

13 marzo 2011 di **Joanna Rutkowska**

[illegible]

Una rapida digressione sulle etichette dei domini (colori) – in Qubes OS a ogni dominio, a parte il nome distinto, viene assegnata anche *un'etichetta*, che fondamentalmente è uno dei tanti colori definiti. Questi colori, che sono usati per disegnare le decorazioni delle finestre dal Window Manager fidato (cornice di colore), dovrebbero essere facili da usare, facili da notare, indicatori di quanto sia affidabile una data finestra. Sta totalmente all'utente come interpreta questi colori. Per me è stato in qualche modo ovvio associare il colore *rosso* a qualcosa di inaffidabile e pericoloso (la "luce rossa" -- stop! pericolo!), il *verde* a qualcosa di sicuro e affidabile, mentre il *giallo* e l'*arancione* con qualcosa in mezzo. Ho anche esteso questo schema, per includere anche *blue*, e *black*, che interpreto come indicanti domini progressivamente più attendibili rispetto al verde, con il nero che alla fine è qualcosa di attendibile.

Per altre attività legate al lavoro che richiedono un accesso al Web, come la modifica di Qubes Wiki, o l'accettazione di inviti di LinkedIn, o il download di fantastiche immagini da fotolia.com per le mie presentazioni, o specifiche e manuali da intel.com, per tutto questo utilizzo il **lavoro-pub** domain, a cui ho assegnato l'etichetta gialla, il che significa che lo considero solo in qualche modo attendibile,

e sicuramente non metterei mai le mie chiavi PGP lì o qualsiasi informazione riservata relativa al lavoro.

Il dominio **personale** è il luogo in cui sono conservate tutte le mie cose non relative al lavoro, come e-mail e calendario personali, foto delle vacanze, video, ecc. Non ha davvero accesso al Web, ma se fossi interessato ai social network, probabilmente consentirei HTTPS a qualcosa come Facebook. Essendo in qualche modo paranoico, ho anche uno speciale dominio **molto personale**, che uso per comunicare con il mio partner quando sono lontano da casa. Usiamo PGP, ovviamente, e ho chiavi PGP separate per questo scopo. Anche se non discutiamo di cose segrete e delicate lì, preferiamo comunque mantenere private le nostre conversazioni intime.

Uso lo **shopping** per accedere a tutti i siti di e-commerce su Internet. Fondamentalmente ciò che definisce questo dominio è l'accesso ai miei numeri di carta di credito e al mio indirizzo personale (per la spedizione). Poiché non ho una carta di credito "aziendale" dedicata, faccio tutti gli acquisti in questo dominio, dalla spesa, alle attrezzature sportive, alla fine delle prenotazioni di hotel/aereo. Se avessi carte di credito aziendali separate, probabilmente dividerei il mio dominio di **acquisto** in **personal-shopping** e **work-shopping**. Dispongo anche di un dominio **bancario**, che utilizzo solo per la gestione del mio conto bancario (che ancora una volta unisce il mio conto personale e quello aziendale).

Ho anche alcuni domini specializzati nel lavoro, che uso raramente. Il dominio **work-admin** viene utilizzato per gestire quasi tutti i server ITL, come il nostro server web, i server Qubes repo e wiki, il server di posta elettronica e la gestione DNS, ecc. A questo dominio è consentito solo il traffico SSH a quei server e HTTPS a un pochi server di gestione basati sul Web. Il **blog di lavoro** viene utilizzato per gestire proprio questo blog che stai leggendo ora. Il motivo per cui è separato da **work-admin** o **work** è perché sono troppo paranoico e perché temo che se qualcuno compromette il servizio di blogger e successivamente sfrutti un bug nel mio browser che uso per modificare il mio blog, allora Non voglio che questa persona sia in grado di ottenere anche l'accesso come amministratore a tutti i server ITL.

Allo stesso modo, se qualcuno in qualche modo ha compromesso, ad esempio Amazon Web Management Console, e poi ha sfruttato il mio browser in **work-admin**, vorrei almeno mantenere l'accesso al mio blog. Se usassi Twitter, probabilmente lo gestirei anche da questo dominio del **blog** di lavoro, a meno che non si tratti di un account Twitter personale, nel qual caso lo eseguirei da **personal**.

Il dominio **qubes-dev** viene utilizzato per tutto lo sviluppo di Qubes, unendo i rami di altri sviluppatori (dopo aver verificato le firme sui loro tag, ovviamente!), creando RPM/ISO (sì, Qubes Beta 1 verrà spedito come DVD ISO!), e infine firmarli. Poiché le chiavi di firma sono presenti, questo dominio è molto sensibile. A questo dominio è consentito solo l'accesso alla rete SSH al nostro server git Qubes. Di nuovo, anche se qualcuno compromettesse questo server Git, non sarebbe comunque un grosso problema per noi, perché firmiamo e verifichiamo tutti i tag negli altri repository (a meno che qualcuno non possa anche modificare i demoni SSH/Git in esecuzione lì in modo che successivamente sfruttare un ipotetico bug nel mio software client git quando mi collego al server).

