Applicazioni di tecniche crittografiche e steganografiche alle comunicazioni in rete ed agli archivi di dati

Gianni Bianchini
giannibi@firenze.linux.it

Convegno “E-Privacy: riservatezza e diritti individuali in rete”

Firenze, Palazzo Vecchio - 27 Aprile 2002

Sommario

- Su disco. File system ed archivi crittografici
  - International Linux kernel extension, PPDD
  - BestCrypt, Scramdisk
  - UMPF
- Cancellazione sicura
- File system ed archivi steganografici
  - StegFs
  - Outguess / Stegdetect
- In rete. File system crittografici distribuiti
  - SFS
- Supporto crittografico per servizi di rete generici
  - Secure Sockets Layer (SSL/TLS)
  - Secure Shell (SSH)
  - IPSec e reti private virtuali (VPN)

Su disco...

File system crittografici - Motivazioni

- Riservatezza dell'informazione contenuta in memorie di massa
  - Assenza di controllo d'accesso sul sistema (DOS, Windows 9x/ME)
  - Controllo d'accesso insufficiente
  - Possibile compromissione dell'account utente o amministrativo
  - Privacy nei confronti degli account amministrativi legittimi
  - Sistema non protetto dall'accesso fisico
  - Sottrazione dei supporti
  - Sottrazione dei backup
- Requisiti / desiderata
  - Dispositivi che permettano la protezione dati con l'uso di crittografia forte rivelandoli ai soli utenti legittimi
  - Massima trasparenza nell'uso

Linux International Kernel Extension

- Aggiunta di funzionalità crittografiche al dispositivo loopback
  - ⋆ L'informazione è sottoposta a cifratura di blocco e memorizzata all'interno di file regolari (container) che vengono presentati al sistema come dispositivi fisici (loopback devices)

1. Creazione del container e creazione file system (ext2, vfat, ...)
2. Mount del dispositivo a fronte della corretta passphrase

- API crittografica generica in modalità kernel
- Supporto modulare per vari algoritmi di cifratura (3DES, Twofish, Blowfish, IDEA, Rijndael, ecc.) e di digest (MD5, SHA1)
- URL: ftp://ftp.kernel.org/pub/linux/kernel/crypto/
- Licenza: GPL

PPDD

- Basato sulle funzionalità del crypto loopback (Linux)
- Possibilità di cifratura dell'intero insieme di filesystem del sistema (incluse partizioni di scambio per memoria virtuale)
- Avvio del sistema da filesystem crittato (master passphrase)
- Insieme di utilities per crittazione / decrittazione fuori linea dei volumi, gestione passphrase, verifica integrità
- URL: http://linux01.gwdg.de/ alatham/ppdd.html
- Licenza: GPL

BestCrypt

- Piattaforma Linux / Windows 9x/NT/2k
- “Container” visibili al sistema sotto forma di device (Linux) o unità logiche (Win) a fronte di passphrase corretta
- Formato cross-piattaforma del container
- Algoritmi di cifratura di blocco: DES, 3DES, Blowfish, Twofish, IDEA, Rijndael, ecc.
- Supporto per container “nascosti” (steganografici) nello spazio libero
- Necessità di supporto a livello kernel
- URL: http://www.jetico.com
- Licenza: Proprietaria con sorgente aperto (evaluation 30 gg.)

Scramdisk

- Piattaforma Windows 9x
- Volumi crittati visibili come unità logiche con supporto in
  - File regolari
  - Partizioni FAT o raw
  - File audio (steganografico)
- Supporto per vari algoritmi di cifratura di blocco e stream
- URL: http://www.scramdisk.clara.net
- Licenza: Liberamente distribuibile ed utilizzabile, sorgente aperto

UMPF

- Piattaforma *nix
- Opera a livello dei singoli file
- Non richiede supporto a livello kernel né accesso privilegiato (mount)
- Accesso trasparente agli archivi crittati
  - Wrapping delle funzioni di libreria di accesso ai file con riconoscimento e sottoposizione a cifratura/decifratura stream degli archivi di tipo umpf
- Licenza: GPL
- Abbiamo qui l'autore!!! :)

