Protocollo di Sicurezza ISO27 (ISO27 Security Protocol)

Protocollo di Sicurezza ISO27

Zoino Francesco

19 luglio 2018 - 6 giugno 2020

Introduzione

Gli *attacchi DDoS* hanno l'obbiettivo di *sovraccaricare* una Rete, attraverso l'invio di numerose richieste al millisecondo. Quando il Server che riceve le richieste inviate dagli *host* (che eseguono l'attacco), non riuscirà più a rispondere a tutte le richieste, inviando la propria risposta, si andrà a considerare come sovraccarico. Per risolvere tale problema, normalmente si esegue il riavvio della Rete, anche se probabilmente l'attacco continuerà continuando con il proprio obbiettivo, questo per causare un *down* dei servizi, rendendo indisponibile una risorsa, e/o impedendo ad altri *host legittimi* di stabilire una connessione con il Server e/o Rete attaccata.

> Il 19 luglio del 2018 è stato creato il ***protocollo di Sicurezza ISO27***, che ha il compito di eseguire una *Mitigazione DDoS*, ovvero di proteggere i Server della Rete (che riceve l'attacco DDoS). Il protocollo di Sicurezza ISO27 è stato ideato e sviluppato per garantire la protezione alle Reti che ospitano i Server di Gioco, molto probabilmente grazie ai vari protocolli di Sicurezza stabiliti dallo stesso si potranno proteggere altre Reti di Computer che offrono altre Risorse e Servizi mediante protocolli di connessione differenti.

Introdurremo il funzionamento del protocollo di Sicurezza ISO27, analizzando una ***connessione standard*** (senza ulteriori protocolli e sistemi di sicurezza alla Rete che ospita le risorse***) da parte dell'utente, successivamente si andrà ad osservare l'applicazione del protocollo di Sicurezza ISO27 a tale connessione sempre da parte dell'host legittimo.

Connessione Standard

La connessione Standard si forma tramite una semplice richiesta da parte dell'*host legittimo**, che riceverà una risposta da parte della *Risorsa***.

*Si definisce l'*host legittimo* con "U";
**Si definisce la *Risorsa* con "x1";

La connessione Standard avviene ***se e solo se*** l'host legittimo è presente in Rete con un Indirizzo IP *Statico* o *Dinamico*, e se la Risorsa è presente anch'essa nella Rete con un Indirizzo IP *Statico* o *Dinamico*, con delle regole presenti tramite il *Port Forwarding*, che permette l'apertura (e quindi la ricezione delle richieste da un host esterno all'interno della Rete) grazie alle porte dei Servizi utilizzati considerate come "aperte" e mediante la specifica dell'utilizzo del *protocollo TCP* e/o *UDP.*

In tal caso, secondo l'idea della Connessione Standard, "U" invia una richiesta di connessione (quindi di visualizzazione e utilizzo della risorsa) a "x1" che risponderà a sua volta permettendo a "U" la visualizzazione e l'utilizzo della risorsa richiesta.

***Bisogna considerare che l'accesso alla Risorsa ("x1") venga sempre filtrato, in questo caso ci sarà una analisi da parte del *Port Forwarding* che permetterà all'host legittimo "U" (e non) il permesso di accedere a "x1" reindirizzando la sua richiesta iniziale a "x1" sollecitando l'invio di una risposta a "U".

Se e solo se "U" avrà l'accesso alla Risorsa ("x1"), avverrà uno scambio continuo di *richieste* da parte di "U" e *risposte* da parte di "x1".

Abbiamo dimostrato come avviene l'ideale Connessione Standard (diretta) tra "U" e "x1"*4.

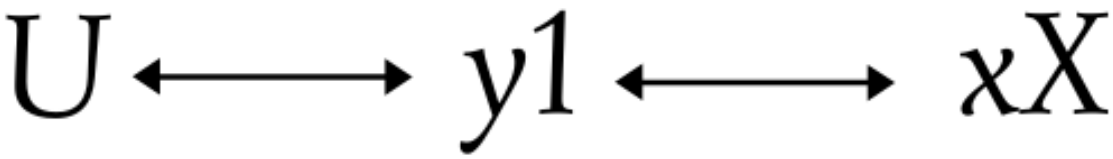
*4 Questo in caso non ci siano ulteriori protocolli e/o sistemi di sicurezza nella connessione che si è stabilita tra di essi e nella Rete che ospita e che gestisce i servizi in Rete di “x1”.

