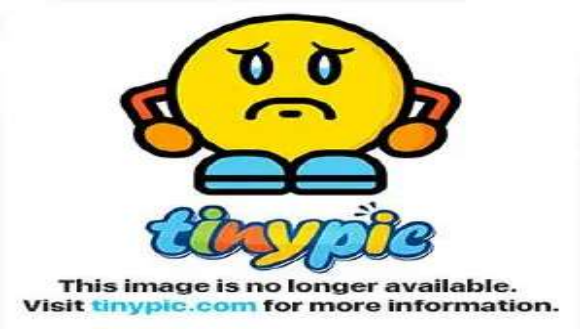
Alice AGPF: l'algoritmo!

June 2, 2010 whitehatcrew Go to comments Leave a comment



Ricordiamo che l'accesso abusivo ad un sistema informatico o telematico è un reato perseguibile a termine di legge (art. 615-ter c.p.). Inoltre ricordiamo che la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici o telematici è un reato penale perseguibile secondo la legge 615-quater c.p.

Pertanto l'utilizzo di quanto esposto è da riferirsi a un test di sicurezza sulla propria rete o su una rete la quale il proprietario abbia espressamente dato il libero consenso al fine di giudicarne la sicurezza e porre rimedio ad eventuali vulnerabilità.

Gli Autori di questo Blog non potranno essere ritenuti responsabili di eventuali violazioni derivanti da un uso proprio o improprio delle tecniche esposte in questo articolo aventi uno scopo prettamente informativo e didattico. Qualsiasi implementazione dell'algoritmo di seguito riportato è illegale secondo gli articoli sopracitati.

Premessa

Dopo il precedente articolo abbiamo deciso di espandere le nostre ricerche verso altri tipi di router. Quello che andrete a leggere fra poco tratta di un modello molto diffuso di router rilasciati da Telecom Italia (Alice).

Come al solito ribadiamo che il nostro obiettivo è quello di tutelare l'utente che utilizza questi dispositivi per navigare in internet. Per le notazioni di base rimandiamo alla pubblicazione precedente. Inoltre si avvisa che l'articolo risulta essere parzialmente incompleto. Non si escludo aggiornamenti successivi alla pubblicazione.

Con il precedente ci siamo accorti conto che alcuni individui con obiettivi molto lontani dai nostri hanno sfruttato il nostro lavoro per scopi prettamente *personali* e *lucrativi*. Teniamo a precisare, per chi non l'avesse notato, che le nostre ricerche sono rilasciate sotto licenza Creative Commons 3.0, ciò significa che i nostri articoli non possono essere utilizzati per fini commerciali e chi vorrebbe riportarli in blog, riviste ecc., è tenuto ad attribuirne la paternità dell'opera. Vi consigliamo di prendere visione di tutte le clausole della licensa.

Nonostante la scoperta di questo algoritmo sia avvenuta alcuni mesi fà abbiamo preferito pubblicare solo adesso la *full disclosure* per un motivo molto importate secondo la nostra etica. La tecnica che vedrete esposta più avanti ci permette di risalire alla WPA di default conoscendo solo SSID e MAC Address della rete in considerazione. La cosa più grave però fino a qualche mese fà era l'impossibilità di cambiare la chiave preassegnata, ciò rappresentava effettivamente un grave rischio per moltissimi utenti, considerando che Alice copre circa il 70% dei servizi per la fornitura dell'ADSL nel nostro Paese. Ciò significa che non ci si poteva difendere facilemte da questa grave vulnerabilità. Per fortuna però gli ingegneri di Telecom sono riusciti a progettare un nuovo firmware, per la precisione l'**AGPF 4.5.0sx**, che dà la possibilità all'utente di poter cambiare (finalmente) la chiave WPA di default preassegnata. Alla fine di questo articolo trovere alcuni utili consigli per aumentare la sicurezza nelle vostre reti, qualora avreste un router come quello descritto in questo articolo.

Introduzione

Tra gli operatori ADSL italiani, Telecom Italia si distingue per l'enorme varietà degli apparati hardware che fornisce ai propri clienti, con nomi commerciali spesso così simili tra loro che

RSS feed

Meta
- Register
- Log in
- Entries feed
- Comments feed
- WordPress.com

Blog Stats
- 259,091 hits

neanche si distinguono. Inoltre altrettanto spesso a oggetti esteticamente identici

è relativo al router commercialmente denominato *"PIRELLI Alice Gate VoIP 2 Plus Wi-Fi"* in dotazione con l'abbonamento *"Alice tutto incluso"* e con firmware **AGPF**, di seguito lo chiameremo per comodità *router AGPF*.

Come è evidente, il primo problema da considerare è capire se dal semplice SSID (nome) della rete è possibile riconoscere un router con firmware AGPF, questo sarà il primo problema che andremo ad affrontare. Successivamente, ci occuperemo dell'algoritmo che viene usato dai router AGPF per calcolare la chiave WPA di default.

Riconoscere un router AGPF

Le reti WiFi di Alice vengono contraddistinte dalle altre per l'SSID avente la forma: "**Alice-xxxxxxxx**", quindi costiuite da un prefisso *Alice-* seguito da una serie numerica di 8 cifre. La parte numerica è necessaria a rendere univoci gli SSID tra tutti i clienti gestiti dall'ISP. Inoltre attraverso confronti e ricerche abbiamo notato che, come avveniva similmente per gli HAG Fastweb, le prime (2-3) cifre individuano la serie del router. La serie è un parametro cruciale: ci dà informazioni sul di tipo di router (quindi il firmware che monta), e aiuta nella determinazione del numero seriale del router. A differenza del caso Fastweb Pirelli, in cui la parte variabile dell'SSID è l'unica informazione necessaria, nei router Telecom sono necessari dei codici non direttamente intercettabili via etere dal wardriver, ma tuttavia spesso calcolabili algoritmicamente conoscendo l'SSID della rete e il MAC della scheda WiFi interna al router: si tratta di un seriale anch'esso univoco associato al router. Il seriale (SN) di un router AGPF è formato da una parte variante per serie, un simbolo fisso e una parte variante per singolo apparato: ***12345X1234567***. Le cinque cifre prima della *X* variano per serie di router, iniziano per ***6790*** o ***6910*** (almeno dai dati fino adesso analizzati). La *X* è un simbolo costante, e separa le due parti del SN. Le altre cifre cambiano da router a router secondo un particolare meccanismo che abbiamo dedotto, li abbiamo denominati ***numeri magici*** (altri modelli di router usano un formato analogo per i seriali ma non è chiaro se rispettano lo stesso meccanismo di generazione).Verificare se un router è AGPF (o di un altro tipo, AGIF, da cui non è a priori possibile distinguerlo) richiede l'emulazione dell'algoritmo usato dal router per generare l'SSID a partire dal MAC WiFi e verificare la coincidenza del risultato calcolato con quello che effettivamente si riscontra dal tool di sniffing. Siccome nè l'SSID nè il MAC sono parametri variabili nelle reti Alice, l'esito positivo della verifica dirà al 100% se si tratta di un modello AGPF (o AGIF).

L'algoritmo di questa parte, estratto e commentato dal reverse del firmware, è il seguente:

```
.text:004C70F0
la $t9, atomac // Ottiene il puntatore al mac e lo mette in v0
lbu $v1, 2($v0) // Prende il 3° byte
move $s0, $v0 // Copia il putnatore perchè gli serve il registro
lbu $v0, 3($v0) // Carica il 4° byte
lbu $a0, 4($s0) // Carica il 5°
andi $v1, 0xF // Prende solo un nibble dal 3° byte
lbu $a1, 5($s0) // Carica il 6° ed ultimo byte
sll $v0, 16
sll $v1, 24
or $v1, $v0
sll $a0, 8
or $v1, $a0
lui $v0, 0x55E6 // Questa non serve a niente
or $v1, $a1 // Le funzioni fino quì servono a prendere una parte del mac e conve
```

Come al solito chiariamo tutto con un semplice esempio: supponiamo che **00238e5e5f68** sia il nostro mac.
L'algoritmo fino a questo punto punto avrà in *v1* il valore *e5e5f68* che, come si può notare, è una parte del mac stesso.

```
li $v0, 0x55E63B89 // Carica il valore in v0
mult $v1, $v0 // Lo moltiplica per la parte del mac
li $a3, 0x5F5E100 /// Carica il valore in a3
mfhi $v0 // solita storia della hiword dopo la moltiplicazione
srl $v0, 25 // Shift della hiword
mul $t0, $v0, $a3 // moltiplica il valore 0x5F5E100 per quello ottenuto dal prece
subu $a3, $v1, $t0 // sottrae alla parte del mac il nuovo valore ottentuo dalla p
```

Adesso, con quest'altra parte dell'algoritmo avremo finalmente in *a3* il nostro *ssid* generato. Quindi se dal mac non ricavo un ssid uguale a quello noto deduco che non sia AGPF/AGIF. Come si vede, è un semplice algoritmo basato su operazioni logico-aritmetiche, banalmente implementabile da chiunque abbia minime conoscenze di programmazione.

Seriali, Serie e Numeri Magici

Come detto in precedenza, ogni router oltre ad avere un proprio firmware ha anche una serie, corrispondente alla prima parte del seriale (SN) riportato su ogni router. Da un'accurata analisi del tutto statistica siamo riusciti a trarre alcune conclusioni in merito solo per alcune serie. Siamo però convinti che deve esistere un algoritmo universale in grado di individuarli tutti. Non essendo il nostro interese di natura statistica abbiamo limitato le nostre ricerche sui dati a cui abbiamo avuto la possibilità di analizzare.

Riprendendo il discorso dei *numeri magici* siamo riusciti, tramite confronti tra due o più seriali, ad individuare dei valori costanti che si ripeteno. Il seriale è calcolabile mediante un'equazione tutto sommato abbastanza semplice conoscendo solamente la parte numerica dell'SSID della rete. E' stato infatti scoperto che la relazione che sussiste tra SN e SSID è di aritmetica modulare: esistono due costanti, che definiremo con **k** e **Q**, dipendenti dalla serie del router, tale che **SSID=k*SN+Q** (dove con SN indicheremo la seconda parte del seriale, quella dopo la X, la prima parte è fissa per ogni serie), da questa formula ricaviamo la formula finale **SN=(SSID-Q)/k**. Naturalmente un'equazione e due incognite non ammette un'unica soluzione, per questo abbiamo impostant un sistema che prende in considerazione i dati di due router della stessa serie.

Supponiamo ad esempio di avere questi due dati:

1. SSID: Alice-**96154825** SN: 69102X**0010598**
2. SSID: Alice-**96140044** SN: 69102X**0009461**

Dalla precedente formula impostiamo un sistema lineare di due equazioni in due incognite:

$$\begin{cases} SN1 = (SSID1 - Q)/k \\ SN2 = (SSID2 - Q)/k \end{cases}$$

ottenendo così le seguenti soluzioni:

$$Q = \frac{(SSID2 \cdot SN1) - (SSID1 \cdot SN2)}{(SN1 - SN2)} \qquad k = \frac{(SSID1 - SSID2)}{(SN1 - SN2)}$$

Da questa soluzione ricaviamo che, per i dati di esempio, otteniamo **Q=96017051** e **k=13**. Una volta ottenuti questi "numeri magici" siamo ingrado di calcolare il SN completo di qualsiasi router facente parte della stessa serie, conoscendo solamente l'SSID. Le serie fino adesso indviduate sono:

- **Alice-96xxxxxx Serie: 69102X******* k=13 Q=96017051**
- **Alice-93xxxxxx Serie: 69101X******* k=13 Q=92398366**
- **Alice-56xxxxxx Serie: 67902X******* k=13 Q=54808800**
- **Alice-55xxxxxx Serie: 67904X******* k=8 Q=55164449**
- **Alice-54xxxxxx Serie: 67903X******* k=8 Q=52420689**
- **Alice-48xxxxxx Serie: 67903X******* k=8 Q=47896103**
- **Alice-46xxxxxx Serie: 67902X******* k=13 Q=39015145**

Analisi dell'algoritmo di generazione WPA

La generazione della WPA dipende sostanzialmente da tre parametri: due variabili e uno costante, quest'ultimo utilizzato in una procedura analoga descritta nell'algoritmo Pirelli Fastweb: calcolo dell'hash con input MAC del router e SN del router. Come noto, il MAC è ottenibile mediante i più comuni strumenti di sniffing WiFi, è un dato appena un pò meno plateale del SSID. Ammettendo tuttavia di aver reperito le tabelle note, e di saper quindi calcolare il SN e conoscendo il MAC, l'operazione di generazione è molto simile a quella descritta in precedenza. Si usa, stavolta, un algoritmo di hashing diverso dall'MD5, l'SHA256. In particolare, si inizializza un vettore di calcolo dell'SHA256, e si forniscono in sequenza i seguenti tre elementi:

- Mac Address delle scheda WiFi del router (considerato in byte)
- Seriale completo del router (considerato come stringa)
- Sequenza speciale (costante, in byte)

Procedura

1. Si inizializza una SHA256
2. Si aggiorna la SHA con i 32 byte della sequenza speciale
3. Si aggiorna la SHA con il SN
4. Si aggiorna la SHA con i 6 byte del MAC
5. Si finalizza l'hash SHA di tutti questi dati
6. Si usa una tabella di encoding speciale che a ciascun byte dell'hash fa corrispondere un altro simbolo
7. I primi 24 byte della trasformazione così ottenuta rappresentano la WPA

I punti dell'algoritmo dall'**1** al **5** equivalgono sostanzialmente ad effettuare l'ash utilizzando l'algoritmo SHA256 della concatenazione di *Hash=SHA256(MagicN+SN+MAC)*. Dove il primo e l'ultimo argomento devono essere trattati come sequenza di byte, mentre il serial viene inserito come "stringa".

