



Email sicura, possibilmente Open Source

A casa e in ufficio la posta elettronica è uno dei servizi Internet più longevi e diffusi. Ma è anche tra i meno sicuri.

La posta elettronica ha quasi cinquant'anni e nessuna intenzione di farsi da parte. Pur avendo limiti non trascurabili, e vivendo in un'era di app mobili, l'email è ancora in ottima salute e rimarrà impossibile da ignorare per diversi anni ancora. Le ragioni sono ovvie. La posta elettronica è integrata in applicazioni di tutti i tipi, da database aziendali ai forum Web, ed è inevitabile in mille altri contesti, quando non funge addirittura da documento d'identità elettronico. Soprattutto, l'email è semplicissima da usare. Magari lo farà violando tutte le regole della netiquette, ma chiunque abbia accesso a un computer riesce quasi subito a scrivere o leggere email da solo. Allo stesso tempo, come ci è stato platealmente ricordato in questi tempi di Datagate, la posta elettronica non è sicura. D'altra parte, che significa "sicura"? Niente virus? Niente spam? Anonima?

Impossibile da usare anonimamente? Privata, ovvero utilizzabile senza far sapere a nessun altro non solo quali email abbiamo scambiato, ma anche *con chi e quando*? Oppure non ripudiabile, nel senso di non poter negare di aver inviato un certo messaggio perché porta la propria firma digitale?

Come è facile vedere da queste domande, basta pensarci un attimo per capire che la questione è più ampia di quanto potrebbe sembrare. La buona notizia è che i recenti sviluppi dell'affare Datagate hanno stimolato moltissimo la ricerca in questo settore. Oggi sono in corso parecchi studi e progetti per fornire posta elettronica (o qualcosa che *sembra* posta elettronica) che sia sicura, in almeno uno dei sensi appena elencati, ma anche facile da usare. Perché il vero problema della posta elettronica sicura è come rendere quella "sicurezza"

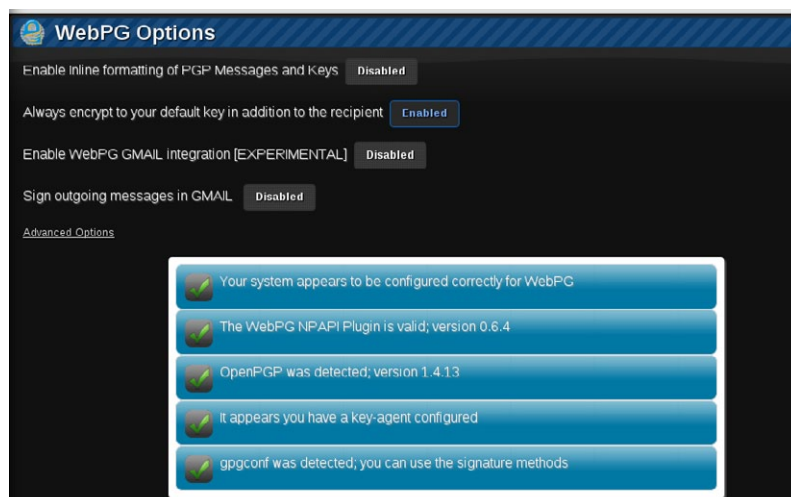
quasi invisibile, per non rallentarne l'adozione.

Problemi e limiti della email attuale

La posta elettronica di oggi funziona in un modo che appartiene al passato (ne parliamo nel box in queste pagine): un'epoca in cui solo gli utenti di network molto ristretti e isolati dal resto del mondo potevano scambiarsi messaggi e potevano fidarsi l'uno dell'altro, se già non si conoscevano di persona, perché appartenevano tutti a istituti di ricerca, università o altre organizzazioni del genere.

