

# Una minaccia dovuta all'uso dell'SNMP su WLAN

Gianluigi Me, gianluigi@wi-fiforum.com

Traduzione a cura di Paolo Spagnoletti

## Introduzione

Gli attacchi al protocollo WEP compromettono la confidenzialità delle comunicazioni, minacciate dalla possibile intercettazione di comunicazioni private su wireless LAN 802.11b. Tuttavia, esiste una minaccia ancor più pericolosa nascosta nella rottura delle comunicazioni WEP: infatti, alcuni Access Point possono essere gestiti, mediante applicativi proprietari basati sul protocollo SNMP, attraverso il collegamento wireless. L'esecuzione di tali operazioni può rappresentare una pericolosa vulnerabilità per l'intera wireless LAN, poiché l'intercettatore potrebbe entrare a conoscenza delle password per accedere in lettura/scrittura sull'Access Point. In altri termini, potrebbe condividere gli stessi privilegi dell'amministratore della WLAN e gestirla in maniera non autorizzata.

## Un modello dell'SNMP

Il Simple Network Management Protocol (SNMP) utilizza un paradigma manager/Management Information Base (MIB)/agent, come mostra la Figura 1

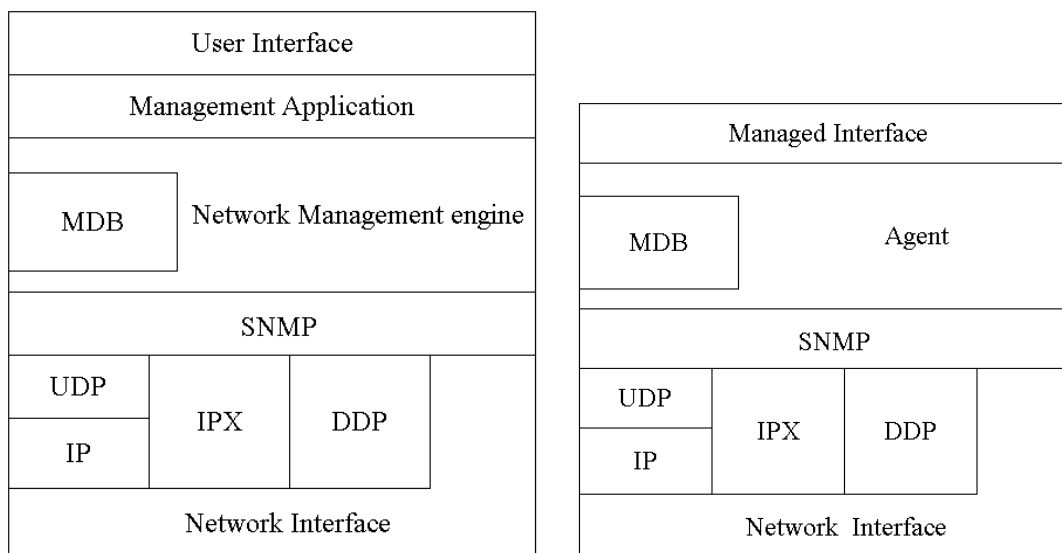


Figura 1

Questo paradigma si basa su un manager che richiede informazioni ad un agent in un determinato formato di codifica detto MIB. L'agent invocato processa la richiesta, recupera l'informazione e la invia al manager, se disponibile. In caso contrario invia la causa dell'indisponibilità. Secondo il paradigma manager/MIB/agent, l'interfaccia utente si limita a svolgere soltanto il ruolo di strato di presentazione ed è progettata utilizzando accorgimenti grafici con il solo scopo di aumentare l'usabilità delle funzioni di recupero e consultazione dei dati. Le applicazioni di gestione, inoltre, offrono uno strumento per la formattazione dei dati recuperati e forniscono uno strato aggiuntivo composto di funzioni di controllo della Network Management Station (NMS).

