La sicurezza informatica dei nuovi servizi digitali: un nuovo approccio architetturale

Author : Raffaele Bolla

Date : 28 Ottobre 2019

Abstract

Le più recenti architetture per la realizzazione di servizi in rete, basate sui paradigmi del *cloud computing,* della *Network Function Virtualization* e dell'*Internet of Things,* prevedono l'interazione di processi *software* distribuiti su una complessa infrastruttura ICT, a sua volta composta da molteplici dispositivi eterogenei che operano nativamente in più domini amministrativi. In questo contesto gli approcci alla sicurezza informatica tradizionali - basati sul concetto di "perimetro di sicurezza" - si rivelano di scarsa efficacia, quando non completamente inadeguati. Nasce quindi l'esigenza di sviluppare nuove soluzioni di *cyber security*, che siano adatte ai mutati contesti tecnologici e applicativi.
Il presente articolo riassume le innovative soluzioni architetturali per la sicurezza dei nuovi servizi digitali proposte e in via di sviluppo e validazione nell'ambito di due progetti europei finanziati dal programma Horizon 2020 : ASTRID e GUARD.

Nuovi paradigmi per i servizi digitali

La stretta integrazione tra le più recenti tecnologie software (*cloud/edge/fog computing*) e di rete (5G, *Software-Defined Networking*, *Network Function Virtualization* e *Internet of Things*) rappresenta l'elemento cardine per lo sviluppo di infrastrutture ICT innovative in grado di supportare i servizi applicativi prefigurati dai noti e popolari paradigmi che vanno sotto il nome - tra gli altri - di *Smart City*, *Smart Factory* e *Smart Grid*.

Come schematizzato in Fig.1, le nuove tecnologie disponibili permettono, infatti, di implementare tali servizi come una composizione di processi *software* supportati da una complessa infrastruttura ICT distribuita, composta da molteplici ed eterogenei dispositivi fisici (dai semplici sensori ai potenti *server* di elaborazione presenti nei *cloud data centre*) i quali operano, tipicamente, in diversi domini amministrativi.

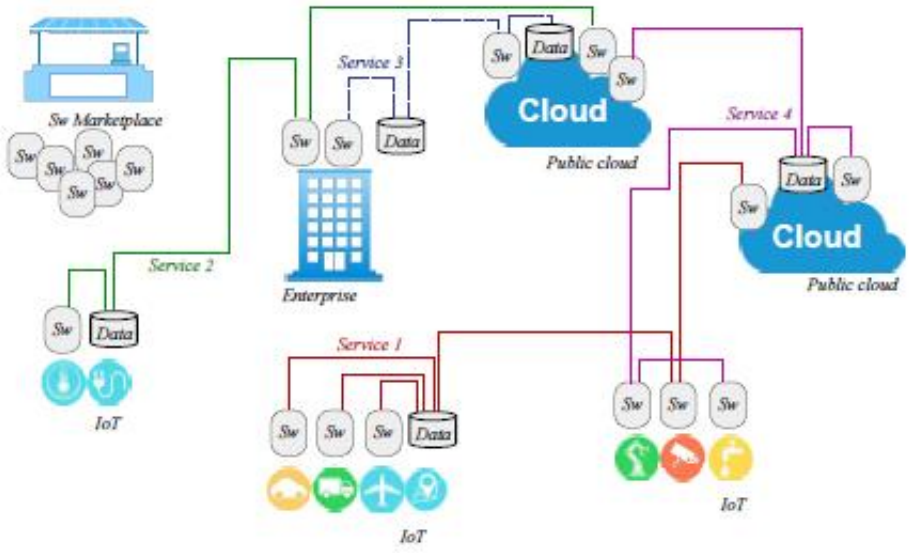

Figura 1: Nuove architettura ICT abilitanti catene di servizi digitali

La sicurezza dei servizi digitali innovativi: la debolezze delle soluzioni tradizionali

Analizzando la Fig. 1 appare immediatamente evidente la difficoltà di garantire la sicurezza di un ambiente distribuito come quello rappresentato, semplicemente applicando le soluzioni più tradizionali [1].