Connessione Standard con Bungeecord

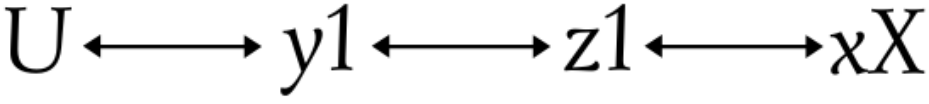
Negli anni a venire in successione al 2009 si sono ideati e sviluppati nuovi Sistemi di Sicurezza che permettessero non solo alla Rete di “x1” una maggiore stabilità nascondendo l’Indirizzo IP reale della Risorsa (“x1”), ma permettendo la possibilità a “U” di poter usufruire delle Risorse di “x1”, “x2”, “x3” e così via fino all’*infinito**5. Uno di questi sistemi ha preso il nome di Bungeecord che sarà denominato come “y1” nel Protocollo di Sicurezza ISO27.

*5 In relazione ai Server “xX”*6, ai Sistemi Hardware che gestiscono la rete (es. Router, Server DNS, Server Proxy), quindi alla loro possibilità di gestire più connessioni simultanee da parte di “U” e di gestire la comunicazione interna e/o esterna delle varie risorse “xX”.

*6 “xX” dove “x” rappresenta la Risorsa e “X” il numero della Risorsa “x”.



Nella Connessione Standard (con Bungeecord) viene mostrato l’host legittimo “U” (e non) che invia una richiesta a “y1” che esegue il compito di *proxy*, nascondendo il reale Indirizzo IP di “xX”, allo stesso tempo “y1” gestisce la richiesta di “U” reindirizzando “U” alla risorsa richiesta”, cambiando ancora una volta lo schema della Connessione Standard (con Bungeecord).



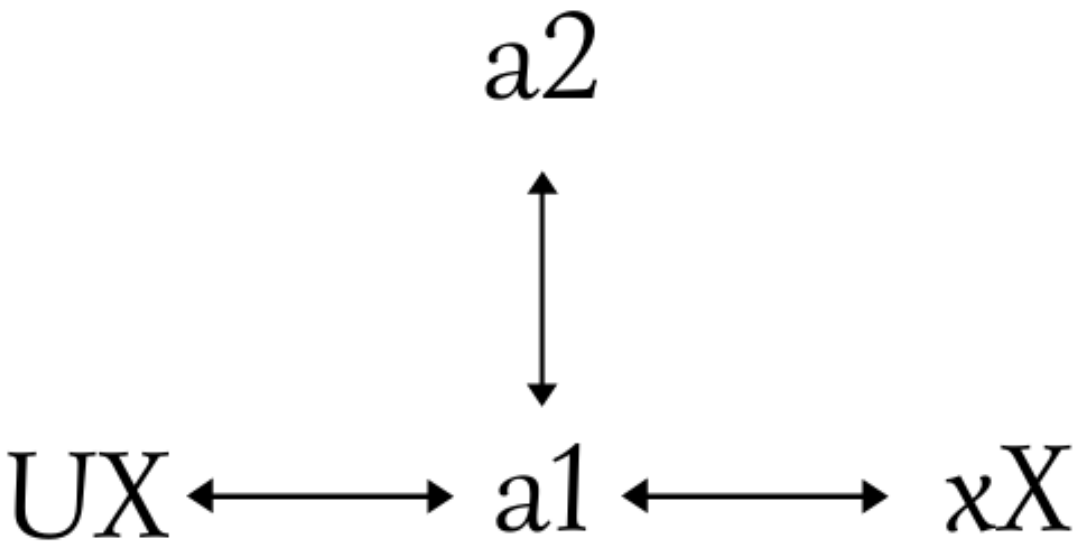
Dove “z1” avrà il compito di permette all’host “U” (in tal caso all’interno del gioco) di scegliere la risorsa “xX” a cui collegarsi, la connessione e lo smistamento verrà sempre gestito da “y1”, l’host “U” riceverà un’ulteriore risposta a seguito delle sue richieste, e avvierà così un ciclo di richieste e risposte indeterminabile, finché la connessione tra “U”,”y1”,”z1”,”xX” non verrà cessata*7.