### ***Rendere sicuri gli Agent e le NMS***

La versione 1 del protocollo SNMP offre strumenti deboli per rendere sicuri i processi di comunicazione tra l'NMS e l'agent. La sola forma di autenticazione prevista dall'SNMP consiste nell'uso di un *Community Name*, mentre meccanismi più robusti per rafforzare la sicurezza possono essere forniti da software di terze parti.

Più dettagliatamente, la sola protezione offerta dal *Community Name* contro gli accessi non autorizzati consiste in una stringa di caratteri contenuta nell'header dell'SNMP. Tale stringa rappresenta un valore che, se riconosciuto dall'agent, autorizza l'NMS ad eseguire l'attività richiesta con il messaggio SNMP. Il comando *Get Community Name* consente all'agent la lettura delle variabili MIB, mentre il comando *Set Community Name* autorizza l'agent alla scrittura degli oggetti MIB di tipo read-writable. Alcuni testi identificano tali nomi come Read and Write Community Name.

Molti produttori preconfigurano come "public" i *Community Name* dei propri agent ed NMS. Il primo passo per l'amministrazione via SNMP consiste generalmente, perciò, nella modifica di tale impostazione al fine di evitare che un qualsiasi NMS possa modificare le informazioni degli agent.

### ***La minaccia dell'SNMP in ambiente WLAN***

L'amministrazione di un Access Point mediante un collegamento wireless può avere implicazioni realmente pericolose: infatti, considerati i diversi attacchi al protocollo WEP effettuabili attraverso strumenti facilmente reperibili su Internet, è opportuno considerare un collegamento wireless 802.11b assolutamente insicuro. Ciò dovrebbe essere già sufficiente per convincersi sull'inopportunità di qualsiasi

operazione di tipo confidenziale attraverso un tale tipo di collegamento. Di seguito verrà quindi mostrato quale sia il rischio legato all'utilizzo dell'amministrazione di un Access Point via SNMP wireless.

Consideriamo perciò un Access Point con indirizzo fisso pari a 153.69.254.250 ed una stazione con indirizzo IP 153.69.254.53 ed ipotizziamo che l'amministratore utilizzi l'applicativo di gestione proprietario fornito sul CD-ROM associato all'apparato wireless. Come descritto in precedenza, il *Community Name* assumerà il suo valore di default: `public`. Innanzi tutto l'amministratore modificherà questo valore attribuendogli un nuovo nome che tenga conto delle regole per la costruzione di una password robusta. In questo articolo, per fini di semplicità e chiarezza (e solo per questo!), ipotizzerò che il valore scelto sia `rw_pwd`. A questo punto l'amministratore potrà utilizzare tale stringa per l'accesso (esattamente come con una password) all'applicativo proprietario per la gestione dal lato client, ovvero per l'accesso diretto all'Access Point utilizzando il protocollo SNMP. In tal modo il *Community Name* consentirà all'amministratore (e a chiunque ne sia a conoscenza!) di accedere in lettura/scrittura ai parametri di configurazione dell'Access Point. La figura 2 mostra ciò che è visibile ad un intercettatore che riesce nel suo attacco al WEP e che è in ascolto sulla stessa wireless LAN.