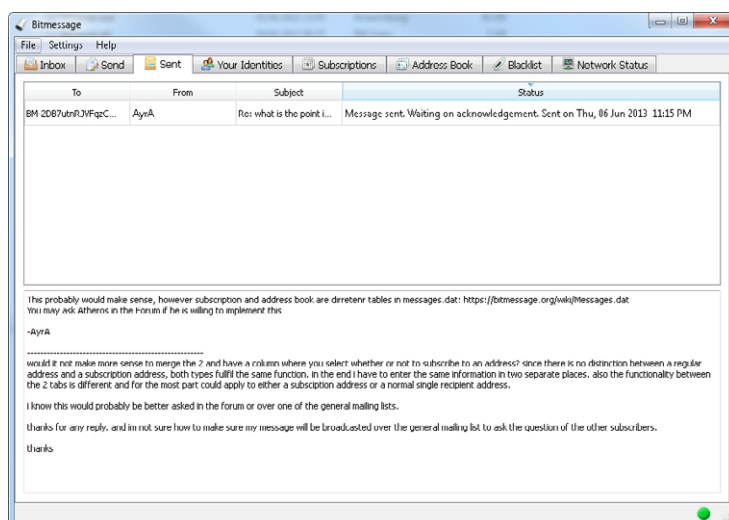
Oggi quell'architettura presenta diversi problemi non trascurabili di affidabilità e riservatezza, anche per chi non è una spia operante in territorio nemico o un "whistleblower", cioè un impiegato che decida di segnalare a un giornalista qualche reato commesso dall'azienda in cui lavora.

Il primo problema è che la cifratura dei messaggi, anche se possibile con elevato grado di sicurezza da diversi anni, non viene praticamente mai usata. I metodi più diffusi, almeno nel mondo Unix da cui Linux discende, sono varianti dei certificati digitali X.509 conservati su smart card o dello standard di cifratura software nato come Pgp (Pretty Good Privacy). Le smart card sono più facili da usare, perché diversi client di posta elettronica sono già in grado



La finestra iniziale di configurazione per Chrome di WebPG, il software Open Source che "porta la crittografia Gpg all'interno del browser".

PyBit è un client di posta elettronica davvero spartano, ma è anche il modo migliore per sperimentare l'email anonima con il sistema BitMessage.



di riconoscerle senza installare o configurare da soli software come gpg e le sue interfacce grafiche su Linux, o GPG4Win (gpg4win.org) su Windows. D'altra parte per un privato procurarsi una smart card valida e riconosciuta per questo tipo di uso non è la cosa più semplice (o economica) del mondo. La cifratura con chiavi asimmetriche, alla base di Pgp e di tutte le sue varianti Open Source e non, ha una complessità effettiva ancora eccessiva per molti utenti. Occorre creare più o meno da soli, o almeno questa è la percezione, chiavi di cifratura pubbliche e private separatamente dagli indirizzi email veri e propri, capire la differenza fra i due tipi di chiavi, scambiarsi *solo* le seconde in maniera affidabile e infine sapere sia quando sia *come* usarle.

Tutte queste operazioni non sono ancora gestite dai client e fornitori di email attuali in maniera standard e sufficientemente trasparente per l'utente medio. D'altra parte, almeno in certi casi, non potrebbero fare più di tanto. Se si ottiene o si usa per errore la chiave pubblica sbagliata, il messaggio sarà leggibile solo da un'altra persona, non da chi avrebbe dovuto riceverlo in esclusiva. È per questo che, quando per qualsiasi motivo non si può pubblicarla su un sito Web ufficiale, la prassi più comune è scambiarsi le chiavi di persona, per sapere con certezza sia a chi appartengono, sia a chi si consegnano le proprie.

Anche superando questi ostacoli, purtroppo, il problema peggiore rimane: anche dopo aver capito come muoversi, aver generato le proprie chiavi e aver configurato a perfezione il proprio

client di posta elettronica... non si ha comunque alcun controllo su quello che possiamo ricevere o spedire. Per ricevere email standard cifrata è necessario che chiunque ci scrive decida (o possa essere costretto) di lavorare in quel modo, ammesso che sappia che il destinatario vorrebbe la cifratura. Per lo stesso motivo non si può essere sicuri in anticipo che il titolare di un indirizzo email standard potrà gestire messaggi cifrati, o quali chiavi vorrebbe usare.