*7 La connessione tra “U” e “z1” verrà automaticamente cessata a seguito dello smistamento e della connessione a “xX” gestita da “y1”, indi per cui “U” interrompendo la comunicazione con “z1” non interromperà il ciclo indeterminabile di richieste e risposte, chiaramente tenendo conto che “U” potrebbe cessare la connessione a “y1” e “z1” ancor prima che lo smistamento di “U” venga gestito da “y1”, in tal caso il ciclo indeterminabile di richieste e risposte da parte di “y1” e “z1” si interromperà.

Mitigazione DDoS

Attualmente i Sistemi di Mitigazione DDoS vengono già messe in pratica, ancor prima del 2009, però a differenza del Protocollo di Sicurezza ISO27 si ha un falla di Sicurezza, che distrugge una parte del loro funzionamento, ciò significa che i risultati tra i Sistemi di Mitigazione e tra il Protocollo di Sicurezza ISO27 variano.

Si pensi a “UX”, “a1”, “a2” e “xX”, dove “UX” sono i vari host (in questo caso malevoli), “a1” e ”a2” sono i Server che eseguono la mitigazione e dove “xX” sono le Risorse che finora abbiamo osservato.



Ogni sistema di Mitigazione è differente, vengono tutti strutturati in maniere differenti, ci sono quindi i Sistemi che hanno un maggior risultato in termini di sicurezza e ci sono quelli che non ottengono molti risultati positivi, però hanno tutti una cosa in comune ovvero non interrompono le tentate richieste che vengono inviate da “UX”, e in questa maniera le richieste vengono “filtrate” da “a1” che le smista, reindirizzando tutte quelle malevoli a “a2” che verranno poi analizzate ed eliminate, ciò richiede un alto impegno all’interno di una Rete e molto spesso questi sistemi non funzionano correttamente, portando la richiesta malevole a “xX”.

In entrambi i casi però le richieste malevoli entrano comunque all'interno della Rete (anche se essa divisa in parte da "xX").

In una mitigazione generica osserviamo l'invio delle richieste nocive per la Rete da parte di "UX" a "a1" che vengono poi analizzate in concomitanza con "a2" (per poi essere eliminate), attraverso alcuni protocolli come i DNS, l'ICMP, TCP Null, RST, SYN, ACK e UDP, l'IP Fragmentation, Null e Private, invece le richieste legittime verranno reindirizzate a "xX".

Questo è un Sistema abbastanza efficace, però aumenta la latenza all'interno della Rete con la comunicazione tra "U" e la Rete stessa, e potrebbe non essere pienamente efficace.

Il Protocollo di Sicurezza ISO27 evita il problema rendendo impossibile l'attacco alle Risorse e agli apparati di Rete che andranno a gestire la sicurezza della Rete.

Il Protocollo di Sicurezza ISO27

Il Protocollo di Sicurezza ISO27 è stato ideato e sviluppato partendo con il concetto della Connessione Standard, e della Connessione Standard con Bungeecord.

Esso garantisce una migliore protezione rispetto ai normali Sistemi di Mitigazione DDoS, in quanto è stato ideato in modo dedicato al protocollo e al metodo di Connessione che viene stabilito tra "UXL" e "x2", esso gestisce l'intera Rete tramite dei Software applicativi, analizzando in autonomia gli attacchi DDoS, gestendo le Richieste e le Risposte, in contemporanea garantirà altri vantaggi quali minor inattività nella Rete da parte di "UXL" (ovvero "UX" legittimi), minori crash da parte di "UXL", con una latenza stabile (grazie alla presenza pari a zero di attacchi DDoS)*8.

Indi per cui il Protocollo di Sicurezza ISO27, oltre a garantire una sicurezza superiore e una connettività stabile*9, mostra maggiori garanzie all'host "UXL" nello stabilire una connessione alla Rete gestita interamente dal protocollo di Sicurezza in questione*10.