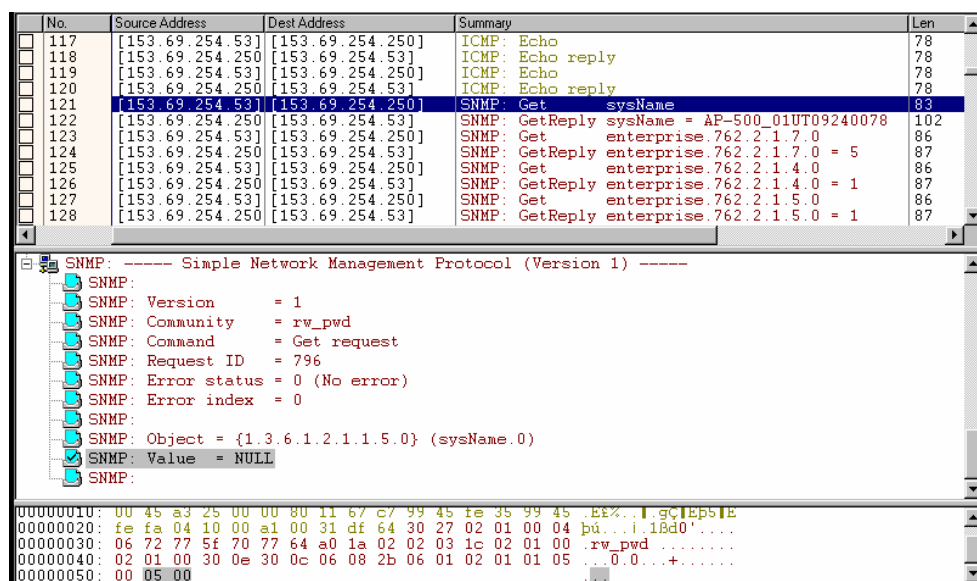


Figura 2

La figura mostra che il *Community Name* dell'SNMP, posto a `rw_pwd`, è stato inviato in chiaro (su WEP) dalla stazione di gestione all'Access Point e tale valore, come detto in precedenza, corrisponde alla password che consente l'accesso all'applicazione. In questo modo l'intercettatore condivide con l'amministratore la possibilità di gestione dell'Access Point conoscendone la password di lettura/scrittura.

Qual è, allora, l'utilità di utilizzare un *Community Name* robusto se verrà poi inviato in chiaro sul canale WEP? L'utilità è nulla, fatto salvo il caso in cui l'attacco al WEP non abbia successo, ove eviterebbe almeno attacchi (forza bruta, dizionario) alle password dell'applicativo di gestione.