Cancellazione sicura

- Le funzioni di cancellazione file dei S.O. in generale modificano le sole informazioni di allocazione del disco e non rimuovono i dati fisicamente. La sovrascrittura è solo occasionale
  - Paradosso: si può vanificare l'utilità degli archivi crittati
- Altri "serbatoi" d'informazione sensibile
  - Cache dei browser
  - Contenuto di file o partizioni di scambio per la memoria virtuale
- Paranoia: isteresi del supporto - Riscritture multiple
- Software per cancellazione sicura
  - Kremlin, Scorch, BCWipe (Win)
  - Secure deletion kernel patch, Wipe (Linux)

Steganografia - Generalità

- Obiettivo: celare non solo il contenuto dell'informazione ma la sua stessa esistenza, potendola negare con ragionevole certezza
- Approccio ideale: "nascondere" dati (e.g. testo) in altri dati di tipo diverso (contenitori) senza che questi ultimi assumano connotazioni tali da rivelarne la presenza. I dati divengono evidenti solo a fronte di una chiave di lettura
- Impiego tipico
  - ⋆ Ambienti dove l'uso della crittografia è ristretto
  - ⋆ Marchiatura digitale (watermarking) (immagini, audio)
- Il messaggio celato è soggetto a degradazione con la modifica del contenuto "originale" (nessun meccanismo, se non la chiave, può rivelarlo)
- Esistono tecniche di stegoanalisi volte ad identificare le "tracce" che il procedimento steganografico lascia nel messaggio, in modo indipendente dalla conoscenza dei dati originali. Necessità di robustezza

