



EUTRONSEC

INFOSECURITY

L'OTP di nuova generazione



WebOTP



NOW A MEMBER OF Aladdin
EUTRONSEC



www.webotp.it

WebOTP

WebOTP è la soluzione dal prezzo assolutamente aggressivo che permette un'autenticazione sicura con un server WEB. La prerogativa principale di questo token è la possibilità di inviare le informazioni di autenticazione tramite la porta USB del computer senza dover installare nessun software e/o driver e senza la necessità di avere privilegi amministrativi. Al server WEB viene trasmessa una stringa di autenticazione, (che contiene l'identificativo dell'utente e un contatore incrementale), resa estremamente sicura da una doppia crittatura eseguita con algoritmo AES a 256 bit utilizzando prima la chiave privata dell'utente e poi quella del server WEB.

WebOTPtime

WebOTPtime utilizza la medesima tecnologia del prodotto base con l'aggiunta però del fattore tempo all'interno della stringa di autenticazione. Il token USB contiene infatti un timer che è sincronizzato con quello del WEB server. Una soluzione ancora più sicura, ideale anche per progetti di home banking.



Applicazioni pratiche

Controllo accesso ad aree riservate di siti Internet per:

- Gestione remota reti di vendita e Competence Center
- Vendita servizi a consumo su Internet
- Editoria on-line
- Gestione sicura servizi ASP
- Vendita software e servizi informatici su Internet
- Accesso sicuro a servizi finanziari e assicurativi
- Distribuzione controllata di informazioni
- Home Banking

WebOTP caratteristiche tecniche

Le caratteristiche principali di WebOTP che lo differenziano da un disposto OTP tradizionale sono:

Usabilità L'interazione richiesta all'utente è estremamente limitata. L'utente deve solamente inserire il dispositivo in un porta USB al momento dell'autenticazione.

Identificazione L'utente oltre ad essere autenticato è anche identificato. Non è quindi necessario richiedere un identificatore come un username all'utente prima dell'autenticazione.

Autenticazione sicura L'autenticazione si basa su 128 bit di informazione e sull'algoritmo AES a 256 bit. Non sono quindi possibili attacchi a forza bruta. In WebOTP l'autenticazione si basa sull'utilizzo dell'algoritmo di crittografia simmetrica AES 256 bit, contrapposto al comune algoritmo di hash utilizzato dai dispositivi OTP tradizionali. L'utilizzo di un algoritmo di crittografia simmetrica è possibile per WebOTP grazie alla connessione USB che non pone limiti di lunghezza nel codice di autenticazione. La crittografia simmetrica richiede di operare con un codice di autenticazione di almeno 128 bit, molti di più di quanto si possano rappresentare su un display con poche cifre di un OTP tradizionale.

I vantaggi dell'utilizzo di un algoritmo di crittografia simmetrica nella autenticazione OTP sono molteplici:

Identificazione Oltre ad autenticare l'utente, si può anche identificarlo. Si può quindi evitare all'utente di inserire un identificatore al momento dell'autenticazione. Per confronto, un OTP tradizionale richiede sempre di sapere a priori chi è l'utente.

Sicurezza Il codice di autenticazione contiene 128 bit di informazione di sicurezza. Per confronto, gli OTP tradizionali con display usano un massimo di 40 bit, spesso molti meno.

Velocità L'operazione di verifica dell'autenticazione è semplice e veloce. Il server di autenticazione avrà quindi un carico molto ridotto. Per confronto, un OTP tradizionale con funzione di hash richiede un processo per tentativi per indovinare i valori di tempo o eventi usati dal dispositivo.

Resistenza a Brute Force Attack Data l'elevata sicurezza dell'autenticazione, non è necessario bloccare l'accesso agli utenti dopo un certo numero di tentativi falliti. Per confronto, un OTP tradizionale è obbligato ad utilizzare tecniche di blocco per prevenire attacchi a forza bruta.

Resistenza a DoS Attack Il server di autenticazione è particolarmente resistente ad attacchi di tipo Denial Of Service, che prevedono la richiesta di un numero elevato di autenticazioni fittizie, nel tentativo di bloccare l'accesso agli utenti. L'operazione di verifica di autenticazione è molto veloce anche in caso di fallimento. Per confronto, in un OTP tradizionale basato su funzione di hash, il caso di autenticazione fallita è sempre il caso peggiore in termini di tempo di esecuzione.

Efficace gestione degli errori Nel caso l'autenticazione fallisca, è possibile conoscere la ragione esatta del fallimento. In particolare è possibile distinguere tra errori dovuti a dispositivi difettosi ed errori dovuti a tentativi di attacco. Ad esempio, è possibile continuare ad utilizzare un dispositivo time-based con batteria scarica come se fosse un dispositivo event-based. Per confronto, un OTP tradizionale con funzione di hash ha sempre solo un tipo di fallimento di autenticazione e non si possono desumere altre informazioni sull'errore.

Requisiti

- **Client** Windows 98 o superiore, Mac OSX, Linux 2.4 o superiore
- **Browser web** Internet Explorer, Netscape, Mozilla, Firefox, Camino
- **Server** Il software developer's kit permette l'integrazione con qualsiasi piattaforma di autenticazione Web
- **Sistema di autenticazione** OTP event based, opzionalmente challenge/response
- **Crittografia** AES 256 bit on board, SHA 256
- **Variabili di autenticazione** counter incrementale, timer per il token per WebOTPtime
- **PIN applicativo** implementabile
- **Batteria di alimentazione** WebOTPTime ha la batteria interna garantita per 5 anni di utilizzo
- **Driverless**



Opzioni di personalizzazione sono disponibili per quanto riguarda il colore del guscio, le iscrizioni sullo stesso e gli accessori abbinabili, dai portachiavi, al neck strap, dal cappuccio per il connettore USB, alla stampa di documentazione customizzata.