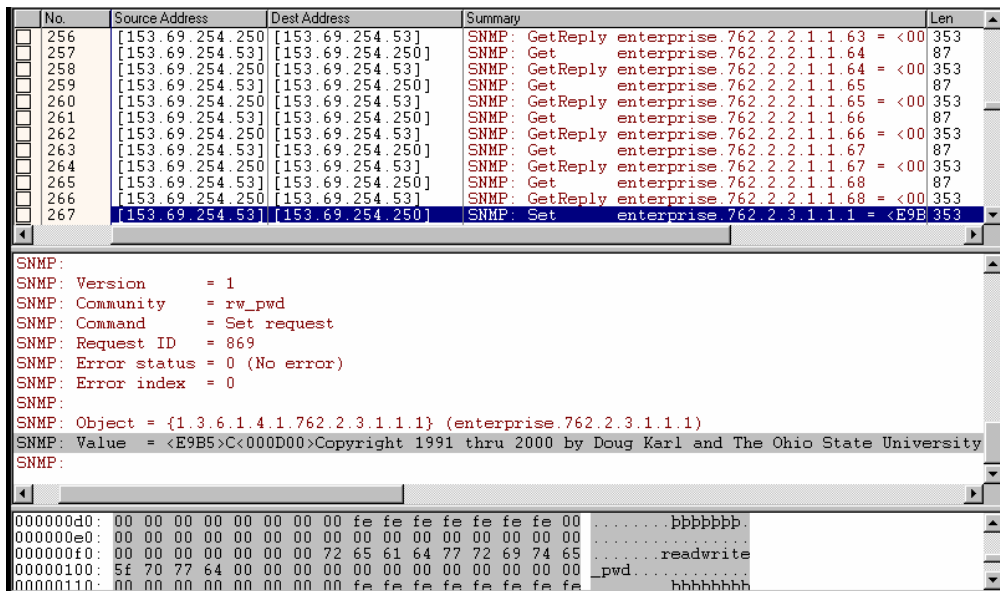


Figura 3

A questo punto l'hacker, se decidesse di manifestare la propria presenza, potrebbe modificare le chiavi WEP ed il *Community Name* introducendo valori a sua scelta. Potrebbe, ad esempio, attribuire al *Community Name* il valore `readwrite_pwd`. Tale operazione verrebbe effettuata, analogamente alla precedente, in chiaro su WEP, come mostrato in figura 3. Così facendo, se il legittimo amministratore non fosse in grado di attaccare a sua volta l'hacker con tecniche analoghe, perderebbe la possibilità di accedere logicamente al proprio Access Point (figura 4), pur mantenendo le responsabilità sullo stesso! In questa situazione l'unica contromisura consisterebbe, perciò, nell'accesso fisico all'Access Point per re-inizializzarlo con i valori di default del costruttore.

No.	Source Address	Dest Address	Summary	Len
430	00601D2074B5	Broadcast	ARP: C PA=[153.69.254.100] PRO=IP	60
431	00022D20980E	00022D3270E3	SNAP: ID=00601D Type=0001	80
432	00601D2074B5	Broadcast	ARP: C PA=[153.69.254.100] PRO=IP	60
433	[153.69.254.53]	[153.69.254.250]	SNMP: Get sysName	90
434	[153.69.254.250]	[153.69.254.53]	SNMP: GetReply sysName = AP-500_01UT09240078	109
435	[153.69.254.53]	[153.69.254.250]	SNMP: Get enterprise.762.2.1.7.0	93
436	153.69.254.250	153.69.254.53	SNMP: GetReply enterprise.762.2.1.7.0 = 5	94
437	[153.69.254.53]	[153.69.254.250]	SNMP: Get enterprise.762.2.1.4.0	93
438	[153.69.254.250]	[153.69.254.53]	SNMP: GetReply enterprise.762.2.1.4.0 = 1	94
439	[153.69.254.53]	[153.69.254.250]	SNMP: Get enterprise.762.2.1.5.0	93
440	[153.69.254.250]	[153.69.254.53]	SNMP: GetReply enterprise.762.2.1.5.0 = 1	94
441	[153.69.254.53]	[153.69.254.250]	SNMP: Set enterprise.762.2.1.9.0 = 1	94

```

UDP:
SNMP: ----- Simple Network Management Protocol (Version 1) -----
SNMP:
SNMP: Version      = 1
SNMP: Community    = readwrite_pwd
SNMP: Command       = Get response
SNMP: Request ID   = 941
SNMP: Error status = 0 (No error)
SNMP: Error index  = 0
SNMP:
SNMP: Object = {1.3.6.1.4.1.762.2.1.7.0} (enterprise.762.2.1.7.0)
SNMP: Value  = 5
SNMP:
00000000: 00 02 2d 32 70 e3 00 60 1d 20 74 b5 08 00 45 00  .-2pã. . tp..E
00000010: 00 50 00 04 40 00 40 11 0a de 99 45 fe fa 99 45  .P.@. .b|EpuIE
00000020: fe 35 00 a1 04 11 00 3c 49 45 30 32 02 01 00 04  b5.i. .<IE02...
00000030: 0d 72 65 61 64 77 72 69 74 65 5f 70 77 64 a2 1e  .readwrite_pwd.
00000040: 02 02 03 ad 02 01 00 02 01 00 30 12 30 10 06 0b  -  n n

```

Figura 4

L'ultima considerazione riguarda l'aumento del rischio per la rete nel caso in cui l'hacker non avesse intenzione di rendersi visibile. Nel precedente caso l'attività fraudolenta era immediatamente percepibile dall'amministratore, che avrebbe potuto quindi adottare adeguate contromisure per evitare danni peggiori: in questo caso, invece, l'hacker avrebbe accesso a tutte le informazioni di gestione all'insaputa di tutti e potrebbe sfruttarle in tempi e modi a sua scelta, non consentendo all'amministratore alcuna contromossa.