Il codice speciale utilizzato nell'algoritmo e ricavato per ispezione nel disassemblato è il seguente:

```
unsigned char ALIS[32] = {
 0x64,0xC6,0xDD,0xE3,0xE5,0x79,0xB6,
 0xD9,0x86,0x96,0x8D,0x34,0x45,0xD2,
 0x3B,0x15,0xCA,0xAF,0x12,0x84,0x02,
 0xAC,0x56,0x00,0x05,0xCE,0x20,0x75,
 0x91,0x3F,0xDC,0xE8
};
```

Alla fine di quest'operazione otterremo un hash costituito da una sequenza di 32 byte (64 caratteri HEX).
A questo punto, è stata prevista nell'algoritmo alcune trasformazioni sui singoli byte memoryless

(ovvero, ciascun byte viene trasformato in modo indipendente dagli altri e secondo lo stesso identico algoritmo). Sarebbe possibile replicare in qualsiasi linguaggio il codice ASM MIPS (non si tratta di altro che di shift, trasformazioni aritmetiche, …) ma da un'attenta osservazione si è arrivati a costruire un vettore che contiene tutte le possibili combinazioni dalla conversione. Bisogna partire dal presupposto che ogni byte della sequenza dell'hash può assumere 16^2 (256) combinazioni possibili quindi da 0x00 a 0xFF o in decimale da 0 a 255. Il charset utilizzato in una generica WPA è costituito dalle cifre da 0 a 9, e da tutte le lettere dell'alfabeto in minuscolo. Replicando questa sequenza su un vettore a 256 elementi si ottiene lo spazio di varizione di tutti i byte. Ciò significa che ogni byte verrà convertito grazie a questo vettore in un carattere corrispondente. Tra poco vedremo un esempio che ci chiarirà le idee.
Questo è il vettore che andremo ad utilizzare:

```
unsigned char preInitCharset[] = {
'0','1','2','3','4','5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f', 'g',
'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z',
'4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j',
'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2', '3',
'8', '9', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n',
's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2', '3', '4', '5', '6', '7',
'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l','m', 'n', 'o', 'p', 'q', 'r', '
'w', 'x', 'y', 'z', '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b',
'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v',
'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f',
'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z',
'4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j',
'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2','3'
};
```

Ogni byte dell'hash ottenuto dall'algoritmo viene inizialmente convertito in decimale, questo numero può essere utilizzato come indice nel vettore appena descritto ottenendo man mano tutte le lettere o cifre che compongo la WPA. Quindi ad esempio CharSet[37] = '1', CharSet[19] = 'j', CharSet[200] = 'k', ecc..
Naturalmente questo non è l'unico modo per effettuare la conversione, ma è sicuramente molto semplice da implementare ed efficace nell'utilizzo.

Esempio pratico

Come al solito i dati che vedrete in seguito sono di pura fantasia avente solamente lo scopo di confermare il corretto procedimento dell'algoritmo.

Supponiamo di avere una rete WiFi Alice avente i seguenti dati:

- SSID: Alice-12345678
- MAC: 00:23:8E:01:02:03
- SN: 67902X0587411

Applicando l'algoritmo sopra spiegato otteniamo con questi dati un hash sha256 di questo tipo:
b1d5d0dc8f3a2132d7872641250f998d53e58824ecb9118e046a943239bf1220

Adesso considerando un byte per volta dobbiamo effettuare le conversioni per ottenere la WPA nella forma che conosciamo.

0xB1 = 177 –> 'x'
0xD5 = 213 –> 'x'
0xD0 = 208 –> 's'
0xDC = 220 –> '4'
0X8F = 143 –> 'z'
……..
ottenendo alla fine la seguente WPA: **xxs4zmxezr2t1f9xbds0k5hy**
Naturalmente per l'estrazione della WPA interessano solo i primi 24 byte dell'hash.

Coclusioni

Inizialmente il progetto di Alice Telecom Italia è stato studiato principalemente per scoraggiare ogni tentativo di bruteforce sulla chiave di crittazione della rete. Disporre di una WPA costituita da 24 simboli tra cifre e numeri scoraggia ogni vano tentativo di "indovinarla". Infatti se ci pensiamo le combinazioni possibili sono "appena" 36^24 un numero di inimmaginabile grandezza. Nonstante ciò, Telecom però ha pensato di disabilitare la modifica della chiave di default preassegnata per evitare magari che gli utenti mettessero chiavi meno sicure. Questo però rappresenta una lama a doppio taglio. E' vero che quella preassegnata è una chiave molto robusta, ma se si trova un modo (come quello appena descritto) di ricavare questa chiave è evidente che l'utente non può più difendersi da questa insicurezza.

Abbiamo già parlato nella premessa del modello successivo di AGPF (la variante sx), in cui apparentemente cambia il criterio di creazione dell'SSID e la WPA è configurabile, finalmente, dall'utente. finale Tuttavia l'algoritmo utilizzato è ugualmente reperibile operando attravero il reverse engineering. Ma rimane un problema fondamentale.
L'aggiornamento del nuovo firmware viene attuato attraverso la telegestione, in pratica, il router connesso ad internet si dovrebbe aggiornare in modo del tutto automatico. Questo è possibile verificarlo accedendo attravrso l'interfaccia di rete al router e controllando la sezione "Dettagli modem" dove sono riportate tutte le caratteristiche.
Il problema di fondo di cui acennavamo prima rimane sempre lo stesso. Quanti utenti cambieranno la chiave WPA di default? Quanti utenti vengono informati di questa possibilità?

Sperando di aver dato un contributo positivo alla sicurezza nelle reti da parte nostra vi

consigliamo sempre di cambiare la WPA di default in una totalmente random, complessa e non inferiore ai 24 caratteri. Qualora qualcuno si accertasse che la propria versione di firmware per il router in questione sia inferiore alla 4.5.0sx è possibile richiedere un aggiornamento contattando direttamente l'assistenza di Alice.

**** ***White Hats*** ****

Alice

agpf, agpf algoritmo, algoritmo alice, alice agpf, alice wpa, chiave default alice, full disclosure, pirelli alice, White Hat

Leave a comment Trackback Trackbacks (16) Comments (266)

????

June 3, 2010 at 6:16 pm Reply

Avete provato l'algoritmo ragazzi?
Di 4 ssid in mio possesso(serie 56xxxxxx e 96xxxxxx) non corrisponde neanche una chiave(e le wpa sono quelle di default!!!)…Mmha…

saxdax

June 3, 2010 at 6:44 pm Reply

Finalmente!!!
Sono due anni che avevo condiviso le idee base per arrivare a questo risultato e che aspettavo che qualcuno ci arrivasse.

Complimenti

P.S. manca qualcosina sui seriali, ma è già ottimo così

giubari

June 3, 2010 at 7:03 pm Reply

Grandi!

Entro una settimana ritengo che questo articolo possa essere contestualizzato agli Altri Modelli di Router per fare una analisi Generale di quella che è la situazione Attuale sul fronte Alis. Graziè a Dio gli obiettivi e i traguardi sono ancora Molti (Telsey FW etc.) e quindi potremo vedervi ancora all'opera.

tiresi@

June 3, 2010 at 8:38 pm Reply

C'è una formula universale per legare tutti i seriali?
Questa sarà nuova fonte di ricerca.

cioki

June 3, 2010 at 10:46 pm Reply

Altri dati…
ESSID: Alice-37588990

MAC: 00:23:8e:48:e7:d4 (Wi-Fi)

SERIAL: 67902X0339534

K: 13

Q: 33175048

WPA: 9j4hm3ojq4brfdy6wcsuglwu

spero siano utili a far crescere i magic number noti!

tiresi@

June 3, 2010 at 11:44 pm Reply

eccellente:
quindi MAC=00238E2951FE
e tutto torna..

campo

September 8, 2010 at 9:32 am Reply

Volevo capire una cosa, per la generazione dell'essid si utilizza il mac ethernet e non quello wifi (come è scritto sopra), quindi non capisco come sia possibile verificare da un essid il tipo di modello (agpf o no). Al limite è possibile dire quale sarebbe il mac ethernet nel caso sia un agpf. Ho capito male ?

smartguy

June 4, 2010 at 8:27 am Reply

utente tiresi@ tu riferisce yourself a mac ethernet with that value? io domanda because mac WiFi già a te dato da utente in comento precedente.

Cioki

June 4, 2010 at 8:33 am Reply

> **tiresi@ :**
> eccellente:
> quindi MAC=00238E2951FE
> e tutto torna..

Intendi il MAC ethernet? se si non posso confermare in quanto sono fuori sede fino a lunedì e non ho il router!

tiresi@

June 4, 2010 at 10:15 am Reply

si
377269068 –> E2951FE–>00238E2951FE
ed ecco il mac ethernet da cui ricavo il tutto.
Non occorre che controlli è giusto.

mah

June 4, 2010 at 5:16 pm Reply

Quindi? Conti di spiegare?

tiresi@

June 4, 2010 at 7:03 pm

Sorry ho dimenticato il due ;)

enzo

June 4, 2010 at 11:22 am Reply

> **tiresi@ :**
> si
> 377269068 –> E2951FE–>00238E2951FE
> ed ecco il mac ethernet da cui ricavo il tutto.
> Non occorre che controlli è giusto.

Non capisco da dove proviene questo numero: 377269068

basar

June 4, 2010 at 12:03 pm Reply

si,infatti,o la racconti tutta o lascia stare di postare risultati senza una spiegazione,altrimenti fai parte della stessa razza di saxdax….
Da dove vengono quei risultati??(10 a 1 che non risponde).

blowmast

June 4, 2010 at 12:21 pm Reply

BUFALA???:
Oggi ero in giro e ho provato ben 6 ssid appartenenti alle serie postate.
Tutti e 6 davano AGPF validi usando l'algoritmo,provato sia con mac wifi che con mac eth…….ne avesse azzeccata una!!!

enzo

June 4, 2010 at 12:27 pm Reply

Subito pronti ad accusare…. stiamo calmi….

Probabilmente ha sbagliato qualche copia incolla… E2951FE corrisponde al ssid postato preceduto dal 2, cioè:

237588990 >> hex >> E2951FE

quindi corretto.

bob

June 4, 2010 at 1:24 pm Reply

@basar
esatto….
tutti criticano saxdax……semplicemente invidiosi di chi sa tutto già da due anni…

tiresi@

June 4, 2010 at 7:01 pm Reply

Scusate ho dimenticato il due per strada, ma prima di brontolare potevate accorgervene con un minimo di deduzione come ha fatto il buon Enzo (che ringrazio). Per chi mi conosce sono stato sempre disposto a dare una mano, quindi non capisco questo tono.

SmartGuy

June 4, 2010 at 7:17 pm Reply

I think that the people who wrote this post are risking something to help out others and share knowledge. And those who are explaining details and adding information are taking their fare share of potential problems as well. Attacking them for forgetting a slight detail that could easily be worked out, provided you're clever enough to think without being spoon-fed, doesn't seem quite fair to me!
White Hats, WiFi Researchers, whatever.. you're doing a great job. Keep going!

cioki

June 4, 2010 at 8:05 pm Reply

ottimo! ma poi come mai il 2?

tafo

June 5, 2010 at 2:48 am Reply

Davvero complimenti per essere riusciti a scoprire l'algoritmo! Mi sfugge soltanto una cosa, non tanto nell'implementazione del procedimento, quanto nei commenti:

qualche riga in alto cioki ha postato questi dati:

ESSID: Alice-37588990
MAC: 00:23:8e:48:e7:d4 (Wi-Fi)
SERIAL: 67902X0339534
K: 13
Q: 33175048
WPA: 9j4hm3ojq4brfdy6wcsuglwu

In effetti il numero seriale mi ritorna, ma quando vado a calcolare la WPA key il risultato è sballato usando il MAC 00238E48E7D4.