Cifratura a parte, qualsiasi indirizzo email si usi occorre sempre connettersi a server esterni svelando, come minimo, il proprio indirizzo IP, cioè da dove ci si connette a Internet. Questo problema rimane (anzi, si aggrava) anche quando si è in grado di gestire in proprio un server di posta elettronica. Volendo essere davvero paranoici, anche utilizzando indirizzi a perdere come anonimo91@gmail.com, connettendosi a Gmail con il sistema di navigazione Web anonima Tor descritto nei paragrafi successivi si potrebbe essere intercettati, se qualcuno riuscisse a craccare i certificati SSL utilizzati per autenticare e poi cifrare le connessioni a gmail.com. L'unico modo per evitare questi problemi è usare qualcosa che sembra email, ma in realtà non lo è affatto.

BitMessage

Il nome BitMessage (<https://bitmessage.org>) indica un protocollo di comunicazione e del software Open Source che cercano di risolvere il problema dei metadati in chiaro, rendendo però facile e trasparente, oltre che obbligatorio

POSTA ELETTRONICA CIFRATA E WEBMAIL

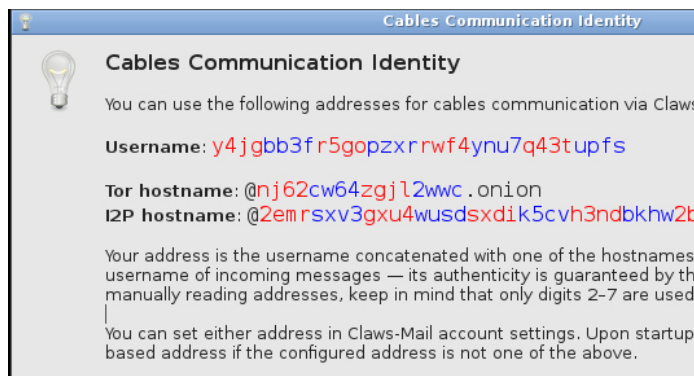
È possibile utilizzare firme e crittografia digitali anche con un browser qualsiasi, ovvero per spedire posta cifrata tramite Webmail? In generale, è possibile spedire testo cifrato dai generici moduli che troviamo in qualsiasi pagina Web? La risposta è senz'altro sì, tutto sta a nel decidere quanto si voglia "soffrire". A rigor di termini, l'unico modo davvero sicuro di fare qualcosa del genere è lavorare all'esterno del browser: scrivere e salvare il risultato come testo semplice (quindi con un vero e proprio text editor, non con word processor come Libre Office!), cifrare quel file con Gpg, Gpg4win o altri programmi del genere, copiare e incollare il risultato nella finestra del browser. La procedura per decifrare i messaggi ricevuti potrebbe essere esattamente l'opposto di questa: copiare e incollarne quanto si vede nel browser in un file di testo semplice, e passare quest'ultimo a qualche interfaccia Gpg. Questa strada, per quanto complicata, è anche l'unica possibile quando non si ha accesso a Internet e Webmail direttamente dal proprio computer, ma solo da un altro, per esempio aziendale, che non è modificabile ma può caricare file da chiavi Usb.

Quando invece è possibile installare software sul computer che si usa per navigare su Internet, ci si può servire dei plugin Open Source per browser che utilizzano la libreria JavaScript chiamata OpenPGP.js (<http://openpgpjs.org>).

