



LINUX
DAY
ITALIA

Sicurezza Informatica

Iptables & Embedded Devices

Giuseppe Augiero



25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it



Agenda

- **Sicurezza informatica**
- **Norme Legislative**
- **Il protocollo IP**
- **Firewall**
- **Le regole di sicurezza**
- **Iptables**
- **Sistemi Embedded**



Sicurezza Informatica

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

IT Security

- In ambito informatico con la parola “Sicurezza” si intende la *sicurezza dell’informazione*.
- La sicurezza informatica definisce le regole per il controllo dell’accesso all’informazione e alle risorse.

Principi di base

Occorre garantire:

- **Confidenzialità:** solo chi e' autorizzato conosce l'informazione.
- **Integrità:** l'informazione non può essere manomessa da chi non e' autorizzato.
- **Disponibilità:** l'informazione e' disponibile per chi ha l'autorizzazione ad usarla.
- **Non ripudiabilità:** il mittente non può disconoscere la paternità del messaggio, cioè non può negare di aver inviato il messaggio.

Costo della sicurezza

- Esiste un conflitto tra sicurezza e facilità di utilizzo di un computer.
- La sicurezza è considerata un costo e non un beneficio.
- Non si comprende il valore dei dati da proteggere.
- Quanto costa non adottare la “sicurezza”?

Costi vivi

I costi associati alla sicurezza sono:

- Selezionare, formare e mantenere personale qualificato.
- Acquistare tecnologia hardware e software.
- Aggiornamento della tecnologia.
- Aumento della complessità operativa ed organizzativa, incremento dell'overhead e degrado delle performance del sistema (dovuti alla tecnologia).

Tuttavia questi costi sono inferiori al costo che l'organizzazione sosterrrebbe in caso di compromissione del sistema.

Da dove iniziare?

- La definizione della politica di sicurezza non può che partire da una **analisi dei rischi**.
- L'analisi dei rischi deve individuare i punti critici.
- I punti critici rappresentano elementi di ridotta robustezza dell'infrastruttura informatica.

Robustezza informatica

- La robustezza di un componente è la capacità di **non danneggiare** il sistema in cui è inserito quando vengono violate le specifiche del componente stesso.
- **Violazione delle specifiche** significa:
 - input diversi da quelli specificati
 - risorse diverse da quelle specificate

Essere sicuri

- **E' inutile cercare di essere impenetrabili, occorre essere costosi (tempo e danaro) da penetrare.**
- **Per proteggere un bene non si dovrebbe mai spendere di più del valore reale del bene stesso.**
- **La sicurezza di un sistema può essere paragonata ad una catena. La misura del livello di sicurezza dell'intero sistema è determinato dalla robustezza dell'anello più debole della catena.**

Sicurezza relativa

- La nozione di sicurezza è un qualcosa di relativo e non di assoluto. Non esiste un sistema sicuro in assoluto.
- La sicurezza è un concetto relativo. “Il sistema A è più sicuro del sistema B”. Il corretto quesito da porsi dovrebbe essere: **“Il sistema è sufficientemente sicuro da sostenere il mio business?”**

Usabilità

- **Sicurezza ed usabilità sono spesso in antitesi**
- Il sistema più usabile è quello privo di misure di sicurezza. Un sistema completamente sicuro è un sistema che opera localmente, staccato dalla rete, collocato in un bunker, senza finestre, con un plotone di guardie armate e cani ringhiosi dietro del filo spinato e con un sistema di sorveglianza con telecamere. Sistema davvero sicuro, ma chi vorrebbe lavorare in tali condizioni ?
- Bisogna trovare il giusto equilibrio tra usabilità e produttività da un lato e sicurezza dall'altro.

Politiche per la sicurezza

- Tre sono le politiche fondamentali per la robustezza:
 - controlli nell'accesso agli oggetti
 - controlli di identificazione
 - politiche di crittografia
 - per l'identificazione dei soggetti
 - per la confidenzialità dei dati

Risk Assessment

- Il concetto di risk assessment è fondamentale per sviluppare una difesa adeguata.
- Identificazione dei beni.
- Identificazione delle vulnerabilità.
- Identificazione delle minacce e della loro probabilità.
- Identificazione delle contromisure.
- Analisi costi e benefici.
- Sviluppo di politiche e procedure di sicurezza.