Invece, utilizzando il MAC 00238E2951FE (segnalato da tiresi@), la WPA esce come deve, ossia 9j4hm3ojq4brfdy6wcsuglwu. Non capisco come le due cose possano essere in relazione: è necessario derivare anche il Mac? Non basta utilizzarlo così com'è? Cosamista sfuggendo?!
Grazie, e ancora complimenti.

tafo

June 5, 2010 at 3:05 am Reply
Ah scusate, mi era sfuggito il fatto che stessimo parlando del mac ethernet e non del wifi-fi, ora mi torna: mi accodo a cioki però, come mai il 2? E per calcolare la WPA è SEMPRE necessario utilizzare il Mac ethernet?

blowmast

June 5, 2010 at 6:18 am Reply
si

clshack

June 5, 2010 at 7:40 am Reply
Complimenti ragazzi ;)

mah

June 5, 2010 at 8:08 am Reply
Il 2 è forse una costante da aggiungere in caso di serie 37*? O in caso di serie inferiore a qualcosa? Intanto, cercando in rete altri dati, ho ricavato questa serie aggiuntiva:

Alice-62* serie=67904X k=13 Q=61841695 mac=00:25:5"
valida anche con k=8 Q=62174795

qualcuno può confermare o smentire? O fornire altri dati, così da ricavare ulteriori serie…

????

June 5, 2010 at 10:48 am Reply
Bravi ragazzi ,cerchiamo di collaborare e fornire altri dati.

????

June 5, 2010 at 10:52 am
x confermare dovresti fornire anche una wpa

romolo8

June 5, 2010 at 11:17 am Reply
@saxdax
Sapresti decriptare questo?
VFC

romolo8

June 5, 2010 at 11:18 am Reply
Bravi ragazzi.

romolo8

June 5, 2010 at 11:19 am Reply
Saxdax e delex se la tiravano non poco

Banias89//I

June 5, 2010 at 11:28 am Reply

> **mah :**
> Il 2 è forse una costante da aggiungere in caso di serie 37*? O in caso di serie inferiore a qualcosa? Intanto, cercando in rete altri dati, ho ricavato questa serie aggiuntiva:
> Alice-62* serie=67904X k=13 Q=61841695 mac=00:25:5”
> valida anche con k=8 Q=62174795
> qualcuno può confermare o smentire? O fornire altri dati, così da ricavare ulteriori serie…

Non posso confermare…

Ho una alice 62xxxxxx e il calcolo mi da:

k1=8 => Q1=62174801
k2=13 => Q2=61841706

pinco pallino

June 5, 2010 at 3:58 pm Reply
Guardate che se avete fatto i calcoli soltanto con la vostra ssid*serie
che dovrebbero essere circa:
67904x6661X—627077XX
67904x6662X—627077XX
i risultati K,Q sono giusti!
Però se i dati che ho scritto sui vostri ssid+serie sono giusti ci troviamo con una nuova coppia k,q.
Dove Q=62574515 e K=2 ditemi se sbaglio sono solo un pinco pallino :)

pinco pallino

June 6, 2010 at 2:49 pm
a meno che non è la stesso ssid e ha sbagliato k e q

gaucho

June 5, 2010 at 1:11 pm Reply
ciao mah, banjas,
potete postare i dati qua?
così facciamo i confronti.
siamo in presenza di 2 reti dove il giochino di k e q non vale.
avrei uno strumentino da testare sui dati..

Banias89//I

June 5, 2010 at 2:34 pm Reply
Non credo…
la parte mac interessata alla generazione della WPA combacia…
anche nel mio caso si tratta di un 00:25:53…

Tuttavia credo che sia preferibile postare questi dati in un luogo un po meno alla portata di tutti….
Son certo che unendo un pò di dati arriviamo ad una regola generale o quantomeno ingrandiamo sto db Q/k che al momento è fin troppo striminzito…

Comunque gaucho, anche io ho creato un programmino (sempre in VB.Net :D) che mi permette di generare in maniera abbastanza veloce ed esente da errori di calcolo ste benedette coppie Q/k…

Magari per confrontarci su tale punto, ci possiamo sentire nel forum in cui ci siamo sentiti stamattina.

Comunque disponibilissimo a collaborare e a lavorare insieme, a condizione però di un sistema stanadard e soprattutto sicuro.

beos

June 5, 2010 at 2:47 pm Reply

Concordo con banias,comunque a me risultano errati anche k e q del utente che ha postato i dati Alice-37588990

henry13

June 5, 2010 at 2:55 pm Reply

Chissa' se il discorso vale per Alice-95730556

Banias89//l

June 5, 2010 at 2:58 pm Reply

> **beos :**
> Concordo con banias,comunque a me risultano errati anche k e q del utente che ha postato i dati Alice-37588990

Sono esatti invece…

k1=8 Q1=34872718
k2=13 Q2=33175048

Semmai il problema è trovare un altro router della serie 37xxxxxx e quindi quale delle 2 coppie è quella universalmente valida…

beos

June 5, 2010 at 5:57 pm Reply

Esatto, intendevo in quel senso,con K=8 anche io ottengo quel risultato di Q, e' evidente che e' meglio provare prima di tutto con K=8 e poi con K=13 secondo me.

saxdax

June 5, 2010 at 10:55 pm Reply

Se mi date 50 euro a testa vi passo l'algoritmo completo.

Banias89

June 5, 2010 at 11:14 pm Reply

@ commento 38

Guarda, si capisce immediatamente che non sei saxdax, da tante cose…quindi gentilmente non iniziate a fare come su pillolhacking…
Se non avete nulla di meglio da fare, prendete una lunga rincorsa e puntate con la testa la prima cosa appuntita e spigolosa che trovate…
Ma per favore non sporcate anche questo sito !

saxdax

June 6, 2010 at 10:10 am Reply

Una cosa appuntita e spigolosa….ha si….il tuo uccello…hahahaha.
Cmq era evidente che era una battuta quanto era evidente che non sono saxdax….tardo.

void*

June 6, 2010 at 12:22 am Reply

Seguendo passo per passo l'algoritmo ho scritto un piccolo tool in python..

Mettendo in input i dati dell'ap fittizio da voi riportato il risultato è il medesimo, ma se lo provo con altri dati (serie 54*) la wpa riportata non è corretta.

Vorrei quindi porvi una domanda: il MAC che si visualizza tramite sniffer o similari è quello wi-fi immagino, e a quanto ho capito per generare la wpa si ha bisogno del mac ethernet, che si può calcolare correggetemi se sbaglio aggiungendo un "2" come costante alla parte numerica dell'essid, per poi portarla in esadecimale.

Nell'articolo c'è scritto "Come noto, il MAC è ottenibile mediante i più comuni strumenti di sniffing WiFi", mentre leggendo i commenti ho intuito che bisogna derivarlo con il metodo precedentemente descritto, quale è il procedimento realmente da seguire?

Prendendo i dati fittizi riportati nell'articolo:
wormhole void #
SPECIAL="\x64\xC6\xDD\xE3\xE5\x79\xB6\xD9\x86\x96\x8D\x34\x45\xD2\x3B\x1
wormhole void # SERIAL="67902X0587411"
wormhole void # MAC="\x00\x23\x8E\x01\x02\x03"
wormhole void # echo -ne $SPECIAL$SERIAL$MAC|sha256sum
b1d5d0dc8f3a2132d7872641250f998d53e58824ecb9118e046a943239bf1220
–

Qui non si usa un mac derivato, visto che se si calcolasse non sarebbe 01:02:03.
Grazie anticipatamente per la risposta.

Dario

February 22, 2011 at 3:46 pm Reply

scusami ma io concatenando i tuoi dati,
concatenandoli(\x64\xC6\xDD\xE3\xE5\x79\xB6\xD9\x86\x96\x8D\
e processandoli in sha ottengo questo risultato :
c32e3e120ae07108844d6ef83aa97ee1f81a6614e79b7bf228348c8

alfred1234

June 6, 2010 at 6:33 am Reply

Ciao a tutti, sto provando a fare i calcoli per vedere se un router è effettivamente AGPF ma non mi trovo.
Secondo l'algoritmo io dovrei prendere il MAC, fare dei calcoli e vedere se mi combacia con il SSID.
Allora prendo i dati già postati cos' a titolo di esempio
MAC: 00238e48e7d4
ESSID: Alice-37588990

L'algoritmo dice che nel vettore v1 mette gli ultimi 7 caratteri del mac e quindi e48e7d4. E fin qui ok.
Passiamo alle operazioni logico-matematiche.
In v0 ci carico il valore hex 55E63B89.
Effettuo la moltiplicazione tra quello in v1 e quello in v0 che risulta essere 4CB0DCC1EE9EC74 (in hex).
Carico in a3 il valore hex 5F5E100.
Prendo la parte alta della moltiplicazione precedente e cioè 4CB0DCC.
Faccio lo shift a destra di 25 caratteri del valore precedente e cioè 2.
Moltiplico tale valore per quello contenuto in a3 e lo metto in t0 e cioè BEBC200.
Sottraggo alla parte del mac il valore della moltiplicazione e lo metto in a3 e cioè e48e7d4 – BEBC200 = 25D25D4.
Quindi il SSID trovato è Alice-25D25D4 e non Alice-37588990. Quindi non è un router AGPF? cosa sbaglio? Grazie mille

pezio84

June 6, 2010 at 8:00 am Reply

Invece di considerare gli ultimi 7 caratteri del mac considera 0xE2951FE cioè il hex
di 237588990 cioè l essid preceduto dal 2 (come già detto da tiresi) e otterrai il risultato voluto

pezio84

June 6, 2010 at 8:15 am

Invece di considerare gli ultimi 7 caratteri del mac considera 0xE2951FE cioè il hex
di 237588990 cioè l essid preceduto dal 2 (come già detto da tiresi) e otterrai il risultato voluto; si ottiene lo stesso risultato considerando anche 137588990; quindi non si può stabilire seguendo questa procedura se l essid deve essere preceduto da 1 o 2

June 6, 2010 at 1:43 pm

pinco pallino

> **pezio84 :**
> Invece di considerare gli ultimi 7 caratteri del mac considera 0xE2951FE cioè il hex di 237588990 cioè l essid preceduto dal 2 (come già detto da tiresi) e otterrai il risultato voluto; si ottiene lo stesso risultato considerando anche 137588990; quindi non si può stabilire seguendo questa procedura se l essid deve essere preceduto da 1 o 2

vedi che preceduto da 1 in hex viene:
0x83370FE

SmartGuy

June 6, 2010 at 7:11 am Reply

The problem that is causing so much confusion (as far as I know) is that the original algorithm discovery was performed on pre-4.5.0sx router firmware version, and those release (almost?) universally make use of the WiFi interface MAC to calculate the WPA PSK. On the very contrary, the new firmware release, 4.5.0sx is using the Ethernet interface MAC to perform the same calculation. This is the (most probable) cause of confusion in the article and comments.
All the ideas behind the article are still 100% good in the new firmware, it's just a different MAC and the community must work to confirm the hypothesis that the Ethernet MAC is so simple to find out given all other information! Now, stop making dumb comments about selling knowledge, stop making dumb comments about the people here not wanting to share with others. Work seriously! As I always say, when one works seriously results always come. Se tu lavora serio risultato sempre vengono.

skyzed

June 6, 2010 at 10:25 am Reply

Ragazzi sto' cercando di ampliare il database dei numeri magici:
Se avete l'handshake di un router AGPF includete ssid e MAC e speditemelo via mail,vi rispondero' con i risultati di Wpa, Q e K
Se invece avete Numeri magici di nuove serie sono pronto a condividerli con i miei.
Il mio indirizzo mail e':

skyzedout@gmail.com

Tafo

June 6, 2010 at 10:56 am Reply

La scelta se usare 1 o 2 potrebbe dipendere da una tabella del genere:

Range degli ultimi 7 caratteri MAC WiFi
———————
0000000-5F5E0FF (v0=0) cioè in intero: 00000000 – 99999999
5F5E100-BEBC1FF (v0=1) cioè in intero: 100000000 – 199999999
BEBC200-FFFFFFF (v0=2) cioè in intero: 200000000 – 268435455

Nell'esempio citato, e48e7d4 ricade nel terzo caso e quindi si usa 2. Che ne pensate? Questo permette si di dedurre (forse) il Mac ethernet corretto, però non riesco ancora, partendo dal MAC, a generarmi l'SSID. In pratica, funziona se già conosco l'SSID, ma se sono l'apparato devo creare anche quello dal niente. Mi manca questo passaggio!

