescindere dalla conoscenza del meccanismo difensivo utilizzato

Soluzione:

- uso di sequenze di knock "usa e getta": una sorta di *one time password*
- uso della crittografia: viene sfruttato il segmento *data* del pacchetto TCP per l'invio di *nonce* crittografate

Possibili attacchi:

Man in the Middle:

- l'attaccante si interpone nella comunicazione tra client e server, con la possibilità di modificare il messaggio corrompendo l'indirizzo ip sorgente

Soluzione:

- uso della crittografia: anche in questo caso viene sfruttato il segmento *data* del pacchetto TCP per l'invio di crittografato dell'indirizzo IP del client. Il server verificherà che questo corrisponde all'indirizzo richiedente: se così non fosse scarta il pacchetto e la richiesta

Possibili attacchi:

Denial of Service:

- il demone che gestisce il meccanismo di port knocking, sotto attacco DoS, potrebbe subire malfunzionamenti se non addirittura l'interruzione
- *single point of failure*: c'è il rischio di rimanere definitivamente tagliati fuori dalla macchina

Soluzione:

- implementare un servizio di *monitoring* che controlla il corretto funzionamento del pk-daemon e che si occupa del suo eventuale riavvio
- in casi estremi potrebbe essere necessario garantire un indirizzo IP sicuro da cui effettuare comunque la connessione

Possibili attacchi:

Brute Forcing:

- tentare di indovinare la giusta sequenza con attacchi a forza bruta

Soluzione:

- dato che abbiamo $2^{16} = 65536$ porte le possibili combinazioni sono 65536^n: per n adeguato il risultato è abbastanza grande da scoraggiare questo tipo di attacchi
- implementare un meccanismo che esclude gli indirizzi IP che sbagliano un certo numero di sequenze di knock

Fine