Ho anche deciso di mantenere tutte le cose relative alla contabilità in un dominio separato: ogni volta che ricevo una fattura, la copio nel dominio della **contabilità**. La logica di ciò è che mi fido di quei PDF molto meno di quanto mi fido dei PDF che tengo nel mio dominio di **lavoro**.

Una volta all'anno sposto le vecchie cose dal mio dominio di **lavoro**, come vecchi spool di posta elettronica, vecchi contratti e NDA, al dominio degli **archivi** di lavoro. Questo per minimizzare il potenziale impatto del potenziale attacco sul mio dominio di **lavoro** (il mio dominio di lavoro potrebbe essere attaccato ad esempio sfruttando un ipotetico bug nell'handshake del protocollo di Thunderbird usando un attacco MITM o un ipotetico bug in GPG).

Il dominio del **vault** è in definitiva un dominio affidabile in cui genero e conservo tutte le mie password (usando KeePass) e le chiavi GPG principali. Ovviamente, questo dominio del vault non ha accesso alla rete. La maggior parte di queste password, come la password di accesso al server di posta elettronica, viene conservata anche nei domini specifici che le utilizzano, come il dominio di

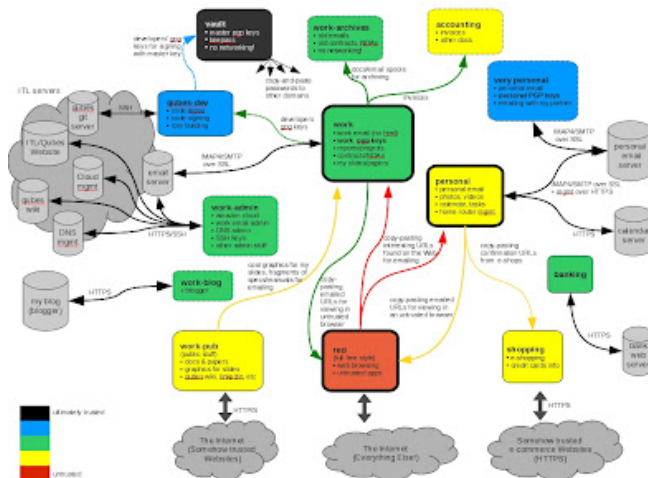
lavoro , e più specificamente nel client Thunderbird (non ha assolutamente senso non consentire, ad esempio, a Thunderbird di ricordare il password: se venisse compromessa, la ruberebbe la prossima volta che la inserisco manualmente)

E infine, c'è il dominio **rosso** precedentemente menzionato (ho provato a chiamarlo *spazzatura* o *casuale* in passato , ma penso che il **rosso** sia ancora un nome migliore dopo tutto). Il dominio **rosso** è totalmente non attendibile - se viene compromesso, non mi interessa - lo ricreerei in pochi secondi. Non l'ho nemmeno eseguito il backup! Fondamentalmente faccio lì tutto ciò che non rientra in altri domini e che non mi richiede di fornire alcuna informazione sensibile. Non distinguo nemmeno tra la navigazione legata al lavoro e quella personale: non mi interessa l'anonimato per tutte quelle attività che svolgo lì. Se fossi preoccupato per l'anonimato, creerei un **anonimo** separato domain e da lì **eseguire il proxy** di tutto il traffico tramite un **proxy tor** .

Ora, tutto questo sembra bello e facile ;) ma c'è una cosa che complica l'immagine sopra...

Flussi di dati tra i domini

Il diagramma seguente mostra gli stessi domini, ma in aggiunta con le frecce che simboleggiano i flussi di dati tipici tra di loro.



(http://4.bp.blogspot.com/-6iEN6AFqWMU/TXyqaqgbtZI/AAAAAAAAAHY/FScd_uk9uso/s1600/qubes%2Bpartitioning%2B-%2Bdata%2Bflows.jpg)

Puoi vedere che la maggior parte dei normali flussi di dati provengono da domini *più attendibili* a domini *meno attendibili* , ad esempio copia e incolla un URL che ricevo via e-mail nel mio dominio di **lavoro** , in modo che possa aprirlo nel mio browser non attendibile in **rosso** , oppure spostare le fatture dal mio dominio di **lavoro** (dove le ricevo via email) al dominio di **contabilità** .