Banias89//l

June 6, 2010 at 11:32 am Reply

> **Tafo :**
> La scelta se usare 1 o 2 potrebbe dipendere da una tabella del genere:
> Range degli ultimi 7 caratteri MAC WiFi
> ———————
> 0000000-5F5E0FF (v0=0) cioè in intero: 00000000 – 99999999
> 5F5E100-BEBC1FF (v0=1) cioè in intero: 100000000 – 199999999
> BEBC200-FFFFFFF (v0=2) cioè in intero: 200000000 – 268435455

> Nell'esempio citato, e48e7d4 ricade nel terzo caso e quindi si usa 2. Che ne pensate? Questo permette si di dedurre (forse) il Mac ethernet corretto, però non riesco ancora, partendo dal MAC, a generarmi l'SSID. In pratica, funziona se già conosco l'SSID, ma se sono l'apparato devo creare anche quello dal niente. Mi manca questo passaggio!

Davvero non capisco …

ma l'avete letto l'algoritmo di generazione dell'SSID ????

Il tuo discorso secondo me non è universalmente applicabile…
In giro si sono visti router aventi mac ethernet classici (00:25:53 ect etc) e mac wi-fi di tutt'altro tipo e "folli" come diceva qualcuno…

Ergo l'unico modo per ottenere il mac corretto è quello del bruteforce…
Ad es.

For i as byte = 0 to 3
SSID = SSID & i.toString
MAC_Str = "&h" & Hex(SSID)

Select Case Mac_Str.Substring(0,1)
Case "E"
'Si tratta possibilmente di un mac serie 00:23:8E
Case "B"
'Si tratta possibilmente di un mac serie 00:1D:8B
Case "3"
'Si tratta possibilmente di un mac serie 00:22:33
oppure 00:25:53

eccetera eccetera eccetera…

proes

June 6, 2010 at 11:47 am Reply

Ma,mi sa' parli tanto ma anche tu non hai capito molto…non serve nessun bruteforce per ottenere il mac corretto

Banias89

June 6, 2010 at 2:15 pm Reply

Ma per favore…evitiamo si innescare flame inutili…
E poi stai certo che se mi espongo cosi è perchè di sicuro ci ho capito più io di te…

proes

June 6, 2010 at 2:22 pm Reply

Se ne sei convinto….contento tu,contenti tutti…….

pezio84

June 6, 2010 at 2:18 pm Reply

> **pinco pallino :**
>
> > **pezio84 :**
> > Invece di considerare gli ultimi 7 caratteri del mac considera 0xE2951FE cioè il hex
> > di 237588990 cioè l essid preceduto dal 2 (come già detto da tiresi) e otterrai il risultato voluto; si ottiene lo stesso risultato considerando anche 137588990; quindi non si può stabilire seguendo questa procedura se l essid deve essere preceduto da 1 o 2
>
> vedi che preceduto da 1 in hex viene:
> 0x83370FE

si lo so; per "stesso risultato" intendevo che eseguendo tutti i vari calcoli considerando 137588990 si riottiene alla fine 37588990(se ho fatto tutto correttamente in caso contrario corregete), spero di essere stato piu chiaro ora.
grazie cmq per la precisazione

Tafo

June 6, 2010 at 5:16 pm Reply

Per quanto riguarda il discorso di stamattina della "tabella", è vero…non è universalmente applicabile e quindi non ha molto senso.

Però, appurato che si parte da 7 caratteri del Mac (Wifi o Eth che sia), il massimo valore ottenibile FFFFFFF è in decimale 268435455 (9 cifre, una in piu di 8)… questo significa che in teoria gli ultimi 7 caratteri del Mac Eth potranno avere 3 valori (0…1…2…), no?.

WPA (0): ja7rp7tdmwj4hdwurdvhipiw utilizzando il Mac: 0023823d8ffe
WPA (1): 3hi27vs51cgvh1vfmow5nytw utilizzando il Mac: 0023883370fe
WPA (2): 9j4hm3ojq4brfdy6wcsuglwu utilizzando il Mac: 00238e2951fe

A sto punto, confrontando i Vendor OUI, solo l'ultimo MAC è un Pirelli ed è poi la soluzione. Qualcuno può postare un esempio di situazione in cui Mac eth e wifi hanno OUI e Vendor diverso?
Grazie

anonimo

June 6, 2010 at 7:53 pm Reply

ciao a tutti,
ho provato a riprodurre in codice c le istruzioni mips per verificare se il router ha la versione corretta, riporto qui il link al codice: http://pastebin.com/jZMUpTGD
ma non ottengo il risultato cercato…
sapreste dirmi dove sbaglio?
grazie

daniele

June 8, 2010 at 12:49 am Reply

io non capisco questo ,credo che debba essere 25 lo shift di destra

v0 = v0 >> 57;

e poi forse il risultato va in v1 qui…

v0 = (v1*v0);

curiosità: che compilatore usi??

lufuscu

June 6, 2010 at 8:43 pm Reply

quello che dice Tafo sembra avere senso…forse posso provare la prima fascia di tabella (la 0)…vi farò sapere

void*

June 6, 2010 at 10:20 pm Reply

Tanto non ottiene il rusultato sperato ha detto :P

void*

June 6, 2010 at 10:45 pm Reply

per capire quali serie sono agpf si possono fare due conti con i dati di questo database: http://www.rave-party.net/alis

skiNauz

June 7, 2010 at 9:21 am Reply

non serve a una mazza questa tabella.

Tafo

June 7, 2010 at 4:36 pm

vero

dangerous

June 7, 2010 at 9:51 am Reply

Salve raga, una domanda…secondo voi a questo SSid corrisponde questo mac:

Alice-54887113 00:25:53:45:82:C9 , nel senso ho la wpa in questione, ma da procedura sopracitata non mi risulta.
Di nuovo Dangerous

Pig

June 7, 2010 at 2:14 pm Reply

Ragazzi qualcuno è in grado di chiarire qual e' la situazione del mac address? Vale a dire partendo da mac wifi e ssid come calcolare il mac ethernet?

Alby

June 7, 2010 at 7:43 pm Reply

> **Tafo :**
> La scelta se usare 1 o 2 potrebbe dipendere da una tabella del genere:
> Range degli ultimi 7 caratteri MAC WiFi
> ———————
> 0000000-5F5E0FF (v0=0) cioè in intero: 00000000 – 99999999
> 5F5E100-BEBC1FF (v0=1) cioè in intero: 100000000 – 199999999
> BEBC200-FFFFFFF (v0=2) cioè in intero: 200000000 – 268435455
> Nell'esempio citato, e48e7d4 ricade nel terzo caso e quindi si usa 2. Che ne pensate? Questo permette si di dedurre (forse) il Mac ethernet corretto, però non riesco ancora, partendo dal MAC, a generarmi l'SSID. In pratica, funziona se già conosco l'SSID, ma se sono l'apparato devo creare anche quello dal niente. Mi manca questo passaggio!

ho provato con un mac wifi che cade nel secondo caso (intero compreso tra 100000000 – 199999999) e aggiungendo 1 all'ssid e sottraendo BEBC200 non ottendo l'essid di partenza; invece aggiungendo 2 ed usando sempre BEBC200 lo ricavo…

non so se è una cosa normale…ma con tanti essid ho ottenuto lo stesso risultato: aggiungendo 2 all'ssid e poi al hex ottenuto sottraendo (usata come costante) BEBC200 ottendo l'hex che poi convertito in decimale mi da l'ssid di partenza…

non vorrei fosse invece un gioco matematico del tipo aggiungere 2 e poi sottrarre 200000000 quindi sempre 2 dopo gli shift…penso proprio di si!!

corregetemi se sbaglio in v0 metto 55E63B89, in a3 il valore hex 5F5E100 si può considerare BEBC200 come costante oppure ogni volta devo fare tutti i calcoli tra v1, v0 ecc.??
scusate, vorrei capire ma non sono tanto afferrato in materia, scusate le "scelleratezze" che scrivo

skiNauzFucc

June 7, 2010 at 8:31 pm Reply

ti quoto "aggiungendo 2 all'ssid e poi al hex ottenuto sottraendo (usata come costante) BEBC200 ottendo l'hex che poi convertito in decimale mi da l'ssid di partenza…"
ma scrivi con un filo porcoil***

daniele

June 7, 2010 at 9:24 pm

bhè un pò si capisce…

1)aggiungi 2 all'ssid
2)converti il decimale del passo 1, in hex
3)sottrai al risultato del passo 2 BEBC200
4)converti in decimale il risultato del passo 3 ed ottieni ssid

si è espresso un pò male ma questo è il succo di ciò che voleva dire…non offendiamo!

Alby

June 7, 2010 at 7:48 pm Reply

> **dangerous :**
> Salve raga, una domanda…secondo voi a questo SSid corrisponde questo

> mac:
> Alice-54887113 00:25:53:45:82:C9 , nel senso ho la wpa in questione, ma da procedura sopracitata non mi risulta.
> Di nuovo Dangerous

magari mi sbaglio ma forse il mac eth di quella rete è 00:25:53:45:82:C9….

Alby

June 7, 2010 at 7:50 pm Reply
anche a me usando la procedura descritta su nel mio post precedente ottengo quel mac!!

lufuscu

June 7, 2010 at 7:52 pm Reply
appunto quello che ha scritto…l'indirizzo dovrebbe essere quello, magari fai degli errori durante il calcolo della wpa. Se magari ci scrivi la wpa (o anche metà se proprio non la vuoi scrivere) magari può servire a risolvere la questione

daniele

June 7, 2010 at 8:31 pm Reply
non capisco una cosa del codice postato rispetto all'algoritmo
v0 = v0 >> 57;

nell'algoritmo c'è scritto:
mfhi $v0 // solita storia della hiword dopo la moltiplicazione (che vuol dire???)
srl $v0, 25 // Shift della hiword

perchè invece di 25 si shifta di 57??

daniele

June 7, 2010 at 8:33 pm Reply
mfhi $v0 vuol dire parte alta del risultato giusto??

nessuno

June 7, 2010 at 11:19 pm
si penso sia sbagliato,
bisogna fare lo shift di 25 solo sul valore del registro alto (hi). io non capisco sta cosa di aggiungere il 2 … da dove viene?

pezio84

June 7, 2010 at 8:36 pm Reply

> **dangerous :**nrgg4zi43lsu
> Salve raga, una domanda…secondo voi a questo SSid corrisponde questo mac:
> Alice-54887113 00:25:53:45:82:C9 , nel senso ho la wpa in questione, ma da procedura sopracitata non mi risulta.
> Di nuovo Dangerous

la prima parte della wpa è questa?
nrgg4zi43l

pinco pallino

June 9, 2010 at 1:15 pm Reply
oppure una di queste:
ybq0hetdq..
01yloucor..
0nh2z6627..
ottenute con padding

dangerous

June 9, 2010 at 10:13 pm
Scusa anche usando il Padding come arrivi a questo risultato? ybq0hetdq

June 10, 2010 at 7:02 am
come abbiamo visto "dall'altra parte" cambiando

pinco pallino

q=52420673
e ottenendo serial=67903X0308305
senza un pool di serial e ssid non penso possiamo trovare dati corretti.
@benias89:se ssid 62707753 è il tuo, puoi inserire il serial ciao e grazie.

skiNauzFucc

June 7, 2010 at 9:02 pm Reply
sei proprio un deficente,
questa non è full-disclosure. o fai una divulgazione come si deve o te ne stai zitto che fai più bella figura.
baci

proes

June 7, 2010 at 9:16 pm Reply
NON e' full-disclosure????,leggi bene prima di parlare….a scusa… forse prima dovresti imparare a leggere…..e' grazie alle CAPRE IGNORANTI come te che l'Italia va' a rotoli.

skiNauzFucc

June 7, 2010 at 9:51 pm
è un POC senza codice e con beneficio del dubbio..

daniele

June 7, 2010 at 9:28 pm Reply
ragazzi non litigate, non serve a nulla e poi perchè "sporcare" la pagina con insulti!!

whitehatc

June 8, 2010 at 1:29 am Reply
Anche se i commenti non vengono moderati non significa che non vengono controllati. Per cui vi consiglierei di darvi una regolata o prenderemo provvedimenti.

Saluti, WH

Pig

June 8, 2010 at 7:25 am Reply
Confermo che anche nella mia reta ssid preceduto dal 2 e trasformato in hex=mac ethernet e wpa corretta…

giubari

June 8, 2010 at 8:16 am Reply
Se continuiamo a commentare non riusciremo a quagliare niente, apritevi una BOARD e discutiamone in un Topic con dei Moderatori che possano verificare i nostri risultati, filtrare la feccia e mettere in STICKY le cose serie, se no faremo la fine del Blog di AngeloRighi dove ogni 200 post si ripetevano sempre le stesse domande e le stesse risposte, come un cane che si mangia la coda

kayrin

June 8, 2010 at 9:57 am Reply
> **pezio84 :**
>
> > **dangerous :**nrgg4zi43lsu
> > Salve raga, una domanda…secondo voi a questo SSid corrisponde questo mac:

> Alice-54887113 00:25:53:45:82:C9 , nel senso ho la wpa in questione, ma da procedura sopracitata non mi risulta.
> Di nuovo Dangerous

la prima parte della wpa è questa?
nrgg4zi43l

se la wpa è quella allora allora il MAC da usare è quello ethernet calcolato con 002550000000+HEX(2 SSID)= 00255F3144C9,giusto?
ma se fosse questa:2jozhteslt8n6lc…. allora il mac da usare sarebbe direttamente quello postato.
Per questo serial 67903X0308303;
E se non e' nessuna delle due vuol dire che il serial non e' corretto e se non lo fosse il Q o il k postati per quella serie sono sbagliati.
Se il serial fosse SN=67903X0308305, Q=52420673 e la wpa ybq0hetdqly0a… (usando MAC postato)…Dangerous come inizia la wpa?

