Peer Reviewed, Open Access, Free Online Journal
Published monthly : ISSN: 2308-832X
Issue 12(33); December 2015

Original Article: ANALISI DI STRADE DI PROTEZIONE DI DOMANDE DI CLIENTE

Citation
Grishin E.V., Irinina Ju.S. Analisi di strade di protezione di domande di cliente. *Italian Science Review*. 2015; 12(33). PP. 1-4.
Available at URL: http://www.ias-journal.org/archive/2015/december/Grishin.pdf

Authors
Evgeniy V. Grishin, Samara State Aerospace University named after academician S.P. Korolev (National Research University), Russia.
Julia S. Irinina, Samara State Aerospace University named after academician S.P. Korolev (National Research University), Russia.

Submitted: November 15, 2015; Accepted: November 29, 2015; Published: December 16, 2015

Il tema di questo lavoro è ispirato dalle condizioni della moderna industria dell'informazione. L'utente finale deve essere in grado di utilizzare la licenza, software di qualità, ma non pagare i soldi subito creato la frase "versione di prova", che include tutte le caratteristiche del software principale, e quindi sono limitati nel tempo. Alla fine della possibilità di utilizzare la versione di prova, l'utente decide se acquistare il software o meno. Particolare attenzione dovrebbe essere prestata alla questione della protezione dei dati dei prodotti sul metodo di consegna all'utente l'accesso alla versione completa del programma, come l'unicità dei permessi per diffondere software pirata.

Una versione di prova del software può essere protetto in molti modi diversi: limitando il numero di giri del programma di test, tempo limitato uso termine da una singola sessione, un insieme limitato di funzioni (versione fornisce funzioni per ottimizzare il processo di lavorare con il prodotto software), etc. In questo documento, l'attenzione è focalizzata su un tale metodo come una limitazione del numero di versione di prova lanci del software.

Si consideri la classificazione dei metodi di protezione:

- L'uso della rete;
- uso di hardware aggiuntivo.

Secondo il primo aspetto dei metodi possono essere suddivisi in locale (effettuata senza l'uso della rete) e remoto (uso della rete).

In base alla seconda caratteristica - in programma sul particolare hardware e software e hardware. Software protegge locali

Il tipo più comune di protezione è la protezione del programma locale.

Questo metodo ha i seguenti vantaggi:

- La facilità di sviluppo;
- sostegno facile;
- La relativa economicità.

Ma ha un grave inconveniente, ossia:

- L'inaffidabilità.

Con questo metodo, la questione principale è come convalidare le credenziali dell'utente.

Ci sono diverse opzioni:

- gli account utente;
- Usando il test.

Nel primo caso, il programma non è protetto quando le credenziali di compromesso di almeno un utente

legittimo. Abbastanza per mettere una chiave in Internet, e chiunque può utilizzare il software illegalmente.

Nel secondo caso, l'account viene controllato una funzione speciale, che è spesso dipende dalle costanti definite nel sistema (gli identificatori della scheda madre, CPU, ecc). Per attaccare questo tipo di programma crea generatore di chiavi (keygen), che viene calcolato chiave sulla vostra macchina.

E 'possibile fare senza l'uso di qualsiasi account. Ad esempio, memorizzare il numero di avviamenti del programma in un file speciale nei nomi dei file nel Registro di sistema, etc. Si può venire con un metodo molto sofisticato, ma questi metodi sono anche inaffidabili. Facile da trovare che cambia all'avvio del programma e ripristinare lo stato originale del programma.

Protezione locale Hardware

Protezione hardware è un dispositivo elettronico con la funzione di eseguire limitazioni.

Esso presenta i seguenti vantaggi:

- affidabilità.

Svantaggi:

- Il costo elevato;
- L'ambito ristretto di applicabilità.

Ad esempio, tale protezione sono i telefoni usa e getta che dopo un certo numero di lanci smettono di funzionare.

Attaccare tale protezione è estremamente difficile. Dovete fare un hardware ingegneria inversa (engineerng inversa), e questo è un complesso e costoso il funzionamento, che è solo in grado di eseguire specialisti altamente qualificati.

L'hardware e il software per proteggere il locale

Software e hardware di protezione è un software complesso e dispositivi elettronici. Il programma utilizza un dispositivo elettronico per la memorizzazione sicura o utilizzare alcune delle funzioni hardware.

Questo metodo ha i seguenti vantaggi e svantaggi:

- affidabilità relativa;
- Il costo medio di sviluppo e manutenzione.

Ci sono diversi tipi di attacchi a tale protezione:

- il reverse engineering (engineerng inversa) del programma (codice macchina);
- contraffazione del dispositivo elettronico;
- chiave pubblica dalla rete;
- driver di scrittura per il dispositivo virtuale.

