UNIVERSITÀ DEGLI STUDI DI CATANIA

FACOLTÀ DI INGEGNERIA

Dipartimento di Ingegneria Informatica e delle Telecomunicazioni

Marco Orazio Garozzo

Monitoraggio del traffico di posta elettronica

TESI DI LAUREA

Relatore:

Chiar.mo Prof. Ing. Aurelio La Corte

ANNO ACCADEMICO 2004-2005

Un sogno si è avverato.

Una parte della mia vita è stata dedicata al raggiungimento di questo difficile obiettivo. I miei sforzi, le mie difficoltà sono però state sempre accompagnate dalle persone a me care. Grazie a mio Padre Antonio e mia Madre Giovanna che con il loro sacrificio ed entusiasmo hanno permesso i miei studi.

Dedico il lavoro di questi anni alla mia compagna per la vita, Manuela, che pazientemente e con dedizione è stata al mio fianco, nella gioia e nella difficoltà.

Catania, Aprile 2006

Indice

1 – Introduzione

Lo sviluppo del “governo elettronico” (e-government) comporta profondi cambiamenti sia di tipo organizzativo che di tipo tecnico all’interno della pubblica amministrazione. si intende il processo di informatizzazione della pubblica amministrazione. L’e-goverment cambia il modo di lavorare della pubblica amministrazione ed il modo di comunicare della stessa, sia all’interno che nei confronti del cittadino.

Se da una parte la diffusione delle tecnologie dell’informazione in tutti i settori della vita quotidiana agevolano la penetrazione di tali tecnologie nella pubblica amministrazione, le stesse tecnologie pongono in evidenza nuove problematiche. Basti pensare al problema della sicurezza dei dati sensibili e personali trattati con strumenti automatici, o alla possibilità che le tecnologie dell’informazione possano essere usate per scopi non leciti.

Tra gli strumenti informatici di maggiore diffusione ed interesse ricopre un ruolo strategico la posta elettronica. Essa è diventata ormai uno strumento di comunicazione molto diffuso grazie ai suoi pregi di economicità, istantaneità ed affidabilità. L'evoluzione di questa semplice ed efficiente tecnologia, proprio di recente, ha corretto i molti deficit in termini di sicurezza che tale sistema presentava dalla nascita.

Un così formidabile mezzo non poteva quindi non avere numerose applicazioni in campo economico, amministrativo e gestionale, ed in particolare nell’e-

government, utili a gestire con maggiore razionalità una mole di dati e di comunicazioni sempre in crescita. Il recente "codice dell'amministrazione digitale" ha sancito l'importa di tale strumento nella comunicazione tra pubbliche amministrazioni e nelle comunicazioni tra imprese e cittadini con la stessa pubblica amministrazione.

Se da un lato però l'evoluzione tecnologica spinge in avanti il benessere dei cittadini, dall'altro, questa può essere utilizzata per fini che ledono i cittadini stessi; per esempio, la posta elettronica può consentire ad individui insospettabili di costituire cellule di gruppi terroristici anche senza essersi mai incontrati. Questi pericoli insiti nella natura stessa dello strumento comunicativo potrebbero spingere i vari governi nazionali a sviluppare un concetto di controllo delle telecomunicazioni abbastanza ingerente nella sfera sociale dei cittadini: secondo il principio di sicurezza nazionale lo Stato potrebbe controllare ogni email alla ricerca di contenuti potenzialmente dannosi. Il rischio che si corre in questi casi è che comunicazioni intercettate dallo Stato possano essere utilizzate per fini non assimilabili a sicurezza nazionale: si potrebbero creare elenchi di persone discriminabili per fede, ideologia politica, vita sociale, scelte commerciali, etc.

Rischi ancor più grandi che si possono correre nell'utilizzo della posta elettronica sono anche quelli dovuti ai malintenzionati che potrebbero intercettare le nostre email, forzare l'accesso alla casella di posta o utilizzare maliziosamente l'identità della vittima.

Si evidenzia, quindi, la necessità di tracciare una linea di confine tra il diritto alla propria privacy e la necessità di garantire stabilità e sicurezza alla totalità dei cittadini.

Obiettivo di questa tesi è di studiare preliminarmente il problema della "tracciatura" delle informazioni relative all'uso della posta elettronica e, al contempo, sviluppare uno strumento di controllo per il fornitore del servizio di posta elettronica in una rete telematica che adempia gli attuali obblighi imposti dallo Stato Italiano sulla sicurezza, rispettando la riservatezza dei contenuti delle comunicazioni personali.

In particolare si individua lo scenario di una pubblica amministrazione che fornisce ai propri dipendenti un servizio di posta come previsto dalle recenti linee guida del governo sull'e-government. E' da sottolineare che tale scelta risulta una estensione del caso di ente privato, avendo, quest'ultimo, minori doveri verso il cliente e le istituzioni.

La tematica affrontata costituisce solo una parte degli adempimenti necessari, allo stato attuale, che una pubblica amministrazione deve implementare in tema di sicurezza. L'insieme delle politiche attuate viene raccolto in un documento denominato "documento programmatico di sicurezza", in esso sono anche individuate le responsabilità e gli obblighi dei soggetti interessati (amministratore del sistema e utenti).

Si vuole sottolineare che il fine della tesi, esistendo già soluzioni tecniche per adempiere gli obblighi di legge, è lo sviluppo di un approccio alternativo al problema in esame.

2 – Scenario di riferimento normativo italiano

Il ruolo dell'Ingegnere, nella realizzazione di un servizio di comunicazione quale la posta elettronica, è di analizzare i problemi e le esigenze dei soggetti interessati fornendo soluzioni tecniche adeguate. Quest'azione è però imprescindibile dall'interpretazione della normativa che può essere complessa e controversa, avendo principi spesso contrastanti.

A confronto ci sono proprio due grossi temi contrastanti: da un lato la riservatezza delle comunicazioni che non può essere violata neppure da chi gestisce il sistema, dall'altro la necessità di effettuare un controllo, volto ad impedire un uso improprio dello strumento comunicativo.

Per trovare il punto di incontro, su cui impostare i termini del problema, è necessario un attento esame delle leggi di riferimento:

- D.L. 144 del 16/8/2005 – "Misure di sicurezza contro il terrorismo". Convertito nella legge 155 del 31 luglio 2005 [3] [4].
- D. Lgs 196 del 30/6/2003 – "Codice in materia di protezione dei dati personali" (ex 675/96) [5].
- D.L. 354 del 24/12/2003 – "Conservazione dei dati di traffico per altre finalità". Convertito nella legge 45 del 27 febbraio 2004 [6] [7].
- Direttiva del Presidente del Consiglio dei Ministri 16/01/2002 - "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" [8].

- Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003 “Impiego della posta elettronica nelle Pubbliche Amministrazioni” [9].
- D. Lgs 82 del 07/03/2005 – “Codice dell’amministrazione digitale” [10].
- Direttiva del Ministero per l’innovazione e le tecnologie del 18/11/2005 “Linee guida per la Pubblica Amministrazione digitale” [11].

DL 144 DEL 16/8/2005

Questo decreto fornisce una serie di direttive eterogenee, volte a integrare quelle già esistenti in tema di sicurezza.

Il legislatore, mediante tale norma, consolida il principio per cui si deve poter ricondurre ogni azione o comunicazione effettuata da terminali nel territorio italiano ad individui identificabili.

Di interesse, ai fini del campo di studio, è l’art. 6 che recita: “[…] è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi e dei servizi, debbono essere conservati fino al 31 dicembre 2007 dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico […]”.

Di fatto, tale legge impone al fornitore di un servizio di posta elettronica l'obbligo di registrare e mantenere sino ad una certa data (non è detto che in futuro il legislatore trasli nel tempo tale scadenza) mittenti, destinatari e marche temporali di ogni email in entrata o uscita dai propri server, evitando categoricamente la consultazione o addirittura la registrazione dei contenuti scambiati dagli utenti. Questo aspetto è ridondantemente presente in altre leggi preesistenti che spesso però risultavano inapplicate. Questa norma vuole sottolineare l'importanza investigativa che potrebbero avere i dati sul traffico per la salvaguardia dei cittadini dal terrorismo internazionale.

D. LGS 196 DEL 30/6/2003

Questo decreto sostituisce e amplia la famosa legge sulla privacy (legge 625/96). Esso impartisce direttive sul trattamento, sulla tipologia dei dati trattati, sugli addetti al trattamento, nonché sulle pene inflitte ai trasgressori. In linea generale sancisce il diritto da parte dell'utente di conoscere e chiedere la modifica o la cancellazione di qualunque dato riguardante la propria persona registrato da terzi. Tale legge fornisce la definizione di "Comunicazione elettronica" come "[…] *ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico* […]", ma soprattutto di "dati relativi al traffico" come "[…] *qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione* […]" e di "posta elettronica come "[…] *messaggi contenenti testi, voci, suoni o immagini*

trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza […]".

Secondo tale codice, il titolare del trattamento (che nel caso in esame coincide con il fornitore del servizio di posta) non ha l'obbligo *del consenso* al trattamento dei dati relativi al traffico da parte del soggetto fruitore del servizio in quanto per l'art. 24 comma 1: "[…] *Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento: è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria* […]" e nella fattispecie la legge di riferimento è proprio il D.L. 144 esaminato in precedenza.

Il titolare non ha nemmeno l'obbligo *di informare* l'utente della raccolta di queste informazioni in quanto per l'art. 13, comma 2 "[…] *L'informativa* […] *puo' non comprendere gli elementi gia' noti alla persona che fornisce i dati o la cui conoscenza puo' ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalita' di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati* […]".

Esaminando tale legge, potrebbe fuorviarci l'art. 123 che recita: "[…] I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono piu' necessari ai fini della trasmissione della comunicazione elettronica […]. Il

trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, […]. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento. […]".

Tale articolo parrebbe imporre limiti stringenti alla conservazione dei dati e darebbe all'utente il potere di chiederne la cancellazione, ma una rilettura attenta suggerisce che questa possibilità si riferisce solamente ai dati trattenuti solo a fini commerciali e di fornitura del servizio.

Leggendo oltre si ha una riconferma di quanto detto nell'art. 132: "[…]Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi, per finalita' di accertamento e repressione di reati, secondo le modalita' individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante. […]".

L'analisi di tale legge quindi sottolinea due adempimenti a cui il gestore del servizio non è tenuto: chiedere il consenso alla registrazione dei dati sul traffico e dare conoscenza che questa registrazione avviene. Permane comunque l'obbligo di fornire una lettera informativa sulle condizioni del servizio e

richiedere il consenso per il trattamento dei propri dati personali per la registrazione del servizio per gli utenti che non rientrano nella definizione di dipendente (per cui non si dispongono i dati anagrafici disponibili all'assunzione).

La 196 contiene un altro principio sul trattamento dei dati personali: cioè che le "misure minime" di protezione del dato da qualunque evento sono solo una parte degli accorgimenti obbligatori in materia di sicurezza (art. 33); principio di importanza tale da indurre il legislatore a prevedere anche una sanzione penale. In materia si distinguono due distinti obblighi [12]:

a) l'obbligo più generale di ridurre al minimo determinati rischi. Occorre cioè custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.

Resta in vigore, oltre alle cosiddette "misure minime", l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze, avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi (art. 31). L'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola, inoltre, i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice in materia di protezione dei dati personali), ed espone a responsabilità

civile per danno anche non patrimoniale, qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice).

b) Nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime": nel quadro degli accorgimenti più ampi da adottare per effetto dell'obbligo ora richiamato, occorre assicurare comunque un livello minimo di protezione dei dati personali.

Pertanto, in aggiunta alle conseguenze appena ricordate, il Codice conferma l'impianto secondo il quale l'omessa adozione di alcune misure indispensabili ("minime"), le cui modalità sono specificate dal Codice stesso, costituisce anche reato.

Fra codeste "misure minime di sicurezza" vi è la redazione, da parte del titolare del trattamento di un documento denominato "documento programmatico della sicurezza" (DPS), da aggiornare annualmente entro il 31 marzo, che contiene l'elenco dei trattamenti, la distribuzione dei compiti e delle responsabilità, l'analisi dei rischi e le misure da adottare, i meccanismi di ripristino in caso di incident, la formazione degli utenti.

A testimonianza che la 196/03 è un Codice che unifica molteplici principi sulla privacy e sicurezza del dato è da evidenziare che soppianta in toto il DPR 318/99, che originariamente aveva introdotto il concetto di "misure minime", volto a garantire la tutela del "flusso dell'informazione" dalla sua raccolta alla trasmissione alla banca dati, dall'archiviazione alla sua consultazione,

prevenendo accessi non autorizzati, sia da malintenzionati in rete che da persone che accedono illecitamente ai locali fisici dove i dati possono essere accessibili.

D.L. 354 DEL 24/12/2003

Tale Decreto sostanzialmente modifica l'art. 132 del Codice sulla privacy estendendo da ventiquattro a trenta mesi l'obbligo per il gestrore di un servizio di comunicazione di trattenere i dati del traffico per finalità di accertamento e repressione dei reati generici e, di fatto, a 60 mesi per consentire le indagini su reati di una certa gravità, individuati dall'art. 407, comma 2, lettera a) del codice di procedura penale (fra i quali figurano i delitti di strage, terrorismo, associazione mafiosa) e sui crimini informatici. Il decreto impone che, passati i primi 30 mesi, i dati vengano scorporati, conservati separatamente ed accessibili solo per le finalità suddette e solo con esclusiva autorizzazione del magistrato giudicante. Dopo tale scadenza i dati devono essere definitivamente distrutti.

DIRETTIVA PCM DEL 16/01/02

"Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese.

Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse. E' noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio.

Lo stesso processo di innovazione tecnologica produce da un lato strumenti più sofisticati di "attacco", ma d'altro lato idonei strumenti di difesa e protezione.

Assume quindi importanza fondamentale valutare il rischio connesso con la gestione delle informazione e dei sistemi.

Inoltre per poter operare in un mondo digitale sempre più aperto, le Pubbliche Amministrazioni devono essere in grado di presentare credenziali di sicurezza nelle informazioni conformi agli standard internazionali di riferimento.

Nell'ambito delle rispettive responsabilità il Ministro per l'innovazione e le tecnologie ed il Ministro delle comunicazioni sono quindi chiamati ad interpretare il tema rischio-sicurezza non solo nell'ottica della riduzione della vulnerabilità, per garantire integrità e affidabilità dell'informazione pubblica, ma anche al fine di creare e mantenere una posizione primaria a livello europeo.

Si raccomanda pertanto a tutte le Pubbliche Amministrazioni in indirizzo di avviare nell'immediato alcune azioni prioritarie tali da consentire il conseguimento di un primo importante risultato di allineamento ad una base minima di sicurezza". Tale linea guida comprende due allegati: il primo è un test di autovalutazione sugli accorgimenti presi e da prendere in ambito di sicurezza; il secondo è di fatto una integrazione e una guida alla compilazione del DPS.

DIRETTIVA MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE 27/11/2003

"[…] Il Consiglio dei Ministri, in data 31 maggio 2002, ha approvato le «Linee guida per lo sviluppo della società dell'informazione nella legislatura» nelle quali

è contenuto l'obiettivo di adottare, entro la fine della legislatura, la posta elettronica per tutte le comunicazioni interne alla Pubblica Amministrazione.

L'impiego della posta elettronica consente e facilita quel cambiamento culturale ed organizzativo della Pubblica Amministrazione che risponde alle attese del Paese ed alle sfide della competitività: bisogna accelerare questo processo di cambiamento e darne concreta percezione anche all'esterno, abbandonando inutili ed onerosi formalismi, considerati, anche, i consistenti risparmi di risorse che potranno derivare alla Pubblica Amministrazione dall'uso intensivo della posta elettronica. Bisogna concretamente operare affinché di tale cambiamento possano beneficiare, al più presto, anche i cittadini e le imprese in modo da consentire loro un accesso più veloce e più agevole alle Pubbliche Amministrazioni.

[…] A tal fine la completa attuazione del protocollo informatico […] consentirà la gestione dei flussi dei procedimenti in corso presso le Pubbliche Amministrazioni permettendo di conoscerne lo stato e realizzando, così, un più elevato livello di trasparenza dell'azione amministrativa.

Nell'esercizio della suddetta delega saranno anche fissati i tempi di attuazione dell'intero nuovo processo che deve tener conto della necessità di operare il cambiamento in tempi rapidi, per evitare la coesistenza prolungata delle procedure elettroniche con quelle tradizionali, allo scopo di superare difficoltà organizzative e gestionali e ridurre i relativi costi operativi.

[…] In considerazione dei vantaggi che possono derivare a tutta la Pubblica Amministrazione dall'applicazione della presente direttiva si raccomanda di

curarne, con tutti i mezzi possibili, la più ampia ed immediata attuazione e di garantirne la massima diffusione a tutti i dipendenti.

Ogni amministrazione, pertanto, è tenuta a porre in essere le attività necessarie al raggiungimento dell'obiettivo di legislatura, in modo da garantire che, entro la data della sua scadenza, tutte le comunicazioni nelle Pubbliche Amministrazioni possano avvenire esclusivamente in via elettronica.

[…] Appare necessario che le Pubbliche Amministrazioni provvedano a dotare tutti i dipendenti di una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) e ad attivare, inoltre, apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza. Queste ultime dovranno procedere alla tempestiva lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta, adottando gli opportuni metodi di conservazione della stessa in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

La posta elettronica può essere utilizzata per la trasmissione di tutti i tipi di informazioni, documenti e comunicazioni in formato elettronico e, a differenza di altri mezzi tradizionali, offre notevoli vantaggi in termini di:

- maggiore semplicità ed economicità di trasmissione, inoltro e riproduzione;
- semplicità ed economicità di archiviazione e ricerca;
- facilità di invio multiplo […] con costi estremamente più bassi di quelli dei mezzi tradizionali;

- velocità ed asincronia della comunicazione, in quanto non richiede la contemporanea presenza degli interlocutori;
- possibilità di consultazione ed uso anche da postazioni diverse da quella del proprio ufficio, anche al di fuori della sede dell'amministrazione ed in qualunque momento grazie alla persistenza del messaggio nella sua casella di posta elettronica;
- integrabilità con altri strumenti di automazione di ufficio, quali rubrica, agenda, lista di distribuzione ed applicazioni informatiche in genere.

Le singole amministrazioni, nell'àmbito delle rispettive competenze, ferma restando l'osservanza delle norme in materia della riservatezza dei dati personali e delle norme tecniche di sicurezza informatica, si adopereranno per estendere l'utilizzo la posta elettronica, tenendo presente quanto segue: è sufficiente ricorrere ad un semplice messaggio di posta elettronica, ad esempio, per

- richiedere o concedere ferie o permessi,
- richiedere o comunicare designazioni in comitati, commissioni, gruppi di lavoro o altri organismi,
- convocare riunioni, inviare comunicazioni di servizio ovvero notizie dirette al singolo dipendente (in merito alla distribuzione di buoni pasto, al pagamento delle competenze, a convenzioni stipulate dall'amministrazione ecc...),
- diffondere circolari o ordini di servizio.

Unitamente al messaggio di posta elettronica, è anche possibile trasmettere, in luogo di documenti cartacei, documenti amministrativi informatici in merito ai

quali tale modalità di trasmissione va utilizzata ordinariamente qualora sia sufficiente conoscere il mittente e la data di invio.

La posta elettronica è, inoltre, efficace strumento per la trasmissione dei documenti informatici sottoscritti ai sensi della disciplina vigente in materia di firme elettroniche.

La posta elettronica può essere utilizzata anche per la trasmissione della copia di documenti redatti su supporto cartaceo (copia immagine) con il risultato, rispetto al telefax, di ridurre tempi, costi e risorse umane da impiegare, soprattutto quando il medesimo documento debba, contemporaneamente, raggiungere più destinatari.

Quanto alla certezza della ricezione del suddetto documento da parte del destinatario, il mittente, ove ritenuto necessario, può richiedere al destinatario stesso un messaggio di risposta che confermi l'avvenuta ricezione.

Con l'occasione si fa presente che le amministrazioni, oltre a dotare tutti i loro dipendenti di una casella di posta elettronica sono chiamate ad adottare ogni iniziativa di sostegno e di formazione per promuovere l'uso della stessa da parte di tutto il personale. […]”

D.LGS 82 DEL 07/03/2005

Il Codice tramuta in legge le linee guida testé viste sulla digitalizzazione delle Pubbliche Amministrazioni quali sportelli unici, alfabetizzazione informatica, pagamenti elettronici, archiviazione digitale dei documenti cartacei, carta

d'identità digitale, firma elettronica, posta elettronica certificata. Per il campo di studi affrontato si devono evidenziare

- l'art. 47: "Le comunicazioni di documenti tra le Pubbliche Amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza";
- l'art. 49, primo comma: "Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.";
- l'art. 51: "Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71 garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati […] I documenti informatici delle Pubbliche Amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.";
- l'art. 71: "Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro

> delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e con le amministrazioni di volta in volta indicate nel presente codice, sentita la Conferenza unificata […] ed il Garante per la protezione dei dati personali nelle materie di competenza […]".

In sostanza, dal momento che l'evoluzione tecnologica procede molto più velocemente della burocrazia che la regola, si demanda ad un comitato di esperti, nominato dal governo, l'aggiornamento di quelle che sono le misure necessarie a garantire la sicurezza dei sistemi informativi di una Pubblica Amministrazione.