Un sicuro **elemento di criticità** risiede nell'utilizzo di soluzioni di *cloud computing*, principalmente a causa della loro intrinseca natura *multy-tenancy* (più applicazioni diverse condividono le stesse risorse computazionali e di memoria) e dell'elevato numero di componenti (macchine virtuali, sistemi operativi *host*, *hypervisor*, interfacce di gestione, elementi di *data storage* ed infrastrutture di rete condivisi) che danno luogo a un consistente ampliamento della "superficie" potenzialmente vulnerabile a eventuali attacchi. Infatti, sono ormai noti minacce e modelli di attacco efficaci che sfruttano la condivisione dell'infrastruttura da parte di più *tenant*.

A quanto sopra va ad aggiungersi la proliferazione di dispositivi intelligenti connessi a Internet (le "cose" dello *Internet of Things*) che hanno permesso la nascita di nuove strategie di attacco su vasta scala, comunemente conosciute come *Distributed Denial of Service* (DDoS).

Un ulteriore elemento di rischio risiede nella modalità di dispiegamento dei servizi, che, come precedentemente accennato, sono istanziati combinando, in modo dinamico e flessibile, dispositivi *hardware* e processi *software*, fra loro interoperabili ma (almeno potenzialmente) sviluppati e manutenuti da organizzazioni diverse. La possibilità di reperire sul mercato i blocchi elementari più opportuni e di combinarli dinamicamente per realizzare un servizio fa di questo

approccio la modalità ad oggi più efficace per soddisfare le richieste, in continua evoluzione, degli utenti del mondo digitale. Questa modalità, però, comporta **nuovi problemi di sicurezza**, in quanto un elemento compromesso in una catena di servizi può rappresentare un vettore di attacco privilegiato.

Gli elementi di vulnerabilità sopra descritti possono essere sfruttati dai sempre più sofisticati metodi di attacco, che si sono evoluti nel tempo per:

- combinare più tipologie di azioni (*multi-vector attack*) per stressare i sistemi di sicurezza e sfruttarne le possibili pecche;
- essere altamente personalizzati e variabili nel tempo, così da eludere le strategie di rilevamento basate sull'analisi della loro "impronta digitale";
- utilizzare protocolli di comunicazione di alto livello (livello applicativo) in modo da sfruttare le vulnerabilità del software ed errori di configurazione dei sistemi;
- utilizzare la crittografia per proteggersi dalle ispezioni dei dispositivi di sicurezza intermedi;
- prediligere domini applicativi dove le architetture ICT non hanno raggiunto ancora pratiche consolidate per la protezione da attacchi di diversa natura, ovvero dove ci sono dispositivi con capacità limitate (ad esempio Internet of Things - IoT); rapporti recenti evidenziano un aumento del 600% degli attacchi contro i dispositivi intelligenti, causati da nuove *botnet* come Mirai, Brickerbot e Hajime, e un aumento del 29% delle vulnerabilità del sistema di controllo industriale [2].

Gli approcci *"legacy"* per la cyber security, principalmente legati al modello del "perimetro di sicurezza", sono certamente non ottimali per proteggere i nuovi servizi digitali da attacchi sempre più sofisticati.

Il modello del "perimetro di sicurezza" consiste nell'utilizzare dispositivi quali *firewall*, *antivirus*, sistemi di rilevamento delle intrusioni e sistemi di protezione dalle intrusioni, per segregare e proteggere segmenti di rete, applicando regole di filtro e rilevamento per lo più statiche e predefinite.

A causa di tale rigidità, il modello male si adatta alla flessibilità di implementazione e manutenzione dei nuovi servizi e alla natura sempre più mutevole degli attacchi [1].

Un altro **fattore di rigidità** degli attuali dispositivi di sicurezza risiede nella specializzazione delle rispettive funzionalità. Tali dispositivi sono, infatti, progettati per rilevare solo attacchi ed eventi specifici (DoS di rete o applicativi, rilevamento/prevenzione delle intrusioni, rilevamento di malware). Di fronte a un complesso attacco multi-vettore, questa caratteristica può rendere il singolo dispositivo del tutto inefficace o, nella migliore dell'ipotesi, può aumentare significativamente i tempi necessari per la rilevazione dell'attacco.