Uno di questi è WebPG (<https://webpg.org>) utilizzabile su Linux, OS X e Windows come estensione di Firefox, SeaMonkey e Chrome (ma esiste una versione ridotta per Internet Explorer), nonché del client di posta elettronica Thunderbird. WebPG aggiunge a tutti quei programmi interfacce grafiche per cifrare e decifrare testi (email o di altra natura) e gestire le relative chiavi. MyMail-Crypt (<http://prometheusx.net>) è meno flessibile di WebPG, ma per molti utenti potrebbe essere l'unico software del genere di questa categoria effettivamente necessario. Si tratta infatti di un plugin specifico per Gmail.

l'uso della cifratura. La rete BitMessage, che a fine 2013 conta qualche migliaio di partecipanti, utilizza la crittografia in un modo tale che sia l'utente sia il destinatario di un certo messaggio possono rimanere anonimi, fra di loro e verso il resto del mondo. Utenti particolarmente ossessionati dalla segretezza potrebbero addirittura specificare nei loro indirizzi che non invieranno mai alcuna risposta o ricevuta, per non farsi tracciare.

L'intera rete BitMessage funziona in modalità p2p, senza coordinamento centralizzato o necessità di fidarsi di alcuna organizzazione (a parte gli autori del programma e i sistemi di distribuzione del codice, ovviamente). Gli utenti si trasmettono direttamente l'uno all'altro tutti i messaggi in circolazione del sistema, con meccanismi simili alle



Gli indirizzi email anonimi generati da Cables sono illeggibili ma, con il software giusto, molto meno complicati da usare di quanto si potrebbe temere.

transazioni della moneta digitale Bitcoin. Ognuno tenta di decifrare quanto riceve con le sue chiavi private, per scoprire quali dei messaggi erano effettivamente rivolti a lui, e i messaggi vecchi più di due giorni vengono cancellati. Anche se può sembrare l'antitesi della sicurezza, questa fusione di tutte le mailbox in una comune distribuita a tappeto sono considerate un ottimo sistema per nascondere l'identità dei singoli utenti e quindi impedire intercettazioni o analisi di singoli flussi di messaggi.

Oltre ai messaggi diretti da utente a utente, il protocollo supporta sia trasmissioni in broadcast sia "iscrizioni" a certi flussi di messaggi, come se fossero mailing list tradizionali. Queste due caratteristiche rendono Bitmessage utilizzabile anche come sistema di pubblicazione anonima su Web di contenuti generici.

Il nome dell'equivalente Bitmessage delle mailing list, è *chan*. Esistono già diverse chan più o meno sperimentali, in cui si discutono argomenti che vanno dalla segretezza alla politica e agli scacchi. Ogni utente che conosca la password corrispondente può leggere e scrivere messaggi nella *chan*. Ovviamente le *chan*, come tutto il resto di BitMessage, sono anonime e senza alcuna gestione o controllo centrali, quindi non censurabili o bloccabili.

BitMessage garantisce anche, senza obbligare l'utente a conoscere e verificare la gestione di chiavi crittografiche, che il mittente di un messaggio non possa essere falsificato. Il prezzo da pagare per questa protezione è l'uso di indirizzi alternativi che, anche se in concreto sono abbastanza semplici da usare, all'apparenza non lo sembrano certo. Si tratta infatti di stringhe di trentasei caratteri come "fjkfgjroOJONo905890fj4..", simili a quelle usate per i pagamenti Bitcoin.

Pur essendo assolutamente impronunciabili, questi indirizzi permettono di ignorare non solo i concetti di chiave pubblica e privata, ma soprattutto tutte le relative operazioni di gestione.

Gli indirizzi ermetici sono anche quelli che permettono di eliminare i metadati in chiaro, cioè di spiare a chi si scrive, e impediscono l'invio di messaggi con falsi indirizzi del mittente.

BitMessage è utile, o almeno dovrebbe esserlo, come sistema antispam. Prima di trasmettere ogni *singolo* messaggio come abbiamo spiegato, occorre infatti elaborarlo nel computer con una procedura *deliberatamente* lenta. Questo calcolo, chiamato "*proof of work*", è infatti dimensionato per durare circa quattro minuti su un computer medio. Il suo scopo è provare che non si è uno spammer, ma qualcuno che ha effettivamente

TUTTI IN ATTESA DI MAILPILE

Mentre andiamo in stampa la comunità Open Source, insieme a tantissime altre persone, attende i primi rilasci da un progetto che ha suscitato grandi aspettative. Il software per Webmail chiamato Mailpile (www.mailpile.is) dovrebbe fornire un'interfaccia simile a Gmail ma installabile su qualsiasi computer, o utilizzabile anche da chiave Usb, con parecchie caratteristiche di grande interesse: creazione di rubriche e caselle postali cifrate sul proprio disco locale, funzione di ricerca avanzata e supporto integrato per la cifratura dei messaggi ed etichette stile Gmail per classificarli.