DIRETTIVA MINISTERO PER L'INNOVAZIONE E LE TECNOLOGIE DEL 18/11/2005

"[…] L'obbligo di comunicare per via telematica con i cittadini e le imprese che lo richiedano presuppone che l'amministrazione si adoperi per rendersi facilmente raggiungibile telematicamente; si rende, pertanto, necessario esporre ed evidenziare adeguatamente, sui siti istituzionali di ogni amministrazione, gli indirizzi di posta elettronica utilizzabili dai cittadini, rendendo facilmente reperibili gli indirizzi di posta elettronica degli uffici competenti per gli atti ed i procedimenti di maggiore interesse, con l'indicazione di quelli abilitati alla posta certificata.

[…] È stata più volte ribadita […] l'importanza strategica che l'utilizzo intensivo ed esteso della posta elettronica riveste nell'ottica di un cambiamento radicale della Pubblica Amministrazione […] come mezzo di comunicazione e trasmissione di documenti, informazioni, dati (sia all'interno della P.A. che nei confronti dei terzi) […].

Per tali motivi l'art. 47 del codice sancisce che «Le comunicazioni di documenti tra le Pubbliche Amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica», precisando che esse sono valide ai fini del procedimento amministrativo se ne sia verificata la provenienza specificando le modalità che consentono la verifica della «provenienza» delle comunicazioni allo scopo di conferire ad esse efficacia legale certa.

Si rammenta inoltre che, dal primo gennaio del 2006, tutte le Pubbliche Amministrazioni dovranno privilegiare l'uso della posta elettronica come canale di comunicazione anche con i propri dipendenti.

Alla luce delle considerazioni svolte, la prosecuzione delle tradizionali forme di comunicazione, nonostante sussista la possibilità di ricorrere alla posta elettronica, configura l'inosservanza di una disposizione di legge e una fattispecie di improprio uso di denaro pubblico”.

3 – Pianificazione della sicurezza: il Documento Programmatico della Sicurezza

Come è stato sottolineato, la compilazione del DPS è un importante adempimento che una Pubblica Amministrazione deve compiere secondo il D.Lgs 196/03. Tale importanza è racchiusa nel principio che intende tutelare: troppo spesso, nella Pubblica Amministrazione, è stato sottovalutato il danno che può arrecare l'accesso improprio o la modifica accidentale di atti, documenti o informazioni in genere.

Il DPS, sostanzialmente, si prefigge di sensibilizzare le Amministrazioni al problema, strutturandosi come una lista di verifiche da effettuare per garantire un'adeguata protezione dai rischi a cui i dati sono soggetti.

Per un amministratore di posta elettronica, avendo a che fare con comunicazioni che permangono fisicamente su supporti di cui si ha la responsabilità, è cruciale affrontare il problema della sicurezza, concorrendo alla redazione del DPS della propria Amministrazione.

Si elencano in dettaglio gli elementi chiave che il documento deve racchiudere [13].

Elenco dei trattamenti dei dati personali

Per ciascun trattamento vanno indicate le seguenti informazioni secondo il livello di sintesi determinato dal titolare:

- Descrizione sintetica: si deve menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).
- Natura dei dati trattati: si deve indicare se tra i dati personali sono presenti dati sensibili o giudiziari.
- Struttura di riferimento: bisogna indicare la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse è possibile indicare la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione-contabilità).
- Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture, è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.
- Descrizione degli strumenti elettronici utilizzati: bisogna indicare la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).

- Identificativo del trattamento: alla descrizione del trattamento, se ritenuto utile, può essere associato un codice, facoltativo, per favorire un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle.
- Banca dati: si devono indicare eventualmente la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati, in tal caso è opportuno elencarle tutte.
- Luogo di custodia dei supporti di memorizzazione: bisogna indicare il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile. Il punto può essere approfondito meglio in occasione di aggiornamenti.
- Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.
- Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

Le predette informazioni possono essere completate o sostituite da schemi, tabelle, disegni di architettura del sistema informativo o da altri documenti dell'amministrazione, già compilati e idonei a fornire in altro modo le informazioni medesime.

Distribuzione dei compiti e delle responsabilità

In questa sezione occorre descrivere sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati. Si possono utilizzare anche mediante specifici riferimenti documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli. E' bene indicare i trattamenti di competenza di ciascuna struttura e descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).

Analisi dei rischi che incombono sui dati

Questa sezione descrive i principali eventi potenzialmente dannosi per la sicurezza dei dati e valuta le possibili conseguenze e la gravità in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati. Essa contiene l'elenco degli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali, in genere dovuti a:

Comportamenti degli operatori

- sottrazione di credenziali di autenticazione,
- carenza di consapevolezza, disattenzione o incuria,
- comportamenti sleali o fraudolenti.

Eventi relativi al contesto fisico-ambientale

- ingressi non autorizzati a locali/aree ad accesso ristretto,
- sottrazione di strumenti contenenti dati,
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria,
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.),
- errori umani nella gestione della sicurezza fisica.

Eventi relativi agli strumenti

- azione di virus informatici o di programmi suscettibili di recare danno,
- spamming o tecniche di sabotaggio,
- malfunzionamento, indisponibilità o degrado degli strumenti,
- accessi esterni non autorizzati,
- intercettazione di informazioni in rete .

In dettaglio si evidenziano le seguenti tecniche:

- IP spoofing: L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta

come attività di “falsificazione” di alcuni dati telematici, come ad esempio di un indirizzo IP o dell’indirizzo di partenza dei messaggi di posta elettronica.

- Packet sniffing: Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un’operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L’intercettazione illecita avviene con l’ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell’installazione dello sniffer, la macchina “obiettivo” sia stata oggetto di un precedente attacco e sia di fatto controllata dall’hacker.
- Social engineering: Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest’ultimo.
- Spamming: Saturazione di risorse informatiche a seguito dell’invio di un elevato numero di comunicazioni tali da determinare l’interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

- Password cracking: Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.
- Trojan: Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.
- Worm: Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).
- Logic bomb: Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'infezione.
- Malware e MMC (Malicious Mobile Code): Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l’alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.
- DOS (Denial of Service): Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

- DDOS (Distributed Denial of Service): Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete.

E' possibile, per ulteriori dettagli, rinviare a documenti analoghi già redatti in tema di piani di sicurezza e gestione del rischio, come ad esempio: Business Continuity Plan, Disaster Recovery Plan, ecc. (si tenga però presente che le analisi alla base di questi altri documenti possono avere una natura ben diversa). In questa fase è necessario, altresì, descrivere le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutare la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento (anche in termini sintetici: come ad esempio alta/media/bassa). In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare. L'analisi dei rischi può essere condotta utilizzando metodi di complessità diversa: l'approccio qui descritto è volto solo a consentire una prima riflessione in contesti che per dimensioni ridotte o per altre analoghe ragioni, non ritengano di dover procedere ad una analisi più strutturata.

Misure in essere e da adottare

In questa sezione vanno riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Nello specifico si devono elencare:

- Descrizione dei rischi: per ciascuna misura indicare sinteticamente i rischi che si intende contrastare.
- Misure: descrivere sinteticamente le misure adottate.
- Trattamenti interessati: indicare i trattamenti interessati per ciascuna delle misure adottate. Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati (ad esempio, con riferimento alle misure per la protezione delle aree e dei locali).
- Occorre specificare se la misura è già in essere o da adottare, con eventuale indicazione, in tale ultimo caso, dei tempi previsti per la sua messa in opera. Inoltre si deve indicare la struttura o la persona responsabili o preposte all'adozione delle misure indicate.

Ulteriori elementi per la descrizione analitica delle misure di sicurezza

Oltre alle informazioni sopra riportate può essere opportuno compilare, per ciascuna misura, una scheda analitica contenente un maggior numero di informazioni, utili nella gestione operativa della sicurezza e, in particolare, nelle attività di verifica e controllo. Queste schede sono a formato libero e le informazioni utili devono essere individuate in funzione della specifica misura. A puro titolo di esempio, possono essere inserite informazioni relative a:

- La minaccia che si intende contrastare
- La tipologia della misura (preventiva, di contrasto, di contenimento degli effetti ecc.).

- Le informazioni relative alla responsabilità dell'attuazione e della gestione della misura.
- I tempi di validità delle scelte (contratti esterni, aggiornamento di prodotti, ecc.).
- Gli ambiti cui si applica (ambiti fisici, come un ufficio o un edificio, o logici, come una procedura, un'applicazione, ecc.).

Criteri e modalità di ripristino della disponibilità dei dati

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall' eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci. Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.

Per quanto riguarda il ripristino, si deve indicare la banca dati, il data base o l'archivio interessati; i criteri e le procedure per il salvataggio e il ripristino dei dati, con eventuale rinvio ad un'ulteriore scheda operativa o a documentazioni analoghe e la pianificazione delle prove di ripristino.

Per quanto riguarda i criteri e le procedure per il salvataggio dei dati si deve descrivere sinteticamente la tipologia di salvataggio e la frequenza con cui viene effettuato.

Per il testo unico sulla privacy è importante anche specificare il luogo fisico e la modalità in cui sono custodite le copie dei dati salvate, la struttura o la persona incaricata del salvataggio.

Pianificazione degli interventi formativi previsti

A questo punto si devono pianificare le modalità per l'istruzione dei singoli soggetti, che può avvenire con un corso specifico o mediante un regolamento o una nota informativa. E' necessario descrivere sinteticamente gli obiettivi e le modalità dell'intervento formativo in relazione alla mansione di ogni incaricato. Si deve inoltre individuare le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.

COMPILAZIONE DEL DPS PER UN AMMINISTRATORE DEL SERVIZIO DI POSTA ELETTRONICA

Elenco dei trattamenti dei dati personali

TIPOLOGIA DEL DATO	
FINALITÀ DEL DATO ED ATTIVITÀ SVOLTA	**Anagrafe utenti**
CATEGORIE DI SOGGETTI INTERESSATI	Tutto il personale e gli utenti registrati
NATURA DEL TRATTAMENTO	Il dato è sensibile se associato ad informazioni contrattuali, assistenziali, previdenziali, pensionistici.
STRUTTURA DI RIFERIMENTO	Addetto al centro elaborazione dati
ALTRE STRUTTURE DI RIFERIMENTO (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	Ufficio personale, eventualmente anche INPS o INPDAP
DESCRIZIONE DEGLI STRUMENTI UTILIZZATI	Il dato viene elaborato e conservato all'interno dell'ente su supporto elettronico e cartaceo. Periodicamente vengono effettuati backup per il ripristino in caso di incident.
TIPOLOGIA DEI DISPOSITIVI DI ACCESSO	Armadio metallico chiuso con serratura. Personal Computer con accesso consentito solo tramite password per i dati elettronici
UBICAZIONE FISICA DEI DATI ARCHIVIATI	Server centrale, Ufficio del personale.
IL DATO È CONSERVATO SU SUPPORTO ELETTRONICO?	SI
EVENTUALE BANCA DATI	Si (interna)

TIPOLOGIA DEL DATO	
FINALITÀ DEL DATO ED ATTIVITÀ SVOLTA	**Messaggio di posta elettronica ricevuto**
CATEGORIE DI SOGGETTI INTERESSATI	Tutti gli utenti registrati
NATURA DEL TRATTAMENTO	Il dato è sensibile poiché può riguardare la sfera personale dei soggetti.
STRUTTURA DI RIFERIMENTO	Utente registrato
ALTRE STRUTTURE DI RIFERIMENTO (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	Server di posta elettronica in ingresso.
DESCRIZIONE DEGLI STRUMENTI UTILIZZATI	Il dato viene conservato nel server di posta, su richiesta dell'utente viene cancellato o copiato nel proprio personal computer. Periodicamente vengono effettuati backup per il ripristino in caso di incident.
TIPOLOGIA DEI DISPOSITIVI DI ACCESSO	Personal Computer con accesso consentito solo tramite password. Armadio metallico chiuso con serratura per le copie di ripristino. Accesso remoto alla casella di posta mediante password.
UBICAZIONE FISICA DEI DATI ARCHIVIATI	Server centrale del Centro Elaborazione Dati.
IL DATO È CONSERVATO SU SUPPORTO ELETTRONICO?	SI
EVENTUALE BANCA DATI	Si (interna)

TIPOLOGIA DEL DATO	
FINALITÀ DEL DATO ED ATTIVITÀ SVOLTA	**Messaggio di posta elettronica inviato**
CATEGORIE DI SOGGETTI INTERESSATI	Tutti gli utenti registrati
NATURA DEL TRATTAMENTO	Il dato è sensibile poiché può riguardare la sfera personale dei soggetti.
STRUTTURA DI RIFERIMENTO	Utente registrato
ALTRE STRUTTURE DI RIFERIMENTO (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	Server di posta elettronica in uscita
DESCRIZIONE DEGLI STRUMENTI UTILIZZATI	Il dato inviato dall'utente viene conservato nel server di posta finché non viene inoltrato al server remoto.
TIPOLOGIA DEI DISPOSITIVI DI ACCESSO	Personal Computer con accesso consentito solo tramite password. Armadio metallico chiuso con serratura per le copie di ripristino.
UBICAZIONE FISICA DEI DATI ARCHIVIATI	Server centrale del Centro Elaborazione Dati.
IL DATO È CONSERVATO SU SUPPORTO ELETTRONICO?	SI
EVENTUALE BANCA DATI	Si (interna)

Nella copia fornita all'utente non si aggiungono le informazioni raccolte sui dati del traffico poiché, come già detto, l'amministratore non è tenuto ad informare della raccolta delle informazioni sul traffico. Nella copia interna si devono invece indicare, mediante la tabella:

TIPOLOGIA DEL DATO	
FINALITÀ DEL DATO ED ATTIVITÀ SVOLTA	**Dati relativi al traffico**
CATEGORIE DI SOGGETTI INTERESSATI	Tutti gli utenti registrati
NATURA DEL TRATTAMENTO	Il dato è sensibile poiché può riguardare la sfera personale dei soggetti.
STRUTTURA DI RIFERIMENTO	Amministratore del Centro Elaborazione Dati
ALTRE STRUTTURE DI RIFERIMENTO (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	Eventualmente Polizia Giudiziaria, Magistratura.
DESCRIZIONE DEGLI STRUMENTI UTILIZZATI	Il dato viene elaborato e conservato all'interno del server centrale. Periodicamente vengono effettuati dei Backup.
TIPOLOGIA DEI DISPOSITIVI DI ACCESSO	Personal Computer con accesso consentito solo tramite password per i dati elettronici. Armadio metallico chiuso con serratura per le copie di ripristino.
UBICAZIONE FISICA DEI DATI ARCHIVIATI	Server Centrale del Centro Elaborazione Dati.
IL DATO È CONSERVATO SU SUPPORTO ELETTRONICO?	SI
EVENTUALE BANCA DATI	Si (interna)

Distribuzione dei compiti e delle responsabilità

TRATTAMENTI EFFETTUATI DALLA STRUTTURA	
STRUTTURA	**Amministratore del sistema**
TRATTAMENTI EFFETTUATI DALLA STRUTTURA	L'amministratore può trattare tutti i dati indicati ad eccezione dei messaggi di posta degli utenti in entrata o uscita.
DESCRIZIONE DEI COMPITI E RESPONSABILITA' DELLA STRUTTURA	Si occupa dell'inserimento, correzione, eliminazione di tutti i dati. Presiede al backup e al recovery del sistema e si occupa personalmente di estrapolare i dati del traffico su espressa richiesta degli enti giudiziari. E' il responsabile della sicurezza del sistema e supervisiona l'ottemperamento del D.Lgs. 196/03.

TRATTAMENTI EFFETTUATI DALLA STRUTTURA	
STRUTTURA	**Addetto centro elaborazione dati**
TRATTAMENTI EFFETTUATI DALLA STRUTTURA	L'addetto tratta i dati degli utenti limitatamente alla gestione anagrafica ed al problem solving.
DESCRIZIONE DEI COMPITI E RESPONSABILITA' DELLA STRUTTURA	Si occupa dell'inserimento, correzione, eliminazione degli utenti. Collabora l'amministratore al backup e al recovery del sistema. Si occupa della supervisione delle apparecchiature della struttura.

TRATTAMENTI EFFETTUATI DALLA STRUTTURA	
STRUTTURA	**Utente registrato**
TRATTAMENTI EFFETTUATI DALLA STRUTTURA	L'utente può spedire e ricevere email tramite i privilegi ad esso concessi.
DESCRIZIONE DEI COMPITI E RESPONSABILITA' DELLA STRUTTURA	L'utente è tenuto a: utilizzare legalmente il proprio indirizzo, non installare software non autorizzati nelle proprie postazioni di lavoro, avvertire tempestivamente il centro elaborazione dati su accertati o presunti accessi indesiderati al proprio account, malfunzionamenti o problemi in genere.

Analisi dei rischi che incombono sui dati

L'Analisi dei rischi può essere effettuata considerando due parametri di rischio relativi ai dati della PA.

In particolare ciascun parametro viene valutato come segue:

ENTITA': si valuta l'entità dell'impatto di un uso non corretto del dato considerando le seguenti variabili: danno arrecato al titolare del danno, reversibilità dell'uso non corretto del dato. L'entità può essere valutata come:

- BASSA (punteggio = 1): quando sono presenti rischi che non arrecano danni di particolare impatto e/o il danno creato è facilmente reversibile;
- MEDIA (punteggio = 2): il rischio crea un danno gestibile all'interno della PA e che per essere eliminato comporta un azione diretta dell'ente;
- ALTA (punteggio = 3): il rischio crea un danno che arriva a soggetti esterni all'ente difficilmente reversibile dalla stessa.

FREQUENZA: si valuta il rischio relativo ai dati sulla base della frequenza di accadimento dell'impatto.

Si possono applicare i seguenti criteri di valutazione:

- BASSA (punteggio = 1): il rischio di accesso al dato è limitato nel tempo ed è riservato.
- MEDIA (punteggio = 2): il rischio di accesso al dato avviene con scansione temporale precisa e non è limitato ad un solo accadimento
- ALTA (punteggio = 3): L'accesso potrebbe avvenire in modo continuo e senza aree riservate.

Una maniera semplice per valutare la significatività del rischio valutato è data dall'espressione: Significatività = (Entità x Frequenza). E' così possibile suddividere i rischi per rilevanza considerando:

- ALTO RISCHIO (Significatività con valori pari a 6 o 9: Vi è un forte rischio per l'ente, relativamente a quest'accadimento che provocherebbe un grave danno con altissima frequenza. In questo caso si devono adottare al più presto tutte le misure possibili a limitare il danno sia in relazione all'impatto che alla frequenza. L'ente deve eseguire uno specifica formazione sul rischio ai propri dipendenti sul rischio di trattamento e sui dati interessati a questo rischio.
- MEDIO RISCHIO (Significatività con valori pari a 3 o 5): Vi è un medio rischio per l'ente, relativamente a quest'accadimento che provocherebbe un danno limitato con media frequenza. In questo caso si devono adottare

tutte le misure possibili a limitare il danno sia in relazione all'impatto che alla frequenza con una scadenza di medio periodo ma inferiore all'anno.

- BASSO RISCHIO (Significatività con valori pari a 1 o 2): Vi è un basso rischio per l'ente, relativamente a quest'accadimento che provocherebbe un danno di lievissima entità con una frequenza di accadimento remota . In questo caso si devono adottare tutte le misure di sicurezza minime previste dal D.Lgs. 196/2003.

RISCHIO	Presenza del rischio Si/No	Entità	Frequenza	Classe di rischio
Sottrazione di una credenziale di autenticazione da parte di un altro utente	Si	3	1	Media
Carenza di consapevolezza, disattenzione, incuria da parte degli utenti	Si	3	3	Alta
Comportamenti sleali o fraudolenti degli utenti	Si	3	2	Alta
Azione di Virus informatici	Si	3	3	Alta
Spamming o tecniche di sabotaggio degli strumenti informatici	Si	3	3	Alta
Malfunzionamento o degrado degli strumenti elettronici contenente dati	Si	1	1	Bassa
Suscettibilità a variazioni di temperatura, umidità, polvere, radiazioni elettromagnetiche	Si	1	1	Bassa
Accessi esterni agli strumenti informatici non autorizzati	Si	3	1	Media
Accessi esterni ai locali dell'Organizzazione	Si	3	1	Media
Sottrazione di strumenti contenenti dati	Si	3	2	Alta
Intercettazione di informazioni di rete	Si	2	1	Bassa
Eventi naturali, distruttivi, artificiali	Si	3	1	Media
Guasti ai sistemi complementari (elettricità, etc)	Si	3	1	Media
Errori umani nella gestione della sicurezza materiale dei dati	Si	1	1	Bassa

Misure in essere e da adottare

Non partendo da una base preesistente, non si suppone nessuna misura in essere.

RISCHIO	DATO INTERESSATO	MISURE DA ADOTTARE	RESP. MISURA
Carenza di consapevolezza, incuria, disattenzione degli utenti	Tutti i dati	Lettera Informativa sulla sicurezza; Rinnovo delle password semestrale; Utilizzo di Screen saver a password nei locali del CED.	Ammin.
Comportamenti sleali o fraudolenti degli utenti	Tutti i dati.	Password di accesso ai dati elettronici; Firewall sul server; Back-up dei dati dei server, teso a garantire la sicurezza dei dati su base quotidiana e settimanale; Informativa sulle sanzioni amministrative e penali legati a comportamenti sleali in materia di trattamento dei dati.	Ammin.
Spamming o tecniche di sabotaggio degli strumenti informatici, Azione di virus informatici	Tutti i dati	Firewall sul server (con aggiornamento delle Patch periodico) teso a proteggere la rete da accessi provenienti dall'esterno; Antivirus installato su ogni PC della LAN; Back-up dei dati sul server teso a garantire la sicurezza dei dati su base quotidiana e settimanale; Impostazione di regole anti-spamming sulla posta elettronica.	Ammin.