Ma ci sono, purtroppo, anche alcuni trasferimenti da domini *meno attendibili* a domini *più attendibili* . Un esempio è copiare e incollare un URL interessante in cui mi sono appena imbattuto durante la navigazione nel dominio **rosso** e che vorrei condividere con un'università al lavoro o con un amico, quindi devo copiarlo e incollarlo nella mia email cliente in ambito **lavorativo** (collega) o **personale** (amico).

Ora, la copia dei dati da domini *meno affidabili* a quelli *più affidabili* presenta un problema significativo. Mentre si potrebbe pensare che incollare un URL nell'editor di posta elettronica di Thunderbird sia un'operazione piuttosto innocua, è ancora un input non attendibile e non sappiamo davvero cosa il dominio **rosso** *abbia effettivamente* incollato negli appunti locali, e quindi cosa incolleremo in l' editor di posta elettronica Thunderbird del dominio di **lavoro** (forse 64 kB di posta indesiderata che traboccherà del buffer di annullamento nell'editor?). E ancora più spaventoso è l'esempio con la copia del file grafico dall'aspetto accattivante dal Web nel mio **lavoro** domain in modo da poterlo utilizzare nelle mie diapositive di presentazione (ad es. un xkcd . Da **più di un decennio** (<http://www.openwall.com/advisories/OW-002-netscape-jpeg/OW-002-netscape-jpeg.txt>) sono **noti** (<http://www.openwall.com/advisories/OW-002-netscape-jpeg/OW-002-netscape-jpeg.txt>) attacchi originati da JPEG dannosi o altri formati grafici e lo sfruttamento di bug nel rendering del codice .

Ma questo problema - come gestire i flussi di dati da sistemi meno affidabili a sistemi più affidabili - non è facilmente risolvibile in pratica, purtroppo...

Alcune persone che progettano e costruiscono sistemi ad alta sicurezza per uso militare e governativo adottano un approccio in qualche modo opposto: affermano di non essere preoccupati per i trasferimenti di dati da meno attendibili a più attendibili purché possano assicurare che non c'è modo per eseguire un trasferimento nella direzione opposta.

Quindi, se potessimo costruire un sistema che garantisca che un dominio più affidabile non possa mai trasferire dati a un dominio meno affidabile (anche se entrambi i domini sono compromessi!), Allora sono felici di consentire "trasferimenti unidirezionali". In pratica questo significa che dobbiamo eliminare tutti i canali nascosti tra due domini *cooperanti*. La parola *cooperare* è una parola chiave qui, e il che rende l'intera idea non affatto pratica, IMHO.

Eliminazione dei canali segreti tra *cooperantidomains* è effettivamente richiesto in questo schema, perché il presupposto è che il trasferimento dei dati dal dominio meno attendibile potrebbe aver effettivamente compromesso il dominio più attendibile. Ma questo, almeno, non dovrebbe comportare alcuna perdita di dati al dominio di origine e successivamente alla rete meno classificata, a cui questo dominio meno affidabile è presumibilmente connesso. Uno dei presupposti qui è che l'utente di un tale sistema sia connesso a più di una rete isolata. Anche in tal caso, l'eliminazione di tutti i canali nascosti tra i domini (o almeno la riduzione della larghezza di banda a qualcosa di inutilizzabile - cos'è davvero inutilizzabile?) è una grande sfida, e probabilmente può essere fatta solo quando siamo pronti a sacrificare le prestazioni del sistema (sono necessari trucchi di pianificazione intelligenti per ridurre al minimo i canali segreti temporali).

Vorrei chiarire che non siamo interessati ad eliminare i canali segreti cooperativi tra i domini in Qubes in qualsiasi momento nel prossimo futuro, e forse anche a lungo termine. Semplicemente non credo in tale approccio e non mi piace nemmeno che questo approccio non faccia nulla per preservare l'*integrità* del dominio più affidabile: si concentra solo sull'aspetto dell'isolamento. Quindi, forse l'attaccante potrebbe non essere in grado di divulgare i segreti al dominio meno attendibile, ma può fare tutto il resto in questo dominio più attendibile. A che serve l'isolamento, se non manteniamo l'integrità?

Una soluzione alternativa alla gestione dei trasferimenti di dati da meno attendibili a più attendibili consiste nell'avere "convertitori" o "verificatori" affidabili in grado di gestire tipi di file specifici, come i JPEG, e assicurarsi di ottenere un file non dannoso in il dominio di destinazione. Anche se questo potrebbe ricordare la vecchia tecnologia A/V, è qualcosa di diverso. Qui, i convertitori attendibili sarebbero probabilmente alcuni programmi scritti in un linguaggio sicuro, in esecuzione in un altro dominio attendibile, piuttosto che un grosso e brutto A/V con un enorme database di firme di modelli "cattivi" di ciò che potrebbe apparire in un file JPEG. L'ovvio problema con un tale approccio è che qualcuno deve scrivere quei convertitori e scriverli per tutti i tipi di file che desideriamo consentire il trasferimento a domini più affidabili. Forse fattibile a lungo termine, e forse lo faremo in qualche futura versione di Qubes...

