Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

Progetto *SPACE*

Obiettivo

Il presente breve documento ha lo scopo di presentare la soluzione *Hacking Team / Space* opportunamente personalizzata e disegnata per soddisfare appieno le esigenze di RAS.

La personalizzazione di tale software è realizzata sulla base di alcune assunzioni fondamentali illustrate di seguito. La loro conferma da parte di RAS rappresenta una condizione necessaria e sufficiente all'inizio dei lavori di customizzazione.

Finalità del software

Il software SPACE è realizzato per effettuare il censimento di macchine che accedono a determinate risorse in rete; nel caso specifico, il prodotto sarà customizzato per essere applicato al presidio degli accessi all'applicazione WEB utilizzate dalle agenzie RAS.

Il software permetterà di ottenere informazioni sulla macchina che accede all'applicazione e sull'utente di sistema che effettua tale operazione. Tali informazioni potranno poi essere utilizzate dalla logica applicativa per catalogare le macchine e gli utenti che accedono al servizio WEB (es: associazione fra un utente dell'applicazione e un determinato client, censimento dei sistemi utilizzati, rilevazione di nuovi client non forniti da RAS, etc.). Questi dati potranno inoltre essere usati dall'applicazione per inibire l'accesso al servizio, in base a

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

determinate politiche definibili dal Cliente, in aggiunta ai dati discriminanti già utilizzati[1] (username e password per l'applicazione).

Space quindi consentirà di far pervenire le informazioni concordate al sistema di autenticazione ed autorizzazione dell'applicativo; saranno poi le politiche decise da RAS ed implementate nella procedura applicativa a discernere cosa fare, cosa inibire e a fronte di quali informazioni.

Tecnologie utilizzate

La tecnologia alla base del prodotto è *ActiveX*. Tale tecnologia è stata scelta in relazione ai vincoli tecnologici sui client imposti dall'applicazione (sistema operativo di tipo Microsoft Windows, utilizzo di Internet Explorer, configurazione ad hoc delle *Security Zone* del browser, etc.). L'ActiveX contenente il software potrà essere richiesto ed istanziato all'interno di una delle pagine HTML coinvolte nel processo di logon all'applicazione.

Dati di sistema

Il personale di Hacking Team ha selezionato, in base alle esigenze espresse da RAS, una serie di elementi discriminanti di una macchina o di un utente:

- che non siano facilmente modificabili (accidentalmente o con finalità di sovversione del sistema).
- che offrano sufficiente entropia per identificare in maniera univoca una determinata piattaforma client o un determinato utente di sistema.
- che non rendano facile l'impersonificazione di un determinato utente o piattaforma (difficilmente reperibili a meno di non poter accedere direttamente alla macchina).

[1] Il software in questione non è realizzato per effettuare l'identificazione di un determinato utente o postazione, ma solo per la loro verifica. Lo username applicativo dovrà in ogni caso rimanere l'unico dato discriminante per l'identificazione delle utenze.

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

I parametri identificati sono elencati nella seguente tabella, specificando per ogni piattaforma di riferimento quando questi sono reperibili (SI) e quando invece sono irreperibili o non presenti (NO).

	Windows 2000/XP/NT/2003	**Windows 95/98/Me**
Utente/Dominio	SI	NO
Nome Macchina	SI	SI
MAC Address	SI	SI
MBR Signature	SI	NO
SPACE Timestamp	SI	SI

Il software SPACE può inviare i dati raccolti in due forme diverse (nel rispetto dei termini di privacy):

- **Dato completo:** permette di ottenere informazioni specifiche sulla macchina o sull'utente (es: versione del sistema operativo, username di sistema, etc.)
- **Hash:** è un derivato del dato completo e non consente di ottenere informazioni sul dato originale. Ad esempio non rende possibile identificare con esattezza un determinato sistema operativo, ma solo distinguere due sistemi operativi differenti.

Canale di comunicazione

Per garantire l'integrità e la confidenzialità dei dati inviati è necessario affidarsi ad un sistema di cifratura/firma. Sono possibili due tipi diversi di approccio in tal senso:

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

- Utilizzo della cifratura del canale di comunicazione a livello di trasporto (SSL). Tale canale viene già utilizzato dall'applicazione e non richiederebbe quindi ulteriori modifiche a livello di server.
- Utilizzo di algoritmi di cifratura/firma (es: RSA/DSA) implementati a livello applicativo. Questo tipo di approccio rende necessaria la scrittura di codice ad hoc lato-server per la corretta interpretazione dei dati ricevuti. L'utilizzo di questa soluzione è consigliato unicamente se l'utilizzo del canale SSL non è praticabile per forti vincoli tecnologici/implementativi dell'applicazione o dell'infrastruttura.