Asset

- Per identificare e dare una priorità ai beni (**asset**) informativi aziendali e per sviluppare un'analisi di costo/beneficio è necessario rispondere alle seguenti domande:
 - ❑ Cosa si vuole salvaguardare?
 - ❑ Perché si vuole salvaguardare il bene?
 - ❑ Quale è il suo valore?
 - ❑ Quali sono le minacce?
 - ❑ Quali sono i rischi?
 - ❑ Quali sono le conseguenze della perdita?
 - ❑ Quali sono i possibili scenari?
 - ❑ Quale sarà il costo associato alla perdita delle informazioni o del sistema?

Modelli di sicurezza

- Esistono 3 approcci di base per sviluppare un modello di sicurezza:
 - **“By Obscurity” (occultamento)**
 - **Difesa perimetrale**
 - **Difesa in profondità**
- Per conseguire la sicurezza, in generale le aziende impiegano una combinazione dei tre approcci.

Azioni da intraprendere

- **Prevention**: E' necessario implementare delle misure per prevenire lo sfruttamento delle vulnerabilità.
- **Detection**: E' importante rilevare prontamente il problema; prima si rileva il problema, più semplice è la sua risoluzione.
- **Response**: bisogna sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e le azioni da intraprendere.

Dinamicità

- La sicurezza non ha uno sviluppo statico ma è un processo iterativo.



Analisi del rischio

- Comprensione delle insicurezze.
- Definizione di priorità.
- Implementazione di Sistemi Esperti.
- Occorre effettuare un Trade-Off !!!

Politiche di sicurezza

- Fornire linee guida.
- Soluzioni implementabili.
- Accettabile da parte di tutti.
- Controllare che siano rispettate (audit)
- Responsabilizzare.
- Scegliete gli obiettivi per valutare il trade-off.
- Facilità di utilizzo.
- Valutare i costi.

Progettare la sicurezza

- **Minimi privilegi.**
- **Prevedere diversi livelli.**
- **Prevedere diversi sistemi di sicurezza.**
- **Centralizzare la gestione.**
- **Concentrare l'attenzione sui punti deboli.**
- **Fail-over.**
- **Partecipazione di tutti gli utenti.**

Audit

- **Analisi dei log non e' una operazione banale.**
- **Le ragioni di analisi possono essere:**
 - **controllo delle operazioni effettuate.**
 - **controllo del rispetto delle politiche di sicurezza.**
 - **Ricerca di segni di intrusione.**

Da chi dobbiamo difenderci

- Hackers.
- Crackers.
- Ricercatori di informazioni.
- Procutatori di Denial of Service.
- Virus e Cavalli di Troia.

Motivazioni

- Furto.
- Modifica delle informazioni.
- Odio.
- Motivazioni politiche/religiose.
- Sfida intellettuale.



Norme Legislative

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Legge sulla privacy (196/2003)

- La **legge sulla Privacy**, cita in modo esplicito l'obbligo di adottare delle misure minime di sicurezza per i dati ed i sistemi che trattano elettronicamente tali dati.
- L'articolo 34 e l'allegato B indicano quali sono tali misure minime e la loro attuazione.

Misure minime

- **Sinteticamente le misure minime di sicurezza riguardano:**
 - **Sistemi di autenticazione, tali da controllare l'accesso alle informazioni.**
 - **Sistemi di salvataggio periodico dei dati e loro ripristino.**
 - **Sistemi che mantengano l'integrità dei dati e degli strumenti informatici (Antivirus).**
 - **Sistemi per impedire accessi non autorizzati tramite Rete.**
 - **Gestione e manutenzione degli strumenti informatici utilizzati, sia Hardware che Software.**



Il protocollo IP

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

IP: connectionless

- Un protocollo privo di connessione non stabilisce di per se un percorso coerente per la trasmissione dei dati.
- Non e' necessario, nè probabile che in una rete abbastanza grande e trafficata due pacchetti in sequenza seguano il medesimo percorso tra sorgente e dest.
- IP non richiede che venga riservato un percorso fisico o banda passante nel momento in cui la sessione di comunicazione viene impostata.

Router

- I router rappresentano la chiave del successo per una rete che opera a layer 3 con IP.