Infine, anche i dispositivi di sicurezza possono essere sorgenti di rischi, in quanto essi stessi vulnerabili agli attacchi e frequentemente soggetti a guasti o malfunzionamenti: la Fig. 2 mostra il numero di vulnerabilità segnalate a NIST per le applicazioni di sicurezza dei principali fornitori dal 2016 [3].

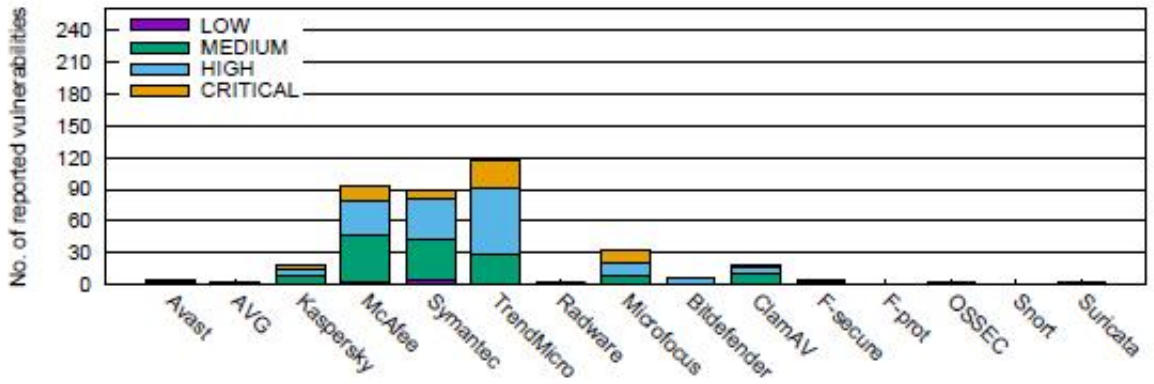

Figura 2: Vulnerabilità dei principali fornitori di dispositivi di sicurezza
Fonte: NIST - National Vulnerabilities Database

Oltre che alla **revisione delle soluzioni tecniche**, la necessità di proteggere i nuovi servizi digitali dovrà necessariamente portare a una **riconsiderazione dei processi di sicurezza**. Attualmente, infatti, la gestione delle minacce e degli attacchi informatici è ancora basata in modo consistente sulla presenza e sull'intervento di personale umano: si tratta tipicamente di esperti altamente qualificati che sono direttamente coinvolti nella messa in opera, configurazione e gestione degli apparati di sicurezza (ad es. selezionano i prodotti, identificano la loro posizione, li configurano, correlano avvisi e indicazioni da essi generate, eseguono azioni in risposta agli attacchi). Un tale processo, che richiede in modo massivo e sistematico l'intervento di personale, pone evidenti problemi di costo ed efficacia e appare incompatibile con la prevista pervasività del processo di digitalizzazione in tutti i settori sociali ed economici.

Infine, una questione importante è rappresentata anche dalla garanzia d'affidabilità dei componenti del servizio. Le attuali soluzioni di protezione - che sfruttano, ad esempio, le reti private virtuali, il *firewalling*, il controllo degli accessi basato sull'identità e altri approcci correlati - richiedono configurazioni quasi statiche, tradizionalmente eseguite da operatori umani e non sono adatte a garantire la dinamicità richiesta ai nuovi servizi digitali.

Un nuovo approccio architetturale

La protezione dei nuovi servizi digitali richiede, quindi, una profonda revisione degli attuali paradigmi della sicurezza informatica. In tale contesto, si può identificare un insieme di **sfide tecnologiche** che è necessario affrontare per rendere l'approccio alla sicurezza informatica adeguato alle nuove soluzioni di dispiegamento dei servizi. In sintesi tali sfide consistono nell'individuare soluzioni in grado di:

I) produrre strumenti automatici, basati su metodi formali, utilizzabili per attestare l'affidabilità dei componenti *hardware* e *software* che compongono il servizio e del servizio nel suo complesso;
II) permettere l'incremento delle capacità di identificazione e analisi degli attacchi, nel rispetto

dei vincoli legali imposti per il rispetto della *privacy* (degli utenti) e della riservatezza dei dati (degli amministratori dei diversi domini che cooperano al supporto del servizio);
III) mettere in correlazione i dati tra diversi sistemi di individuazione degli attacchi per incrementare l'efficacia complessiva;
IV) permettere l'automazione della risposta agli attacchi, per minimizzare la necessità di intervento umano;
V) migliorare la *situational awareness* degli operatori dei nuovi servizi e facilitare la propagazione delle informazioni a tutte le organizzazioni coinvolte (sia interne agli operatori che esterne come, ad esempio, *Computer Emergency Response Team* nazionali).

