

VM usa e getta

1 giugno 2010 di **Joanna Rutkowska**

Mentre siamo ancora impegnati con gli **ultimi biglietti** (<http://www.qubes-os.org/trac/report/3>) rimasti per il traguardo di Qubes Alpha 2, Rafal ha già iniziato a lavorare su una nuova funzionalità per Qubes Beta 1: sulle macchine virtuali usa e getta. Penso che questo sarà davvero un film killer, e volevo dire qualche parola al riguardo.

Le macchine virtuali usa e getta saranno macchine virtuali molto leggere che possono essere create e avviate in un tempo molto breve, diciamo $< 1s$, con il solo scopo di ospitare una sola applicazione, ad esempio un visualizzatore PDF o un lettore multimediale.

Per capire perché le macchine virtuali usa e getta sono importanti, immagina la seguente situazione: ricevi un'e-mail da un cliente che contiene un allegato PDF, ad esempio una fattura o un contratto. Ovviamente stai aprendo e leggendo il messaggio in un client di posta in esecuzione nella tua AppVM "di lavoro" (o AppVM "di lavoro-email", se sei paranoico), solo perché è una corrispondenza relativa al lavoro, che arriva al tuo professionista indirizzo e-mail (per molte ragioni è bene utilizzare indirizzi e-mail diversi per le attività lavorative e per la vita personale).

Tuttavia, le possibilità che qualcuno comprometta il tuo client di posta elettronica semplicemente inviandoti un messaggio creato in modo dannoso che sfrutterebbe il tuo corpo o i parser dell'oggetto sono molto ridotte, se hai disabilitato il parser HTML completo per i corpi dei messaggi (cosa che penso che la maggior parte delle persone attente alla sicurezza faccia comunque). Forse un vettore di attacco più efficace sarebbe che qualcuno possedesse prima il tuo server di posta elettronica e poi provasse a sfruttare il parser del protocollo IMAP/POP/SMTP nel tuo client di posta elettronica. Ma ehi, in tal caso, avrebbero già accesso a tutte le tue e-mail sul server aziendale, senza sfruttare il tuo client di posta elettronica (beh, potrebbero comunque accedere alle tue chiavi PGP in questo modo - se questo ti dà fastidio, potresti volere utilizzare le smartcard per le chiavi PGP). C'è anche la possibilità di eseguire un attacco Man-In-The-Middle e provare a sfruttare i primi parser del protocollo SSL,

Ma ora vorresti aprire questo PDF che ti ha appena inviato un cliente. È abbastanza ragionevole temere che il PDF possa essere dannoso e potrebbe tentare di sfruttare il tuo visualizzatore PDF, e quindi provare a rubare le tue e-mail o altre cose che conservi nell'AppVM "lavoro" (o AppVM "lavoro-e-mail"). Non importa se ti fidi del mittente, poiché il sistema operativo del mittente potrebbe essere compromesso da alcuni malware e potrebbe infettare tutti i PDF in uscita senza il consenso dell'utente.

Potresti provare ad aprire il PDF in una delle tue VM non sensibili, ad esempio la

VM "casuale" che usi per la navigazione Web causale, per assicurarti che anche se il PDF è dannoso, non otterrai l'accesso a nessun file sensibile dati. Ma cosa succede se il PDF non è dannoso e cosa succede se contiene alcuni dati riservati? In tal caso potresti buttare via il bambino con l'acqua sporca (la tua VM "casuale" potrebbe essere già stata compromessa e ora sarebbe in grado di rubare i segreti dal tuo file PDF).

Una macchina virtuale usa e getta è una soluzione ideale qui. Crei una macchina virtuale pulita e usa e getta, solo allo scopo di visualizzare il PDF. Poi, una volta che hai finito, lo butti via. Se il PDF fosse dannoso, potrebbe danneggiare solo la propria VM usa e getta, che non contiene nulla tranne... questo stesso PDF. Allo stesso tempo, la VM usa e getta viene sempre avviata in uno stato pulito, quindi non c'è modo che qualcuno possa rubare il documento. Solo il documento può rubare se stesso :)

Sembra tutto facile, ma per renderlo pratico abbiamo bisogno di un'implementazione molto efficiente di macchine virtuali usa e getta e una buona integrazione di sistema, quindi l'esperienza è stata perfetta per l'utente. Ad esempio, all'utente dovrebbe essere richiesto solo di fare clic con il pulsante destro del mouse su un file e scegliere "Apri in una VM eliminabile" e Qubes dovrebbe occuparsi di tutto il resto: creare la VM, avviarla, copiare il file nella VM e avviare un Applicazione associata a MIME per questo tipo di file (es. PDF) nella VM. E tutto questo in un tempo inferiore a 1s!

Il supporto di base per le macchine virtuali usa e getta è pianificato per la Beta 1, programmata alla fine delle vacanze estive. Ma posso dire che è solo l'inizio. L'obiettivo finale, dal punto di vista dell'utente, sarebbe quello di fare in modo che il sistema operativo Qubes appaia e si comporti proprio come un normale sistema operativo mainstream come Linux, Windows o persino Mac, ma sempre con tutta la forte sicurezza fornita dall'architettura Qubes, implementata dietro le quinte. Il supporto continuo per le macchine virtuali usa e getta è uno dei primi passi per raggiungere questo obiettivo.

Crediti speciali vanno a Matt Piotrowski, che ha appena lasciato la Berkeley University e la cui **tesi pubblicata di recente è (<http://radlab.cs.berkeley.edu/wiki/Virtics>)** stata una diretta ispirazione per implementare VM usa e getta in Qubes. Anche se abbiamo menzionato le VM "una tantum" nel nostro **documento sull'architettura (<http://qubes-os.org/files/doc/arch-spec-0.3.pdf>)** a gennaio (vedi capitolo 4.6), è stato davvero l'articolo di Matt a convincermi che dovremmo davvero averli a Qubes. Virtics, un'implementazione proof-of-concept scritta da Matt, condivide molte somiglianze con Qubes, come ad esempio l'architettura e l'implementazione della virtualizzazione della GUI. Ci sono anche differenze però, e rimando i lettori al documento di Matt per maggiori dettagli.

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/>)