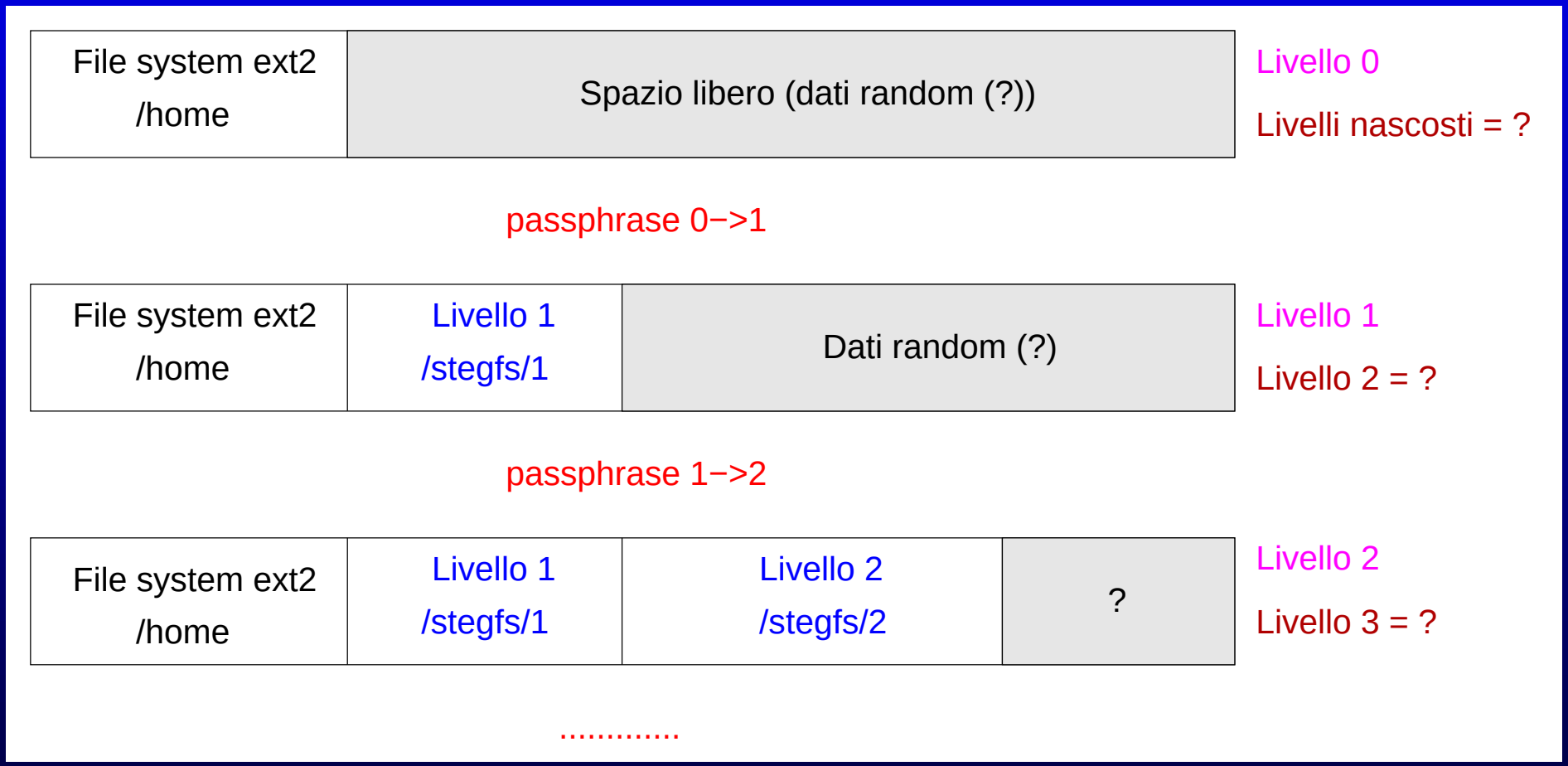
Steganografia - Approcci

- Approccio sostitutivo: modificare i dati del contenitore in modo che questi contengano il messaggio nascosto subendo alterazioni minime
  - Esempio: codifica all'interno di un segnale audio digitale a 16 bit
    - Il bit meno significativo di ogni campione è sostituito un bit del cifrato
    - 128 bit per ogni carattere
    - La presenza del cifrato è tanto meno riconoscibile quanto più rumoroso è il segnale di partenza
- Approccio selettivo: ripetizione di un esperimento con esito aleatorio finché non si verifica una condizione desiderata
  - L'esito dell'esperimento è il contenitore, la condizione il messaggio nascosto
  - Esempio: acquisizione di un'immagine da scanner
- Approccio costruttivo: applicato a segnali rumorosi, mira a sostituire al rumore esistente un contenuto segreto con caratteristiche statistiche analoghe al rumore

File system steganografici - StegFS

- Piattaforma Linux (2.2.x)
- Aggiunta di uno o più livelli “nascosti” a regolari filesystem ext2 sullo spazio non allocato, rivelabili a fronte della corretta passphrase
- Ad ogni livello, risulta ragionevolmente complesso rivelare l’esistenza dei livelli successivi
- Ogni livello, una volta rivelato, viene visto come una partizione
- La modifica dei dati contenuti in un livello *può* danneggiare i livelli successivi
- La presenza del driver sul sistema può essere giustificata dalla presenza del solo primo livello
- Effettua cancellazioni sicure

File system steganografici - StegFS



- URL: http://www.mcdonald.org.uk/StegFS
- Licenza: GPL

Archivi steganografici - Outguess

- Piattaforma: varie
- Incapsulamento di dati nei bit ridondanti di vari formati (immagini jpeg)
- Considerato immune ai test steganalitici statistici conosciuti
- Fornisce una misura della rivelabilità della presenza del contenuto
- Stegdetect - Tool di steganalisi per rivelare la presenza di contenuto steganografico generato da vari algoritmi
  - ⋆ Usato in congiunzione con tool per attacchi a dizionario (Stegbreak)
- URL: http://www.outguess.org
- Licenza: BSD

In rete...

File system crittografici distribuiti

- Riservatezza dei dati su filesystem di rete (NFS, NetBIOS, ecc.)
  - Assenza di supporto crittografico $\Rightarrow$ lettura del contenuto degli archivi mediante intercettazione del traffico di rete “sniffing”
  - Procedure di autenticazione del client presso il server deboli e insicure
  - Modifica non autorizzata del contenuto degli archivi mediante attacchi network-based
- Necessità di
  - Meccanismi di autenticazione host e utente crittografici a chiave pubblica e gestione sicura delle file handle
  - Crittazione del contenuto in transito
  - Verifica dell’integrità

Self-Certifying File System (SFS)