Bargad

June 8, 2010 at 10:58 am Reply

@Saxdax
Visto che non posso rispondere sul tuo blog lo faccio qui:
Certo che sei proprio in cretino..e fai pure lo spiritoso…telecom avrebbe ascoltato i tuoi consigli per il nuovo AGIPF???…haha.
A parte il fatto che non ci crede nessuno che tu abbia avuto contatti con i tecnici di telecom riguardo questo argomento,penso che se telecom saprebbe chi sei ti farebbe ingabbiare istantaneamente..non tanto per aver reversato il fw ma per il fatto che ti fai ancora pagare per trovare le chiavi di accesso.
E poi anche la battutona…chissa' se la sigla sx sta' per saxdax…haha che ridere.
Sarai pure una persona valida ma rimani cmq un cretino… intelligente non vuol dire anche furbo.
Infatti solo uno stupido puo' farsi pagare qualche decina di euro senza pensare all'enorme rischio a cui va' incontro.

matteo

June 8, 2010 at 11:00 am Reply

per la cronaca l'algoritmo che genera l'ssid e' una soluzione economica per calcolare il resto modulo 10^8 degli 7 nibble meno significativi del mac.
In parole povere converte in decimale gli ultimi 7 caratteri del mac e poi prende le ultime 8 cifre.
es: 0xE2951FE -DEC> 237588990 -MOD> 3758890
Inoltre la cifra cancellata puo' essere solo 0 1 2

Per interpretare l'algoritmo basta fare il calcolo:
0x200000000000000 / 100000000 che arrotondato e' 0x55E63B89
(quel 10^8 e' in decimale, gli altri sono hex)
Servono altri suggerimenti?

Forse ho risolto anche la generazione di un qualsiasi serial a partire dal mac. Pero' avrei bisogno di un firmware leggibile da ida pro.
Chiedo gentilmente a qualcuno di inviarmelo alla mia email:
matteoTOGLILOgeniaccio chiocciola yahoo.it

Ovviamente pubblichero' i risultati appena ne saro' sicuro.

Perlonz

June 8, 2010 at 12:59 pm Reply

a geniaccio…quello che hai scritto lo avevamo capito tutti…a parte i tardi naturalmente.

matteo

June 9, 2010 at 1:20 pm

e' stato spiegato solo cosa fa l'algoritmo, non come lo fa e perche'.
Inoltre la mia intenzione era far capire che sono bravo con l'assembly cosi' la mia richiesta di firmware scompattato verrebbe presa sul serio.

Peppe

June 8, 2010 at 3:59 pm Reply
Ecco perchè googlando bisogna sempre eseguire le ricerche in lingua inglese, onde evitare di imbattersi in queste forme di stupidi insulti.


Perlonz

June 8, 2010 at 5:05 pm Reply
Questa proprio me la devi spiegare perche' non l'ho capita……ma che c….zo centra?????????????


o7

June 8, 2010 at 6:25 pm Reply
ho provato a scrivere il codice di verifica agpf seguendo il codice mostrato nell'articolo, ma sicuramente sbaglio qualcosa…
http://pastebin.com/7Z0c0FTM
ho un sistema a 32 bit
grazie


o7

June 8, 2010 at 6:30 pm Reply
errata corrige dovuto alla fretta..
http://pastebin.com/ajDbsq5Q
:)


swsooue

June 20, 2010 at 1:53 pm
Ho dato un'occhiata al codice ed ho trovato l'errore per cui non ti riesce il calcolo :-)
Contattami alla mia email swsooue@gmail.com così ti dico che cosa hai sbagliato.
Ciao
Gigi


void*

June 8, 2010 at 8:40 pm Reply
Lascio questo commento, perchè ho letto alcuni di voi che dicevano che nonostante tutto non riescono ad arrivare alla chiave esatta.
Nel mio caso (AGPF-4.5.0sx) ha beccato ogni cosa: wpa, serial, mac eth.
Mi complimento con i wi-fi researchers per l'ottimo lavoro svolto.


enzo

June 9, 2010 at 10:41 am Reply
Qualcuno potrebbe postare un ssid, mac-wifi e handshake di una rete??

Cosi da fare un paio di prove mediante bruteforce per confermare una teoria…

Grazie e tutti per la collaborazione…


Chupito

June 9, 2010 at 6:03 pm Reply
Ragazzi novita sui magic numbers per altri ssid? La mia reta è del tipo alice-53XXXXX ma i numeri magici non sono noti…


arbe5

June 9, 2010 at 6:55 pm Reply
se posti il nome completo ed il seriale potrei ricavare i magic number (mio fratello ha la stessa rete)


enzo

June 9, 2010 at 6:54 pm Reply
> **Chupito :**
> Ragazzi novita sui magic numbers per altri ssid? La mia reta è del tipo alice-53XXXXX ma i numeri magici non sono noti…

Posta ssid, mac wifi e un handshake cosi si prova a risalire ai magic number

Thorn

June 9, 2010 at 9:19 pm Reply

Magari sto dicendo banalità ma cercando di dare un senso a quel 2 nella conversione mac wi->mac eth ho notato una cosa.
L'esempio funzionante mostrato da @tiresia all'inizio del commenti è il seguente:

SSID: Alice-37588990

237588990 >> hex >> E2951FE

Mac wifi: 00:23:8e:48:e7:d4
Mac eth: 00:23:8e:29:51:fe

Come avrete notato aggiungendo 2 e convertendo in hex si ottengono 7 caratteri. Per ottenere il mac wifi ne vanno cambiati solo 6. Nell'esempio in questione tuttavia il primo carattere dei 7 e l'ultimo dei primi 6 coincidono ('e').

Dato che i primi 6 caratteri ossia i primi 3 byte del'MAC indicano il produttore direi che quelli debbano rimanere invariati.

A questo punto le alternative sono due: o si tronca uno dei 7 caratteri ottenuti per ottenere il MAC ethernet oppure si cerca di ottenere un numero esadecimale la cui prima cifra corrisponda con la sesta del mac address originario.

Con questo post non ho dimostrato niente e si tratta solo di intuizioni ma penso che potrebbe essere una strada per capire come manipolare l'ssid per ottenere il mac wifi.

Altra piccola nota frutto di esperienza personale che francamente non so come interpretare:
tramite kismac ho trovato una lista dei mac address relativi ad un access point.
Il mac del wifi era 00:25:53:13:8B:8C. E fin qui niente di strano.
Ad un certo punto noto della lista un altro mac address classificato come 'unknow': 00:25:53:42:71:D1. Sul momento lascio perdere.

A posteriori noto poi una cosa:
54686161 (l'ssid) in hex da come risultato 34271D1, guarda caso proprio le ultime 7 cifre del MAC "misterioso" trovato per caso e, faccio notare, con la cifra '3' che va a combaciare perfettamente con l'inizio del mac wifi 00:25:53.

Altra particolarità: applicando la funzione descritta nell'articolo per la verifica del tipo di modem si ottiene proprio l'ssid di partenza cosa che non il MAC wifi non succede!

Francamente, come dicevo sopra, non so come interpretare questo risultato.
Sta di fatto che calcolando la wpa con il resto dell'algoritmo sembra essere sbagliata, tuttavia il segnale è debole e non mi è possibile verificarlo con certezza.
Domani proverò a catturare un handshake su cui fare dei test.

Per ora buona serata :)

framag

July 2, 2010 at 9:39 am Reply

ho rifatto i calcoli con Alice-37588990 e anche me tornano i tuoi stessi risultati aggiungendo 2 davanti all'SSID; però con il seguente esempio la password wpa corretta la ottengo senza mettere il 2 davanti, infatti:

con Alice-54011409 e MAC WIFI 00.25.53.0d.61.9c
54011409>hex>3382611 il MAC diventa 00.25.53.38.26.11
e la password corretta è: p3mu81nj4hd4v07af54h8dre

chiedevo
con Alice-38392429 e MAC WIFI 00.23.8e.4d.1f.28 non mi tornano i conti… c'è qualcuno che mi può dare una mano?

grazie

dangerous

June 9, 2010 at 10:15 pm Reply

> **pinco pallino :**oppure una di queste:ybq0hetdq..01yloucor..0nh2z6627..ottenute con padding

Scusa anche usando il Padding come arrivi a questo risultato? ybq0hetdq

The King

June 10, 2010 at 8:46 am Reply

Dari presi da un altro blog, qualcuno è in grado di definire quali siano i numeri magici?

alix-53847953
mac 00255335a791
seriale 67903×0178409
pass 7nfyuqlahytaml3bkcjasmtf

alix-53023425
mac ethernet 00:25:53:29:12:C1
mac wifi 00:25:53:05:e3:50
seriale 67903X0103387
pass gi0wdaa3crf6wsb53sf7bv5t

Thorn

June 10, 2010 at 9:14 am Reply

Basta risolvere il sistema di due equazioni in due incognite.
Con wxMaxima si fa con il comando:

linsolve([178409=(53847953-Q)/k, 103387=(53023425-Q)/k], [Q,k]);

che da come risultato (semplificato):

Q=51887151,35846
k=10,37154

Non molto incoraggiante…

The King

June 10, 2010 at 9:18 am
Secondo i miei calcoli k=10,9904 dati che cmq non portano a nessun risultato

lufuscu

June 10, 2010 at 10:32 am Reply

come scritto su quel blog c'è qualcosa che non va con il secondo alice-53 perchè confrontando il primo ed uno in possesso q=52420681 e k=8 e 'tutto' torna

The King

June 10, 2010 at 10:59 am
In effetti con questi valori di k e q tutto torna, allora probabilmente cè qualche errore nei dati riportati da quell'utente…

Pocho

June 10, 2010 at 10:03 am Reply
Quindi la formula per calcolare i numeri magici non è valida per tutti gli ssid?

ballard

June 10, 2010 at 6:58 pm Reply
Tabella di tutti i seriali quesi completata :)

Enzo

June 10, 2010 at 9:47 pm Reply
Condivisione è Potere!

lufuscu

June 11, 2010 at 12:06 am
quoto enzo

skyline

June 10, 2010 at 9:26 pm Reply
eccomi x contribuire con la linea.
Mac adress acces point: 00:23:8E:49:50:A8
Nome dell'acces point:Alice-37753804
Canale acces point: 1
Wpa; y1x3n69f0ogjspy94qh1t5bq


void*

June 10, 2010 at 10:49 pm Reply
Il canale non era necessario, mentre era preferibile lasciare il seriale.


lufuscu

June 11, 2010 at 12:05 am Reply
67902X0352212

K: 13
Q: 33175048

per alice-37 si sanno già era uno dei primi commenti. Comunque meglio così conferma le ipotesi :D


@NOMALY

June 11, 2010 at 4:29 am Reply
ragazzi mi aiutate a confermare che questo non è un agpf?
alice-56010026
mac wifi 00:1d:8b:65:8c:ec

con i metodi per ricavare il mac eth non viene fuori la prima lettera della conversione dovrebbe essere b…ma cio' non avviene,vorrei un parere perche' penso che esso non è un agpf.grazie in anticipo.


Chupa

June 11, 2010 at 8:21 am Reply
Ragazzi si potrebbe fare un riepilogo dei magic numbers noti fino ad adesso per tutte le serie, cè un po' di confusione, thanks.


@NOMALY

June 11, 2010 at 12:28 pm Reply
> **@NOMALY :**
> ragazzi mi aiutate a confermare che questo non è un agpf?
> alice-56010026
> mac wifi 00:1d:8b:65:8c:ec
> con i metodi per ricavare il mac eth non viene fuori la prima lettera della conversione dovrebbe essere b…ma cio' non avviene,vorrei un parere perche' penso che esso non è un agpf.grazie in anticipo.
>
> qualche consiglio….


Thorn

June 11, 2010 at 12:52 pm Reply
Ci vorrebbe qualcuno che postasse per ogni serie delle coppie MAC eth-wi in modo da poter verificare la relazione che intercorre tra i due.
Solitamente i primi 3 byte coincidono ma nei router di altre marche ho notato che l'ultimo nibble può anche cambiare…


lufuscu

June 11, 2010 at 1:06 pm Reply
per alice-56 AGPF il mac dovrebbe essere 00:25:53 quindi la tua quasi sicuramente non lo è


notnow

June 11, 2010 at 1:19 pm Reply
bl1k2yto… ?