I problemi del protocollo IP

- I router ricevono i frame layer 2 in arrivo, li spaccettano, leggono i dati layer 3 e li inoltrano, scartando le informazioni layer 2. Questo meccanismo impedisce verifiche di sicurezza punto-punto.
- I router calcolano, poi, il percorso ottimale tra tutti i percorsi disponibili per raggiungere la destinazione.
- Ogni router si preoccupa soltanto di inviare il pacchetto al router successivo



Firewall

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Firewall

- E' un sistema di protezione perimetrale tra due reti (p.es.lan e Internet).
- Un firewall, è un dispositivo che connette una rete fidata "trusted" (presumibilmente sicura) con una rete non fidata "untrusted" (potenzialmente insicura).
- Tutto il traffico da e verso Internet deve passare da un unico nodo (il firewall).
- Il firewall non deve essere visibile.

I punti di forza

- **Centralizza le politiche di sicurezza.**
- **Centralizza i log e i messaggi di allarme.**
- **Previene il foot-printing.**
- **Permette di usare sistema di strong security.**

Tipologie

- **Packet filters e screening routers.**
- **Application gateways e proxy servers.**
- **Stateful inspection.**
- **Soluzioni ibride.**

Packet Filter

- Un packet filtering firewall esamina la intestazione di ciascun pacchetto (IP) e decide se lasciarlo transitare o di bloccarlo in funzione delle regole definite dall'amministratore del firewall.

Vantaggi

- Economicità e funzioni di packet filtering svolte anche a livello di router.

Svantaggi

- Reporting degli eventi limitato.
- Non controllano lo stato della connessione, ma solo i singoli pacchetti.

Stateful Packet Inspection

- **Mantengono informazioni sullo stato della connessione**
 - **Mantenendo una tabella delle connessioni correnti e dei loro eventi, sono in grado di rilevare sequenze anomale che potrebbero rappresentare degli attacchi.**

Stateful Packet Inspection

Aspetti negativi

- Non effettuano controlli profondi a livello applicazione.
- Non permettono controlli sull'autenticazione utente.

Application Gateway

- Utilizzano un set di proxy, uno per ogni applicazione
- Possono richiedere o no la connessione iniziale
- Possono forzare l'autenticazione utente
- Funzionano da intermediari e ogni sessione è sempre il risultato di due connessioni:
 - Client Firewall
 - Firewall Server
- Consente al Firewall di riscrivere l'IP header
- Non attaccabile con procedimenti basati su routing

Rovescio della medaglia:

- Prestazioni condizionate dalla profondità e complessità dei controlli

Limiti di un Firewall

- Non protegge contro virus e trojan
- Non protegge contro nuovi (sconosciuti) attacchi
- Non protegge contro le connessioni che non lo attraversano (modem)
- Non protegge da cattive o inesistenti policy
- Non protegge da attacchi interni (75%-80%)
- Non protegge da attacchi fisici
- Non può funzionare da unico punto di difesa

Personal Firewall

- A differenza dei firewall perimetrali, il personal firewall e' eseguito direttamente sul s.o. che dovrebbe proteggere.
- E' soggetto alla disattivazione da parte di malware.
- La configurazione e' lasciata agli utenti finali spesso poco esperti.
- Può conoscere quale sia l'applicazione che ha generato il pacchetto.



Policy rule

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Le regole

- Definizione di una lista in cui ogni elemento (regola) definisce se un particolare tipo di traffico deve passare o non passare.
- Possibilità di utilizzare operatori relazionali.
- **E' importante l'ordine delle regole !**

“La filosofia del gioco”

- Il design delle policy di un firewall può seguire uno dei seguenti approcci:
 - permetto, e nego tutto il resto
(+ sicuro)
 - nego, e permetto tutto il resto
(- sicuro)

Le regole d'oro

- **Stealth rule:**

E' buona norma inserire come all'inizio della lista, una regola che rende il firewall invisibile.

- **Clean Up rule:**

Alla fine della lista occorre inserire una regola che neghi tutto il traffico non permesso (drop su catch-all).

Antispoofing e Rfc 1918

Iptables

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Iptables

- Iptables e' parte integrante di netfilter.
- Netfilter e' il framework di manipolaggio pacchetti che mette a disposizione il kernel di Linux.
- Supporto kernel 2.4 e 2.6
- Successore di ipfwadm e ipchains

Come installare Ipt

- Iptables e' parte integrante del kernel 2.4 e 2.6.
- Per usare le funzionalità di iptables occorre attivare il supporto dal Kernel.
- Ricompilazione del Kernel.