Questa anteprima dal sito mostra come potrebbe essere, quando sarà pronta, l'interfaccia Webmail di Mailpile.



RISORSE

Le differenze principali fra Tor e I2p sono discusse nel saggio (in inglese) intitolato "Perché Tor ha fallito ma I2P non lo farà" (<http://wilfredwordpress.nfshost.com/?p=21>). Un confronto più schematico, ma più dettagliato, è disponibile all'indirizzo www.i2p2.de/how_networkcomparisons. Per saperne di più sulla Perfect Forward Secrecy consigliamo invece la presentazione in Italiano su Slideshare www.slideshare.net/Alessio.Mosto/ipsec.

bisogno di spedire un singolo messaggio a uno specifico utente. Lo spam, infatti, conviene economicamente solo finché è possibile trasmettere centinaia di messaggi al minuto da ogni computer che si controlla.

Uno dei limiti più grossi di BitMessage è la scalabilità: il suo sistema di distribuzione a tappeto corre un rischio evidente, cioè quello di collassare sotto il peso del suo stesso traffico con l'aumentare del numero di utenti. La soluzione proposta consiste nel suddividere i messaggi in vari flussi (stream) organizzati gerarchicamente. In pratica, il software Bitmessage dovrebbe agganciarsi automaticamente al flusso di default, per ricevere liste di tutti i flussi disponibili. Questo consentirebbe all'utente di scaricare e ridistribuire regolarmente solo i messaggi dei flussi che interessano senza preoccuparsi dei dettagli. Agli altri ci si potrebbe agganciare solo quando necessario, cioè quando si vuole scrivere a chi normalmente non segue gli stessi flussi.

È possibile provare subito BitMessage? Certo, in diversi modi. Installazione e configurazione del client di posta elettronica disponibile sul sito sono praticamente identici a quelli dei programmi tradizionali dello stesso tipo. L'unica differenza significativa è che occorre generare gli indirizzi. Impostando una "passphrase", cioè una frase di riconoscimento, e stando attenti a non perderla perché non c'è possibilità di recupero, si possono utilizzare gli stessi indirizzi (fino a 8) anche su diversi computer. In alternativa, il sito <https://bitmessage.ch/> da un'idea di come potrebbe essere usare Bitmessage anche senza installare alcun software. Si può impostare quel sito come server di posta entrante e uscente nel proprio client standard, e raggiungerlo anonimamente attraverso reti Tor, di cui parleremo fra poco.

Cables

Oltre alla scalabilità BitMessage ha due problemi abbastanza seri, su cui si sta lavorando ma senza avere ancora raggiunto una soluzione soddisfacente. Il primo è la mancanza di "Perfect Forward Secrecy": l'espressione indica la capacità di un sistema di continuare a fornire la massima segretezza e riservatezza anche nel caso che, in un certo momento, una delle chiavi o dei certificati digitali vengano scoperti. L'altro è il fatto

che qualunque utente connesso a un certo flusso può farsi una copia privata permanente di tutti i messaggi che contiene, per provare con tutta calma a decifrarli.