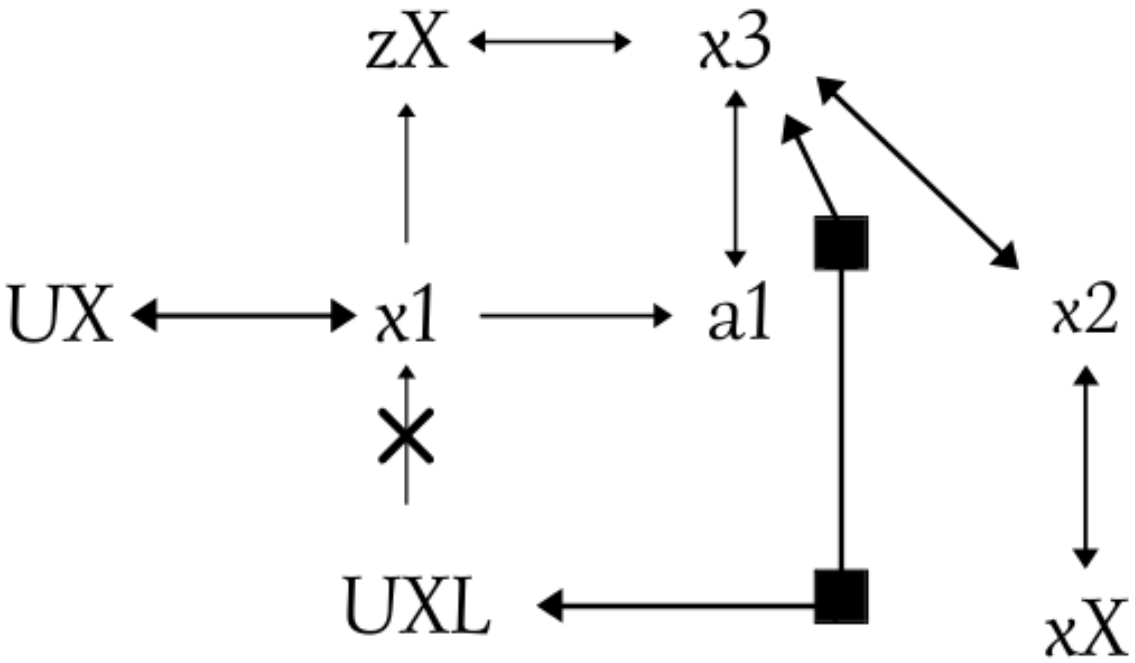
*8 La latenza è migliore grazie al Protocollo di Sicurezza ISO27, per la minor presenza di Attacchi DDoS agli apparati di Rete, ai Servizi generici e alle Risorse "xX", chiaramente la latenza è un fattore indeterminabile che può variare nel corso del tempo a seconda degli apparati Hardware utilizzati nella Rete e grazie ai Sistemi di comunicazioni nella Rete WAN (es. Nei Centri di Interscambio), inoltre, il risultato può variare per la connettività alla Rete WAN da parte di "UX" (legittimo).

*9 Si intende Connettività Stabile tra "UXL" e "x2", chiaramente nei propri limiti, senza contare problemi di connettività maggiori legati all'hardware, alla Rete WAN e alla Connettività alla Rete WAN di "UXL".

*10 Il Protocollo di Sicurezza ISO27, gestisce la Rete sin dalla prima richiesta da parte di "UXL", tra i vari apparati di smistamento e di distribuzione delle richieste e delle risposte da parte di "UXL", con "x2" fino alle Risorse "xX"*18, con "…nello stabilire una connessione alla Rete" (da parte di "UXL") si fa relazione al fattore umano.

Nelle prime versioni del Protocollo di Sicurezza ISO27 si è dimostrata un'ideale connessione tra "U" e "xX" (19 luglio 2018) che si è andata poi a migliorare nel tempo grazie alle versioni successive (8 novembre 2018, 10 maggio 2019, 15 gennaio 2020, 15 aprile 2020) fino al giorno della sua pubblicazione 6 giugno 2020 (in stesura per la visualizzazione pubblica dal 17 maggio 2020), il Protocollo di Sicurezza ISO27 verrà costantemente aggiornato.

Analizziamo l'ultima versione del Protocollo di Sicurezza ISO27, senza osservare le prime versioni del 2018 considerate obsolete.



*11 Si definisce “UX” (legittimo) con “UXL”, ovvero, un host “U” legittimo, che esegue una richiesta alla Rete continuando a comunicare con tutti gli apparati della stessa fino alla cessazione della comunicazione tra “UXL” con “x3”*12.