Architettura

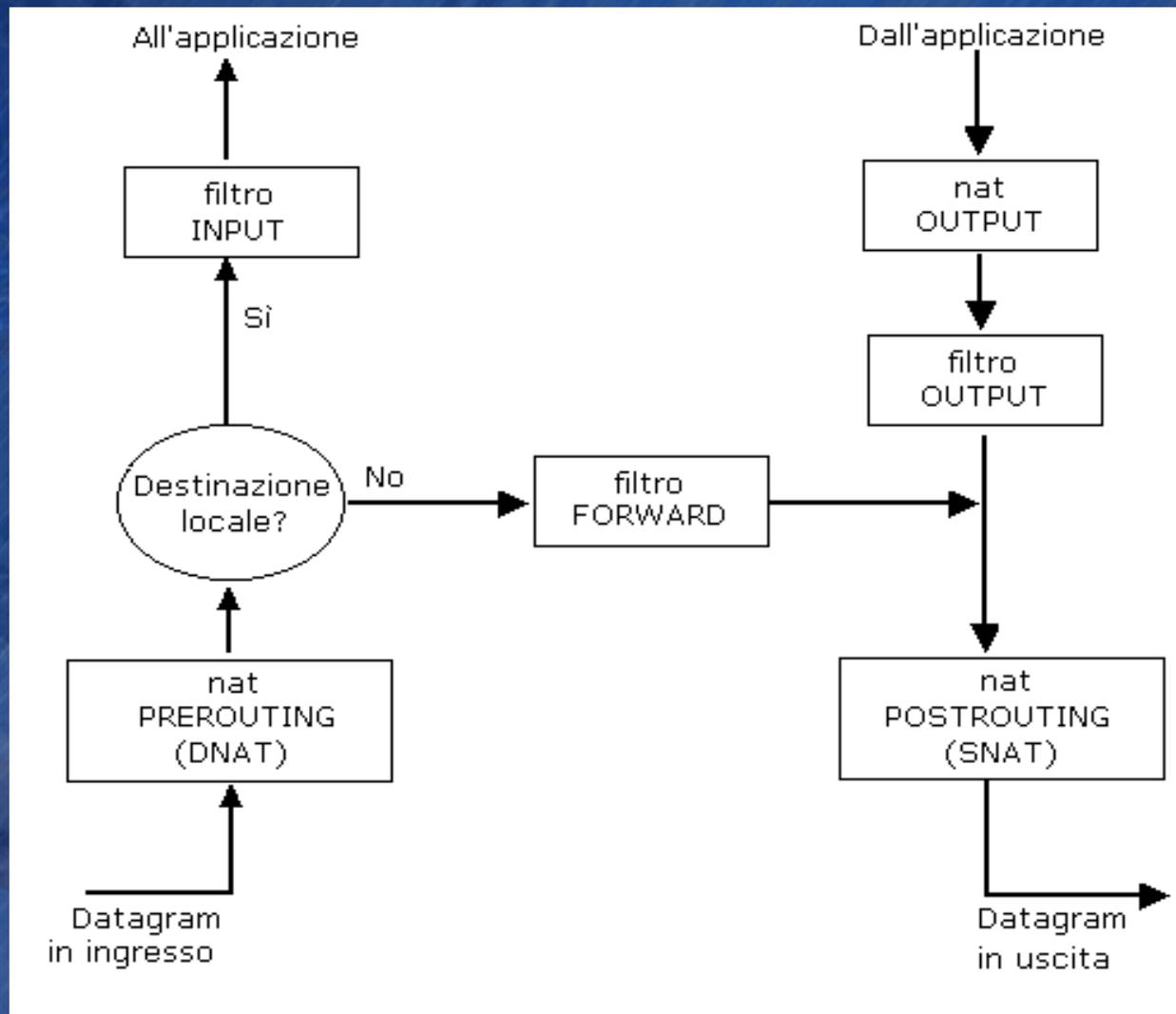
Di default iptable e' composto da 3 **tabelle**:

- Filter
- Nat
- Mangle

Ogni tabella contiene più **catene**.

Ogni catene e' una lista di **regole ordinate**.

Filter



Le policy

- Di default esistono tre catene (Input/Output/Forward).
- Una catena e' un insieme di regole
- Ogni regola definisce cosa bisogna fare con il traffico identificato.
- Se non esiste una regola per il traffico viene applicata la policy generale della catena.