In questo momento stiamo ignorando questo problema e diciamo che tutti i trasferimenti da meno attendibili a più attendibili devono essere eseguiti a rischio dell'utente :) Puoi inviare convertitori attendibili per i tuoi tipi di file preferiti Intanto!

Copiare file tra domini

Parlando di copiare file tra domini, c'è un altro problema di sicurezza qui. Se immaginassimo due macchine fisicamente separate che non condividono risorse di rete comuni, l'unico modo per spostare i file tra queste due macchine air gap sarebbe tramite qualcosa come una chiavetta USB o un CDROM o un disco DVD. Ma l'inserimento di un'unità USB o di un CDROM in una macchina attiva molte azioni: dall'analisi delle informazioni fornite dal dispositivo, dal caricamento dei driver richiesti (per USB), dall'analisi della tabella delle partizioni del driver, dal montaggio e infine dall'analisi del filesystem. Ognuna di queste fasi richiede che il sistema operativo della macchina esegua molte elaborazioni di input non attendibili e il potenziale spazio di attacco qui è piuttosto ampio. Quindi,

anche se potessimo limitarci a copiare solo file innocui tra macchine/domini (forse sono stati in qualche modo verificati da una parte fidata nel mezzo,

In Qubes Alpha abbiamo utilizzato un meccanismo di copia file simile, utilizzando una chiavetta virtuale per la copia di file tra domini. In Qubes Beta 1 forniremo un nuovo schema basato sullo stesso canale di memoria condivisa che utilizziamo per la virtualizzazione della GUI: i dettagli tecnici di questa soluzione saranno presto disponibili nel **nostro wiki** (<http://wiki.qubes-os.org/trac>) . L'elemento più sensibile in questo nuovo schema è l'utilità simile a cpio che viene eseguita nel dominio di destinazione e decompime il blob in arrivo nell'albero di directory predefinito (ad esempio `/home/user/incoming/from-{domainname}/`). Riteniamo di poter scrivere un'utilità simile a cpio piuttosto sicura, in contrasto per proteggere tutti gli elementi menzionati in precedenza (parsing del dispositivo USB, parsing delle partizioni, parsing fs). La Beta 1 di Qubes dovrebbe essere rilasciata alla fine di marzo, BTW.

Applicazione del partizionamento e facilità d'uso

Affinché qualsiasi schema di partizionamento di sicurezza abbia senso nella vita reale, è necessario disporre di un meccanismo di imposizione che garantisca che l' *utente* non lo ignori erroneamente. In particolare per questo scopo abbiamo creato un supporto firewall speciale, precedentemente menzionato, in Qubes Beta 1 , che tratterò presto in un articolo separato.

Un'altra cosa è rendere il partizionamento facile da usare. Ad esempio, vorrei essere in grado di impostare un suggerimento nella politica, che quando faccio clic su un URL in un'e-mail che ho ricevuto nel mio dominio di **lavoro** , dovrebbe essere aperto automaticamente nel browser Web predefinito del dominio **rosso** . Attualmente non lo facciamo a Qubes, ma stiamo pensando di farlo nel prossimo futuro. **Riepilogo** Partizionare il proprio di

la vita virtuale nei domini della sicurezza non è certamente un processo facile e richiede un po' di riflessione. Anche questo processo è molto specifico per l'utente. Lo schema di partizionamento che mi sono inventato è piuttosto sofisticato e la maggior parte delle persone probabilmente vorrebbe qualcosa di molto più semplice. In caso di implementazioni aziendali, lo schema sarebbe progettato dal CIO o dagli amministratori IT e applicato automaticamente agli utenti. Un problema molto più grande sono gli utenti domestici e delle piccole imprese, che dovrebbero inventarsi il partizionamento da soli. Forse nelle versioni future di Qubes forniremo alcuni modelli pronti per l'uso per gruppi selezionati di utenti "tipici".

Joanna Rutkowska

Qubes OS (<https://qubes-os.org>) e laboratorio di cose invisibili (<http://invisiblethingslab.com/>)

Feed RSS (</feed.xml>)

del blog Fonte di questo blog (<https://github.com/rootkovska/rootkovska.github.io>)



(<http://creativecommons.org/licenses/by-nc-sa/4.0/>)