Queste complicazioni non sono presenti nell'altro sistema di comunicazione sicura Open Source chiamato Cables (<http://dee.su/cables>): anche in questo caso abbiamo email sicure e anonime tramite indirizzi abbastanza illeggibili e meccanismi che nascondono all'utente tutte le operazioni di cifratura dietro a un normale client di posta elettronica. La differenza principale rispetto a BitMessage è che Cables è proposto principalmente come complemento per la messaggistica tramite reti Tor o I2P. Tor (www.torproject.org) è un sistema per navigare sulla normale rete Internet, che però rende estremamente difficile capire da dove nasce una certa connessione a un sito. I2P (www.i2p2.de) ha un altro obiettivo: invece di far navigare su Internet senza essere riconosciuti, I2P crea una vera e propria rete invisibile al di sopra di quella normale, il cui traffico è quasi tutto *interno*, cioè da e fra utenti completamente anonimi.

I messaggi spediti con Cables sono automaticamente instradati su una qualunque di quelle due reti. Come in BitMessage, gli indirizzi sono in realtà hash di certificati digitali, quindi non falsificabili. A questa funzione Cables aggiunge però la cosiddetta *ripudiabilità*: in parole povere, mentre il destinatario può capire, al momento della sua ricezione, se un messaggio è stato falsificato, dopo non è più possibile associarlo a uno specifico utente Internet. Questo è dovuto anche al fatto che, sempre grazie all'uso di protocolli di routing anonimi come Tor e I2P, è impossibile stabilire se un certo computer supporta Cables o se l'ha già usato.

Il modo migliore per avere un'idea di come funzionano le comunicazioni via Cables è provarle dall'interno della distribuzione Live sicura chiamata Liberté Linux (<http://dee.su/liberte>), che è stata sviluppata anche come esempio pratico delle possibilità di quel sistema. Il client utilizzato per Cables da Liberté Linux, Claws-Mail (www.claws-mail.org) è comunque installabile senza procedure particolari su qualunque altra distribuzione Linux, nonché su Windows.

Linux Foundation: si virtualizza

La Open Virtualization Alliance (Ova, <http://openvirtualizationalliance.org>) è un'organizzazione creata nel 2011, che oggi conta già più di 250 membri incluse aziende come Ibm, Intel, Hp e, in campo Linux, Red Hat. La missione di Ova è favorire l'utilizzo di macchine Linux virtuali basate sulla tecnologia Kvm (Kernel-based Virtual Machine). A ottobre 2013 Ova si è aggregata alla Linux Foundation, diventando un progetto collaborativo ufficiale. Questa mossa dovrebbe accelerare l'adozione di tecnologie di virtualizzazione Open Source in tutti i settori dell'informatica, dai servizi per le Pmi alle scuole e alle Pubbliche Amministrazioni in generale.

Tradurre il software, tutti insieme

Anche nel mondo globalizzato di oggi, traduzione e localizzazione corrette dei programmi software e della relativa documentazione rimangono essenziali. Purtroppo le procedure più comuni in questo campo rendono al massimo solo quando può occuparsene personale specializzato. Il progetto chiamato B-Translator o progetto Bee_Translator (<http://info.btranslator.org/about.html>) cerca di risolvere proprio questo problema, puntando proprio di chi può contribuire solo saltuariamente. L'interfaccia Web di B-Translator permette infatti di caricare anche solo poche frasi e soprattutto di eliminare duplicazioni, anche fra progetti o piattaforme di localizzazione diversi. È possibile anche votare le traduzioni migliori e inviare suggerimenti.

WordPress 3.7, aggiornamenti automatici più sicuri

WordPress è il motore che manda avanti circa 72 milioni di siti Web, incluso il sito di *Pc Professionale*. La versione 3.7, disponibile da ottobre 2013, contiene diverse novità, ma quella che farà più rumore è l'aggiornamento automatico, in background. Le versioni precedenti del software supportavano solo aggiornamenti manuali. È solo per questo motivo, per quanto banale, che parecchi blog rimangono fermi a versioni precedenti, con tutti i rischi che questo comporta. L'aggiornamento automatico di WordPress avverrà solo per aggiornamenti minori e/o limitati alla sicurezza, che interessino solo pochi file. In generale, lasciare il software libero di aggiornarsi da solo non è mai una buona idea ma gli sviluppatori sono comunque convinti che, almeno in situazioni del genere WordPress sarà all'altezza.