Azioni da intraprendere

- **Accept**
 - **Drop (timeout)**
 - **Reject**
-
- **Il traffico in drop o reject può essere loggato.**

NAT & PAT

- Consente la trasformazione di indirizzi e porte dei pacchetti.
- **SNAT** permette di modificare l'indirizzo IP sorgente.
- **DNAT** permette di modificare l'indirizzo IP di destinazione.

Falso senso di sicurezza

- Il NAT non permette la raggiungibilità universale punto-punto tra gli host connessi ad Internet.
- Un host spesso non e' in grado di iniziare una comunicazione con un host di una rete privata.
- L'isolamento, rispetto ad internet, crea un falso senso di sicurezza.



Sistemi Embedded

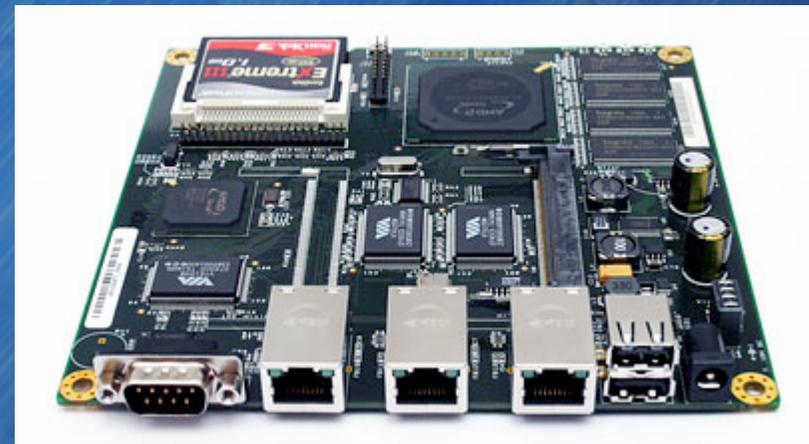
25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Architettura di un firewall

- Il firewall può essere un prodotto hardware o software.
- Se il firewall è software occorre “*bastionizzare*” la macchina su cui gira.
- In generale la configurazione di un firewall e' una operazione complessa.

Soluzioni Embedded

- Architettura hardware nota.
- Basso consumo.
- Nessuna parte meccanica in movimento.
- Maggiore affidabilità.
- Dimensioni ridotte.
- Dissipazione nulla.
- Basso costo.



Interfacce di rete ?

- Fino a 3 interfacce di rete Ethernet
- 2 MiniPci
 - 2 sk wifi
 - 2 sk isdn
 - 2 HSSI
- 1 seriale
- 2 USB



Processore?

- Scelta da non sottovalutare.
- Meglio x86.
- Sistemi crittografici.



HD?

- No grazie.



Sistema Operativo?

- Soluzioni ah hoc.
- Utilizzo di una distribuzione conosciuta.
- Attenzione alle immagini che caricate sul vostro sistema embedded.

Expertise

- Il modo migliore per garantire la sicurezza di una macchina è quello di padroneggiare pienamente tutto quello che avviene su di essa.
 - Avere la conoscenza di come vengono avviati e gestiti tutti i servizi.
 - Controllare che siano presenti tutti e soli i processi necessari alle nostre esigenze.
 - Saper interagire con il software in modo da poterlo configurare ad hoc.

Hardening

- **Disabilitare tutti i servizi di rete.**
- **Disinstallazione di tutti i programmi non necessari.**
- **Syslog remoto.**
- **Login limitato in SSHv2.**
- **Utilizzo di chroot & c.**
- **RamDisk.**
- **Halt Firewall.**

Minimi permessi

- Uno dei modi migliori per cercare di limitare i danni dovuti ad una intrusione è quello di fornire ad ogni processo il minimo dei permessi che gli servono per svolgere con successo il suo compito.
- Il dropping dei privilegi va associata ad una attenta gestione dei permessi dei file.

Sicurezza Locale

- Se esistono utenti che hanno accesso alla macchina, occorre renderla sicura anche dall'interno.
- E' possibile impedire una scalata verso root.
- Controllare la presenza del bit suid sui binari presenti all'interno del sistema.