Per rispondere alle sfide sopra elencate, è necessario che le nuove soluzioni per la sicurezza siano basate non più su dispositivi fisici o strumenti *software* locali ma, piuttosto, su sistemi pervasivi che prevedano l'interazione di elementi distribuiti di monitoraggio e di elementi (logicamente) centralizzati di elaborazione, responsabili dell'individuazione degli attacchi, dell'implementazione (largamente automatica, sulla base di politiche predefinite) delle azioni conseguenti e del consolidamento e presentazione della situazione agli operatori umani (Fig. 4).

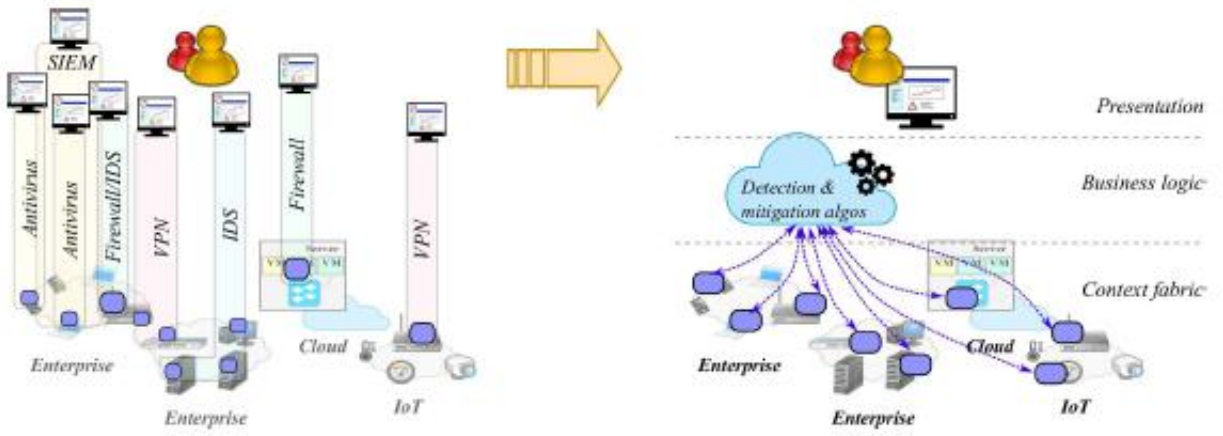

Figura 4: La transizione dall'attuale alla nuova soluzione per la sicurezza

Il nuovo approccio prevede, quindi, un **profondo mutamento di paradigma** relativamente ai dispositivi di sicurezza, assecondando l'evoluzione, già in atto, illustrata in Fig. 5.

I dispositivi di sicurezza più tradizionali oggi in uso (come *antivirus* e *firewall*) sono concepiti per proteggere parti dell'infrastruttura fisica, e sono rigidamente associati a tali parti (Fig. 5-a).

Il primo passo dell'evoluzione consiste nel passare da un approccio finalizzato alla protezione dell'infrastruttura ad un nuovo approccio finalizzato alla **protezione del servizio**. Per esempio, come mostrato in Fig. 5-b, nello scenario in cui un servizio è supportato da un'infrastruttura *cloud* secondo il paradigma IaaS (*Infrastructure as a Service*[1]), delle istanze virtuali di dispositivi per la sicurezza sono inserite nella catena di processi software che

realizzano il servizio stesso e dedicate alla protezione di tale servizio. In questo modo, ogni utente dell'infrastruttura mantiene la piena gestione della sicurezza del servizio che questi gestisce.