June 11, 2010 at 6:04 pm

Tafo

0m4550 …
3dw3tf …

@NOMALY uno di questi due?!

skyline

June 11, 2010 at 8:39 pm Reply

Secondo voi si può riuscire a sbloccare il modem di mio zio? è un mac address 00:1D:8B:D4:F9:EE ALICE-76477566 ” così lo convinco a cambiare modem, lui ama la telecom XD”

dangerous

June 11, 2010 at 9:47 pm Reply

tranquillo tuo zio e’ al sicuro……

skyline

June 11, 2010 at 11:23 pm

Spero solo x ora!, voglio divertirmi a farlo impazzire XD.

Enzo

June 12, 2010 at 8:19 am

Come mai sostieni questo? Non è un AGPF?

pippopippo7

June 11, 2010 at 10:42 pm Reply

Un saluto a tutti i partecipanti.

Debug

June 11, 2010 at 11:36 pm Reply

sto cercando di completare il database delle serie, se c’è qualcuno interessato a conoscere i numeri magici della propria serie può inviarmi i dati del proprio router a webmaster[nospam]@gibit.net ovviamente eliminate il [nospam]

i dati da inviare sono: SSID della rete, Numero di serie, un MAC address a scelta tra Wireless ed Ethernet e la wpa (o solo la prima parte della wpa)

Se volete posso scambiare anche numeri di altre serie…

arbe5

June 12, 2010 at 2:25 am Reply

Praticamente tutto.Fossi in te mi farei pagare.come ha detto enzo poco fa “condivisione è potere”

@nomaly

June 12, 2010 at 12:37 am Reply

grazie x la risp. tafo, ma nessuna delle due…ma sei riuscito a calcolare il mac ether?come hai fatto? a me non esce…

arbe5

June 12, 2010 at 1:51 am Reply

ahahah…scommetto che hai messo solo le prime 5 lettere che ti hanno dato…ovvio che non è in tuo possesso quel modem altrimenti avresti detto subito qual è il mac eth…

Tafo

June 12, 2010 at 11:52 am Reply

In base al SSID che hai postato direi che ci sono solo due Mac Ethernet compatibili Pirelli:
00223356A52A
00255356A52A
Devi utilizzare il primo carattere dei 7 delle 3 possibili stringhe derivate dal SSID per fare le tue valutazioni. Probabilmente allora non è AGPF

gonzo

June 12, 2010 at 6:12 pm

3 possibili stringhe?
perché sono 3? io sapevo che il MAC eth si calcolava convertendo in HEX il SSID… c'è qualcosa che mi sono perso?

lufuscu

June 12, 2010 at 10:43 am Reply

da dati del web:
Numero seriale: 67902X0294925
Indirizzo MAC Ethernet: 00:23:8E:19:87:4C
Indirizzo MAC Wi-Fi: 00:23:8e:43:46:c4

si capisce che è un alix-36, e facendo le varie prove con il database:
k=13
q=32720035
serie=67902X*******

come sempre pregherei di testare e confermare questi dati, ricordo che il mac deve essere 00:23:8E….

Tafo

June 12, 2010 at 7:39 pm Reply

Ti faccio un esempio,
con SSID = 34567899

(0)34567899 -> 20f76db
(1)34567899 -> 80557db
(2)34567899 -> dfb38d8

Quindi i possibili Mac sono tutti quei Pirelli che hanno come lettera/cifra finale del Vendor code: (2-8-d). Questo nel caso in cui tu non abbia trovato la key corretta direttamente con il Mac Wifi ;)

skyline

June 13, 2010 at 4:07 pm Reply

ma non si potrebbe creare un forum x raccogliere informazioni pulite alla portata di tutti?????

Debug

June 14, 2010 at 11:32 am Reply

Ragazzi questa pagina sta diventando lunga in modo illeggibile (così come le altre 2 discussioni presenti in rete). Che ne dite se metto su una pagina nel mio forum dove riassumo tutto quello che c'è scritto qui e continuiamo a parlarne lì?

romolo8

June 14, 2010 at 11:57 am Reply

Certo. Qual e' il tuo blog?

enzo

June 14, 2010 at 1:11 pm Reply

Ho creato un forum molto semplice in cui poter parlare e discutere e raccogliere piu facilmente le varie info:

hxxp://alicedb.forumup.it

A presto

romolo8

June 14, 2010 at 1:26 pm Reply

Ma come ci si iscrive, sembra chiuso…

The King

June 14, 2010 at 1:38 pm
Bisogna registrarsi, basta andare alla voce "registrati" in alto a destra.

skyline

June 23, 2010 at 9:55 pm Reply
xkè creare un forum dove ci vuole un accesso speciale? bha -.-"

skyline

June 14, 2010 at 5:21 pm Reply
Si si! facciamo un forummmmmmmmmmmmmmm, non si capisce + na mazza tra sti bimbi che litigano! XD

pluto70

June 15, 2010 at 3:45 pm Reply
Ciao a tutti sono neofita di questo BLog,
avete notizie dei magic number K e Q della serie Alice-58xxxx ed Alice-87xxxxx, ho fatto delle ricerche sulla rete, ma non ho trovato nulla a riguardo.
Grazie!

Debug

June 17, 2010 at 5:16 pm Reply
Ragazzi come promesso a tutti quelli che mi hanno scritto in questi giorni ho messo su un piccolo software che permette di calcolare le WPA con il metodo descritto, ma soprattutto di fare il brute force sui seriali per calcolare un seriale o per calcolare le possibili combinazioni di K e Q.

In questo modo potremo ampliare di molto la banca dati in nostro possesso e comprendere quali reti sono effettivamente vulnerabili.

E' anche possibile creare un dizionario da utilizzare con aircrack, il software è scaricabile dal mio sito, insieme alla breve guida:

http://www.gibit.net/2010/06/17/alice-wpa-calculator-ecco-come-gli-hacker-scoprono-la-password-della-tua-rete/

Mi raccomando, ragazzi, diffondete il verbo xD ed aiutatemi a completare la banca dati (il file config.txt). Sono aperto a qualunque critica o suggerimento (se postate qualcosa di costruttivo postatela anche sul mio sito come commento, in modo da renderla disponibile anche a chi non bazzica questo forum)
ciao a todos!

Debug

Debug

June 20, 2010 at 6:39 pm Reply
Aggiornata la lista dei magic numbers

http://forum.gibit.net/viewtopic.php?f=10&t=3

lonewolf

June 21, 2010 at 11:01 pm Reply
00-1c-a2-cb-00-3c alice-48713244 WPA = 5p9rwsz3ll5fk3qw5y5m1iz5
00-1d-8b-6f-43-9c alice-58022517 Wpa = u89vkpgbmy31s1xfj2kxg6j3
00-1D-8B-57-97-A4 alice-94503669 Wpa = z5rhzgz0nx5q2qr5w96ph9le
la seconda ((258022517 = f611c75)) non mi trovo con il mac ethernet dove sbaglio? comunque credo vadano bene per aggiornare config.txt

Debug

June 22, 2010 at 2:07 pm Reply
grazie lonewolf sei stato utilissimo, ho ricavato dei magic che non c'erano.aggiornerò la lista dei magic entro sera

zukky

July 1, 2010 at 3:51 pm Reply

@lonewolf

Mac eth 002233755A75

cambia mac non devi paddare nulla.

Ciao zukky.

deinde

June 23, 2010 at 10:10 am Reply

ciao complimenti per la ricerca!!
da quello che ho capito hai fatto un reverse del firmware dei vari pirelli!!
io ho un pirelli DiscusTM DRG A112 che però è della tele2/teletu, mi sono accorto che la wpa di default è il serial number e dato che sono quasi sicuro che l'algoritmo per ricavarlo è nel firmware volevo sapere che strumenti hai utilizzato.
ho provato ad aprire il firmware (.bin) con ida pro ….con peid kanal ma non trovo niente!!
mi potresti dare qualche consiglio??

IODO

June 26, 2010 at 11:41 am Reply

Alice-791xxxxxxx qualcuno ha i magic?

REMO

June 27, 2010 at 1:34 pm Reply

Ma quante balle mi tocca sentire !!!!!!!! Comunque mi fa piacere che ci sono ancora un sacco di persone che ci credono alle balle…….

lufuscu

June 27, 2010 at 1:47 pm Reply

a quali balle ti riferisci?

Antonio

June 28, 2010 at 11:38 pm Reply

Ho da poco scoperto che si è aperto un nuovo Forum! E sembra anche molto interessante… http://www.pppusername.altervista.org, non ho capito chi è l'admin ma ci ho parlato in PM ed è molto cortese e preparato!
Stavo guardando la formula universale forse qualcuno di voi ne capisc più di me..

Jigen

June 30, 2010 at 11:31 am Reply

Smettila di fare pubblicità al tuo forum, ridico!

Tiff

June 30, 2010 at 11:36 am Reply

Che merdata di forum, vai a fare pubblicita' da un'altra parte.

Vegeto

July 12, 2010 at 9:45 am Reply

ma che bravi…ora gli innumerevoli bimbominkia-lamer che non hanno un ca..o da fare essendo chiuse le scuole, inizieranno a fare danni.
se avessi un router alice vi denuncerei.

Marcofe

July 14, 2010 at 10:22 pm Reply

State facendo troppa “sciangazza”(traduzione: troppa polvere) come si dice dalle mie parti..un pò di serietà per favore sopratutto dai bimbiminchia che non fanno altro che vivere sul lavoro degli altri, andando a raccontare in giro che sono degli hacker potentissimi che craccano le chiavi di tutto il mondo…smettiamola…dai..

delfo

July 19, 2010 at 8:09 am Reply

Ciao raga ma sto blog sembra morto!! Cmq girovagando in rete ho trovato un tool simile a quello di Debug ma a mio parere piu’ performante e intuitivo, si serve sempre del file confix.txt
http://rapidshare.com/files/407399588/Alixrecovery.rar
Ah dimenticavo non mi assumo responsabilita’ sull uso illecito del tool….usatelo su reti proprie ciau!

Paolo

July 20, 2010 at 11:52 pm Reply

Salve mi chiamo Paolo, dietro suggerimento di un amico posto qui la mia richiesta e mi scuso in anticipo. Da una settimana mi sono trasferito in vacanza e ho la disperata necessità di avere internet perchè mi serve sia per lavoro che per svago. Ho acquistato 2 chiavette ma niente, qui l’umts è defunto in questa zona. Dovrò rimanere quasi 2 mesi qui e non posso attivarmi assolutamente un abbonamento per diversi motivi. L’unica via sarebbe agganciarmi in una rete del vicinato, dal mio portatile rilevo 5-6 linee alice ma sono tutte protette, ho chiesto anche a qualcuno la cortesia (pagando) di farmi accedere alla wi-reless ma con una scusa o un’altra si rifiutano. Sono naturalmente disposto a pagare chiunque mi possa aiutare, capisco la situazione ma è l’unica soluzione che mi rimane. Spero che qualcuno mi contatti presto, la mia email è: paolo.brandi78@libero.it
Vi pregherei la massima serietà.

Marcofe

July 26, 2010 at 10:05 am Reply

Paolo che reti alice vedi?

Lol

January 7, 2011 at 11:33 am

E soprattutto, ci spieghi come hai postato questo messaggio?

wpa

August 2, 2010 at 2:30 pm Reply

Ho torvato questa rete, se puo’ essere di aiuto per calcolare K e Q di questa serie:

SSID: Alice-72361982
WiFi MAC: 00:1C:A2:1A:95:51

gijsaw

August 27, 2010 at 5:47 pm Reply

Tfdgczdvekz Uvslx! Yrz wrkkf le fkkzdf rikztfcf jl NzeDrxrqzev.. gvttrkf tyv efe trgzjtz le klsf uz hlvccf tyv yrz jtizkkf! C’zdgfikrekv v’ tyv kz yreef grxrkf svev. Retyv gvi uvtzwiriv hlvjkf dvjjrxxzf kz jvz wrkkf rzlkriv ur hlrctlef.

campo

September 7, 2010 at 8:50 pm Reply

Mac ethernet : 00:1D:8B:A7:15:C0
SN : 67902X0051618
ESSID : Alice-95499456

Qualcun’altro ha un SN per la serie Alice-95499456 ?