Il Futuro

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

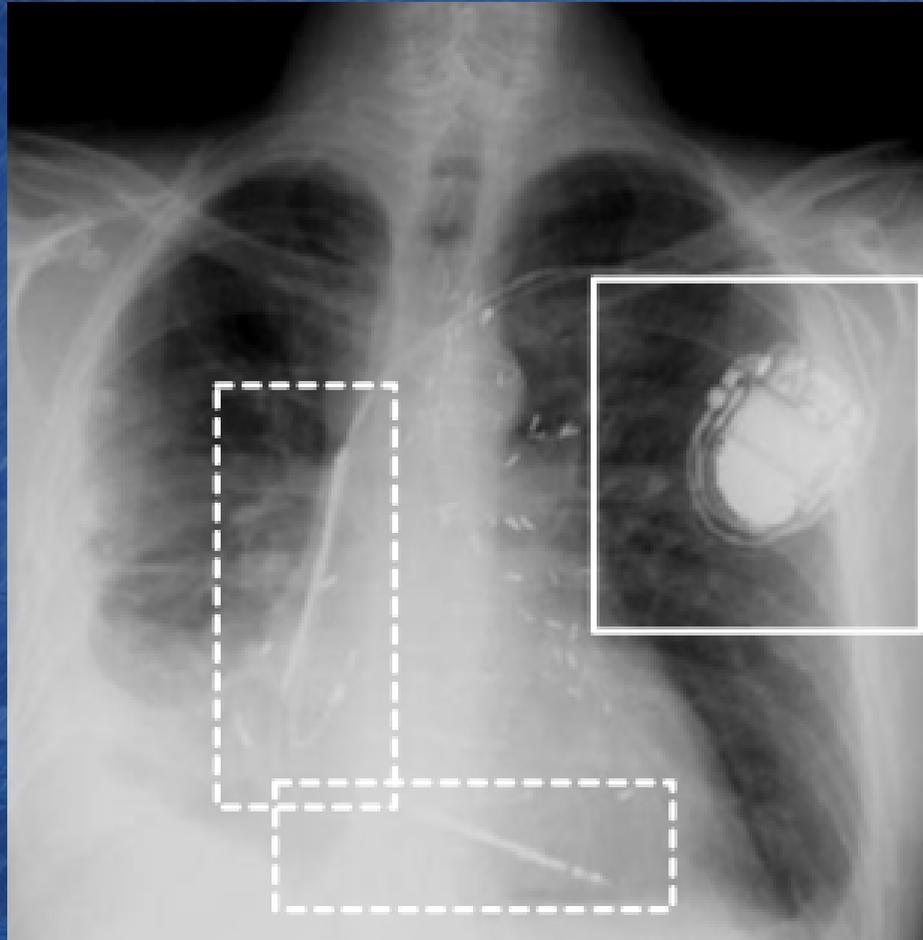
Dubbio amletico

- **Saranno i medici a occuparsi di security o gli esperti di security a occuparsi di medicina?**

Dispositivi ICD e IMD



ICD



Telemetria



25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Home monitoring



Domande?



Risposte!

- **Giuseppe Augiero** giuseppe@augiero.it

Grazie per l'attenzione

- Queste trasparenze (*slide*) sono protette dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo e il copyright delle *slide* (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica, testo, tabella, disegno) sono di proprietà dell'autore.
- Le *slide* possono essere riprodotte e utilizzate liberamente dagli istituti di ricerca, scolastici e universitari italiani afferenti al Ministero dell'Istruzione, dell'Università e della Ricerca per scopi istituzionali e comunque non a fini di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altro utilizzo o riproduzione, completa o parziale (ivi incluse, ma non limitatamente, le riproduzioni su supporti ottici e magnetici, su reti di calcolatori e a stampa), sono vietati se non preventivamente autorizzati per iscritto dall'autore.
- L'informazione contenuta in queste *slide* è ritenuta essere accurata alla data riportata nel frontespizio. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, etc. In ogni caso essa è soggetta a cambiamenti senza preavviso. L'autore non assume alcuna responsabilità per il contenuto delle *slide* (ivi incluse, ma non limitatamente, la correttezza, la completezza, l'applicabilità, l'adeguatezza per uno scopo specifico e l'aggiornamento dell'informazione).
- In nessun caso possono essere rilasciate dichiarazioni di conformità all'informazione contenuta in queste *slide*.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata fedelmente e integralmente anche per utilizzi parziali.