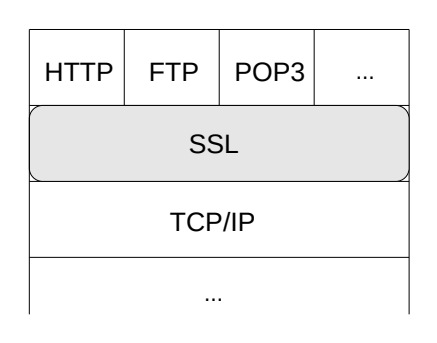
- Piattaforma *nix
- Controllo completamente decentralizzato
- No supporto kernel, uso dell'infrastruttura NFS3 locale
- URL: http://www.fs.net
- Licenza: GPL
- Altri: CFS, TCFS

Secure Sockets Layer (SSL/TLS)

- Fornisce funzioni generiche per le transazioni sicure in rete
  - Autenticazione a chiave pubblica
    - Autenticazione del server presso il client
    - Autenticazione del client presso il server (opzionale)
    - Supporto certificati digitali firmati da C.A.
  - Crittazione della sessione
    - Privacy del contenuto della transazione
    - Supporto di vari algoritmi per le diverse applicazioni
  - Integrità dei dati
    - Protezione da corruzione dei dati (intenzionale o meno)
    - Coerenza della transazione
- Soggetto a tecniche di analisi del traffico

Secure Sockets Layer (SSL/TLS)

- Opera tra i livelli applicazione e trasporto



- Trasparenza al protocollo di applicazione
- Applicazioni lato server con supporto integrato (Apache, IIS)
- Wrapper generici (Stunnel, http://www.stunnel.org)
- Librerie di sviluppo e programmi di supporto (OpenSSL, http://www.openssl.org)

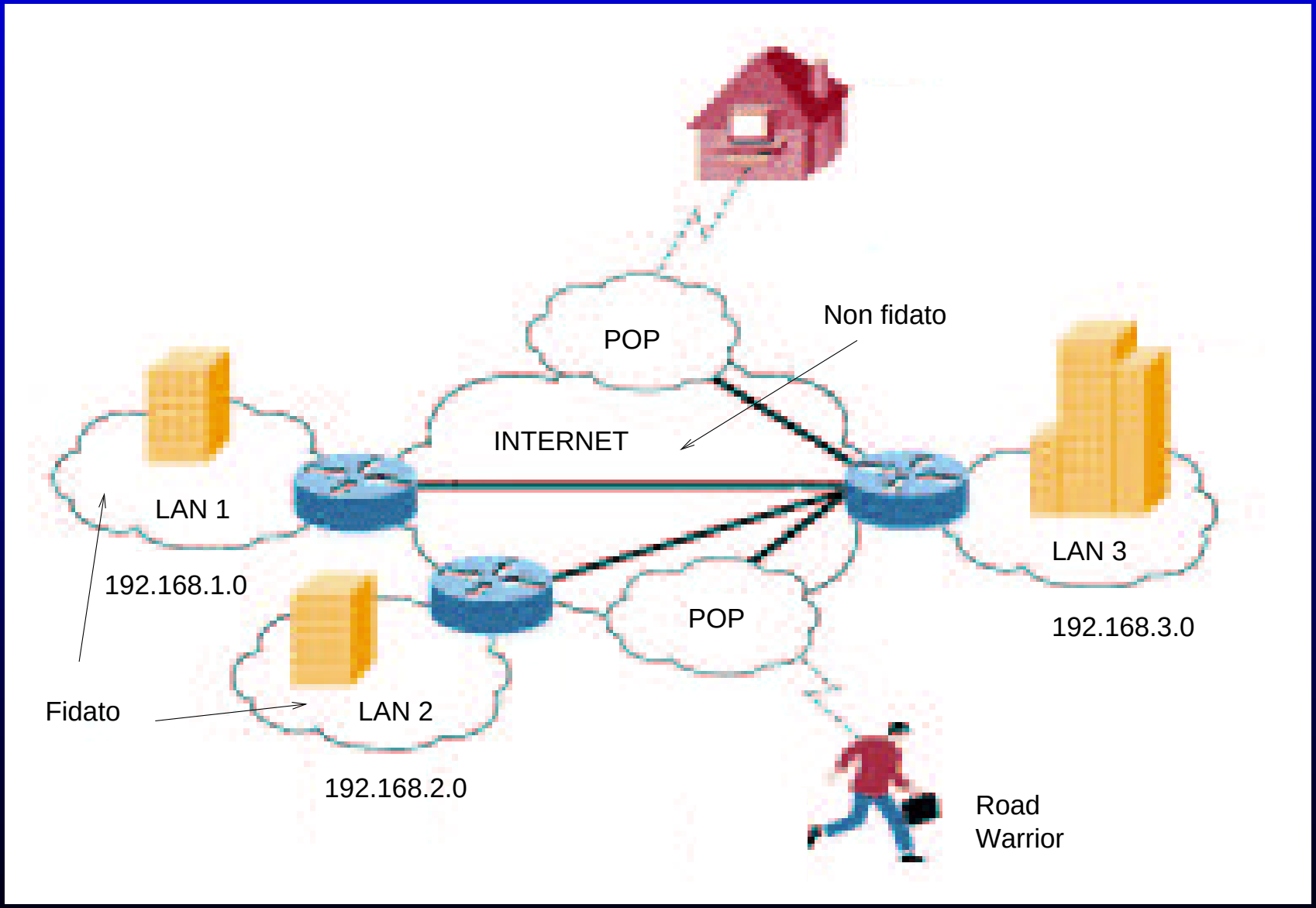
Secure Shell (SSH)