September 7, 2010 at 8:52 pm Reply

campo

Scusate volevo dire Alice-95xxxxxx

pezio5

September 8, 2010 at 1:16 pm
vai sul forum di gibit…

troppodifficil

September 14, 2010 at 10:43 pm Reply
Salve io ho in super router alice il mio ssid e: Alice-73519038 sfido a trovare la mia chiave ho provato i vostri programmi ma non me la trovano sono fortunato? o i router piu vecchi sono megli dei nuovi?

troppodifficil

September 14, 2010 at 10:46 pm Reply
Ola Salve io ho in super router alice il mio ssid e: Alice-73519038 sfido a trovare la mia chiave ho provato i vostri programmi ma non me la trovano sono fortunato? o i router piu vecchi sono megli dei nuovi?

lufuscu

September 15, 2010 at 10:31 am Reply
si vede che neanche hai letto l'articolo…

troppodifficil

September 16, 2010 at 10:58 pm
ho scoprto xke non ci riuscivo la mio roter non e pirelli il mio ssid e: Alice-73519038 e per questo che calcolaric all amno non funziona

fritz

September 20, 2010 at 9:02 pm Reply
Salve avrei un paio di problemi non riesco a capire come calcolare le incognite e il numero seriale sulle serie 38XXXXX 76XXXXXX e 45XXXXXX , mi sapreste dare una mano?

FABRYX

September 30, 2010 at 1:38 pm Reply
"Naturalmente per l'estrazione della WPA interessano solo i primi 24 byte dell'hash"
Scusate ma per ignoranza non riesco a capire, la mia wpa ha 64 caratteri.
ora riuscendo ad ottenere i primi 24 byte, il resto non serve o come lo ricavo????
grazie

Alex

October 14, 2010 at 8:11 am Reply
Ciao, ma non ho capito una cosa riguardo la prima parte: i numeri caricati in v0 e a3 nella seconda sezione sono costanti fisse o c'è un motivo particolare?

iceberg74

October 16, 2010 at 3:53 pm Reply
ragazzi aiuto…ma non capisco perchè quando avvio il programma e immetto ssdi non mi trova nessun mac probabile….e neanche nella ricerca manuale….come devo fare mi date per favore una mano nell'uso giusto del programma

November 25, 2010 at 9:24 am Reply
ciao pure a me succede la stessa cosa, e quando tento il calcolo

moro

seriale mi esce fuori un messaggio di errore del genere….. Cast non valido dalla stringa "" al tipo 'integer'.
il SSID di Alice è 76580515

moro

November 25, 2010 at 9:29 am

> **moro :**
> ciao pure a me succede la stessa cosa, e quando tento il calcolo seriale mi esce fuori un messaggio di errore del genere….. Cast non valido dalla stringa "" al tipo 'integer'.
> il SSID di Alice è 76580515

hacking tribe

October 21, 2010 at 12:13 am Reply
Bel lavoro come sempre ;)

Apollo

October 26, 2010 at 2:52 pm Reply
Ragazzi mi servirebbero i dati tabella di un Alice-63461153
Qualcuno li ha ?

Dave

November 11, 2010 at 3:49 pm Reply
CI SONO RIUSCITO FINALMENTE!!!!!

gianni

November 20, 2010 at 5:02 pm Reply
Ciao,
sono Gianni.
potresti aiutarmi a trovare il wpa di :
Alice-36167336 Mac 001d8b72c834 (visto con inSSIDer 2.o);
Alice-63973041 Mac 002553feb388.

Ti ringrazio anticipatamente.

P.s: dal terrazzo di casa mia, si vedono dei SSID. PARISI SATELLITE, con Vendor Cisco-Linksys LLC e Mac : 001a70341a50;
0018f8aa542f;
001dfe0995c8.
Come posso fare per trovare i wpa di questo ??

Lol

January 8, 2011 at 12:51 pm Reply
Ciao Gianni, non possiamo aiutarti, perché quello che vuoi fare tu non ha alcun senso.
Qua c'è gente che si diverte a scoprire come funziona la generazione delle chiavi WPA, tu invece vuoi solo entrare nella rete dei tuoi vicini.
Impara un minimo di programmazione e scriviti il tuo programma (come fanno la maggior parte di quelli che scrivono qui, io ad esempio ho un programma per windows e persino una bella IPA per iPhone), sennò non rompere il cazzo.

simone

November 28, 2010 at 7:20 pm Reply
riuscireste a trovare la chiave di questa rete?
alice-16712702

eneru

December 5, 2010 at 1:29 am Reply

Ragazzi nessuno dei valori di Q e k da risultato intero con:

Alice-37099405
Mac (Wi-Fi): 5C338E21D98D

silvio

December 10, 2010 at 10:34 pm Reply

ma per sapere per esempio la chiave di questa …

alice-63169297

e nn ce un programma che lo fa da se ?

che ho iniziato a fare 2 calcoli ma mi sono perso ancora prima di comminciare :))

Gianni

December 11, 2010 at 5:31 pm Reply

Qualcuno conosce questo ssid?
Alice-18937454
Mac: 001D883600CF

non l'ho mai visto ancora in giro..

giaba

January 4, 2011 at 3:58 pm Reply

finalmente la telecom si è decisa!! Adesso da la possibilità di cambiare la password predefinita con una personale. Notizia pervenuta dalla mia bolletta del telefono

Nino

January 11, 2011 at 10:03 am Reply

Salve,
qualcuno ha idea di quale possa essere il seriale di Alice-594xxxxx ? Oppure di Alice-766xxxxx ? Come mai nel config.txt non risultano? Qualcuno ha qualche idea, per metter fine al mio calvario? :D grazie, gentilissimi

roxdragon

January 12, 2011 at 12:58 am Reply

Complimenti, ma non ho ben capito come faccio a calcolarmi il S/N.
Ho l'SSID e MAC address a disposizione.
se applico la formula del SN… cioè (ssid-q/)k ma in questo caso non ho nemmeno la q..
e per calcolare la Q devo avere il SN..
Potete darmi delucidazioni? Grazie

blaster144

January 28, 2011 at 4:41 pm Reply

eureka
se qualcuno contesta la forza di questo gruppo vuol dire che non capisce l'essenza della ricerca e gli sforzi fatti
un saluto particolare a saxdax

blaster144

blaster144

January 28, 2011 at 4:44 pm Reply

se non capite l'essenza della ricerca lasciate perdere è facile criticare il lavoro degli altri se siete più bravi fatevelo voi
un saluto particolare a saxdax e tafo

blaster144

Dario

February 10, 2011 at 2:28 pm Reply

Scusatemi ma io non ho capito dal punto della sha256
Comunque, se può essere utile qui ci sono i parametri della 56 per confrontarli:
Alice-56339914
serie = 67902X0117778
k= 13
q= 54808800
mac= 0022335BADCA
La wpa, avendo ciò non ho capito come ricavarla !

kalaris

February 12, 2011 at 3:47 pm Reply

> **Dario :**Scusatemi ma io non ho capito dal punto della sha256Comunque, se può essere utile qui ci sono i parametri della 56 per confrontarli:Alice-56339914serie = 67902X0117778k= 13q= 54808800mac= 0022335BADCALa wpa, avendo ciò non ho capito come ricavarla !

sjgmc0d75hejhsc1rlpuq8r

Dario

February 16, 2011 at 7:39 pm Reply

E' giusta ma non ho capito come sommare i parametri magic sn e mac, per il resto mi è tutto chiaro

Dario

February 16, 2011 at 7:28 pm Reply

Ragazzi io non ho capito bene come sommare msgic sn e mac,
se io ho 54808800 67902X0117778 e 00223335BADCA la stringa, prima di essere criptata in sha256, come viene ?

Dario

February 16, 2011 at 8:41 pm Reply

Ah dimenticavo, qui ci sono tutti i parametri, perdonatemi se li incollo qui ma il link l'ho perso
Spero che siano tutti giusti, ne ho verificati solo alcuni.

"995,69102,13,99208960,001D8B"; 1
"966,69102,13,96214846,001D8B";
"965,69102,13,96214846,001D8B";
"964,67902,13,95026672,001D8B"; 1
"962,67902,13,95027335,001D8B";
"961,69102,13,96017051,001D8B";
"960,69102,13,96017051,001D8B"; 1
"958,67902,13,94829072,001D8B";
"957,67902,13,94831022,001D8B";
"956,67902,13,94831022,001D8B";
"955,67902,13,94828422,001D8B"; 3
"954,67902,13,94831022,001D8B";
"953,67902,13,94829137,001D8B";
"952,67902,13,94829137,001D8B"; 1
"951,67902,13,94829137,001D8B"; 1
"950,67902,13,94831022,001D8B"; 1
"950,67902,13,94830515,001D8B";
"949,67902,13,94830515,001D8B";

"948,67902,13,94830515,001D8B"; 1
"945,67901,13,92873664,001D8B"; 1
"943,67901,13,92873664,001D8B";
"938,69101,13,91472696,001D8B";
"936,69101,13,92723407,001D8B"; 1
"935,69101,13,92727307,001D8B"; 2
"933,67901,13,92016972,001D8B"; 1
"932,69101,13,93062432,001D8B";
"932,67901,13,92016972,001D8B";
"931,69101,13,92398366,001D8B";
"928,69101,13,92303856,001D8B";
"927,69101,13,92303856,001D8B";
"923,69101,13,92017687,001D8B"; 1
"922,67901,13,91105594,001D8B"; 1
"865,67901,13,85548341,001D8B"; 2
"864,67901,13,85548341,001D8B"; 1
"863,67901,13,85548341,001D8B";
"862,67901,13,85548341,001D8B";
"861,67901,13,85535341,001D8B";
"860,67901,13,85535341,001D8B"; 1
"858,67901,13,85518805,001D8B";
"857,67901,13,85518805,001D8B";
"857,69101,13,85507196,001D8B";
"82X,67901,13,82777468,001CA2";
"653,67904,8,62415297,002553"; 1
"649,67904,8,62415249,002553";
"648,67904,8,62415297,002553"; 1
"646,67904,8,62415297,002553"; 1
"645,67904,8,62415297,002553";
"642,69104,8,63703777,002553";
"641,67904,8,62254897,002553";
"639,67904,8,62254897,002553"; 1
"638,67904,8,62254897,002553"; 1
"637,67904,8,62246897,002553";
"636,67904,8,62246897,002553";
"636,67904,8,55226258,002553"; 1
"636,67904,8,62360145,002553";
"635,67904,8,62230897,002553";
"634,67904,8,62238897,002553";
"633,67904,8,62239057,002553";
"633,69104,8,62903297,002553";
"631,67904,8,62219249,002553";
"631,67904,8,62193097,002553";
"630,67904,8,62220849,002553"; 2
"629,67904,8,62220849,002553"; 1
"627,67904,8,61855721,002553";
"627,69104,8,62345169,002553";
"627,67904,8,62174801,002553"; 1
"626,69104,8,62345169,002553"; 3
"625,69104,8,62345169,002553"; 1
"624,69104,8,62345153,002553"; 1
"623,67904,8,61884537,002553";
"622,67904,8,61884537,002553";
"62X,67904,8,62174801,002553";
"588,69102,13,56695373,002233"; 1
"587,69102,13,56695945,002233"; 1
"586,69102,13,56695945,002233";
"585,67902,13,55485918,002233";
"584,67902,13,55485918,002233";
"583,67902,13,55485918,002233";
"582,67902,13,55485918,002233";
"581,69102,13,56332816,002233";
"580,69102,13,56332816,002233"; 2
"579,69102,13,56332816,002233";
"578,67902,13,55119942,002233"; 1
"577,67902,13,55119942,002233"; 2
"576,67902,13,55119942,002233";
"574,69102,13,55844913,002233";
"574,69102,13,55844900,002233";
"573,69102,13,55844913,002233";
"571,67902,13,54791692,002233";
"571,69102,13,55844900,002233";
"570,67902,13,54791692,002233"; 1
"569,67902,13,54809242,002233";
"569,67902,13,54805992,002233"; 1
"568,67902,13,54805992,002233";
"567,67902,13,54808800,002233";