Il successivo passo evolutivo (Fig. 5-c) necessario per il pieno supporto dei nuovi servizi digitali sarà basato sull'integrazione, nei diversi elementi software che compongono il sistema, di funzionalità di monitoraggio che comunicheranno con un processo (logicamente) centralizzato responsabile delle operazioni di rilevazione e gestione degli attacchi. In altri termini, così come un sistema operativo espone verso le applicazioni le risorse computazionali, di rete e di memorizzazione dei dati attraverso specifiche API (*Application Programming Interfaces*), così i futuri servizi digitali esporranno a **sistemi centralizzati di rilevazione e gestione degli attacchi** le funzionalità per la sicurezza in essi integrate.

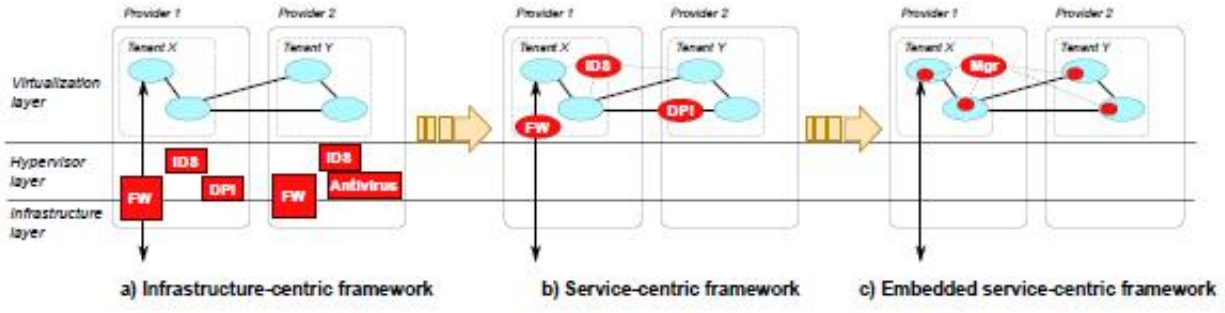

Figura 5: Evoluzione delle soluzioni per la sicurezza dei servizi applicativi

Le Figg. 6 e 7 forniscono una rappresentazione di più alto livello e più completa del Sistema complessivo. Questo sistema è composto da processi (logicamente) centralizzati che raccolgono, attraverso interfacce standardizzate, un'ampia mole di dati eterogenei (*log* applicativi, statistiche di rete, eccezioni software, etc.) dai componenti software del servizio, identificano attacchi o situazioni di rischio, applicano autonomamente contromisure e forniscono agli operatori del servizio - e ad altri soggetti interessati - le relative informazioni.

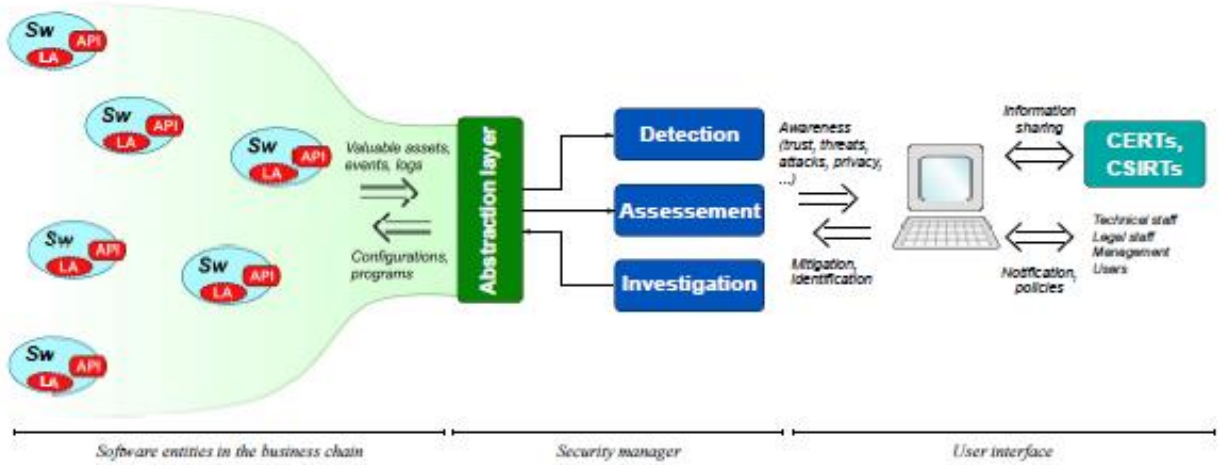

Figura 6: La futura evoluzione dell'architettura per la sicurezza dei nuovi servizi digitali