- Accesso interattivo sicuro a sistemi (tipicamente *nix)
  - Alternativa a telnet e servizi BSD r*
  - Copia sicura di file (SCP)
- Supporto per
  - Autenticazione a chiave pubblica (RSA in SSH-1, DSA-DH in SSH-2)
  - Cifratura della sessione (3DES, Blowfish, ...)
  - Integrità dei dati (CRC in SSH-1, HMAC in SSH-2)
  - Creazione tunnel generici TCP peer-to-peer crittati (port forwarding)
  - Incapsulamento sessioni X-Window
- Implementazioni
  - OpenSSH - http://www.openssh.org - Licenza BSD
  - SSH - http://www.ssh.com - Licenza proprietaria

IPSec

- Supporto per comunicazioni sicure tra reti IP con funzioni di
  - Autenticazione a chiave pubblica dei sistemi partecipanti (IKE, DH-RSA)
  - Autenticazione dati in transito (AH, HMAC)
  - Autenticazione e crittazione del traffico (ESP, 3DES block cypher)
- Realizzazione di “tunnel” sicuri a livello IP tra reti fidate attraverso reti non fidate (e.g. Internet)
- Massima generalità e trasparenza all’utente
  - Indipendenza dai protocolli di alto livello
  - Indipendenza dalla tecnologia di rete (livelli inferiori)
  - Nessuna necessità di supporto da parte del singolo protocollo
- Applicazioni tipiche
  - Creazione di reti private virtuali (VPN)
  - Road warriors

Reti Private Virtuali (VPN)