*12 Dopo l’autenticazione di “UX” la connessione con “x1” cesserà, ma la comunicazione e quindi le richieste e le risposte continueranno il loro percorso da “UXL” a “x3”*18 (finché la connessione stabilita tra “UXL” e con “x3”).

*18 “UXL” ha una connessione stabile con “x3”, esso (“x3”) gestisce tutte le sue richieste e le ritrasmette a “x2” che a sua volta le riporta alla Risorsa in uso “xX” dando come risultato una risposta a “UXL” passante per “x3”.

*13 Si definisce “x1” un apparato della Rete, che gestisce le prime richieste in entrata, la sua funzione principale è il filtraggio delle richieste da parte di “UX” e la funzione di Proxy. “x1” verifica quindi se la richiesta è lecita o meno, per poi aggiungerla nella lista di connessioni accettate presente in “a1”, successivamente “x3” verificherà tale connessione solo ed esclusivamente se proveniente da “x1” confrontando anche l’effettiva presenza della richiesta lecita su “a1” *(La definizione di “x1” e tutti i suoi dettagli e funzioni verranno elencate successivamente)*.

*14 Si definisce “UX” come l’host (non autenticato nella Rete) che esegue la prima richiesta ad essa, tramite “x1”.

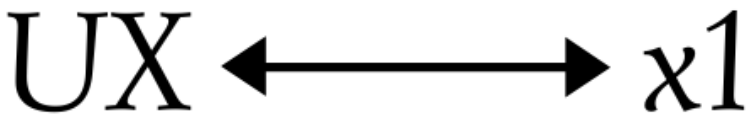
*15 Si definisce “xX” una o più Risorse, ovvero Server di Gioco effettivi che ospitano l’host “UXL” mediante i Sistemi di Smistamento e di Comunicazione di “x3”, “x2” e “a1”. In “xX” gli Sviluppatori del Gioco possono effettuare delle modifiche al gioco stesso (ovvero alle Risorse di cui “UXL” usufruisce), ma anch’essi dovranno effettuare tutti i passaggi del Sistema per l’accesso al Server, venendo quindi considerati come “UX”.

*16 Si definisce “x3” il Centro di Smistamento delle Richieste di “UXL” provenienti da “x1” in confronto con “a1”, provvedendo anche allo smistamento delle risposte da “x2” (per conto di “xX”). “x3” accetta le richieste da smistamento solo ed esclusivamente dalle connessioni provenienti da “x1” e presenti in “a1” tramite l’ID di Sessione. “x2” è invece il Centro delle Connessioni attive con “UXL”, si esplicita che tutte le richieste di connessione a “x2” vengono accettate e ospitate solo e solo se provenienti da “x3”.

*17 Si definisce “a1” un Servizio contenente una seconda funzione di filtraggio dopo “x1”, confermando la richiesta lecita a “x3”. In questo modo se “x1” dovesse andare *offline* tutte le connessioni alla Rete rimarranno comunque attive.*19

*19 Alla Rete vengono applicate delle Regole di Port Forwarding e sono presenti più collegamenti alla Rete WAN con diverse interfacce di Rete (Fisiche e/o Virtuali) con più Indirizzi IP pubblici (statici).

Le funzioni di “x1”



A seguito della prima richiesta*20 da parte di “UX” ad “x1” esso esegue un’analisi della richiesta, se la richiesta è lecita la Connessione verrà stabilita con “x2” e l’Indirizzo IP di “UXL” insieme all’ID di Sessione che verrà registrato in “a1” finché la connessione non cesserà per poi eseguire nuovamente tutto il processo.

*20 Tutte le richieste eseguite a “x1” avvengono solo e solo se “UXL” le esegue direttamente dal gioco stesso con i protocolli di connessione utilizzati dal gioco.*21

21* ***Nel caso dell’applicazione del Protocollo di Sicurezza ISO27 in un altro gioco* *che utilizza delle chiavi di criptazione dei dati, “x1” potrà contenere delle chiavi di decriptazione, accettando solo ed esclusivamente le richieste da parte di “UX” dal gioco stesso, seguendo, inoltre, le regole attuali del filtraggio tramite servizi, protocolli e porte specifiche (Port Forwarding).*

In caso di esito negativo di “UX”, la richiesta verrà rifiutata ed inserita in una blacklist.