RISCHIO	DATO INTERESSATO	MISURE DA ADOTTARE	RESP. MISURA
Sottrazione di una credenziale di autenticazione da parte di un altro utente	Messaggi di posta	Creazione di Regole per la costruzione di password di autenticazioni ben fatte; Rinnovo delle password semestrale; Formazione sulle modalità di creazione delle password all'utente.	Addetto CED
Accessi esterni non autorizzati agli strumenti informatici	Tutti i dati	Firewall sul server teso a proteggere la rete da virus informatici provenienti dall'esterno.	Addetto CED
Accessi esterni non autorizzati ai locali e sottrazione di strumenti contenente dati	Tutti i dati	Divieto di accesso alle persone non autorizzate nella sala server; Chiusura a chiave degli uffici, degli armadi e della sala server; Video-sorveglianza della struttura; Chiusura a chiave dei contenitori contenenti dati.	Ammin.
Eventi naturali distruttivi ed artificiali, guasti ai sistemi complementari	Tutti i dati	Sistema elettrico in conformità alla L. 46/90; Gruppi di continuità elettrica; Manutenzione periodica estintori; Conformità al D.Lgs. 626/94; Formazione per i responsabili evacuazione ed antincendio ai sensi del DM 10/03/1998.	

RISCHIO	DATO INTERESSATO	MISURE DA ADOTTARE	RESP. MISURA
Malfunzionamento o degrado degli strumenti conentenenti dati	Tutti i dati	Pianificazione dell'attivita' di manutenzione dei computer e del server; Back-up dei dati pianificato sia su base quotidiana che su base settimanale; Gruppi di continuità elettrica.	Addetto CED
Suscettibilità degli strumenti informatici a variazioni di temperatura, umidità, polvere, radiazioni elettromagnetiche	Tutti i dati	Back-up dei dati sistematico teso a proteggere i dati; Mantenimento della temperatura costante in sala server; Attivazione Update/Upgrade automatici dei sistemi op.	Addetto CED
Errori umani nella gestione fisica dei dati	Tutti i dati	Lezione formativa per gli addetti al CED sugli strumenti e i supporti in uso.	Ammin.
Intercettazione di informazioni di rete	dati presenti sulla rete lan	Controlli sullo stato di traffico della rete; Controllo fisico della rete in uso.	Addetto CED

Criteri e modalità di ripristino della disponibilità dei dati

Va ricordato che lo scopo dell'Incident response e dell'attività di ripristino è che venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo, un ripristino affrettato del sistema potrebbe però alterare le prove dell'incidente.

Vengono realizzati due tipologie di back-up:

- Back-up non presidiato Disco-Disco: quotidianamente una serie di procedure informatiche implementate sono pianificate nei sistemi server e provvedono alla copia fisica delle Banche Dati nell'ambito dello stesso supporto (Hard Disk).
- Back-up presidiato Disco-Nastro: viene realizzato settimanalmente e consiste nel riportare i dati contenuti nelle banche dati su cassette magnetiche di back-up. Il back-up viene realizzato in modalità presidiata allo scopo di poter monitorare il successo delle operazioni. I Nastri magnetici di back-up vengono custoditi in cassaforte ignifuga posta all'interno della Sala Server.

Tutti gli utenti devono avvisare tempestivamente l'amministratore di sistema o l'addetto CED, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente nei server, cioè di un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni, sono considerate le seguenti priorità:

- evitare danni diretti alle persone;
- proteggere l'informazione sensibile o proprietaria;
- evitare danni economici;
- limitare i danni all'immagine dell'Ente.

L'amministratore del sistema coinvolgerà quindi le autorità competenti.

Successivamente la fase di ripristino del sistema sarà condotta dall'amministratore con l'aiuto di personale esperto di incident response, cercando di eseguire un tentativo per il recupero dei dati presenti sull'hard disk del sistema compromesso. Nel caso in cui non si riesca a recuperare tali dati , verrà ripristinato il sistema e aggiornato con le ultime copie di back-up ritenute valide.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Regole per i computer nella LAN

- Divieto di utilizzare floppy disk come mezzo per il backup.
- Divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screen-saver automatico dopo 10

minuti di non utilizzo, con reinserimento password segreta per la prosecuzione del lavoro.

- Divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati.
- Divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
- Divieto di installazione di software non precedentemente autorizzati dal CED.
- Divieto di Installazione di apparati di rete (Wired, Wireless).
- Controllare (scandire con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti.
- Evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di “scaricare“ dalla rete internet ogni sorta di file.
- Non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus; usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti").

- Non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa).
- Non utilizzare le chat.
- Verificare con periodicità settimanale il corretto aggiornamento del Sistema Antivirus.
- Seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto).
- Avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema).
- Conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC).
- Conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge.
- Conservare la copia originale del sistema operativo e la copia di backup consentita per legge.
- Conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

4 – Protocolli per servizi di Posta Elettronica

La posta Elettronica è destinata a soppiantare una parte sempre maggiore di corrispondenza cartacea e, si è visto, è designata ad avere un ruolo chiave nelle comunicazioni all'interno dell'amministrazione statale.

La normativa richiede, oltre al DPS, che per qualsiasi servizio di comunicazione, e quindi anche per la posta elettronica, venga tenuto un registro dei dati di traffico che escluda elementi riconducibili ai contenuti del messaggio. Per poter individuare la strategia e gli strumenti necessari alla raccolta di tali dati, occorre quindi lo studio del formato con cui si effettua la comunicazione e l'analisi dei protocolli coinvolti.

IL MESSAGGIO DI POSTA ELETTRONICA

La posta elettronica è un servizio che si sintetizza elementarmente, nella consegna, ad opera di due protocolli, il SMTP e il POP3 (o di una sua alternativa l'IMAP, però meno diffusa) di un insieme di byte costituenti il messaggio. Il primo protocollo si occupa di trasmettere il messaggio di un utente al proprio server di uscita che poi lo forwarderà alla casella di posta del destinatario; il secondo, invece, ha il compito di recuperare i messaggi ricevuti dalla casella di posta e recapitarli al destinatario.

Lo standard originario di un messaggio di posta è definito nell'RFC 822 [14]. Nella sua forma primitiva è composto da un file di testo, contenente un

"involucro", alcuni campi di intestazione, una riga vuota e il corpo del messaggio. Ogni campo consiste logicamente di una singola riga di testo ASCII contenente il nome del campo, un carattere di due punti e un valore. L'RFC 822 è stata progettata decenni fa e non distingue chiaramente i campi dell'involucro dai campi dell'intestazione. Successivamente è stata rivista nell'RFC 2822 [15] ma non è stato possibile riscriverla completamente per garantire la retrocompatibilità. I campi principali sono:

- "To:" indica l'indirizzo DNS del destinatario principale.
- "Cc:" indica gli indirizzi dei destinatari secondari.
- "From:" indica la persona che ha creato il messaggio.
- "Sender:" indica la persona che ha spedito di fatto il messaggio.
- "Subject:" indica un breve riepilogo del messaggio.

L'utilizzo di caratteri ASCII a 7 bit fu però una grande limitazione perché con lo sviluppo di Internet nacquero problemi per l'invio e ricezione di:

- Messaggi scritti in lingue con accenti (come italiano e francese).
- Messaggi in alfabeti non latini (come ebraico o russo).
- Messaggi scritti in lingue con alfabeti ideografici (come cinese o giapponese).
- Messaggi contenenti contenuti multimediali.

Fu proposta quindi una soluzione in RFC 1341 [16] (aggiornata da RFC 2045-2049 [17]), chiamata MIME cioè "Multipurpose Internet Mail Extensions". L'idea di base è continuare a utilizzare il formato RFC822, aggiungendo una struttura al corpo del messaggio e definendo le regole di codifica per i messaggi

non ASCII. Non discostandosi da RFC 822, i messaggi MIME possono essere inviati utilizzando i programmi e i protocolli di posta esistenti. Dentro il corpo del messaggio si aggiungono quindi dei nuovi campi che definiscono il contenuto successivo e il tipo di codifica. Si superano così i limiti imposti dallo standard precedente. [18]

IL SIMPLE MAIL TRANSFER PROTOCOL

All'interno di Internet, la posta elettronica viene consegnata costituendo una connessione tra la macchina origine e la porta 25 della macchina di destinazione. Presso il server di posta del destinatario, in ascolto su questa porta esiste un demone (un programma residente in memoria, deputato a ricevere richieste su di una porta) che utilizza tale protocollo. Questo accetta le connessioni in ingresso e copia nelle caselle di posta appropriate i messaggi ricevuti. Se un messaggio non può essere consegnato, al mittente viene restituito un rapporto di errore contenente la prima parte del messaggio non consegnabile. Se il destinatario invece esiste, il server comunica al client di inviare il messaggio. Una volta ricevuto il messaggio, il server fornisce l'acknowledgement. Non sono necessari checksum, poiché il TCP offre un flusso di byte affidabile.

Il protocollo prevede inoltre il Relay ad un altro server di un messaggio, qualora la mailbox del destinatario non risieda nella macchina a cui il messaggio è stato inviato.

Una Tipica sessione SMTP [19] [20], iniziata con un opportuno comando TELNET, può essere riassunta dal seguente esempio (con M si indicano i messaggi del mittente, con S quelli del server):

```
M    telnet mail.libero.it 25
S    220 smtp3.libero.it ESMTP Service (1.1.0-PF-CM) ready
M    helo libero.it
S    250 smtp3.libero.it
M    mail from: marco.orazio@libero.it
S    250 Ok
M    rcpt to: fulvio@libero.it
S    250 Ok
M    data:
S    354 Please start mail input.
M    from: Marco Garozzo
     to: Fulvio
     subject: leggi questa mail di prova.
     MIME-version: 1.0
     content-type: text/enriched
     <bold>Ciao Fulvio</bold>
     Sto provando la mia email
     .
S    250 Mail queued for delivery.
M    quit
S    221 Closing connection. Good bye.
```

Già da quest'esempio si evince la scarsa sicurezza che il protocollo offre non chiedendo nessun tipo di autenticazione per spedire il messaggio con le credenziali di marco.orazio [18].

IL POST OFFICE PROTOCOL VERSION 3

Quando si invia un messaggio di posta elettronica, non è possibile determinare se il destinatario sia on line. Se il messaggio fosse inviato alla macchina del destinatario, si avrebbero quindi poche probabilità di ricezione in breve tempo. In sostanza dovrebbe accadere che nello stesso istante in cui il mittente spedisce, il destinatario dovrebbe essere pronto a ricevere. Per ovviare a questo problema è

stato definito il Post Office Protocol (giunto alla versione 3) definito in RFC 1939 [21], il quale consente ad un utente di recuperare i messaggi residenti in un server di posta remoto. Una volta che l'utente stabilisce una connessione TCP alla porta 110 della macchina server, il protocollo POP3 attraversa sequenzialmente tre stati: autorizzazione, transazione, aggiornamento.

Lo stato di autorizzazione si occupa del login utente; lo stato delle transazioni consente all'utente di raccogliere la posta e cancellarla dalla casella del server; Lo stato di aggiornamento provoca l'effettiva eventuale eliminazione dei messaggi. Anche in questo caso è possibile esaminare il dialogo instaurato dal protocollo attraverso una sessione telnet (i messaggi del server saranno indicati con S, quelli del destinatario con D).

```
D    telnet pop.libero.it 110
S    +OK POP3 PROXY server ready (7.0.027)
<83cae324D2E8E9DE0FF6E8A4f52b733694bdc0a@pop4.libero.it>
D    user marco.orazio
S    +OK Password required
D    pass cavolfiore
S    +OK 3 messages
D    list
S    1 256
     2 1024
     3 768
     .
D    retr 1
S    +OK 256 bytes
     Return-Path: <marco.orazio@libero.it>
     Received: from smtp6.libero.it (193.70.192.59) by
servermittente.it id 12A for
marco.orazio@libero.it; Mon, 20 Feb 2006 20:51:03
+0100
     Message-ID: <000004455993c39583@tom>
     From: ”Fulvio” <fulvio@libero.it>
     To: ”Marco” <marco.orazio@libero.it>
     Subject: RE: Leggi questa mail di prova
     Date: Mon, 20 Feb 2006 21:11:38 +0100
     MIME-Version: 1.0
     Content-Type: text/plain;
     Ho ricevuto il tuo messaggio e ti rispondo con un
altro messaggio di prova
     .
D    dele 1
```

```
S    +OK message marked for deletion
D    quit
S    +OK POP3 server closing connection
```

Durante lo stato di autorizzazione, l'utente invia nome utente e password. Dopo il login l'utente può inviare il comando LIST, che chiede al server di elencare il contenuto della casella di posta, un messaggio per riga, specificando la lunghezza di ogni messaggio. L'elenco è terminato da un punto.

L'utente può recuperare i messaggi utilizzando il comando RETR e contrassegnarli per l'eliminazione con DELE. Una volta recuperati i messaggi e contrassegnati quelli da eliminare, si può terminare lo stato delle transazioni e passare all'aggiornamento, mediante il comando QUIT. Una volta che il server ha eliminato i messaggi contrassegnati, chiude la comunicazione TCP.

Si noti che in questo caso vi è una effettiva autenticazione mediante password, ma questa avviene "in chiaro" un qualunque malintenzionato che sniffi il traffico in rete ha così a disposizione la password utilizzata dall'utente [18].

5 – Tecniche di monitoraggio del traffico di posta elettronica

Avendo adesso ben chiaro come vengono strutturate le transazioni dei messaggi di posta fra mittente, destinatario e servers, si possono delineare alcune possibili tecniche di monitoraggio di tale servizio. Queste, già tuttora in uso presso i gestori di posta elettronica, utilizzano differenti approcci per risolvere la questione. Elemento comune è il fatto che tali tecniche non sono state ideate "su misura", ma si appoggiano a strumenti preesistenti per ottenere ciò che la legge impone.

ALWAYS_BCC

Il Bcc è una funzionalità del servizio di posta elettronica per cui, è possibile celare ad un destinatario principale, il fatto che stiamo mandando copie multiple di un messaggio. Per esempio, se Mario Rossi scrive un email con i campi:

To: luigi.bianchi@tiscali.it

Bcc: anna.verdi@libero.it

Subject: Email riservata.

Si avrà la situazione per cui Luigi Bianchi non saprà che Anna Verdi avrà ricevuto la Email riservata, ma quest'ultima non solo riceverà la mail, ma saprà anche che è stata inviata al Bianchi.

Un mail server ha la possibilità di attivare una funzione, chiamata always_Bcc, che inoltra in maniera nascosta tutte le email transitanti ad un destinatario nascosto. Attivando semplicemente tale funzionalità l'amministratore ha così una tecnica per avere la traccia di tutti i messaggi transitanti, ma è chiaro, però, che in questa maniera si incorre in tre problematiche:

La prima, di natura tecnica, è che potendo contenere Attach (file allegati) di qualunque natura e dimensione, si dovrà fare molto spesso backup su supporti molto grandi per conservare inutili informazioni.

La seconda è una questione di sicurezza della rete. Supponendo che un malintenzionato riesca a penetrare il sistema con credenziali di amministratore nel server, ha diretto accesso, non solo alle informazioni sul traffico, ma anche a tutta la corrispondenza deviata.

La terza e più importante è che questo trattamento è totalmente illecito, poiché di fatto si conserva tutto il contenuto della conversazione. Anche quando tale contenuto fosse filtrato in sede di salvataggio, l'amministratore così ha la possibilità di accedere comunque a dati considerati riservati.

LOG DEL MAIL SERVER

Un altro modo per avere traccia del traffico di posta è quello di analizzare i log di sistema. Per un server postfix, per esempio si deve filtrare adeguatamente il file maillog che si trova su /var/log/. In esso possiamo trovare numerose voci riguardanti l'attività del server, per cui essendo difficoltoso filtrare quelle utili si

è costretti a tenere il file per intero e, all'occorrenza fare un'analisi del traffico localizzata.

Un estratto di tale file è il seguente:

```
Mar 25 11:57:00 linux postfix/smtpd[16824]: 802A54EEF6:
client=unknown[192.168.1.7]
Mar 25 11:57:00 linux postfix/cleanup[16825]: 802A54EEF6:
message-id=<4417F31B.3080705@marco.grz.net>
Mar 25 11:57:00 linux postfix/nqmgr[5332]: 802A54EEF6:
from=<marco@marco.grz.net>, size=670, nrcpt=1 (queue active)
Mar 25 11:57:00 linux postfix/smtpd[16824]: disconnect from
unknown[192.168.1.7]
Mar 25 11:57:00 linux postfix/local[16827]: 802A54EEF6:
to=<sissi@tom.grz.net>, relay=local, delay=0, status=sent
("|/usr/bin/procmail")
Mar 25 12:25:14 linux postfix/smtpd[16851]: connect from
unknown[192.168.1.7]
Mar 25 12:25:14 linux postfix/smtpd[16851]: 0EF5F4EEF6:
client=unknown[192.168.1.7]
Mar 25 12:25:14 linux postfix/cleanup[16852]: 0EF5F4EEF6:
message-id=<4417F763.9060201@marco.grz.net>
Mar 25 12:25:14 linux postfix/smtpd[16851]: disconnect from
unknown[192.168.1.7]
Mar 25 17:58:47 linux postfix/smtpd[5154]: connect from
unknown[192.168.1.6]
Mar 25 17:58:47 linux postfix/smtpd[5154]: 7BF384E826:
client=unknown[192.168.1.6]
Mar 25 17:58:51 linux postfix/smtpd[5154]: 4C8064E826:
client=unknown[192.168.1.6]
Mar 25 17:58:51 linux postfix/cleanup[5155]: 4C8064E826: message-
id=<20060325165851.4C8064E826@tom.grz.net>
Mar 25 17:58:51 linux postfix/nqmgr[4545]: 4C8064E826:
from=<marco@tom.grz.net>, size=626, nrcpt=1 (queue active)
Mar 25 17:58:51 linux postfix/smtpd[5154]: disconnect from
unknown[192.168.1.6]
Mar 25 17:59:01 linux postfix/smtp[5157]: 4C8064E826:
to=<marco.orazio@libero.it>, relay=smtp.libero.it[193.70.192.50],
delay=10, status=sent (250 Ok: queued as 351D0A8C2E)
Mar 25 18:01:19 linux postfix/postfix-script: stopping the
Postfix mail system
Mar 25 18:01:19 linux postfix/master[4543]: terminating on signal
15
Mar 25 18:01:54 linux ipop3d[5192]: pop3 service init from
192.168.1.6
Mar 25 18:01:54 linux ipop3d[5192]: Login user=marco
host=[192.168.1.6] nmsgs=0/0
Mar 25 18:01:55 linux ipop3d[5192]: Logout user=marco
host=[192.168.1.6] nmsgs=0 ndele=0
Mar 25 18:15:42 linux ipop3d[5226]: pop3 service init from
192.168.1.6
```

```
Mar 25 18:15:42 linux ipop3d[5226]: Login user=marco
host=[192.168.1.6] nmsgs=0/0
Mar 25 18:15:42 linux ipop3d[5226]: Logout user=marco
host=[192.168.1.6] nmsgs=0 ndele=0
Mar 25 18:17:55 linux ipop3d[5230]: pop3 service init from
192.168.1.6
Mar 25 18:18:01 linux ipop3d[5230]: Login user=marco
host=[192.168.1.6] nmsgs=0/0
Mar 25 18:18:01 linux ipop3d[5230]: Logout user=marco
host=[192.168.1.6] nmsgs=0 ndele=0
Mar 25 18:47:43 linux postfix/postfix-script: starting the
Postfix mail system
Mar 25 18:47:43 linux postfix/master[5356]: daemon started
Mar 25 18:47:43 linux postfix/nqmgr[5358]: 717464E837:
from=<marcolino@grz.it>, size=386, nrcpt=1 (queue active)
Mar 25 18:47:55 linux postfix/smtp[5360]: 717464E837:
to=<tomcatt@tiscali.it>, relay=smtp.libero.it[193.70.192.50],
delay=29084, status=deferred (host smtp.libero.it[193.70.192.50]
said: 450 <marcolino@grz.it>: Sender address rejected: Domain not
found)
Mar 25 18:48:18 linux ipop3d[5387]: pop3 service init from
192.168.1.8
Mar 25 18:48:19 linux ipop3d[5387]: Auth user=marco
host=tom.grz.net [192.168.1.8] nmsgs=0/0
Mar 25 18:48:19 linux ipop3d[5387]: Logout user=marco
host=tom.grz.net [192.168.1.8] nmsgs=0 ndele=0
Mar 25 18:51:04 linux ipop3d[5394]: pop3 service init from
192.168.1.8
Mar 25 18:51:04 linux ipop3d[5394]: Auth user=sissi
host=tom.grz.net [192.168.1.8] nmsgs=0/0
```

È facile capire che diventa un problema la tracciatura di ogni email, essendo conservata ogni operazione effettuata dal server. In mezzo a tutte queste informazioni i dati sul traffico di una singola email spedita sono:

```
Mar 25 17:58:47 linux postfix/smtpd[5154]: connect from
unknown[192.168.1.6]
Mar 25 17:58:51 linux postfix/smtpd[5154]: 4C8064E826:
client=unknown[192.168.1.6]
Mar 25 17:58:51 linux postfix/cleanup[5155]: 4C8064E826: message-
id=<20060325165851.4C8064E826@tom.grz.net>
Mar 25 17:58:51 linux postfix/nqmgr[4545]: 4C8064E826:
from=<marco@tom.grz.net>, size=626, nrcpt=1 (queue active)
Mar 25 17:58:51 linux postfix/smtpd[5154]: disconnect from
unknown[192.168.1.6]
Mar 25 17:59:01 linux postfix/smtp[5157]: 4C8064E826:
to=<marco.orazio@libero.it>, relay=smtp.libero.it[193.70.192.50],
delay=10, status=sent (250 Ok: queued as 351D0A8C2E)
```

Che rimangono ad una lettura immediata poco chiare, ma che indicano la connessione al server della macchina 192.168.1.6 alle ore 17:58 del 25 Marzo e l'invio di un messaggio da parte di marco@tom.grz.net di 626 bytes per l'utente marco.orazio@libero.it forwardato al server relay=smtp.libero.it[193.70.192.50] poiché la mailbox del destinatario non appartiene al dominio del server locale. Questa, di fatto, è la tecnica utilizzata sinora dal momento che le informazioni raccolte non violano la privacy degli utenti.