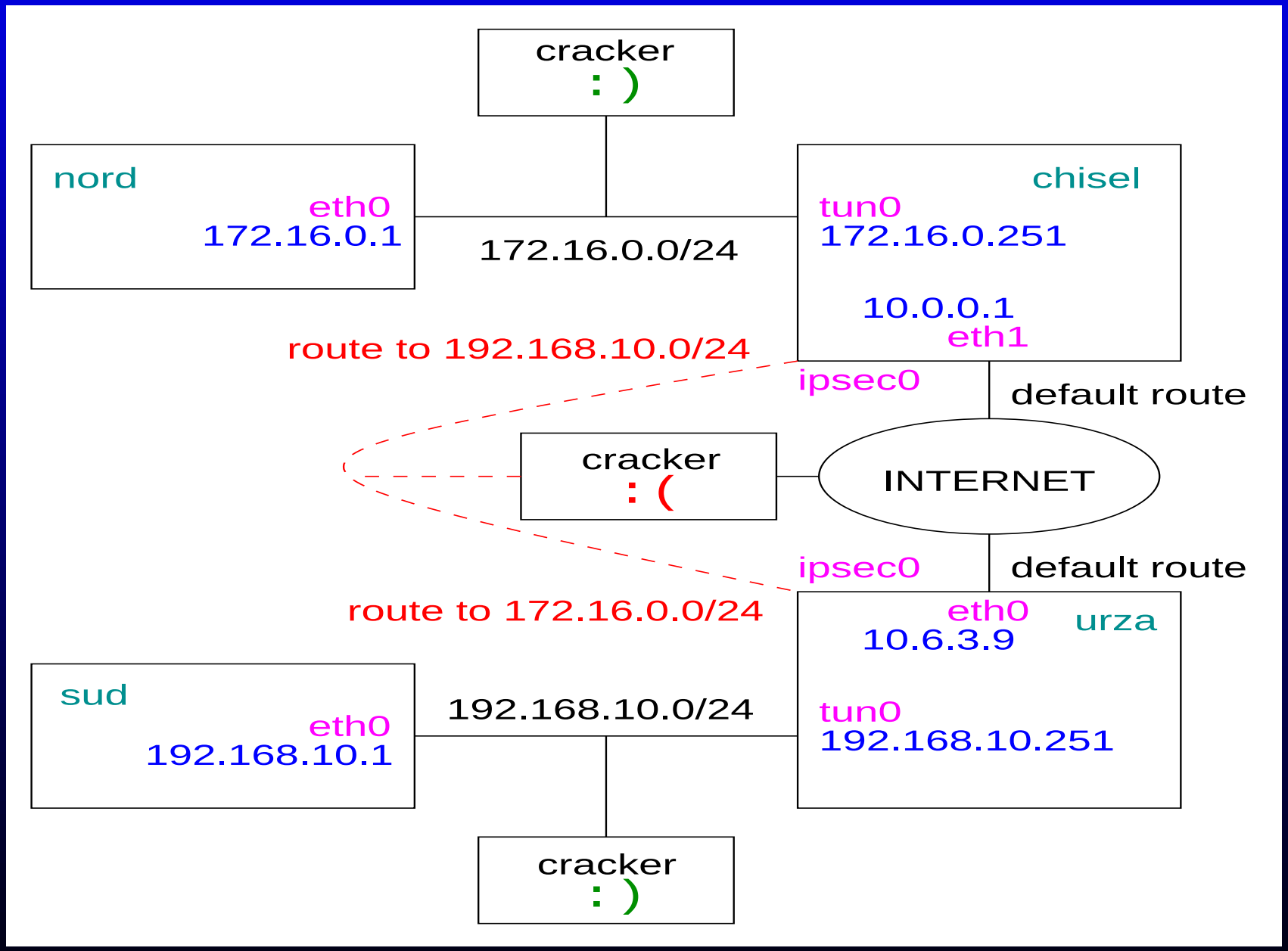
IPSec

- Prevenzione “in blocco” di vari attacchi ai protocolli di livello superiore (e.g. man-in-the middle)
- Sottopone ad autenticazione/crittazione l’intero traffico IP tra le sole reti partecipanti e *non* quello all’interno di esse
  $\Rightarrow$ Non realizza una protezione end-to-end (PGP, HTTP/SSL)
- Soggetto a tecniche di analisi del traffico

IPSec - Opportunistic Encryption

- Permette la creazione di un tunnel crittato senza che le reti partecipanti “si conoscano”, ovvero siano configurate a priori per prendere parte ad una stessa VPN
- L’host verifica la disponibiltà del peer all’O.E. e se possibile la utilizza
- Uso di un record DNS per lo scambio delle chiavi pubbliche RSA di autenticazione
  - ⋆ Sicurezza demandata alla sicurezza del sistema DNS (Secure DNS)
- Impiego estensivo $\Rightarrow$ incremento notevole del livello di sicurezza e di riservatezza del traffico dell’intera rete Internet (ambiente dove la privacy è il “default” per qualunque tipo di transazione)

IPSec (FreeS/WAN) - Esempio



IPSec - Implementazioni

- Libere e/o open source
  - FreeS/WAN - Linux - http://www.freeswan.org
  - Pipsecd, Ipnsec - Linux
  - KAME - *BSD - http://www.kame.net
  - OpenBSD - integrato - http://www.openbsd.org
  - NetBSD - integrato - http://www.netbsd.org/Documentation/network/ipsec
  - IPSec for FreeBSD - http://www.r4k.net/ipsec
- Supporto integrato in SO proprietari
  - MS Windows 2000
  - Sun Solaris 8
  - HP-UX 11i
- Supporto integrato in gran parte dei prodotti firewall, router, VPN di tipo commerciale