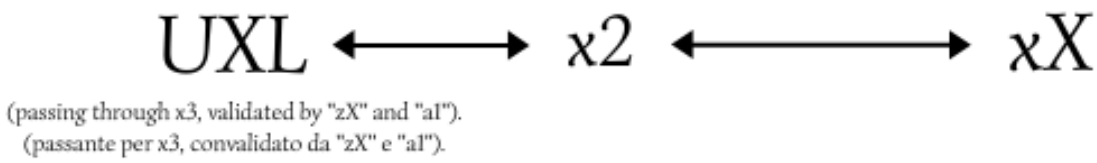
“x1” può identificare se una richiesta non è lecita e se si tratta di un attacco DDoS, poiché durante un Attacco DDoS gli host non rispondono mai ad una richiesta da parte di “x1”*22.

*22 Ci può essere l’eventualità di un sovraccarico di “x1” a seguito di questa operazione, ed è per questo motivo che a seguito della richieste illecite, esso continuerà ad analizzare smistando

le richieste di Connessione, poiché le richieste illecite verranno smistate ad un altro Servizio “zX” che provvederà ad aggiungere in blacklist le richieste illecite, in tal modo verranno rifiutate automaticamente da “x1". Si ricorda che la funzione (ovvero il test) dell’invio di una richiesta all’host illecito verrà sempre e comunque gestita da “x1”, utilizzando “zX” solo come una lista di blacklist, ovvero la funziona opposta di “a1”.

“x1” esegue la prima funzione di paragone con “zX” a seguito di una richiesta, poiché essa potrebbe essere già in blacklist, venendo quindi scartata senza alcuna analisi ulteriore da parte di “x1” o di “zX”.

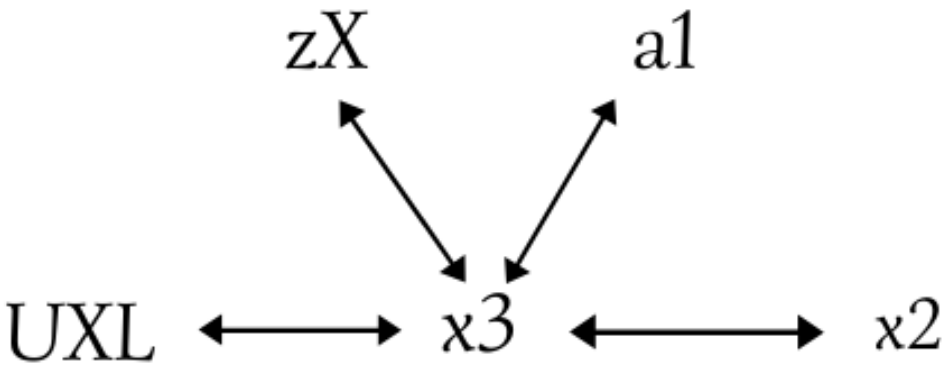
Le funzioni di “x2”



“x2” svolge un’importante funzione all’interno della Rete, in quanto è il Centro delle Connessioni Attive (comunicando con “UXL”, a seguito della filtrazione delle richieste da parte di “x1” e “x3”, ma non solo, infatti, “x2” è il nodo delle Risorse “xX”.

Dopo la verifica dell’utente “UX” che esegue la richiesta di connessione alla Rete, attraverso il lavoro complementare di “a1”, “UX” si converte in “UXL” che ha una comunicazione con “x3” che esegue un ulteriore verifica sulle richieste di connessione solo e solo se presenti in “a1” e se provenienti da “x3”.

Le funzioni di “x3”



Si definisce “x3” l’apparato di Verifica e di Smistamento delle Connessioni a “x2”, mediante la comunicazione con “zX” e “a1”.

“x3” accetta le richieste di “UXL” se e solo se esso è proveniente da “x1” e se l’ID di Sessione è presente in “a1”, se l’ID della richiesta è invece presente su “zX” la richiesta verrà automaticamente rifiutata.

“x3” smista le richieste filtrate a “x2” che si occuperà di mantenere attive le connessioni di “UXL” e di farlo comunicare con le Risorse “xX”.

(Si faccia riferimento alle specifiche nell’introduzione del Protocollo di Sicurezza ISO27 e a tutti gli altri collegamenti e punti dei singoli apparati di rete, presenti sia nell’introduzione stessa e all’interno di questo documento).