Tutti i metodi di protezione locale possono essere escluse impostando la macchina virtuale. Quando la protezione del software, anche quando il fallimento di trovare cambiamenti del sistema, una macchina virtuale può essere restituito a uno stato in cui il programma ha funzionato. Se il software e hardware di protezione, è possibile specificare i dispositivi del sistema di identificazione (se il programma viene utilizzato per elaboratore in modo univoco specifico).

Software di protezione remota

Questo tipo di protezione è basato sull'autenticazione client sul server. In generale, il client invia le credenziali del server, il server invia i dati al client per eseguire il programma.

Questo metodo ha i seguenti vantaggi:

- facilità di sviluppo;
- affidabilità relativa.

Svantaggi:

- la necessità di sostenere assistente;
- inaffidabilità relativa.

L'insicurezza è questo tipo di protezione può essere bypassato con l'ascolto di traffico tra client e server, e la costruzione di un server falso. Ma non ci sono strumenti software universale per fare questo automaticamente, in modo che richiede più competenze di programmazione, che è un elemento di affidabilità.

Hardware remoto e la protezione del software

Questo tipo di protezione unisce le caratteristiche di hardware e software, e protezione remota.

Egli è caratterizzata dai seguenti vantaggi:

- L'elevato grado di affidabilità;

Svantaggi:

- Il costo elevato;
- La grande complessità della costruzione di sistemi di sicurezza.

L'uso di questo metodo di costruzione dei sistemi di protezione in grado di permettersi i statali, grandi aziende o banche a causa del fatto che gli attacchi contro la loro applicazione possono avere conseguenze disastrose per loro. Gli alti costi per la costruzione del sistema di protezione pienamente giustificati i rischi potenziali di perdita.

Esempio

Gli autori di un programma, il programma è un esempio di sicurezza a distanza ed è il seguente. A causa dell'ingombro esempio, codice di causa è insignificante.

Il server memorizza la base di utenti con il numero di corse consentiti. Programma protetto è una DLL, che mostra un messaggio all'utente e chiude dopo la pressatura.

Riassumendo, va detto che questo lavoro è stata valutata da una varietà di modi e metodi di protezione delle applicazioni client. Tutti hanno i loro vantaggi e svantaggi. Nel costruire il proprio sistema di sicurezza per analizzare i potenziali perdite dalla sua pausa, e poi scegliere il metodo migliore per una determinata situazione. Devi sempre tenere a mente che si può costruire un sistema che non può rompere, ma il suo valore non è paragonabile con la possibile perdita della sua rottura. È di trovare la soluzione ottimale in ogni situazione individuale, e ci sono molti modi per risolvere il problema della protezione di applicazioni client.

References:

1. Kasperski K. 2004. Technique protect CDs against copying. SPb, Publisher CVS Petersburg. 458 p.
2. Kasperski K. 2001. Technique network attacks. Moscow, Publishing House "Solomon-R". 400 p.

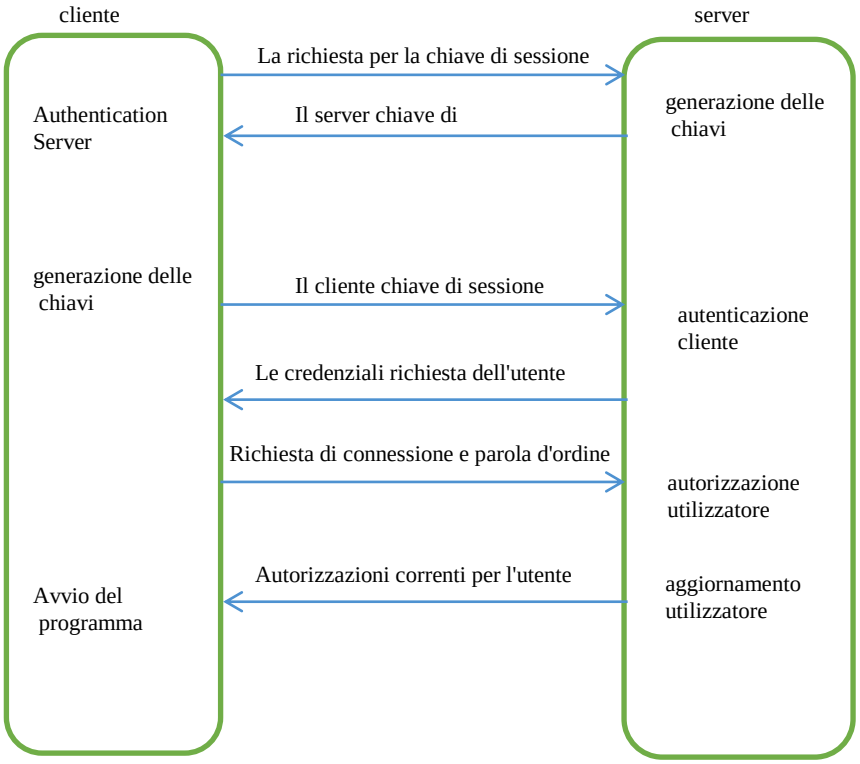

Figura 1. Lo schema di programmi di protezione