SNIFFER

Uno sniffer è un sistema, hardware, software o entrambi, che consente l'intercettazione, la cattura e la successiva analisi dei segnali transitanti un canale di comunicazione. Tale termine deriva da "The Sniffer Network Analyzer", software sviluppato da Network Associates Inc., ma esteso a tutti i sistemi che svolgono il compito descritto.

Supponendo di avere un tale sistema interposto fra il server di posta e la rete è plausibile pensare di catturare il traffico di interesse ed elaborarlo in modo da ottenere le informazioni da conservare per legge. Questa tecnica è tutt'ora poco utilizzata poiché, nonostante goda di molti vantaggi, consente di intercettare e registrare tutta la comunicazione ed è quindi un approccio fortemente invasivo nella privacy dell'utente.

6 – Soluzione tecnica per il controllo o monitoraggio di posta elettronica

Riuscendo a modulare le capacità di uno sniffer è possibile limitare le sue funzionalità alla sola registrazione dei dati sul traffico, per questo, allo scopo di fornire all'amministratore del sistema di posta elettronica di strumenti orientati alle attuali direttive sulla sicurezza, sulla privacy e sull'informazione digitale, si è puntato allo sviluppo di uno sniffer open source delegato esclusivamente alla raccolta dei dati di traffico di posta elettronica che non consenta all'amministratore di accedere alle comunicazioni degli utenti.

ETHEREAL

Il punto di partenza su cui lavorare è stato lo sniffer Ethereal [22], software libero prodotto da un team di programmatori sparso in tutto il mondo e coperto da licenza GNU GPL [23].

Esso consente il monitoraggio di reti basate sull'Internet Protocol, utilizzanti svariati tipi di supporti fisici. In particolare

- conversione e filtraggio dei dati e dei pacchetti in una forma leggibile dall'utente,
- analisi dei difetti di rete, come problemi di comunicazione tra hosts,
- analisi di qualità e portata della rete (performance analisys), ad es. per scoprire colli di bottiglia lungo la rete,

- setacciamento automatizzato di password e nomi di utenti,
- scoperta di intrusioni in rete.

Funzionamento

Innanzitutto occorre definire cos'è una interfaccia di rete e quali compiti svolge nel processo comunicativo. Con tale termine si indica un hardware, residente in una determinata macchina della rete, delegato a gestire il processo fisico della comunicazione mediante, da un lato la connessione al supporto trasmissivo (coppie di conduttori, etere o fibra ottica in genere), dall'altro i processi software che richiedono lo scambio di informazioni con altri processi remoti.

Per poter discriminare una macchina da un'altra, all'interno di una stessa rete, in modo che un dato processo chiamante, comunichi solo con il corrispettivo della macchina chiamata, ad ogni interfaccia viene assegnato dal costruttore un identificativo univoco chiamato "indirizzo MAC" (medium access control).

In "Modalità Normale" tale identificativo impone all'interfaccia di "catturare" solamente i messaggi che hanno per destinatario il proprio indirizzo, ignorando di fatto tutti gli altri messaggi. Si è così sicuri che il messaggio giunga al giusto destinatario o, qualora questo non fosse presente, venga tralasciato automaticamente.

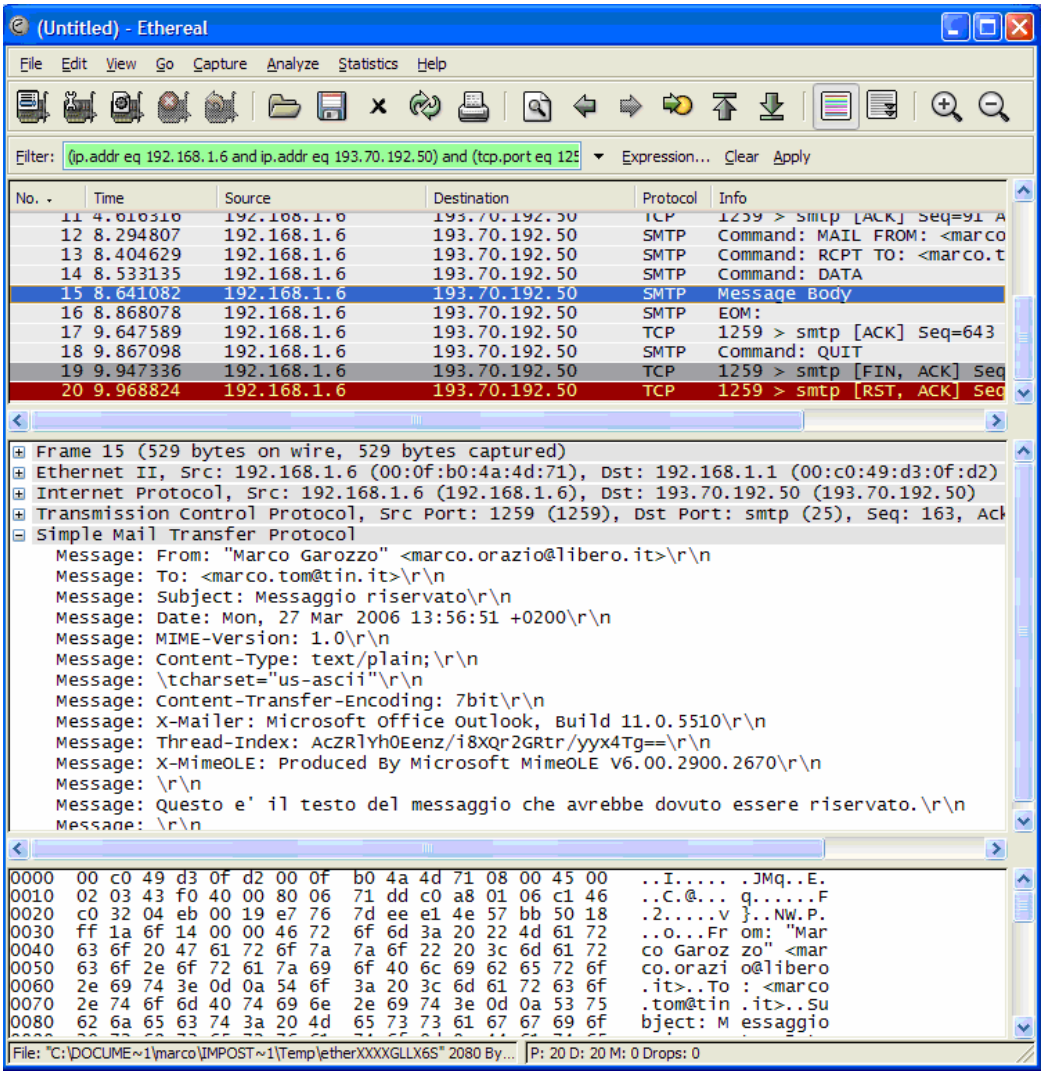
In questo meccanismo entra in gioco Ethereal che, affiancandosi ai driver della scheda di rete selezionata dall'utente, attiva una modalità detta "promiscua". In modalità promiscua tutti i messaggi transitanti il mezzo fisico vengono catturati, indipendentemente siano essi indirizzati alla macchina oppure no, e passati al

processo software di livello superiore, che in questo caso è proprio Ethereal. In tale maniera, di fatto, lo sniffer ha a disposizione il flusso di bit che scorre nel tratto di rete dove insiste l'interfaccia.

Caratteristiche

Avendo a disposizione il flusso di dati in transito, Ethereal lo analizza, separando le informazioni appartenenti a livelli protocollari diversi.

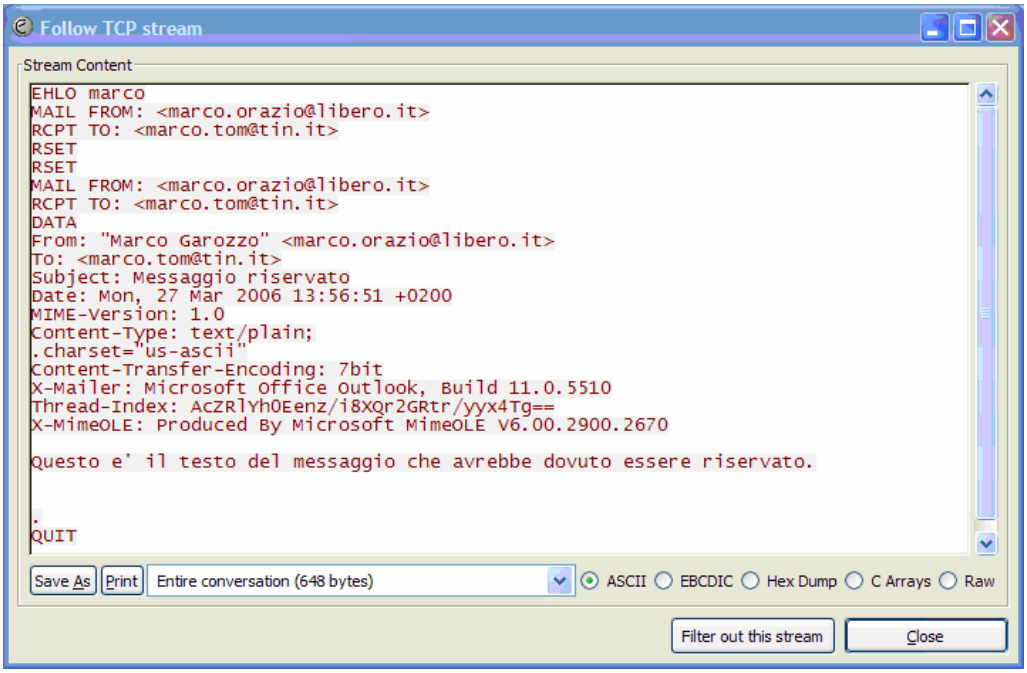
Così se si prende ad esempio la figura,



Ethereal suddivide l'informazione raccolta in:

- frame ethernet, consentendo la discriminazione degli indirizzi Mac del mittente e del destinatario (mitt.: 000fb04a4d71 – dest.: 00c049d30fd2)
- Pacchetto IP, fornendo tutte le informazioni quali indirizzi IP (mitt.: 192.168.1.6 - dest.: 193.70.192.50), TOS, frammentazione, ecc.
- Segmento TCP, individuando la porta (mitt.: 1259 – dest.: 25) o il numero di sequenza, ecc.
- Protocollo applicativo utilizzato, suddividendo le informazioni per i servizi più noti (http, FTP, SMTP, POP, ecc.), nell'esempio si evidenzia bene che il contenuto della comunicazione è un'email inviata da marco.orazio@libero.it a marco.tom@tin.it dal contenuto confidenziale, ma che viene così intercettato dall'utilizzatore di Ethereal.

Con tale programma è inoltre possibile ricostruire tutto il flusso di una sessione TCP, ottenendo una registrazione completa della comunicazione:



Struttura del Programma

Ethereal si può dividere in tre parti: le librerie di Packet CAPturing (PCAP) [24], l'interfaccia grafica e gestionale e i filtri di dissezione.

Le librerie di packet capturing è la parte del software che specificamente si affianca al driver della scheda di rete, ponendola in modalità promiscua e catturando dal flusso di bit, quelle porzioni di informazioni che rispondono a determinate caratteristiche. Una volta catturate le informazioni desiderate, tali librerie restituiscono all'interfaccia gestionale l'indirizzo di memoria dove sono stati posti i dati, per l'elaborazione successiva.

L'interfaccia gestionale ha il compito di fornire all'utente un frontend grafico che consente di indicare il tipo di traffico da catturare e, successivamente, la sua rappresentazione. Tipicamente questa viene fatta come una lista ramificata: gli elementi della lista rappresentano i pacchetti, selezionati i quali, attraverso i nodi è possibile accedere alle diverse informazioni suddivise in livelli protocollari. Attraverso l'interfaccia è anche possibile filtrare i dati raccolti in base a caratteristiche indicate in appositi form.

I Filtri di dissezione sono script del codice di Ethereal che consentono la discriminazione del contenuto dei pacchetti catturati, evidenziando i vari protocolli applicativi, i campi e le richieste protocollari. E' per esempio possibile filtrare i pacchetti che contengono richieste di traffico FTP non accolte, comandi SMTP di invio, ecc.

SMTSNIFF

Per la cattura dei soli dati del traffico è sembrato opportuno basarsi solamente sugli elementi che costituiscono la base di Ethereal, ovvero sulle librerie PCAP, preferendo un approccio down-top, piuttosto che sfoltire l'interfaccia gestionale, complessa e dalle funzionalità intrecciate.

I vantaggi di una opportuna modifica di Ethereal per la raccolta dei dati sul traffico di email, scambiate nel server di posta da gestire sono:

- Ethereal è un software libero, il suo codice sorgente è conosciuto, modificabile, ridistribuibile, rivendibile, a patto di mantenere il software sviluppato sotto la licenza GNU GPL. Modificando quindi le feature che lo rendono lesivo della privacy, è quindi perfettamente utilizzabile. Questo risponde appieno alle direttive sull'e-government che promuovono l'utilizzo di software libero nelle Pubbliche amministrazioni. La possibilità di svincolarsi da un marchio, la personalizzazione, il perfezionamento continuo sono una garanzia di qualità del prodotto, di continuità per il futuro, di risparmio in termini economici.
- Si ottiene esattamente il risultato che si vuole ottenere, registrando esclusivamente l'orario di connessione, e i soggetti coinvolti, escludendo di fatto anche la possibilità di accedere al contenuto della comunicazione.
- La registrazione dei dati avviene su una macchina che può essere diversa da quella che gestisce il server di posta. Questa è una buona scelta strategica, poiché un malintenzionato che volesse cancellare i dati di

traffico, attaccando il server non avrebbe minimamente notizia che tali dati vengono raccolti altrove. Tale soluzione è molto indicata anche per prevenire perdite dovute ad eventi non dolosi, quali i crashes di sistema.

Lo sviluppo del software finale, denominato "Smtsniff", si è dunque articolato in diverse fasi, comprendenti l'analisi dell'output desiderato, l'analisi del traffico di posta, lo sviluppo del software e il testing.

ANALISI DELL'OUTPUT DESIDERATO

Lo studio della normativa inizialmente effettuato, sottolineava che il primo adempimento richiesto dalla legge Italiana è che, di fatto, ogni utente avente accesso ad Internet sul territorio, abbia una identificazione forte. Dal momento che condizione necessaria alla connessione è il possesso di un indirizzo IP pubblico, ciò si traduce nel fatto che chiunque abbia assegnato tale indirizzo deve essere preventivamente registrato. Ciò significa che per gli utenti domestici, fa fede il contratto stipulato con il provider, per gli utenti di postazioni pubbliche (come internet point) è necessaria la registrazione di un documento di identità valido e per gli utenti aziendali o di enti pubblici, un registro che tenga conto dell'assegnazione delle credenziali di accesso.

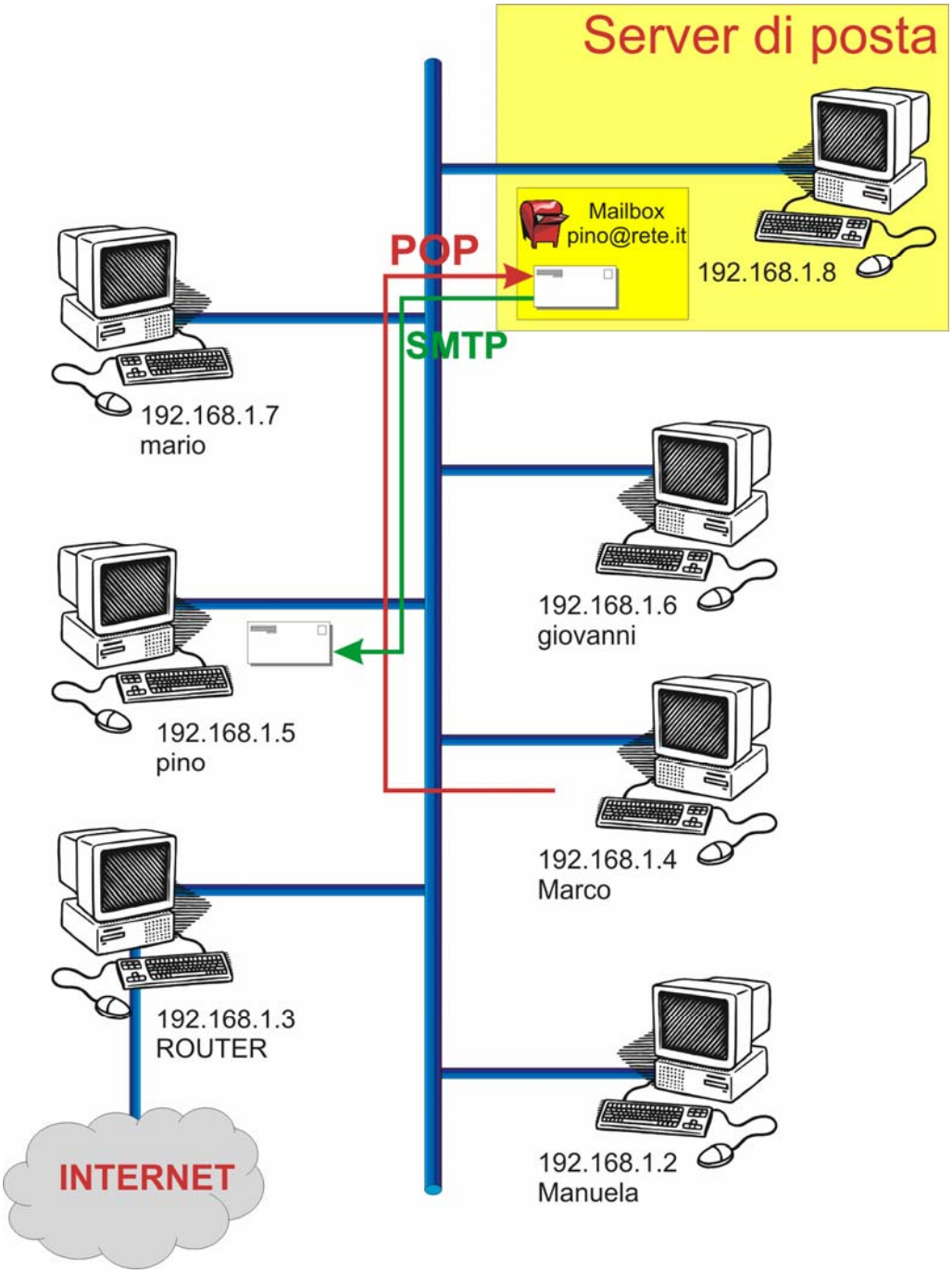
Appurato ciò, con il termine "dato del traffico", si può indicare la registrazione temporale, dell'indirizzo IP del mittente, quello del destinatario e dell'azione di traffico effettuata. Nel caso in esame, dovendo tenere dettaglio del solo invio di un messaggio di posta, è sufficiente la redazione di un registro contenente solo le prime tre informazioni.

Essendo l'invio di un messaggio un'operazione molto frequente e, dovendo automatizzare il processo di tabulazione, è logico redigere tale registro come file di testo in continuo aggiornamento, residente su disco rigido della macchina che esegue il controllo. Tale output è facilmente interpretabile ed esportabile in qualunque formato dalle forze di polizia giudiziaria su mandato della magistratura che ne dovessero fare richiesta.

In aggiunta agli indirizzi IP del mittente e del destinatario, è possibile particolareggiare ulteriormente i dati sul traffico includendo alcune informazioni racchiuse nell'header del messaggio di posta, non assimilabili a "contenuto della comunicazione". Si era visto, analizzando il formato del messaggio, che l'header dello stesso contiene campi come, Received, from, to, subject. Mentre quest'ultimo può ritenersi come parte della comunicazione (pertanto non registrabile), altri campi danno informazioni più dettagliate sul percorso effettuato, sul mittente e sui destinatari. La loro raccolta, quindi, contribuisce a rendere più efficace la documentazione del traffico.

CHE TIPO DI TRAFFICO CATTURARE

Supponendo di dover gestire un server di posta connesso ad una rete locale, basata sul protocollo TCP/IP, è plausibile restringere inizialmente il campo a quei pacchetti che sicuramente riguardano lo scambio di messaggi di posta. Come si è visto i protocolli competenti questo scambio sono il POP (porta 110 TCP) e SMTP (porta 25 TCP). Una analisi più accurata mostra però che questo approccio è fortemente ridondante.



Osservando la figura, si nota infatti che catturando sia il traffico POP che quello SMTP, avremo sempre delle registrazioni raddoppiate dovute al fatto che se un

utente invia un messaggio ad una mailbox residente nel server, questo viene registrato sia quando arriva al server (mediante SMTP), sia quando il proprietario della mailbox scarica la posta. L'utente potrebbe addirittura lasciare la mail nel server e scaricarla diverse altre volte, su postazioni diverse, generando in questa maniera tante false nuove registrazioni duplicate.

Inoltre, dall'analisi delle chiamate effettuate dal protocollo SMTP, si nota che, per una corretta registrazione della comunicazione, basta semplicemente catturare solamente le richieste rivolte verso il server (e quindi aventi la porta 25 TCP come destinazione) e non le conferme che questo ritorna (provenienti dalla porta 25).

