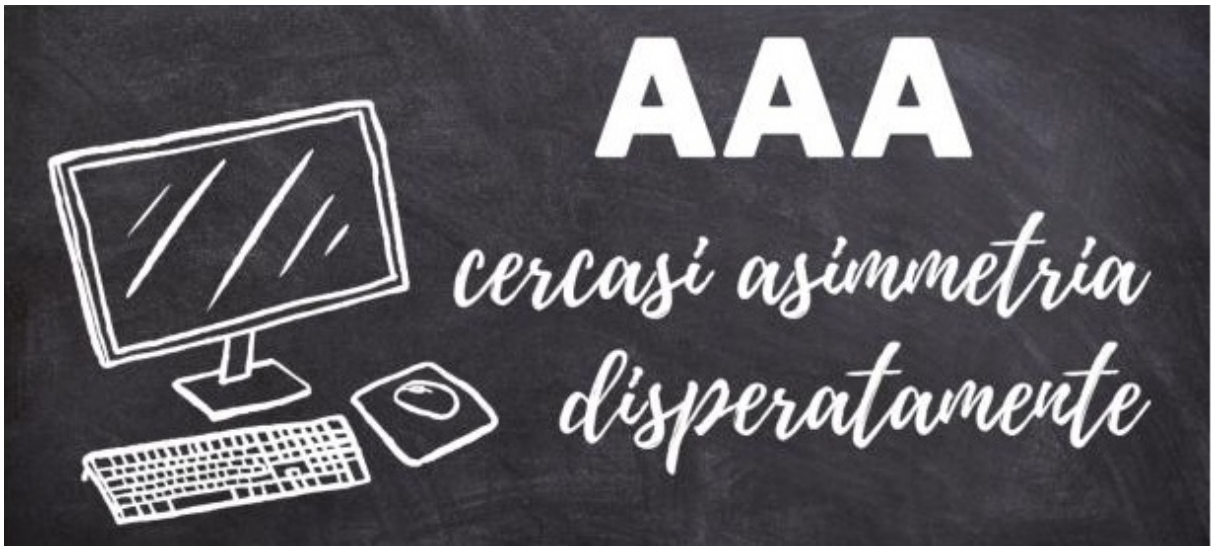
LATERAL NEWS — LATERALCODE

AAA: cercasi asimmetria disperatamente

13 giugno 2023



Ci stiamo prendendo gusto e anche questa volta, come nella precedente, iniziamo con una domanda (in fondo O. Wilde diceva che non esistono domande imbarazzanti ma a volte lo sono le risposte): girereste mai con un mazzo di chiavi, per es. quelle di casa, con appesa una targhetta recante l'indirizzo? Naturalmente non c'è bisogno di rispondere, però, in chiave diversa, facciamo ogni giorno qualcosa di simile, senza rendercene conto…

Prima un passo indietro

Quando ci connettiamo a un servizio online, sia esso un conto bancario, un'area riservata, un'applicazione, un profilo personale ecc., inseriamo le credenziali che ci sono state assegnate o che abbiamo creato durante la registrazione.

Che si usi un normale portale con user e password o qualunque altro sistema di sicurezza ulteriore e più evoluto, seguiamo sempre il processo identificato dalla famosa terna AAA.

La terna AAA (authentication, authorization, accounting) permette

- il controllo selettivo degli accessi alle risorse informatiche
- l’applicazione delle policy
- il controllo dell’utilizzo delle risorse

Il processo relativo alla prima A, l'autenticazione, fornisce un modo per identificare l'utente attraverso i vari metodi che conosciamo e le cui credenziali sono valide prima che venga

concesso l'accesso.

Senza una corretta validazione della prima A, teoricamente, tutto il resto dovrebbe essere impossibile (affermazione vera solo in condizione di ZeroSurface™ ma… transeat).

Ottenuta l'autenticazione, l'utente riceve l'autorizzazione a svolgere specifiche attività, in pratica una profilazione che dice "cosa può fare chi e quando".

La terza A, l'accounting, misura e traccia le "risorse" che un utente consuma durante l'accesso (ai fini del nostro discorso non è importante approfondire).

E ora un passo avanti

Bene: la terna AAA è implementata da tutti i servizi di sicurezza.

Se, da un lato, alcuni fra essi possono in parte differenziarsi nel modo in cui i singoli momenti svolgono la propria funzione, dall'altro è però una costante progettuale che ogni A si leghi in maniera diretta o indiretta a quella adiacente: ciò rappresenta una gravissima debolezza strutturale.

La prima A, l'autenticazione, è infatti sempre direttamente (bordo rete) o indirettamente (triangolazioni, serializzazioni o security hub) riconducibile al target che intende proteggere: per il cattivo di turno basterà seguire le briciole di Pollicino.

In una soluzione ZeroSurface™, invece, la prima "A" è sempre e completamente disarticolata, fisicamente e logicamente, rispetto alle successive: tale condizione rende impossibile ricondurre una "autenticazione" alla rispettiva "autorizzazione" di fatto impedendo tanto l'individuazione quanto l'accesso al target.

Secondo passo avanti

Questo tipo di struttura logica concretizza una seconda e determinante differenza rispetto a qualsiasi altra soluzione:

> *il target resta realmente e integralmente isolato, in qualunque condizione operativa, poiché non deve fornire né essere collegato in alcun modo ad alcun service destinato a risolvere la prima A.*

E ora il salto

Abbiamo detto "in qualunque condizione operativa".

Sì, perché la condizione di ZeroSurface™ è costante e viene mantenuta inalterata anche mentre la rete target sta erogando il servizio a n utenti, ("con n grande a piacere" si diceva a scuola): sappiamo che tutto ciò è controintuitivo ma è esattamente ciò che accade con un perimetro a superficie zero, supposto solo teorico fino a qualche tempo fa.

> *Detta in maniera diversa, la risoluzione di ciascuna delle tre A non costituisce mai una debolezza o una fragilità per le altre o per il sistema target nel suo insieme.*

Questa è l'**asimmetria funzionale** (che tra gli altri regala benefici mai visti prima) necessaria a concretizzare una condizione ZeroSurface™: senza di essa non può esistere "azzeramento totale di ogni superficie d'attacco, in qualunque status operativo".

Una soluzione di protezione perimetrale ZeroSurface™, quale è iceGate di LATERALCODE, agisce sempre e solo a layer 3 dello stack OSI: è per questo motivo che qualsiasi sistema target può essere portato a un tale livello di sicurezza, ivi compresi i sistemi di cyber security eventualmente già presenti che altrimenti, come detto, resteranno sempre esposti e raggiungibili.