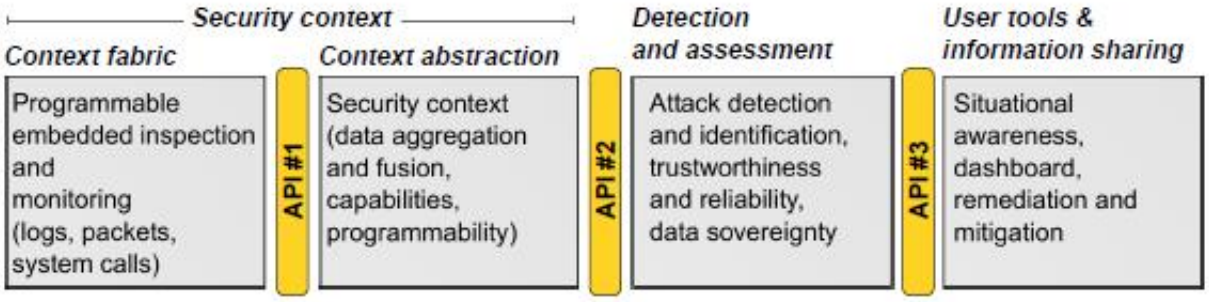

Figura 7: Elementi funzionali

Conclusioni

I nuovi approcci per la fornitura di servizi, basati sulle tecnologie più recenti sia di rete (5G), sia informatiche (*cloud*, *fog*, *edge computing*…) rendono gli approcci tradizionali alla sicurezza poco efficaci. La creazione dei servizi attraverso composizione dinamica di moduli *software* offerti liberamente sul mercato da parte di fornitori differenti e supportati dinamicamente da dispositivi fisici posti in infrastrutture remote non può più essere resa sicura con l'utilizzo di apparati specializzati pensati per la protezione di perimetri fisici ben determinati.

Si ha quindi la necessità di sviluppare **nuovi approcci architetturali** in cui i componenti del servizio integrino nativamente funzionalità di base di sicurezza e in cui le azioni di prevenzione e protezione siano demandate a **sistemi centralizzati** e caratterizzati sulla base delle specificità di ciascun servizio.

Lo studio e la sperimentazione di tali approcci sono parte degli obiettivi di due progetti Europei H2020, di cui CNIT (Consorzio Nazionale Interuniversitario per le Telecomunicazioni, www.cnit.it) è coordinatore tecnico: ASTRID ("*AddreSing ThReats for virtualIseD services*") e GUARD ("*A cybersecurity framework to GUArantee Reliability and trust for Digital service chains*").

Note

[1] Si tratta di una modalità di fornitura dei servizi *cloud* in cui il fornitore di servizi partiziona le risorse di elaborazione, memorizzazione e interconnessione presenti nella propria infrastruttura fisica e mette a disposizione di ciascuno dei suoi utenti una parte di tali risorse. Ogni utente è in grado di distribuire ed eseguire software arbitrario, che può includere sistemi operativi e applicazioni, utilizzando le risorse di elaborazione e memorizzazione rese disponibili dal fornitore di servizi.

Acknowledgement

Questo articolo è stato realizzato sulla base delle attività svolte dagli autori nell'ambito dei progetti ASTRID e GUARD, finanziati dal programma di ricerca ed innovazione dell'Unione Europea Horizon 2020 (grant agreement num. 833456 e num. 786922).

Riferimenti bibliografici

[1] R. Rapuzzi, M. Repetto, Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model, Future Generation Computer Systems 85 (2018) 235–249. doi:10.1016/j.future.2018.04.007.

[2] Symantec, Internet security threat report, Whitepaper, volume 23 (April 2018) [cited January 23rd, 2019]. URL https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

[3] Radware, European application and network security report, Whitepaper (2017) [cited January 23rd, 2019]. URL https://www.radware.com/getattachment/6bdd2d2a-fd3d-48c7-a160-0909dc219113/Radware_ERT_Report_2016-2017.pdf.aspx?disposition=attachment

Articolo a cura di **Raffaele Bolla, Maurizio Giribaldi, Giuseppe Piro** e **Matteo Repetto**