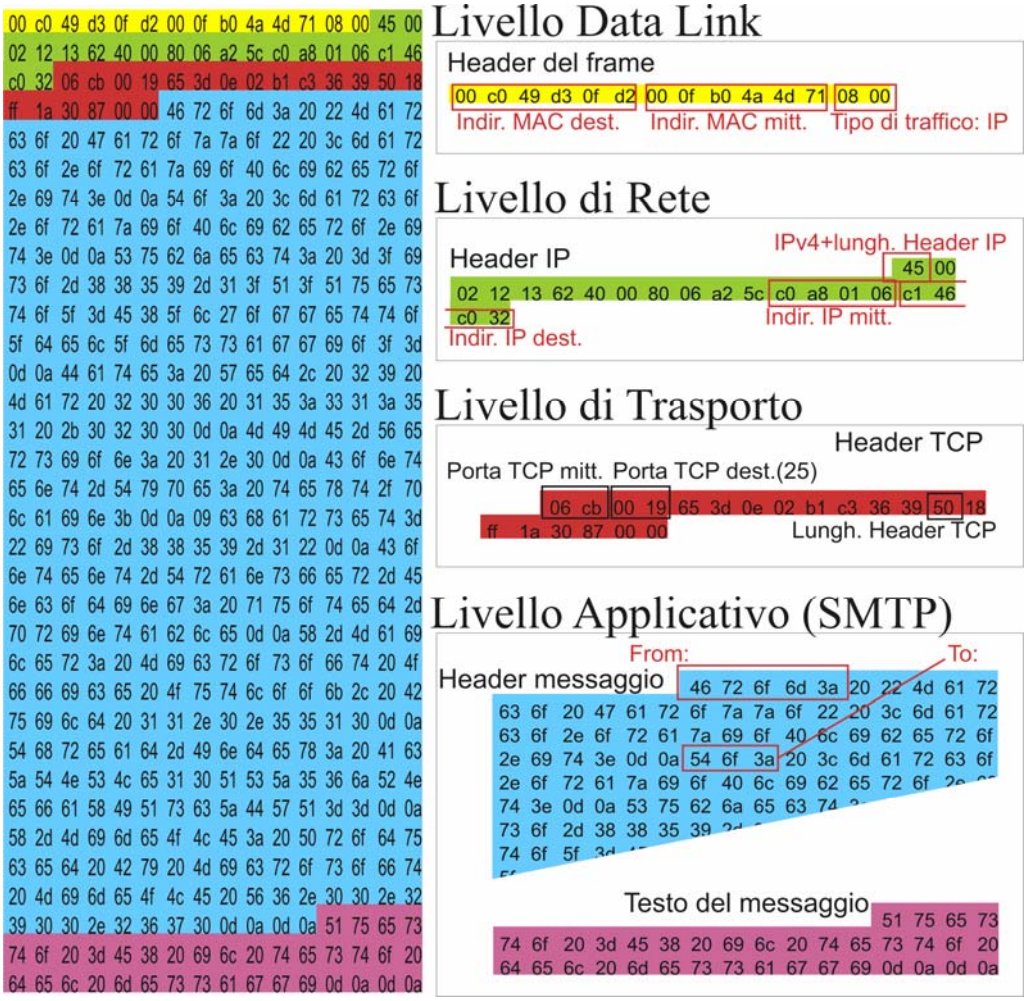
Con questa strategia è possibile discriminare due categorie di traffico di posta: i messaggi rivolti a mailboxes residenti nel server, e messaggi a destinatari di altri domini (quest'ultimo tipo di traffico è detto "di relay"). Infatti se, per esempio, ad un server di posta denominato posta.pippo.com, perviene un messaggio per l'indirizzo mario@pluto.com, il compito del server sarà quello di reindirizzare (o forwardare) la mail al webserver di pluto.com o, in mancanza, ad un altro server SMTP. In tale maniera, il primo tipo di traffico avrà una singola registrazione, mentre il secondo ne avrà due, quella in ingresso e quella in uscita, ma sarà facilmente discriminabile poiché indirizzato a mailboxes con dominio diverso dal proprio.

E' da sottolineare, inoltre, che non serve la cattura e l'analisi di ogni pacchetto rispondente queste caratteristiche: come si vedrà successivamente, ogni trasferimento di email è infatti, costituito dallo scambio di una sequenza ben

determinata di pacchetti che precede il messaggio vero e proprio. Ogni messaggio, che costituisce quindi un flusso di pacchetti, è ben distinguibile dai cosiddetti "endpoints" ovverosia da una quaterna di indirizzi identificativi: l'indirizzo IP e la porta TCP del mittente e l'indirizzo IP e la porta TCP del destinatario (quest'ultima è fissata, per le strategie prefissate, alla 25). In un lasso temporale sufficientemente ampio, gli endpoints consentono di discriminare lo scambio di ogni messaggio, prescindendo il fatto che i pacchetti costituenti diversi messaggi si possono interlacciare cronologicamente. Per ogni quaterna di endpoints è pertanto sufficiente catturare ed analizzare i primi 2000 bytes (poiché è da questi che si discrimina di quale tipo di pacchetto si tratti) e tralasciare tutti i pacchetti successivi al terzo. Si noti che tale scelta contraddistingue Smtsniff da Ethereal per velocità e risorse richieste: mentre il primo si limita a catturare lo stretto indispensabile, il secondo deve memorizzare il messaggio per intero onde poterne fare un analisi efficiente.

DAL FRAME AI DATI DEL TRAFFICO DI POSTA

Accedendo al data link layer in modalità promiscua, si ottiene un frame (supposto di tipo ethernet) grezzo, ovvero un insieme di byte a cui inizialmente non è possibile attribuire alcun significato.



Per poter ricavare informazioni utili, è necessario applicare una formattazione per cui ogni byte fornisca una determinata informazione. Nell'esempio, sapendo che il preambolo del frame è di 14 byte, è possibile individuare l'inizio del pacchetto IP. Essendo note le posizioni degli indirizzi nell'header IP, è possibile estrapolarle dai dati, essendo inoltre trasmessa anche la lunghezza dell'header (in parole di 32 bit) è facile individuare l'inizio del segmento TCP. Da questo si estrapola l'indicazione della porta sorgente (primi 2 byte dell'header) e la

lunghezza dell'header TCP (in parole di 32 bit). E' quindi noto dove inizia il payload applicativo. Si possono presentare a questo punto diverse situazioni.

Richiesta protocollare "mail from:"

Quando vi è trasferimento di un messaggio, la comunicazione inizia con l'invio al server di un messaggio contenente il testo "mail from:" seguito dal nome del mittente. Intercettando tale pacchetto e conservando tale indirizzo si ha una prima informazione sul messaggio in oggetto. Nel codice di Smtsniff, un arrivo di questo tipo è identificato con il termine SRC.

Richiesta protocollare "rcpt to:"

Dopo l'invio del nome del mittente, il protocollo smtp prevede, l'invio di un pacchetto contenente il testo "rcpt to:" seguito dall'indirizzo del destinatario. Raccogliendo quest'altro indirizzo, si caratterizza maggiormente il dato sul traffico SMTP. Nel codice di Smtsniff, un arrivo di questo tipo è identificato con il termine DST.

Header del messaggio e testo del messaggio

Terminate le fasi precedenti vi è l'invio del messaggio vero e proprio, nel cui inizio si troverà l'intestazione, come si è visto analizzando il formato del messaggio. Per avere, quindi, una completa caratterizzazione del percorso dell'email è necessario registrare il contenuto dei campi:

- from:
- to:
- date:
- received:
- delivered:
- return-path:

Alcuni dei quali contengono informazioni ridondanti, ma forniscono una conferma ulteriore dell'identità dei soggetti e sul percorso effettuato.

Si sottolinea ulteriormente che l'ordine cronologico di arrivo dei vari pacchetti è quello esaminato, anche in presenza di perdite o duplicazioni nel cammino. Infatti, prima di inviare il nome del destinatario e prima di inviare il messaggio, il mittente attende che il server abbia ricevuto correttamente i dati e che abbia inviato una conferma. L'arrivo di questo tipo di pacchetto esaurisce le informazioni necessarie per una registrazione definitiva che per tanto deve essere effettuata.

Nel codice di Smtsniff, un arrivo di questo tipo è identificato con il termine HDR.

Parti del testo del messaggio

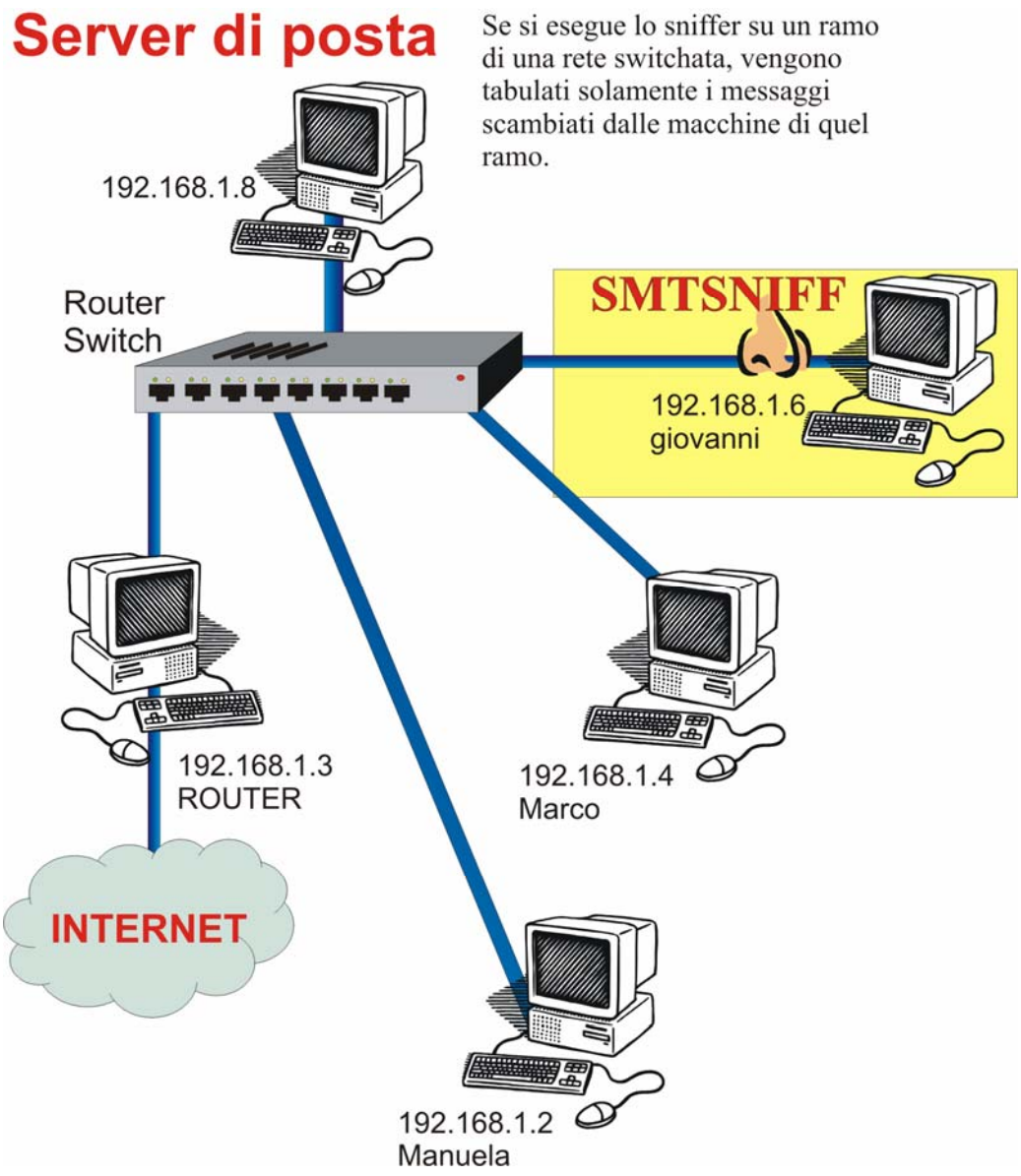
Qualora il messaggio, magari contenente file allegati, eccedesse le dimensioni di un pacchetto, sarebbe distribuito su diversi pacchetti caratterizzati comunque da una quaterna di endpoints ben specificata. Gli eventuali pacchetti successivi al terzo, contengono infatti i byte che non possono essere spediti con l'header e

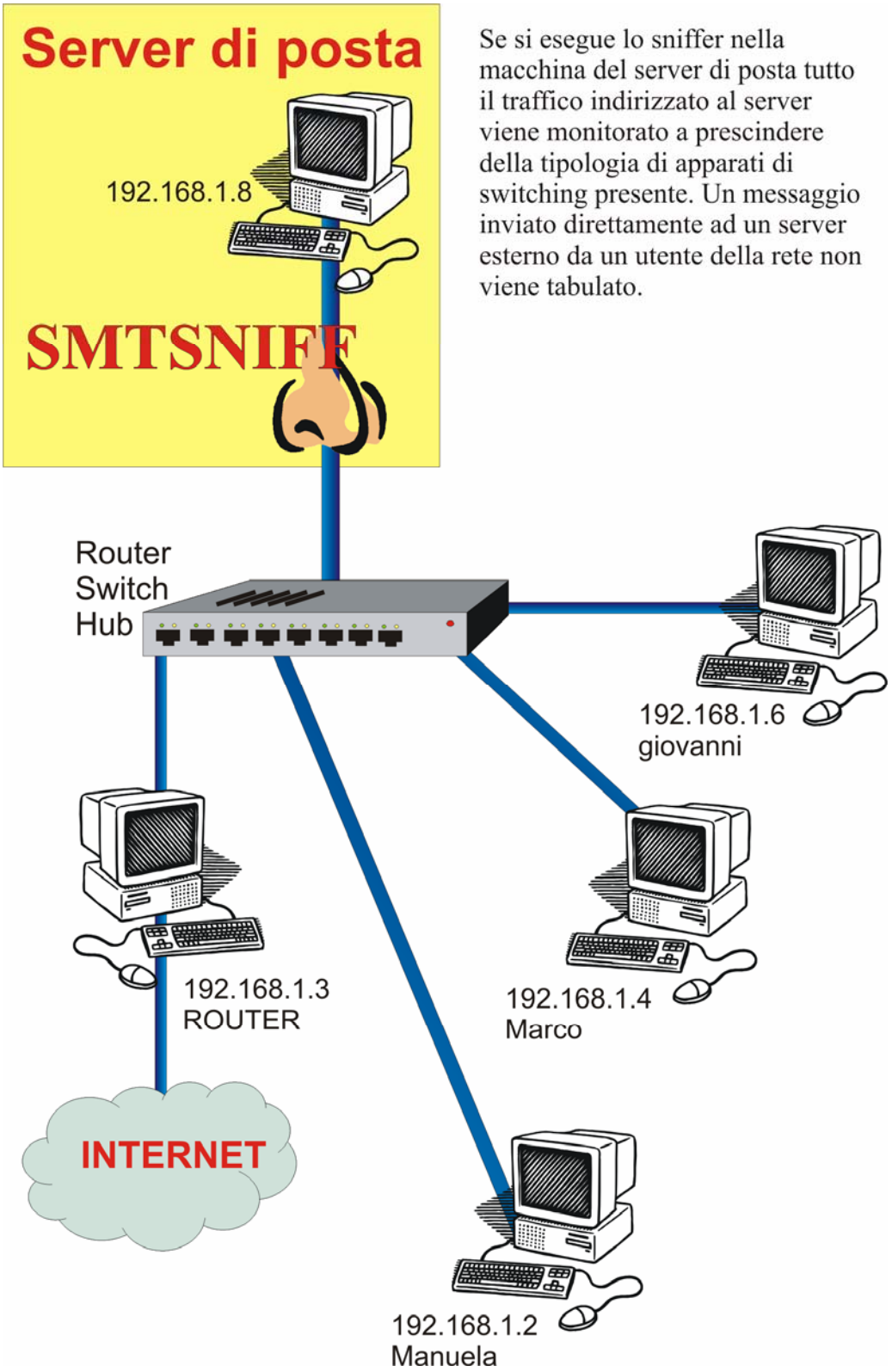
l'inizio del messaggio (un pacchetto IP può contenere al massimo 65356 byte). Tali pacchetti non costituiscono pertanto nuove registrazioni di traffico e devono essere scartati.

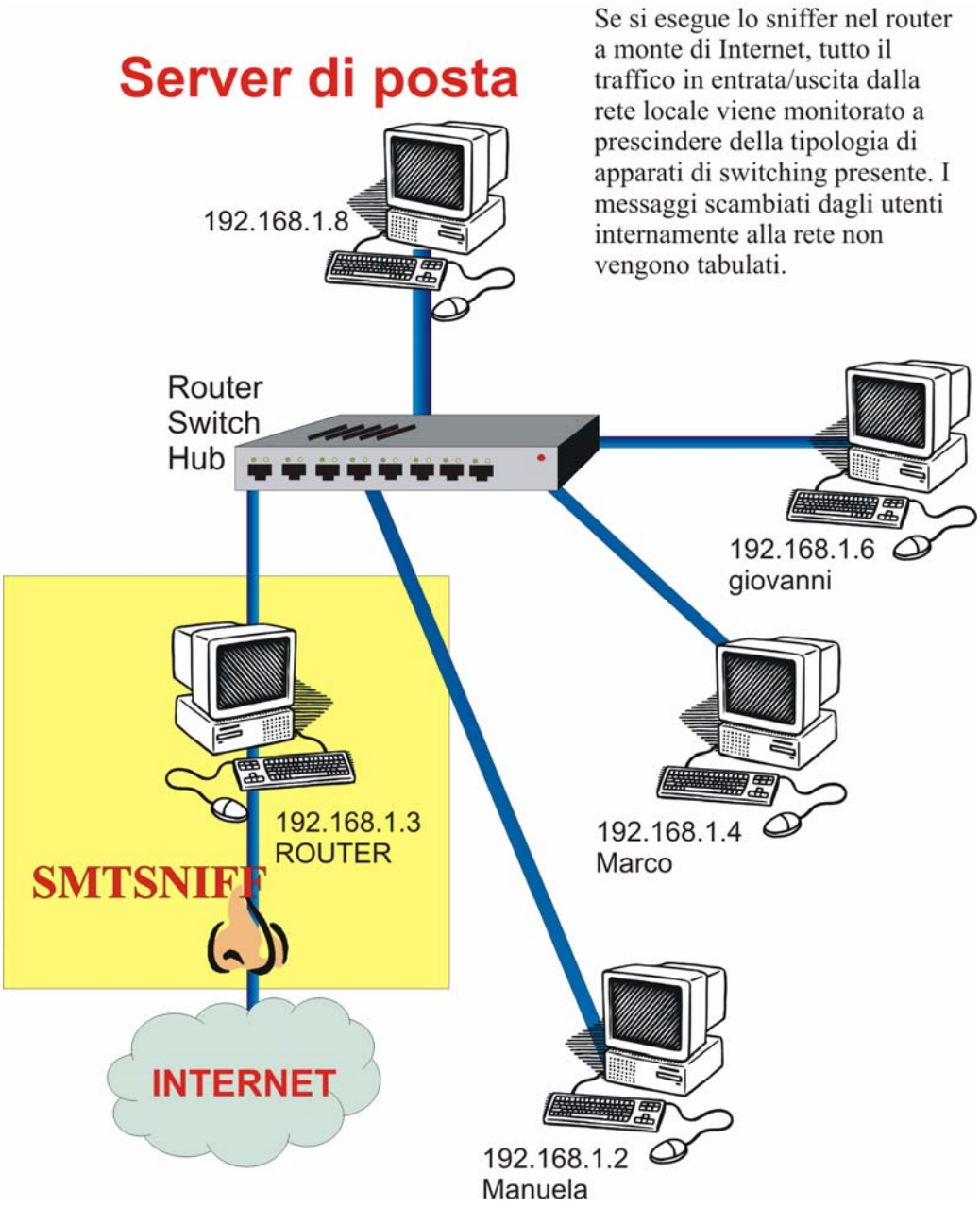
TOPOLOGIE DI RETE E POSIZIONAMENTO DELLO SNIFFER

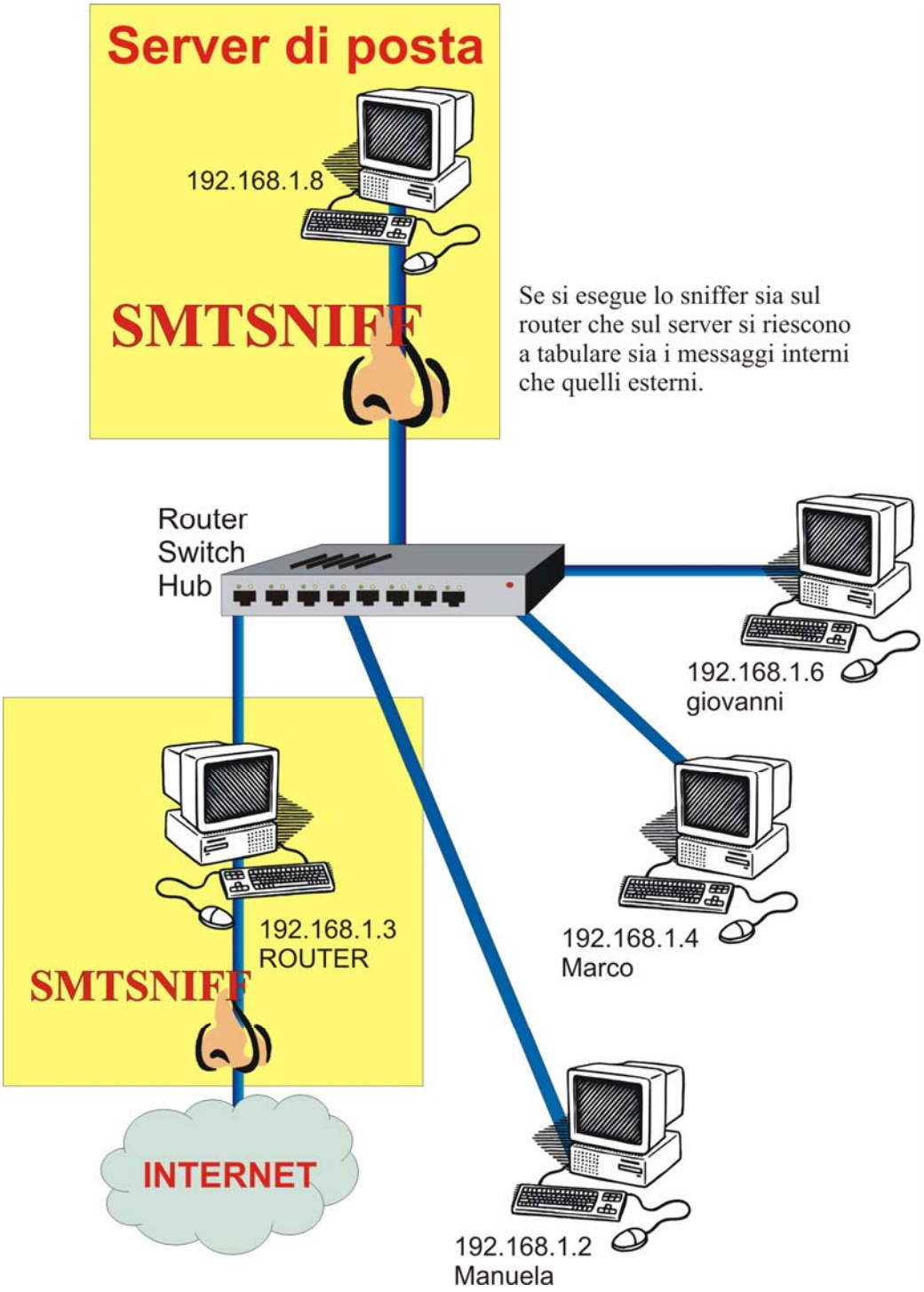
In base alla topologia della rete, alla posizione che lo sniffer ha in essa e alla tipologia degli apparati di instradamento o switching installati, si potrebbero avere diversi risultati. Questo dipende da alcune considerazioni tecniche:

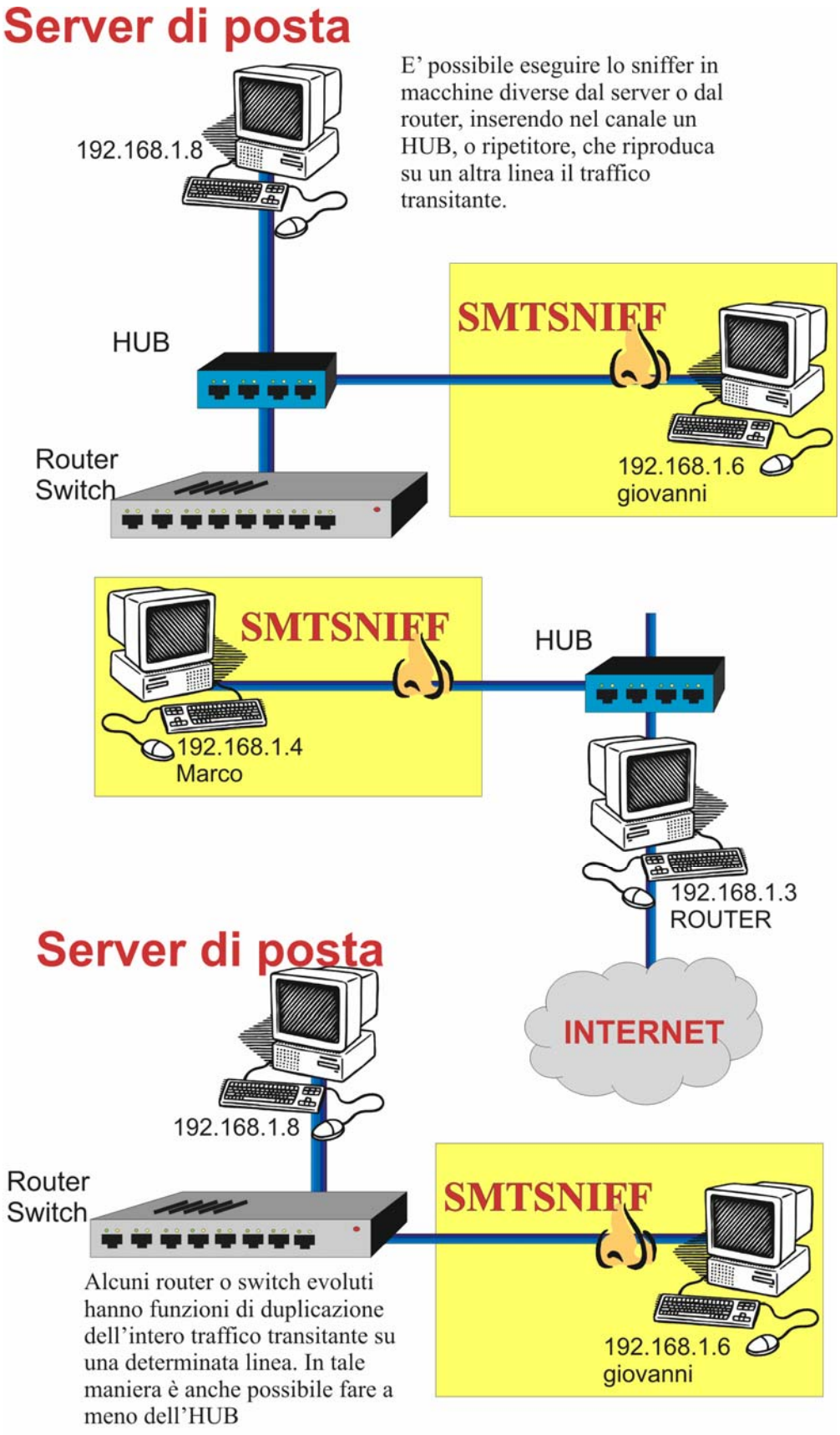
- Lo sniffer registra solamente il traffico presente nel ramo di rete in cui è collocato.
- Apparati di rete come router o switch in genere, sono programmati per indirizzare un frame o un pacchetto nel solo ramo in cui vi è il destinatario.
- Potrebbe anche solo bastare (ai fini legali) tenere le registrazioni del traffico email scambiato con l'esterno della rete aziendale, tralasciando i messaggi scambiati fra gli utenti interni alla rete aziendale (per fare un paragone, se non facessimo questa distinzione, sarebbe come se si tenessero i tabulati delle telefonate effettuate da una stanza all'altra di un medesimo ufficio).


Server di posta
Se si esegue lo sniffer su un ramo di una rete switchata, vengono tabulati solamente i messaggi scambiati dalle macchine di quel ramo.
192.168.1.8
Router
Switch
SMTSNIFF
192.168.1.6
giovanni
192.168.1.3
ROUTER
192.168.1.4
Marco
INTERNET
192.168.1.2
Manuela


Server di posta
192.168.1.8
SMTSNIFF
Se si esegue lo sniffer nella macchina del server di posta tutto il traffico indirizzato al server viene monitorato a prescindere della tipologia di apparati di switching presente. Un messaggio inviato direttamente ad un server esterno da un utente della rete non viene tabulato.
Router
Switch
Hub
192.168.1.6
giovanni
192.168.1.3
ROUTER
192.168.1.4
Marco
INTERNET
192.168.1.2
Manuela


Server di posta
Se si esegue lo sniffer nel router a monte di Internet, tutto il traffico in entrata/uscita dalla rete locale viene monitorato a prescindere della tipologia di apparati di switching presente. I messaggi scambiati dagli utenti internamente alla rete non vengono tabulati.
192.168.1.8
Router
Switch
Hub
192.168.1.6
giovanni
192.168.1.3
ROUTER
SMTSNIFF
192.168.1.4
Marco
INTERNET
192.168.1.2
Manuela


Server di posta
192.168.1.8
SMTSNIFF
Se si esegue lo sniffer sia sul router che sul server si riescono a tabulare sia i messaggi interni che quelli esterni.
Router
Switch
Hub
192.168.1.6
giovanni
192.168.1.3
ROUTER
SMTSNIFF
192.168.1.4
Marco
INTERNET
192.168.1.2
Manuela


Server di posta
E' possibile eseguire lo sniffer in macchine diverse dal server o dal router, inserendo nel canale un HUB, o ripetitore, che riproduca su un altra linea il traffico transitante.
192.168.1.8
HUB
Router
Switch
SMTSNIFF
192.168.1.6
giovanni
SMTSNIFF
192.168.1.4
Marco
HUB
192.168.1.3
ROUTER
INTERNET
Server di posta
192.168.1.8
Router
Switch
SMTSNIFF
192.168.1.6
giovanni
Alcuni router o switch evoluti hanno funzioni di duplicazione dell'intero traffico transitante su una determinata linea. In tale maniera è anche possibile fare a meno dell'HUB

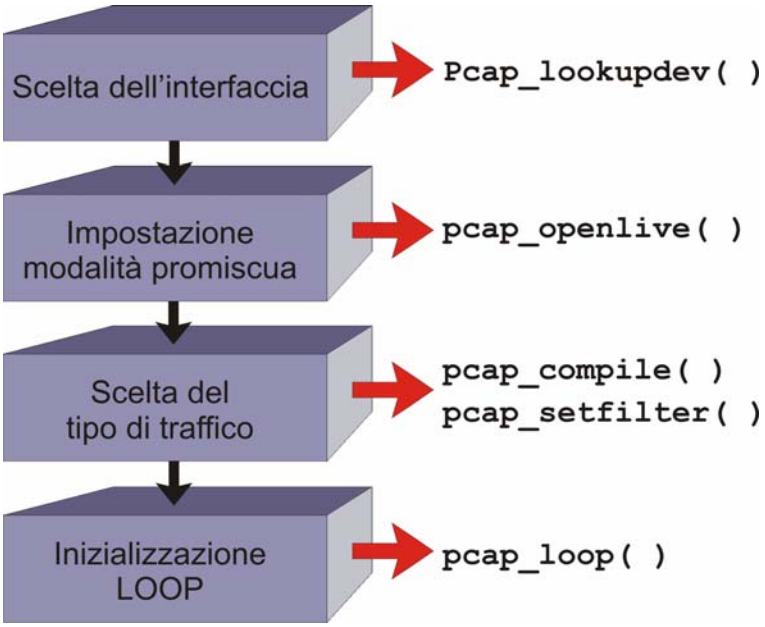
SVILUPPO DEL SOFTWARE

Dal momento che Smtsniff deve svolgere dei semplici compiti di accesso alla rete e scrittura su file, si è scelto di usare il linguaggio C, usando un'interfaccia testuale. Questo semplifica la programmazione, agevola la portabilità e sfrutta librerie preesistenti.

L'accesso diretto al flusso dei dati: Le librerie PCAP.

Si è detto che la prima operazione da effettuare è l'accesso all'interfaccia di rete in modalità promiscua. Questo si ottiene sfruttando una sequenza di primitive i cui prototipi sono definiti nel file lpcap.h. La libPCAP è stata sviluppata inizialmente da Van Jacobson, Craig Leres e Steven McCanne del Lawrence Berkeley National Laboratory, University of California, Berkeley, CA nel 1993, attualmente, la 0.9.4, è distribuita in licenza BSD [25].

Lo schema di tale sequenza [26] è il seguente:



pcap_lookupdev( ) serve a cercare la prima periferica disponibile, qualora questa non fosse indicata da riga di comando.

pcap_open_live( ) serve ad impostare la periferica selezionata in modalità promiscua e le assegna un identificativo (un handle) di riferimento.

pcap_compile( ) serve a tradurre l'espressione del filtro impostata (nel caso in esame "TCP dst port 25") in una forma compatibile per le pcap.

pcap_setfilter( ) serve a rendere attivo il filtro compilato dalla precedente espressione.

pcap_loop( ) serve a richiamare una funzione di callback ogni volta che vi è un frame corrispondente all'espressione del filtro. Il frame viene posto in un'area di memoria il cui indirizzo è passato per riferimento alla callback (denominata arrivo) per consentirne l'elaborazione.

Il riconoscimento del supporto al TCP

Il protocollo SMTP si basa sul protocollo di trasporto TCP, il quale si appoggia a protocolli e apparati di livello inferiori che non sono noti a priori, variando di sistema in sistema. Non essendo supportata la compatibilità verso alcuni di essi si è implementato in Smtsniff un meccanismo di autodetecting che consente di avvisare l'utente della mancata compatibilità del sistema. Le limitazioni possono essere il datalink sconosciuto o non supportato e utilizzo del protocollo di rete IPv6 anziché IPv4. In particolare, la prima limitazione è dovuta al fatto che le librerie PCAP passano alla callback tutto il frame catturato, per cui, essendo

necessario distinguere alla perfezione i byte dell'header di secondo livello dal contenuto, si è puntato a quei protocolli con header fissi e facilmente discriminabili. Il supporto a particolari tipi di datalink, necessitando studi protocollari particolareggiati da caso a caso, e la discriminazione di tipi di indirizzi IP diversi, esulano lo scopo della trattazione. I protocolli di livello due supportati sono dunque IEEE 802.3, il raw IP, e il Linux cooked IP (un formato interno al linux, restituito quando si monitorano diverse interfaccie contemporaneamente).

La funzione che riconosce il datalink è la **pcap_datalink( )**, quest'informazione è passata alla funzione **stampa_data_link( )** che si occupa di visualizzare a video l'informazione e di memorizzare in una variabile, se è un data link supportato, la lunghezza dell'header di livello due.

La Callback

Ad ogni pacchetto contenente un segmento TCP destinato alla porta 25, la funzione **pcap_loop( )** richiama una funzione denominata **arrivo ( )**.

Questa inizializza una struttura dati composta chiamata SM e, in caso di compatibilità del frame, attiva una funzione che riconosce il pacchetto IP, passandole il puntatore all'area di memoria dove esso è contenuto (basta traslare l'indirizzo di memoria del frame di tanti byte quanti ne compongono l'header, essendo già nota la grandezza di quest'ultimo).

La funzione **Leggi_IP( )** ha, per l'appunto, il compito di effettuare un casting sui dati, ottenendo la formattazione dell'header IP. Ciò consente l'individuazione

degli indirizzi IP (che vengono trascritti su SM), e del punto di inizio del segmento TCP.

A questo punto viene lanciata la funzione **Leggi_TCP( )** che ha il compito di applicare il pattern dell'header TCP ai dati restanti. Viene così prelevata la porta di origine e associata al record di SM (così si caratterizzano gli endpoints, che in questa trattazione sono 3, essendo il quarto noto). Se la lunghezza dei dati è pari a zero, si è di fronte ad un pacchetto, inviato dal protocollo TCP per l'handshake, ovvero per instaurare la connessione: non avendo contenuto significativo, questo viene tralasciato. Nel caso siano presenti byte di payload per il TCP, si prosegue con la loro analisi.

Determinato il traffico applicativo, viene eseguita la funzione **riconoscicampi( )** che ha il compito di scandire byte per byte il contenuto del TCP e riconoscere i campi di interesse. Qualora venissero trovati, essi contribuirebbero alla ulteriore caratterizzazione della struttura SM, che, a questo punto, viene completata. **Riconoscicampi( )** restituisce inoltre, la tipologia del pacchetto appena giunto secondo la classificazione attuata in precedenza: SRC, DST, HDR o NULL.

La gestione delle code

La situazione per cui un arrivino i pacchetti SRC, DST, HDR, riferiti ad un'unica quaterna di endpoints, tutti in sequenza è puramente ideale. Ciò è dovuto al fatto che un server SMTP è di tipo concorrente, ovvero può accettare più di una chiamata alla porta 25 contemporaneamente. Ciò comporta che pacchetti corrispondenti a endpoints diversi si interlaccino nel flusso del canale e

determinino ordini di arrivo diversi nella raccolta delle informazioni sul messaggio. Essendo assolutamente da evitare l'errore di associare un mittente di un messaggio, dal destinatario di un altro è necessario prevedere un meccanismo di conservazione temporanea dei dati del messaggio, in attesa del suo perfezionamento. Indici identificativi del messaggio in tale struttura sono propriamente gli endpoints.

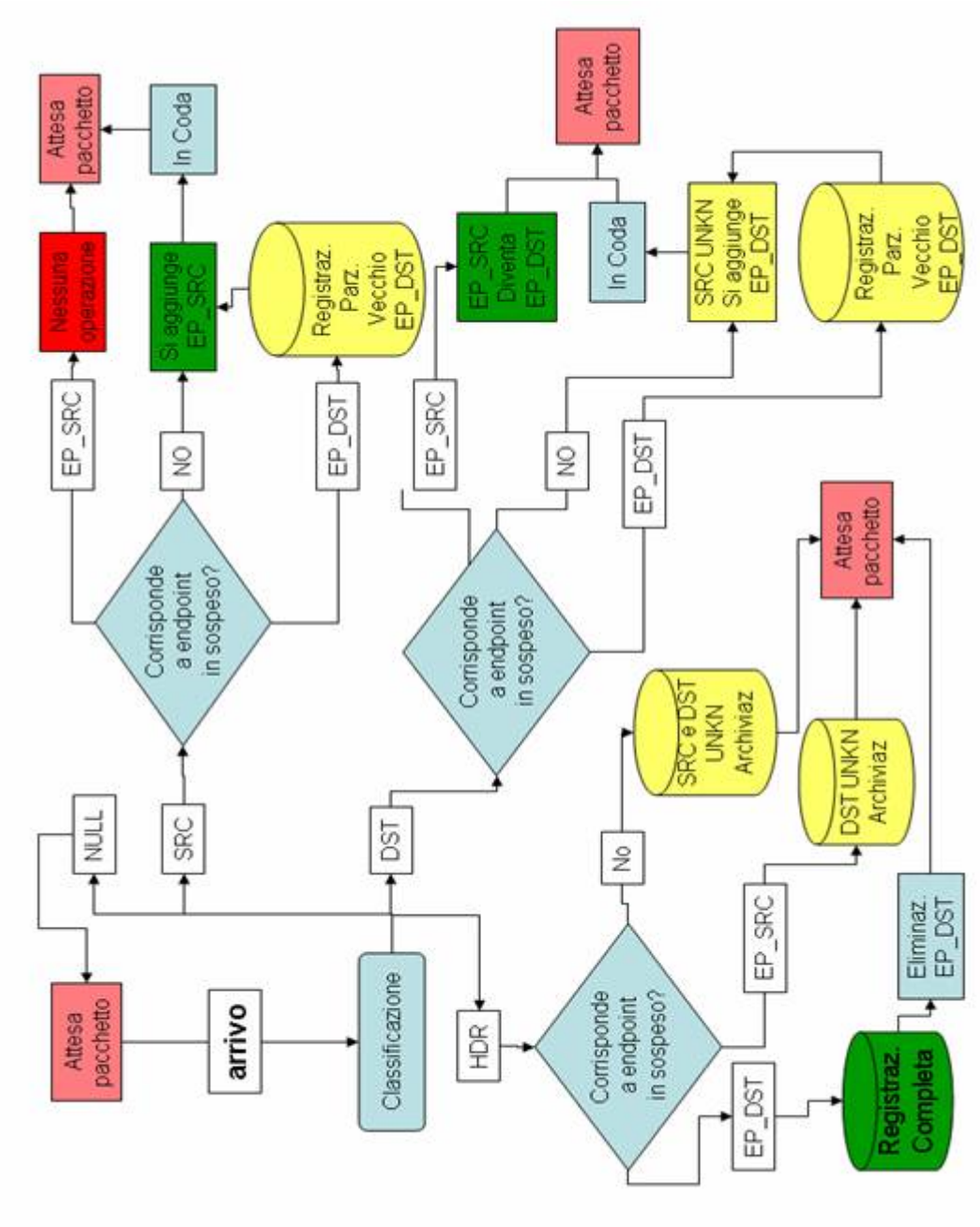
Data la lentezza delle operazioni di accesso al disco, rispette a quelle di accesso alla RAM, si è scelto di creare una coda dinamica che conservi i dati estratti dai pacchetti di tipo SRC o DST.

All'arrivo di un pacchetto, viene discriminato nella seguente maniera:

- Se esso è un SRC, si verifica della presenza nella coda di endpoints corrispondenti, se non vengono trovati, viene aggiunto un elemento denominato EP_SRC, contenente gli endpoints, una marca temporale e il contenuto del campo "mail from:".
- Se esso è un DST, si cerca l'elemento EP_SRC corrispondente, identificato dagli endpoints, si aggiorna la marca temporale e si aggiunge il contenuto del campo "rcpt to:". L'elemento diventa ora di tipo EP_DST.
- Se esso è un HDR, si cerca l'elemento EP_DST, si estrapolano i dati in esso contenuto e, assieme ai campi dell'header del messaggio appena giunto, si effettua la registrazione su disco dello scambio di email appena avvenuto. L'entità EP_DST a questo punto viene cancellata.

- Se esso è un NULL, probabilmente è parte del messaggio e viene tralasciato.

La situazione affrontata, non esaurisce però la casistica delle situazioni che possono accadere e degli stati in cui si può trovare Smtsniff. In generale, è possibile fare riferimento allo schema successivo:



Si noti la presenza di eventi in cui vi è la registrazione parziale dei dati, dovuta a pacchetti di tipo DST o HDR che non hanno endpoints corrispondenti nella coda. Essendo un evento possibile, seppur remoto, è necessario tenerne in considerazione.

Il controllo della coda viene effettuato da un set di funzioni denominato **confronta_endpts**, che scandisce gli elementi della coda, verificandone gli endpoints e il contenuto e eseguendo le operazioni del caso.

La coda ha dimensioni fissate da un parametro modificabile in sede di compilazione dei sorgenti. Ogniqualvolta ecceda il limite fissato, Smtsniff, mediante la funzione **flushlim( )**, provvede all'archiviazione parziale di un certo numero di elementi più vecchi.

Tale coda viene scaricata, anche quando è invocata la funzione **close_all( )**, evento causato da un errore o dall'interruzione dell'utente.

Output ricavato

Le funzioni che si occupano del salvataggio del registro del traffico smtp sono **scrivi_dati( )** e **scrivi_parziali( )**. La prima viene invocata all'arrivo del pacchetto HDR, per cui, avendo tutte le informazioni utili, possiamo effettuare una registrazione completa. La seconda viene invocata in tutte quelle situazioni per cui, per qualche motivo, non si è arrivati a ricevere l'header di un messaggio ancora in coda. Un esempio è quando l'utente decide di chiudere il programma, nonostante siano presenti elementi nella coda: in quel momento interviene la

funzione **scarica( )**, che invoca **scrivi_parziali( )** e, man mano, elimina la coda deallocando la memoria RAM.

L'output ricavato è una serie di record formattati nel seguente modo:

```
Source IP: 192.168.1.6
Dest IP: 192.168.1.8
Sender source Port: 1260
Mail from: <marco@tom.grz.net>
Rcpt to: <marco.tom@tin.it>
mess-id:
date: Thu, 30 Mar 2006 12:11:39 +0200
from: "marco" <marco@tom.grz.net>
to: <marco.tom@tin.it>
received:
delivered:
return Path:
Arrival time: Thu Mar 30 12:11:43 2006

Source IP: 192.168.1.8
Dest IP: 193.70.192.50
Sender source Port: 32921
Mail from: marco@tom.grz.net> SIZE=2168
Rcpt to: marco.tom@tin.it>
mess-id: <20060330101143.AC1764E826@tom.grz.net>
date: Thu, 30 Mar 2006 12:11:39 +0200
from: "marco" <marco@tom.grz.net>
to: <marco.tom@tin.it>
received: from marco (unknown [192.168.1.6])   by tom.grz.net
(Postfix)
with ESMTP id AC1764E826   for <marco.tom@tin.it>; Thu, 30 Mar
200<marco.tom@tin.it>
delivered:
return Path:
Arrival time: Thu Mar 30 12:11:45 2006

Source IP: 192.168.1.7
Dest IP: 192.168.1.7
Sender source Port: 37519
Mail from: marco@marco.grz.net> SIZE=328
Rcpt to: marco.tom@tin.it>
mess-id: <442BD892.5090605@marco.grz.net>
date: Thu, 30 Mar 2006 15:09:38 +0200
from: marco <marco@marco.grz.net>
to:  marco.tom@tin.it
received:
delivered:
return Path:
Arrival time: Thu Mar 30 15:09:39 2006
```

In base all'esigenze di esportazione è facile, modificando di poco il sorgente, ottenere altre tipologie di output, come formati tabulari o untagged.

Il file che si ottiene, soddisfa appieno gli obiettivi preposti.

Testing

Smtsniff è stato compilato su due macchine, per testarne le capacità. La prima, un AMD Athlon 64 con 512 MB di memoria e sistema operativo Linux Mandrake LE 2005 (kernel 2.6.11) su cui era attivato un mailserver Postfix 2.1.5. La seconda, un Intel pentium 3, con 196 MB di memoria e sistema operativo Linux Red Hat 9.b (kernel 2.4.20) su cui era attivato un mail server Postfix 1.1.12. Ambedue le macchine erano in una LAN switchata, connessa ad internet mediante un router NPAT.

La compilazione in entrambe i casi non ha dato alcun problema, l'esecuzione è stata sempre stabile, anche quando Smtsniff è stato eseguito contemporaneamente su due terminali della stessa macchina per sniffare sia l'interfaccia principale che il loopback (smtsniff prevede l'output su file indicabili dall'utente via riga di comando).

Per la relativamente bassa mole di traffico prodotta le dimensioni delle code impostate durante la compilazione si sono dimostrate efficienti.

Il registro ottenuto è comprensibile, rispondente al traffico, forse eccessivamente prolisso per la ridondanza dei TAG, che precedono ogni campo.

Si evidenziano le doppie registrazioni dovute al forwarding, così come previsto.

APPENDICE A – Codice di Smtsniff

FILE SMTSNIFF.C

```
/* Compilazione: gcc -o smtsniff smtsniff.c funzioni.c -lpcap */

#include "smtsniff.h"

extern int link_layer;
extern pcap_t *handle;
extern char *fname;
extern epp ee;

int main(int argc,char* argv[])
  {

/* Definizione delle variabili del Main */

  char err[PCAP_ERRBUF_SIZE],*dev=NULL;
  char *userdev=NULL, *netad=NULL,*netm=NULL;
  bpf_u_int32 netaddr,netmask;
  struct in_addr address;
  epp ep;
  ep=(epp)malloc(sizeof(EPTS));
  ep->stato=NEP;
  ep->next=NULL;
  int i=1;
  struct bpf_program filtro_compilato;
  struct pcap_stat stat;
  u_char arg,data;
  struct pcap_pkthdr header;
  ee=ep;

/* Per i nostri scopi il filtro di cattura è strettamente fissato
*/

  char filtro[16]="tcp dst port 25";

/* A questi segnali lancia la funzione closeall */

  signal(SIGHUP,close_all);
  signal(SIGINT,close_all);
  signal(SIGKILL,close_all);
  signal(SIGPWR,close_all);
  signal(SIGQUIT,close_all);
  signal(SIGTERM,close_all);

/* Analizza la linea di comando */
```

```
  while(i<argc)
    {
    if(argv[i][0]=='-' && argv[i][1]=='h')
      {
      printf("\nUsage: %s (opt.) -f [filename] -d [device]
\n\n",argv[0]);
      exit(0);
      }
    else if(argv[i][0]=='-' && argv[i][1]=='f')
      {
      ++i;
      fname=argv[i];
      ++i;
      }

    else if(argv[i][0]=='-' && argv[i][1]=='d')
      {
      ++i;
      userdev=argv[i];
      ++i;
      }
    }

  if (fname==NULL) fname="file.dat";

  printf("\nFiltro specificato: %s\n\n",filtro);

/* Cerca la prima interfaccia che puo'essere aperta */

  if (userdev==NULL)
    {
    if(dev=pcap_lookupdev(err))
      printf("Device: %s\n\n",dev);
    else
      {
      printf("Errore lookupdev: %s\n",err);
      exit(0);
      }
    }
  else
    {
    dev=userdev;
    printf("Device: %s\n\n",dev);
    }

/* Ottiene l'indirizzo di rete e la subnet mask dell'interfaccia
*/

  if(pcap_lookupnet(dev,&netaddr,&netmask,err)==-1)
    {
    printf("Errore lookupnet: %s\n",err);
    exit(0);
    }
  else
    {
```

```
/* Stampa gli indirizzi in forma di ottetti */

    address.s_addr=netaddr;
    netad=(char *)inet_ntoa(address);
    printf("Network address: %s\n",netad);
    address.s_addr=netmask;
    netm=(char *)inet_ntoa(address);
    printf("Subnet mask: %s\n\n",netm);
    }

/* Apre l'interfaccia per lo sniffing; setta l'interfaccia di
rete in modalità promiscua, sniffa fin quando non occorre un
errore */

  if(!(handle=pcap_open_live(dev,DIM_PKT,1,0,err)))
    {
    printf("Errore open_live: %s\n",err);
    exit(0);
    }

/* Ottiene il tipo di link layer e la lunghezza del frame */

  link_layer=pcap_datalink(handle);
  Stampa_link_layer();

/* Compila l'espressione filtro specificata secondo il formato
delle LPCAP */

  if(pcap_compile(handle,&filtro_compilato,filtro,0,netmask)==-1)
    {
    printf("Errore compile: %s\n",pcap_geterr(handle));
    close_all(0);
    }

/* Applica l'espressione filtro appena compilata */

  if(pcap_setfilter(handle,&filtro_compilato)==-1)
    {
    printf("Errore setfilter: %s\n",pcap_geterr(handle));
    close_all(0);
    }

/* LOOP DI CATTURA */

  if(pcap_loop(handle,-1,arrivo,(u_char *)ep)==-1)
    {
    printf("Errore loop: %s\n",pcap_geterr(handle));
    close_all(0);
    }

/* Chiudiamo la sessione di sniffing, scarichiamo la coda di EP.
*/

  close_all(0);
  }
```

FILE FUNZIONI.C

```
#include "smtpsniff.h"

/* Variabili globali */

int link_layer=0,length_header_frame=0;
struct ether_header *frame=NULL;
struct hdlc_hdr *hdlc_pack=NULL;
pcap_t *handle=NULL;
FILE *miofile;
char *fname=NULL;
epp ee=NULL;

/* Funzione che mostra il tipo di link layer */

void Stampa_link_layer(void)
  {
  char *type=NULL;

  switch(link_layer)
    {
    case DLT_NULL:
      type="Link_layer assente";
      length_header_frame=4;
      break;
    case DLT_EN10MB:
      type="Ethernet";
      length_header_frame=14;
      break;
    case DLT_IEEE802:
      type="IEEE 802.5 Token Ring";
      break;
    case DLT_ARCNET:
      type="Arcnet";
      break;
    case DLT_SLIP:
      type:"Serial Line IP";
      break;
    case DLT_PPP:
      type="Point-to-point protocol";
      break;
    case DLT_FDDI:
      type="FDDI";
      break;
    case DLT_ATM_RFC1483:
      type="LLC/SNAP-encapsulated ATM";
      break;
    case DLT_RAW:
      type="raw IP";
      length_header_frame=0;
      break;
    case DLT_PPP_SERIAL:
      type="PPP o Cisco PPP in HDLC framing";
```

```
      break;
    case DLT_CHDLC:
      type="Cisco HDLC";
      break;
    case DLT_IEEE802_11:
      type="IEEE 802.11 wireless LAN";
      break;
    case DLT_LOOP:
      type="OpenBSD loopback encapsulation";
      length_header_frame=4;
      break;
    case DLT_LINUX_SLL:
      type="Linux \"cooked\" capture encapsulation";
      length_header_frame=16;
      break;
    default:
      type="Link layer sconosciuto";
      length_header_frame=0;
      break;
    }
  printf("Link layer: %s\n\n",type);
  }

/* Callback utilizzata in pcap_loop ad ogni arrivo */

void arrivo(u_char *arg,const struct pcap_pkthdr *header,const
u_char *data)
  {
  static int count=1;
  printf("Pacchetto --------- %d\n",count);
  count++;

  epp ep;
  ep=(epp)arg;
  struct smtp *sm;
  struct smtp smt;
  sm=&smt;

  strcpy(sm->mail_from,"\0");
  strcpy(sm->rcpt_to,"\0");
  strcpy(sm->message_id,"\0");
  strcpy(sm->date,"\0");
  strcpy(sm->to,"\0");
  strcpy(sm->from,"\0");
  strcpy(sm->received,"\0");
  strcpy(sm->delivered,"\0");
  strcpy(sm->return_path,"\0");

/* Selezioniamo le funzioni da invocare in base al link layer */

  if(link_layer==DLT_EN10MB)
    {
    /* E' un frame Ethernet - Discrimino l'header ethernet e il
payload */
    frame=(struct ether_header *)data;
    if(ntohs(frame->ether_type)==ETHERTYPE_IP)
```

```
      {
      /* Che contiene un pacchetto IP */
      Leggi_IP(data+length_header_frame,sm,ep);
      }
    else
      {
      printf("Tipo di frame Ethernet sconosciuto\n\n");
      exit(0);
      }
    }
  else if ((link_layer==DLT_RAW) || (link_layer==DLT_LINUX_SLL)
|| (link_layer==DLT_NULL) || (link_layer==DLT_LOOP))
    {
    /* Non c'è header */
    Leggi_IP(data+length_header_frame,sm,ep);
    }
  else
    {
    printf("Tipo di frame non supportato\n\n");
    exit(0);
    }
  }

/* Funzione che legge il pacchetto IP, Lo discrimina e salva
eventualmente i dati su disco */

void Leggi_IP(const u_char *data,struct smtp *sm, epp ep)
  {
/* Individuo il pacchetto nel Payload del frame ethernet */
  struct iphdr *iph=(struct iphdr *)data;
  int data_length=(ntohs(iph->tot_len) - (iph->ihl)*4);
  int k=0;

/* Se il protocollo IP non è V4 e non ha traffico TCP lo devo
tralasciare */
  if(iph->version==4)
    {
    if ((iph->protocol)!=6)
      {
      printf("Pacchetto IP sconosciuto\n\n");
      }
    else
      {
/* Inizio a caratterizzare la struttura SM con gli indirizzi IP
del Sender e del Receiver */
      sm->src_IP=iph->saddr;
      sm->dst_IP=iph->daddr;

/* Si legge il TCP e si discrimina il tipo di pacchetto */
      switch(Leggi_TCP(data+(iph->ihl*4),data_length,sm))
        {
        case 0:
          printf("NUL\n");
          break;
        case SRC:
          printf("SRC\n");
```

```
            k=confronta_endpts_SRC(sm,ep);
            break;
          case DST:
            printf("DST\n");
            k=confronta_endpts_DST(sm,ep);
            break;
          case HDR:
            printf("HDR\n");
            k=confronta_endpts_HDR(sm,ep);
            break;
          case FWD:
            printf("FWD\n");
            k=confronta_endpts_FWD(sm,ep);
            break;
          }

/* Restituendo le dimensioni della coda, si può verificare se
questa arriva alle sue dimensioni massime */
        if (k>LIM) flushlim(ep);
        }
      }
    }

/* Funzione che legge l'header TCP, caratterizza la source port e
discrimina il contenuto */

int Leggi_TCP(const u_char *data, int tcp_pack_length, struct
smtp *sm)
  {
/* Individuo nel pacchetto IP l'header TCP e i dati trasportati
*/
  struct tcphdr *tcp_hdr=(struct tcphdr *)data;

/* La Lunghezza header Tcp è definita da doff in parole di 4 byte
*/
  int tcp_hdr_length=tcp_hdr->doff*4;

/* La dimensione del contenuto del TCP è la restante parte */
  int data_length=tcp_pack_length - tcp_hdr_length;

/* Caratterizzo la struttura SM con il source TCP port*/
  sm->src_port=ntohs(tcp_hdr->source);

/* Se non è un handshake del TCP (Lunghezza dati pari a zero).
Discrimino i campi del protocollo SMTP contenuti nel payload */
  if(data_length>0)
    {
    data=data+tcp_hdr_length;
    return riconoscicampi(data,data_length,sm);
    }
  }

/* Funzione che discrimina il contenuto SMTP e restituisce il
tipo di pacchetto arrivato*/
```

```
int riconoscicampi(const u_char *data, int data_length, struct
smtp *sm)
  {
/* Si finisce con questa funzione di caratterizzare la struttura
SM*/
  char mail_fr[128]="";
  char rcpt_t[128]="";
  char mess_id[128]="";
  char dat[40]="";
  char fro[128]="";
  char too[128]="";
  char rec[128]="";
  char deli[256]="";
  char retp[128]="";
  int flag[9];
  register int i,j;
  time_t tempo;

/* Si registra il Timestamp locale di arrivo del pacchetto */
  time(&tempo);

/* Si inizializzano i flag */
  for (i=0;i<=8;i++) flag[i]=0;

/* Si scandisce byte per byte il pacchetto alla ricerca dei campi
significativi Questi possono essere al massimo nei primi BYT byte
del messaggio, qualora questo eccedesse */

  if (data_length>BYT) data_length=BYT;

  for (i=0;i<data_length;i++)
    {
    /* Se si trova il campo protocollare SMTP mail from: si
ricopia nella struttura SM e La funzione restituisce il valore
SRC */
    if(!(strncasecmp((data+i),"mail from:",10))&&(!flag[0]))
      {
      i=i+11;
      for (j=0;j<128;j++)
        {
        if ((*(data+i+j))!='\n')
          {
          mail_fr[j]=*(data+i+j);
          }
        else
          {
          mail_fr[j]='\0';
          strcpy(sm->mail_from,mail_fr);
          flag[0]=1;
          i=i+j;
          j=128;
          }
        }
      }
/* Se si trova il campo protocollare SMTP rcpt to: si ricopia
nella struttura SM e La funzione restituisce il valore DST */
```

```
    if(!(strncasecmp((data+i),"rcpt to:",8))&&(!flag[1]))
      {
      i=i+9;
      for (j=0;j<128;j++)
        {
        if ((*(data+i+j))!='\n')
          {
          rcpt_t[j]=*(data+i+j);
          }
        else
          {
          rcpt_t[j]='\0';
          strcpy(sm->rcpt_to,rcpt_t);
          flag[1]=1;
          i=i+j;
          j=128;
          break;
          }
        }
      }

/* Se si trovano indicazioni utili dell'header del messaggio
queste vengono registrate negli appositi campi di SM e La
funzione restituisce il valore HDR */

    if(!(strncasecmp((data+i),"message-id:",11))&&(!flag[2]))
      {
      i=i+12;
      for (j=0;j<128;j++)
        {
        if ((*(data+i+j))!='\n')
          {
          mess_id[j]=*(data+i+j);
          }
        else
          {
          mess_id[j]='\0';
          flag[2]=1;
          i=i+j;
          j=128;
          }
        }
      }

    if(!(strncasecmp((data+i),"date:",5))&&(!flag[3]))
      {
      i=i+6;
      for (j=0;j<40;j++)
        {
        if ((*(data+i+j))!='\n')
          {
          dat[j]=*(data+i+j);
          }
        else
          {
          dat[j]='\0';
```

```
      flag[3]=1;
      i=i+j;
      j=40;
      }
    }
  }

if(!(strncasecmp((data+i),"from:",5))&&(!flag[4]))
  {
  i=i+6;
  for (j=0;j<128;j++)
    {
    if ((*(data+i+j))!='\n')
      {
      fro[j]=*(data+i+j);
      }
    else
      {
      fro[j]='\0';
      flag[4]=1;
      i=i+j;
      j=128;
      }
    }
  }

if(!(strncasecmp((data+i),"to:",3))&&(!flag[5])&&(!flag[1]))
  {
  i=i+4;
  for (j=0;j<128;j++)
    {
    if ((*(data+i+j))!='\n')
      {
      too[j]=*(data+i+j);
      }
    else
      {
      too[j]='\0';
      flag[5]=1;
      i=i+j;
      j=128;
      }
    }
  }

if(!(strncasecmp((data+i),"received:",9))&&(!flag[6]))
  {
  i=i+10;
  for (j=0;j<256;j++)
    {
    if ((*(data+i+j+2)==0x09))
      {
      rec[j]=0x20;
      j++;
      rec[j]=0x20;
      j++;
```

```
        rec[j]=0x20;
        }
      else
        {
        if ((*(data+i+j))!='\n')
          {
          rec[j]=*(data+i+j);
          }
        else
          {
          rec[j]='\0';
          flag[6]=1;
          i=i+j;
          j=256;
          }
        }
      }
    }

  if(!(strncasecmp((data+i),"delivered:",10))&&(!flag[7]))
    {
    i=i+11;
    for (j=0;j<128;j++)
      {
      if ((*(data+i+j))!='\n')
        {
        deli[j]=*(data+i+j);
        }
      else
        {
        deli[j]='\0';
        flag[7]=1;
        i=i+j;
        j=128;
        }
      }
    }

  if(!(strncasecmp((data+i),"return path:",12))&&(!flag[8]))
    {
    i=i+11;
    for (j=0;j<128;j++)
      {
      if ((*(data+i+j))!='\n')
        {
        retp[j]=*(data+i+j);
        }
      else
        {
        retp[j]='\0';
        flag[8]=1;
        i=i+j;
        j=128;
        }
      }
    }
```

```
    }
  if (flag[1])
    {
    sm->time=(unsigned long int)tempo;
    if (flag[0])return FWD;
    return DST;
    }
  if (flag[0])
    {
    sm->time=(unsigned long int)tempo;
    return SRC;
    }

  if
((flag[2])||(flag[3])||(flag[4])||(flag[5])||(flag[6])||(flag[7])
||(flag[8]))
    {
    if (flag[2]) strcpy(sm->message_id,mess_id);
    if (flag[3]) strcpy(sm->date,dat);
    if (flag[4]) strcpy(sm->from,fro);
    if (flag[5]) strcpy(sm->to,too);
    if (flag[6]) strcpy(sm->received,rec);
    if (flag[7]) strcpy(sm->delivered,deli);
    if (flag[8]) strcpy(sm->return_path,retp);
    sm->time=(unsigned long int)tempo;
    return HDR;
    }

/* Se nei primi BYT byte di dati non si trova niente di
significativo la funzione restituisce 0 e il pacchetto viene
tralasciato */

  return 0;

}

/* Funzione che, all'arrivo di un SRC, controlla se corrisponde
ad un EP presente in coda. Non trovandolo, il SRC viene accodato.
La funzione restituisce la dimensione della coda in modo da
effettuare un controllo sulle dimensioni della stessa */

int confronta_endpts_SRC(struct smtp *sm, epp ep)
  {
  int k=0;

/* Questo controllo viene fatto solo per il primo arrivo, in modo
da creare una coda disponibile della lista */
  if (ep->next==NULL)
    {
    ep->next=(epp)malloc(sizeof(EPTS));
    ep=ep->next;
    ep->next=NULL;
    }

/* Quì inizia la scansione della coda presente */
  do
```

```
    {
    printf("<%d>",k);
    if ((ep->src_IP==sm->src_IP) && (ep->dst_IP==sm->dst_IP) &&
(ep->src_port==sm->src_port))
      {
      /* Il SRC arrivato corrisponde ad un EP Presente in coda */
      if (ep->stato==SRC) return k;
      if (ep->stato==DST)
        {
        scrivi_parziali(ep);
        strcpy(ep->mail_from,sm->mail_from);
        strcpy(ep->rcpt_to,"\0");
        ep->time=sm->time;
        ep->stato=SRC;
        return k;
        }
      }
    if (ep->next!=NULL) ep=ep->next; else break;
    k++;
    } while (ep->next!=NULL);

  printf("\nSRC New EP\n");

/* Non essendo trovato un EP corrispondente il SRC viene accodato
*/
  ep->src_IP=sm->src_IP;
  ep->dst_IP=sm->dst_IP;
  ep->src_port=sm->src_port;
  strcpy(ep->mail_from,sm->mail_from);
  strcpy(ep->rcpt_to,"\0");
  ep->time=sm->time;
  ep->stato=SRC;
  ep->next=(epp)malloc(sizeof(EPTS));
  ep=ep->next;
  ep->next=NULL;
  return k;
  }

/* Funzione che, all'arrivo di un DST, controlla se corrisponde
ad un EP presente in coda. Non trovandolo, il DST viene accodato.
La funzione restituisce la dimensione della coda in modo da
effettuare un controllo sulle dimensioni della stessa */

int confronta_endpts_DST(struct smtp *sm, epp ep)
  {
  int k=0;

/* Questo controllo viene fatto solo per il primo arrivo, in modo
da creare una coda disponibile della lista */
  if (ep->next==NULL)
    {
    ep->next=(epp)malloc(sizeof(EPTS));
    ep=ep->next;
    ep->next==NULL;
    }
```

```
/* Quì inizia la scansione della coda presente */
  do
    {
    printf(">%d<",k);
    if ( (ep->src_IP==sm->src_IP) && (ep->dst_IP==sm->dst_IP) &&
(ep->src_port==sm->src_port))
      {
      /* Il SRC arrivato corrisponde ad un EP Presente in coda */
      printf("\nDST Confronta SRC\n");
      if (ep->stato==SRC)
        {
        strcpy(ep->rcpt_to,sm->rcpt_to);
        ep->time=sm->time;
        ep->stato=DST;
        return k;
        }
      if (ep->stato==DST)
        {
        scrivi_parziali(ep);
        strcpy(ep->mail_from,"UNKN");
        strcpy(ep->rcpt_to,sm->rcpt_to);
        ep->time=sm->time;
        ep->stato=DST;
        return k;
        }
      }
    if (ep->next!=NULL) ep=ep->next; else break;
    k++;
  } while (ep->next!=NULL);

  printf("\nDST new EP\n");

/* Non essendo trovato un EP corrispondente il DST viene accodato
*/
  ep->src_IP=sm->src_IP;
  ep->dst_IP=sm->dst_IP;
  ep->src_port=sm->src_port;
  strcpy(ep->mail_from,"UNKN");
  strcpy(ep->rcpt_to,sm->rcpt_to);
  ep->time=sm->time;
  ep->stato=DST;
  ep->next=(epp)malloc(sizeof(EPTS));
  ep=ep->next;
  ep->next=NULL;
  return k;
  }

/* Funzione che, all'arrivo di un HDR, controlla se corrisponde
ad un EP presente in coda. Se lo trova, manda tutto in scrittura
su disco e elimina dalla coda l'EP corrispondente. Se non lo
trova, salva comunque i dati. La funzione restituisce la
dimensione della coda in modo da effettuare un controllo sulle
dimensioni della stessa */

int confronta_endpts_HDR(struct smtp *sm, epp ep)
  {
```

```
  epp eg;
  eg=ep;
  int flag=0;
  int k=0;

/* Quì inizia la scansione della coda presente */
  do
    {
    printf("=%d=",k);
    if ((ep->src_IP==sm->src_IP) && (ep->dst_IP==sm->dst_IP) &&
(ep->src_port==sm->src_port))
      {
      /* Il SRC arrivato corrisponde ad un EP Presente in coda */
      if (ep->stato==SRC)
        {
        strcpy(sm->mail_from,ep->mail_from);
        strcpy(sm->rcpt_to,"UNKN");
        ep->stato=NEP;
        scrivi_dati(sm);
        elimina_endpts(eg,k);
        flag=1;
        break;
        }
      if (ep->stato==DST)
        {
        strcpy(sm->mail_from,ep->mail_from);
        strcpy(sm->rcpt_to,ep->rcpt_to);
        ep->stato=NEP;
        scrivi_dati(sm);
        elimina_endpts(eg,k);
        flag=1;
        break;
        }
      }
    if (ep->next!=NULL) ep=ep->next; else break;
    k++;
    } while (ep->next!=NULL);

/* Se nella coda non viene trovato nessun EP, i dati vengono
comunque salvati */
  if (!flag)
    {
    strcpy(sm->rcpt_to,"UNKN");
    strcpy(sm->mail_from,"UNKN");
    scrivi_dati(sm);
    }
  return k;
  }

/* Funzione che, all'arrivo di un FWD, controlla se corrisponde
ad un EP presente in coda. Non trovandolo, il FWD viene accodato
come DST. La funzione restituisce la dimensione della coda in
modo da effettuare un controllo sulle dimensioni della stessa */
int confronta_endpts_FWD(struct smtp *sm, epp ep)
  {
  int k=0;
```

```
/* Questo controllo viene fatto solo per il primo arrivo, in modo
da creare una coda disponibile della lista */
  if (ep->next==NULL)
    {
    ep->next=(epp)malloc(sizeof(EPTS));
    ep=ep->next;
    ep->next==NULL;
    }

  /* Qui inizia la scansione della coda presente */
  do
    {
    printf("*%d*",k);
    if ( (ep->src_IP==sm->src_IP) && (ep->dst_IP==sm->dst_IP) &&
(ep->src_port==sm->src_port))
      {
      /* Il SRC arrivato corrisponde ad un EP Presente in coda */
      printf("\nDST Confronta SRC\n");
      if (ep->stato==SRC)
        {
        strcpy(ep->mail_from,sm->mail_from);
        strcpy(ep->rcpt_to,sm->rcpt_to);
        ep->time=sm->time;
        ep->stato=DST;
        return k;
        }
      if (ep->stato==DST)
        {
        scrivi_parziali(ep);
        strcpy(ep->mail_from,sm->mail_from);
        strcpy(ep->rcpt_to,sm->rcpt_to);
        ep->time=sm->time;
        ep->stato=DST;
        return k;
        }
      }
    if (ep->next!=NULL) ep=ep->next; else break;
    k++;
  } while (ep->next!=NULL);

  printf("\nDST new EP\n");

/* Non essendo trovato un EP corrispondente il DST viene accodato
*/
  ep->src_IP=sm->src_IP;
  ep->dst_IP=sm->dst_IP;
  ep->src_port=sm->src_port;
  strcpy(ep->mail_from,sm->mail_from);
  strcpy(ep->rcpt_to,sm->rcpt_to);
  ep->time=sm->time;
  ep->stato=DST;
  ep->next=(epp)malloc(sizeof(EPTS));
  ep=ep->next;
  ep->next=NULL;
  return k;
```

```
  }

/* Funzione che scrive i dati su disco  */

void scrivi_dati(struct smtp *sm)
  {
  unsigned long int tempo;
  tempo=sm->time;

  miofile=fopen(fname,"a");

    fprintf(miofile,"Source IP: %s\n",inet_ntoa(sm->src_IP));
    fprintf(miofile,"Dest IP: %s\n",inet_ntoa(sm->dst_IP));
    fprintf(miofile,"Sender source Port: %d\n",sm->src_port);
    fprintf(miofile,"Mail from: %s\n",sm->mail_from);
    fprintf(miofile,"Rcpt to: %s\n",sm->rcpt_to);
    fprintf(miofile,"mess-id: %s\n",sm->message_id);
    fprintf(miofile,"date: %s\n",sm->date);
    fprintf(miofile,"from: %s\n",sm->from);
    fprintf(miofile,"to: %s\n",sm->to);
    fprintf(miofile,"received: %s\n",sm->received);
    fprintf(miofile,"delivered: %s\n",sm->delivered);
    fprintf(miofile,"return Path: %s\n",sm->return_path);
    fprintf(miofile,"Arrival time: %s\n",ctime(&tempo));
  fclose(miofile);
  }

/* Funzione che scrive i dati su disco se eccedono la coda di EP
e quindi non sono associabili a nessun header di messaggio */

void scrivi_parziali(epp ep)
  {
  unsigned long int tempo;
  tempo=ep->time;

  miofile=fopen(fname,"a");

    fprintf(miofile,"Source IP: %s\n",inet_ntoa(ep->src_IP));
    fprintf(miofile,"Dest IP: %s\n",inet_ntoa(ep->dst_IP));
    fprintf(miofile,"Sender source Port: %d\n",ep->src_port);
    fprintf(miofile,"Mail from: %s\n",ep->mail_from);
    fprintf(miofile,"Rcpt to: %s\n",ep->rcpt_to);
    fprintf(miofile,"mess-id: UNKN\n");
    fprintf(miofile,"date: UNKN\n");
    fprintf(miofile,"from: UNKN\n");
    fprintf(miofile,"to: UNKN\n");
    fprintf(miofile,"received: UNKN\n");
    fprintf(miofile,"delivered: UNKN\n");
    fprintf(miofile,"return Path: UNKN\n");
    fprintf(miofile,"Arrival time: %s\n",ctime(&tempo));
  fclose(miofile);
  }

/* Funzione che chiude la sessione, liberando tutte le risorse */

void close_all(int a)
```

```
  {
  printf("\nChiusura in corso\n\n");
  printf("Chiusura interfaccia...\n\n");
  pcap_close(handle);
  printf("Scarico della coda in entrata...\n\n");
  scarica(ee);
  printf("Programma terminato\n\n");
  exit(0);
  }

/* Funzione che elimina il k-esimo elemento della lista degli
EP*/

void elimina_endpts(epp ep,int k)
  {
  epp el, em;
  el=ep;
  int i=0;
  do  {
    el=el->next;
    i++;
    } while (i<=k-1);
  em=el->next;
  el->next=em->next;
  free(em);
  return;
  }

/* Funzione che scarica la coda EP su disco quando si chiude il
programma */

void scarica (epp ep)
  {
  epp el;
  while (ep->next!=NULL)
    {
    el=ep;
    if (ep->stato!=NEP) scrivi_parziali(ep);
    ep=ep->next;
    free(el);
    }
  return;
  }

/* Funzione che scarica la coda EP dei primi FLS elementi quando
questa raggiunge LIM */

void flushlim (epp ep)
  {
  epp el, em;
  int i=0;
  el=ep;
  do {
    em=ep->next;
    el->next=em->next;
    scrivi_parziali(em);
```

```
    free(em);
    i++;
  }while(i<=FLS);
  return;
  }
```

FILE SMTSNIFF.H

```
#include <stdio.h>
#include <time.h>
#include <string.h>
#include <signal.h>
#include <pcap.h>
#include <netinet/in.h>
#include <net/ethernet.h>
#include <netinet/ip.h>
#include <netinet/tcp.h>

/* DIM_PKT è il massimo numero di byte catturati dall'interfaccia
scelta deve essere necessariamente maggiore o uguale a BYT,
inoltre bisogna considerare che 65507 è la massima dimensione di
un pacchetto IP */
#define DIM_PKT 2100

/* Questi valori definiscono lo stato di un pacchetto entrante */
#define SRC 1
#define DST 2
#define HDR 3
#define NEP 4
#define FWD 5

/* LIM è la dimensione massima della coda entrante prima che
vengono scaricati*/
#define LIM 8

/* FLS pacchetti arrivati parzialmente*/

#define FLS 4

/* BYT è il massimo numero di Byte scanditi da riconosci campi */
#define BYT 2000

/* Tale struttura definisce il singolo elemento della coda
dinamica */
struct endpts
  {
    u_int32_t src_IP;
    u_int32_t dst_IP;
    int src_port;
    int stato;
    char mail_from[128];
    char rcpt_to[128];
    unsigned long int time;
```

```
    struct endpts *next;
  };

/* Tale struttura serve ad accogliere tutti i campi necessari
alla tabulazione */
struct smtp
  {
    unsigned long int time;
    u_int32_t src_IP;
    u_int32_t dst_IP;
    int src_port;
    int stato;
    char mail_from[128];
    char rcpt_to[128];
    char message_id[128];
    char from[128];
    char to[128];
    char date[40];
    char received[256];
    char delivered[128];
    char return_path[128];
  };

typedef struct endpts EPTS;
typedef EPTS *epp;

/**--------------- FUNZIONI DEFINITE ----------- */

/* Funzione che mostra il tipo di link layer */
void Stampa_link_layer(void);

/* Callback utilizzata in pcap_loop ad ogni arrivo */
void arrivo(u_char *arg,const struct pcap_pkthdr *header,const
u_char *data);

/* Funzione che legge il pacchetto IP, Lo discrimina e salva
eventualmente i dati su disco */
void Leggi_IP(const u_char *data, struct smtp *sm, epp ep);

/* Funzione che legge l'header TCP, caratterizza la source port e
discrimina il contenuto */
int Leggi_TCP(const u_char *data,int tcp_pack_length,struct smtp
*sm);

/* Funzione che discrimina il contenuto SMTP e restituisce il
tipo di pacchetto arrivato*/
int riconoscicampi(const u_char *data, int data_length, struct
smtp *sm);

/* Funzione che, all'arrivo di un SRC, controlla se corrisponde
ad un EP presente in coda. Non trovandolo, il SRC viene accodato.
La funzione restituisce la dimensione della coda in modo da
effettuare un controllo sulle dimensioni della stessa */
int confronta_endpts_SRC(struct smtp *sm, epp ep);
```

```
/* Funzione che, all'arrivo di un DST, controlla se corrisponde
ad un EP presente in coda. Non trovandolo, il DST viene accodato.
La funzione restituisce la dimensione della coda in modo da
effettuare un controllo sulle dimensioni della stessa */
int confronta_endpts_DST(struct smtp *sm, epp ep);

/* Funzione che, all'arrivo di un HDR, controlla se corrisponde
ad un EP presente in coda. Se lo trova, manda tutto in scrittura
su disco e elimina dalla coda l'EP corrispondente. Se non lo
trova, salva comunque i dati. La funzione restituisce la
dimensione della coda in modo da effettuare un controllo sulle
dimensioni della stessa */
int confronta_endpts_HDR(struct smtp *sm,epp ep);

/* Funzione che, all'arrivo di un FWD, controlla se corrisponde
ad un EP presente in coda. Non trovandolo, il FWD viene accodato
come DST. La funzione restituisce la dimensione della coda in
modo da effettuare un controllo sulle dimensioni della stessa */
int confronta_endpts_FWD(struct smtp *sm, epp ep);

/* Funzione che scrive i dati su disco  */
void scrivi_dati(struct smtp *sm);

/* Funzione che scrive i dati su disco se eccedono la coda di EP
e quindi non sono associabili a nessun header di messaggio */
void scrivi_parziali(epp ep);

/* Funzione che chiude la sessione, liberando tutte le risorse */
void close_all(int a);

/* Funzione che elimina il k-esimo elemento della lista degli
EP*/
void elimina_endpts(epp ep, int k);

/* Funzione che scarica la coda EP su disco quando si chiude il
programma */
void scarica (epp ep);

/* Funzione che scarica la coda EP dei primi FLS elementi quando
questa raggiunge LIM */
void flushlim (epp ep);
```

APPENDICE B – Licenze

Mentre Ethereal è coperto dalla GNU GPL, che consente la libera modifica del suo codice, a patto che il software prodotto rimanga libero e distribuito secondo la stessa GPL, le librerie PCAP sono distribuite sotto la più libera licenza BSD. Essa consente, non solo il libero sfruttamento del codice, ma anche la possibilità che il software sviluppato venga coperto da registrazione proprietaria.

GNU GPL

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed

under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this

License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for

making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot

distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software

Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest

to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

Smtsniff – SMTP protocol traffic monitoring
Copyright (C) 2006 Marco Orazio Garozzo

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Riferimenti Bibliografici

[1] Definizione di “E-government” tratta da “http://www.wikipedia.org”.

[2] Presentazione de “Linee guida del governo per lo sviluppo della Società dell’informazione” – Lucio Stanca, 11/06/02, reperibile su “http://www.mininnovazione.it/ita/normativa/documenti/socinfo11_06_02.pdf”.

[3] DL 144 del 16/8/2005 – “Misure di sicurezza contro il terrorismo” reperibile presso “http://www.camera.it/parlam/leggi/decreti/05144d.htm” – pubblicato sulla Gazzetta Ufficiale n. 190 del 17 Agosto 2005.

[4] L. 155 del 31/07/2005 – “Conversione in legge del DL 144 del 16/8/2005” reperibile presso “http://www.parlamento.it/parlam/leggi/05155l.htm” - pubblicata sulla G.U. n. 177 del 1 Agosto 2005.

[5] D.Lgs. 196 del 30/6/2003 – “Codice in materia di protezione dei dati personali” reperibile presso “http://www.parlamento.it/leggi/deleghe/ 03196dl.htm” - pubblicato sulla Gazzetta Ufficiale n. 174 del 29 Luglio 2003.

[6] D.L. 354 del 24/12/2003 – “Conservazione dei dati di traffico per altre finalità” reperibile presso “http://www.privacy.it/dl2003354.html” – pubblicato sulla G.U. n. 300 del 29/12/2003.

[7] L. 45 del 26/02/2004 – “Conversione in legge, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l’amministrazione della giustizia” reperibile presso “http://www.parlamento.it/parlam/leggi/04045l.htm” – pubblicato sulla G.U. n. 48 del 27/02/2004.

[8] Direttiva del Presidente del Consiglio dei Ministri 16/01/2002 - “Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali” reperibile presso “http://www.mininnovazione.it/ita/normativa/allegati/direttiva_sicurezza.pdf” – pubblicata sulla G.U. n. 69 del 22/03/02.

[9] Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003 - “Impiego della posta elettronica nelle Pubbliche Amministrazioni” - , reperibile presso “http://www.cnipa.gov.it/site/_files/DIR.%2027%20novembre%202003.pdf”, pubblicata sulla G.U. n. 8 del 12/01/2004.

[10] D. Lgs 82 del 07/03/2005 – "Codice dell'amministrazione digitale", reperibile presso "http://www.mininnovazione.it/ita/normativa/allegati/dl_050307.pdf" – pubblicata sulla G.U. n.112 del 16/05/2005.

[11] Direttiva del Ministero per l'innovazione e le tecnologie del 18/11/2005 – "Linee guida per la Pubblica Amministrazione digitale", reperibile presso "http://www.innovazione.gov.it/ita/normativa/allegati/dir_051118.pdf" – pubblicata sulla G.U. 16 del 20/01/2006.

[12] Parere del garante per la protezione dei dati personali 22 marzo 2004, reperibile presso "http://www.garanteprivacy.it" (doc. web n. 771307).

[13] Guida operativa per redigere il DPS, garante della privacy, 11/06/2004, reperibile presso "http://www.garanteprivacy.it" (doc. web. N. 1007740).

[14] IETF, RFC 822 – "Standard for the format of arpa internet text messages", Agosto 1982, reperibile presso "http://www.ietf.org".

[15] IETF, RFC 2822 – "Internet Message Format", Aprile 2001, reperibile presso "http://www.ietf.org".

[16] IETF, RFC 1341 – "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies", Giugno 1992, reperibile presso "http://www.ietf.org".

[17] IETF, dall'RFC 2045 al RFC 2049 – "Multipurpose Internet Mail Extensions – Parts I – II – III – IV – V ", Novembre 1996, reperibili presso "http://www.ietf.org".

[18] Andrew Tanenbaum – "Reti di calcolatori", quarta edizione, trad. italiana di "Computer Networks 4th edition", Ed. Pearson, Anno 2003. Pagg. 592-608.

[19] IETF, RFC 821 – "Simple Mail Transfer Protocol", Agosto 1982, reperibile presso "http://www.ietf.org".

[20] IETF, RFC 2821 – "Simple Mail Transfer Protocol", Aprile 2001, reperibile presso "http://www.ietf.org".

[21] IETF, RFC 1939 – "Post Office Protocol – Version 3", Maggio 1996, reperibile presso "http://www.ietf.org".

[22] La documentazione dettagliata su Ethereal è reperibile, insieme al codice sorgente e al software compilato presso "http://www.ethereal.com".

[23] La licenza GNU General Public License, riportata in appendice B, è stata sviluppata dalla Free Software Fundation, essa è altresì reperibile presso "http://www.gnu.org".

[24] Le Librerie PCAP e una documentazione dettagliata su esse, sono reperibili presso "http://www.tcpdump.org".

[25] La licenza BSD (Berkeley Software Distribuition), riportata in appendice B, è stata sviluppata dall'universita di Berkeley – USA, essa è altresì reperibile presso "http://www.opensource.org/licenses/".

[26] Documentazione sull'utilizzo delle LPCAP e sulla creazione di sniffer ad opera di raccolte varie di studenti del corso "sicurezza su reti" dell'a.a. 2000/01, tenuto dal Prof. Alfredo De Santis dell'Università di Salerno. Materiale reperibile, presso "http://www.dia.unisa.it/~ads/corso-security/www/corso-0001".

La programmazione in linguaggio C è stata supportata dal testo di Brian W. Kernighan e Dennis M. Ritchie - "The C programming language" seconda edizione 1988, Prentice hall.