"566,67902,13,54808800,002233"; 1
"565,67902,13,54808800,002233";
"564,67902,13,54808800,002233"; 1
"563,67902,13,54808800,002233";
"562,67902,13,54808800,002233"; 2
"561,69102,13,55052472,002233";
"560,67902,13,54809242,002233"; 1
"559,69102,13,54778588,002233";
"558,69102,13,54811868,002233"; 5
"557,69102,13,54811868,002233"; 1
"556,69102,13,54811868,002233";
"555,67904,8,55164449,002553";
"555,69102,13,54811868,002233";
"554,67904,8,55164449,002553"; 1
"553,67904,8,55164449,002553"; 1
"552,67904,8,55164449,002553"; 2
"551,67904,8,55164449,002553";
"551,67903,8,52420697,002553"; 1
"550,67903,8,52420697,002553"; 1
"550,67903,8,52420689,002553"; 2
"549,67903,8,52420689,002553"; 1
"548,67903,8,52420689,002553"; 1
"548,67903,8,52420673,002553"; 2
"547,67903,8,52420689,002553";
"546,67903,8,52420689,002553"; 3
"545,67903,8,52420689,002553";
"544,67903,8,52420689,002553";
"543,67903,8,52420689,002553";
"542,67903,8,52420673,002553"; 1
"542,67903,8,52420689,002553"; 3
"541,67903,8,52420689,002553";
"540,67903,8,52420689,002553"; 2
"539,67903,8,52420689,002553"; 1
"538,67903,8,52420681,002553";
"537,67903,8,52420681,002553"; 1
"536,67903,8,52420689,002553"; 2
"535,67903,8,52420689,002553";
"534,67903,8,52420681,002553"; 2
"533,67903,8,52420689,002553";
"532,69103,8,52845953,002553";
"531,69103,8,52845953,002553";
"530,67903,8,52196329,002553"; 1
"529,67903,8,52196329,002553"; 1
"528,67903,8,52196329,002553";
"527,67903,8,52196329,002553"; 1
"526,69103,8,52418353,002553";
"526,67903,8,52196329,002553"; 1
"525,69103,8,52418353,002553";
"524,69103,8,52418353,002553";
"490,69101,13,48968681,001CA2";
"487,67901,13,48559740,001CA2";
"483,67903,8,47896103,00238E";
"482,67903,8,47896103,00238E";
"481,67903,8,47896103,00238E"; 1
"480,67903,8,47896103,00238E"; 1
"479,67903,8,47955247,00238E";
"476,69102,13,43892099,00238E";
"476,69102,13,43892021,00238E"; 3
"475,69102,13,43892021,00238E"; 1
"474,69102,13,43892099,00238E";
"471,67902,13,39177168,00238E";
"470,67902,13,39184782,00238E"; 1
"470,67902,13,38678445,00238E";
"465,67902,13,39015145,00238E";
"464,67902,13,39014716,00238E";
"463,67902,13,39014716,00238E"; 1
"461,67902,13,39015145,00238E";
"460,67902,13,39010595,00238E";
"459,67902,13,39004095,00238E";
"458,67902,13,39010595,0017C2";
"457,67902,13,39010595,00238E";
"455,67902,13,39010595,00238E"; 1
"454,67902,13,39010335,00238E";
"453,67902,13,39010335,00238E"; 1
"451,67902,13,39010335,00238E";
"449,67902,13,38883455,00238E";
"448,67902,13,38883455,00238E";

“447,67902,13,38883455,00238E”;
“446,67902,13,38767105,00238E”; 1
“445,67902,13,38767105,00238E”;
“444,67902,13,38767105,00238E”;
“44X,67902,13,44156697,00238E”;
“430,67901,13,43008155,00238E”; 1
“427,69101,13,42667449,001CA2”;
“390,67902,13,33775765,00238E”; 1
“390,69102,13,35639029,00238E”; 1
“387,69102,13,35639029,00238E”; 1
“386,69102,13,35639029,00238E”; 3
“385,69102,13,35639029,00238E”;
“385,67902,13,33042526,00238E”;
“384,67902,13,33042526,00238E”; 1
“383,69102,13,35639029,00238E”; 1
“382,69102,13,35639029,00238E”;
“382,67902,13,33175048,00238E”;
“377,67902,13,33175048,00238E”; 2
“377,67902,13,33175058,00238E”;
“376,67902,13,33175048,00238E”; 2
“375,67902,13,33175048,00238E”;
“369,67902,13,32716668,00238E”;
“368,67902,13,32719840,00238E”;
“367,67902,13,32720035,00238E”; 1
“366,67902,13,32720035,00238E”; 1
“365,67902,13,32720035,00238E”;
“364,67902,13,32720035,00238E”; 1
“363,67902,13,32720035,00238E”; 1
“362,67902,13,32720035,00238E”;
“361,67902,13,32720035,00238E”;
“312,67904,8,28190287,38229D”;
“181,67902,13,17728255,00268D”;
“181,67902,13,14496838,00268D”;
“181,67902,13,13921842,00268D”;
“181,67902,13,14825009,00268D”;
“181,67901,13,16874837,00268D”;
“181,67902,13,17122778,00268D”;
“181,69102,13,16313301,00268D”;
“181,67904,8,17574389,00268D”;
“181,67904,8,18042064,00268D”;
“181,69102,13,17315130,00268D”;
“181,67902,13,15578953,00268D”;

Dario

February 16, 2011 at 8:44 pm Reply

> **Lol :**
> E soprattutto, ci spieghi come hai postato questo messaggio?

ahahahah

Dario

February 21, 2011 at 3:57 pm Reply

> **kalaris :**
>
> > **Dario :**Scusatemi ma io non ho capito dal punto della sha256Comunque, se può essere utile qui ci sono i parametri della 56 per confrontarli:Alice-56339914serie = 67902X0117778k= 13q= 54808800mac= 0022335BADCALa wpa, avendo ciò non ho capito come ricavarla !
>
> sjgmc0d75hejhsc1rlpuq8r

Ok ma potresti spiegarmi come viene la stringa prima di arrivare all’hash ? qual’è questa sequenza speciale ?

mike

March 6, 2011 at 4:13 pm Reply
63802809…32352411…57535875…86603990.doesn't work.

mike

March 6, 2011 at 4:15 pm Reply
63802809…32352411…57535875…86603990…wpa?pls.

Mod93

March 15, 2011 at 7:40 am Reply
Ciao ragá ho una rete Alice 751 e possibile sapare la wpa?? (anche a pagamento)!
Grazie

OpenCloud

April 6, 2011 at 12:37 pm Reply
IMPORTANTE!

Senti Ragazzi! Questa cosa e molto piu profondo, come sarebbe utilizzare vostro scoperta per tantissimi altri Pirelli router in giro in Europa. Per esempio, lo so che usano i Pirelli DRG A125G e DRG A226G, in paesi come Lithuania, Poland, Serbia, Grecia e Romania!! La cosa bello (o male se vuoi) e che questi router tutto l'usano le quasi-stessi Firmware, almeno cuando si inspetta le CONFIG file e le diversi FW image di quelli. Per farti capire, le diferenza degli WEP/WPA codice pre-produtto e molto simile di quelli spiegato qui (sul AGPF). Per esempio:

DRG A226G> conf show_wifi_data

SSID1: TEO-A1B2C3
WPA 738B4b709fBbFCfaadda68c955
WEP 738B4b709fBbFCfaadda68c955
SSID2: TEO1-A1B2C3
WPA 6AAa243575fC3cAe71A808Fde7
WEP 6AAa243575fC3cAe71A808Fde7

DRG A226G> conf show_wifi_data

SSID1: TEO-A1B2C3
WPA 94D1EB8E5421571Ca4C4A8264F
WEP 94D1EB8E54215

SSID2: TEO1-A1B2C3
WPA C22cBdb7CAeAF0BB3D98A13eBc
WEP C22cBdb7CAeAF

(Non-provatevi, le codici sopra e combiato degli veri!)
Come vedete, qui usano giá la seconda parte del MAC in ESSID e in piu usano soltanto HEX in WEP/WPA. Peró usano anche maiuscoli and minuscoli il lettere…

Volgio sapere come posso aiutarevi a trovare l'algorithmo del qesti due router??
Se volete mie aiuto, come faccio a contattarvi "Wifi Researchers"?

Finalmente, mi dispiace se ho pestato la vostra bella lingua…

Michele

April 6, 2011 at 9:41 pm Reply
Alice-35868206 prego dimilo

Michele

April 6, 2011 at 10:26 pm Reply
ALICE-35868206

OhWOWOW

April 28, 2011 at 6:27 pm Reply

O scusate ma non ho capito cos'è il magic number…
Da dove viene…?

OhWOWOW

April 28, 2011 at 6:30 pm Reply

O scusate ma non ho capito da dove viene sto magic number…
Cos'è…?

OEilà

April 28, 2011 at 6:33 pm Reply

O scusate ma non ho capito cos'è questa sequenza speciale…
Da dove viene…????

Dario

May 6, 2011 at 5:03 pm Reply

> **kalaris :**
>
> > **Dario :**Scusatemi ma io non ho capito dal punto della sha256Comunque, se può essere utile qui ci sono i parametri della 56 per confrontarli:Alice-56339914serie = 67902X0117778k= 13q= 54808800mac= 0022335BADCALa wpa, avendo ciò non ho capito come ricavarla !
>
> sjgmc0d75hejhsc1rlpuq8r

Ti prego è importante: mi dici che stringa hai criptato in sha256 ???

Drakeno

May 23, 2011 at 10:54 pm Reply

Innanzi tutto volevo fare i complimenti a tutti voi per il lavoro che avete svolto davvero notevole.
Volevo comunque chiedervi una cortesia e scusate la mia ignoranza c'è qualcuno che può spiegarmi l'ultimo passaggio da fare quello che tramite il serial il mac e il magic number calcola la wpa? Il mio prob è che non ho capito bene come funziona o cosa sia lo sha256 grz in anticipo e ancora complimentoni.

devis

July 7, 2011 at 12:50 am Reply

ciao ho un problema non trovo la password di alice-84788062
grazie
aiutatemi

lawy

July 16, 2011 at 3:49 pm Reply

hi
what is wpa for Alice-22288046
00:1C:A2:F0:3E:13
PIRELLI BROADBAND SOLUTIONS

alessia

July 25, 2011 at 3:56 pm Reply
mi puoi dire la wpa di qst adsl ke ti sto per dare:alicewifi.
nn riesco a farla xk al posto del codice es:alice-125y7…ce Alicewifi…
oppure se mi puoi consigliare un programma ke oltre al codice puoi scrivere anke le parole..

alessia

July 25, 2011 at 3:57 pm Reply
mi puoi dire la wpa di qst adsl ke ti sto per dare:alicewifi.
nn riesco a farla xk al posto del codice es:alice-125y7…ce Alicewifi…
oppure se mi puoi consigliare un programma ke oltre al codice puoi scrivere anke le parole

janclod

August 24, 2011 at 8:26 pm Reply
ma scusate che linguaggio di programmazione è quello usato per calcolare l'ssid dal mac adress?? che compilatore posso usare??

Stefano

November 3, 2011 at 5:56 pm Reply
Salve a tutti, spero di aver trovato la Salvezza!!!
Ho una rete Alice-18625742
ma non riesco a calcolare la wpa, in nessun modo.
mi potete aiutare????

moonserena

November 11, 2011 at 11:45 pm Reply
x favore mi calcoli alice-32518769 alice-20170846 sei un grandeee

raiden

November 13, 2011 at 1:11 am Reply
ciao e tutti.. ho un problema con alice AGPF:
-trovato il magic number 52420689
-trovato il Seriale 67903X0212845
-trovato il MAC 00255339DBB9
-realizzato l'algoritmo sha256() (che funziona, attraverso varie prove fatte anche su siti web ho dedotto de cripta in sha256)
come devo comporre sha256(5242068967903X021284500255339DBB9) ??
trasformare in binario il magic e il mac?
grazie

Dot Little Devil

February 16, 2012 at 6:30 pm Reply
è quello che sto tentando di capire anch'io!!

filippo

December 2, 2011 at 10:53 pm Reply
alice serie 32727233 cm fare?

Maurizio

December 21, 2011 at 11:39 am Reply
Alice-78677295 non riesco a connettermi. Ho paura che mio fratello abbia cambiato qualcosa senza dirmelo. Ho provato a trovare il WPA tramite qualche

programmino ma niente. Qualcuno potrebbe aiutarmi?

Grazie

PAUL

December 22, 2011 at 9:49 pm Reply

please help me wpa number for alice 46773688 mac 00238E5C6CC4

Giovanni

October 30, 2012 at 2:43 pm Reply

se mi dai il serial number completo te lo calcolo io

Dot Little Devil

January 23, 2012 at 4:11 pm Reply

Scusate, mi sa che ho perso qualcosa: quando impostate il sistema a 2 equazioni date per scontato che si conosca SN (cioè la seconda parte del seriale) ma non ho capito come lo ricavate?
Non so se è stato già spiegato tra i commenti ma sono così tanti che ritrovarlo è impossibile.
Anticipatamente grazie

nobodyx

January 26, 2012 at 9:05 am Reply

Ragazzi sto cercando di implementare l'algoritmo in c++.
Riesco a ricavare correttamente il mac e le costanti q e k, ma non capisco come devo passare la stringa ALIS+SN+MAC all'algoritmo!!

Dot Little Devil

February 16, 2012 at 12:02 pm Reply

> **nobodyx :**
> Ragazzi sto cercando di implementare l'algoritmo in c++.
> Riesco a ricavare correttamente il mac e le costanti q e k, ma non capisco come devo passare la stringa ALIS+SN+MAC all'algoritmo!!

Ciao a tutti, mi sa che la discussione qua è bella che chiusa già che nessuno ha risposto al mio primo commento ma ci provo lo stesso a fare qualche domanda.

Per chi, come me, non capisce molto di programmazione (e sono ottimista) per calcolare il codice hash si può usare uno di quei calcolatori che si trovano on line?

Se la risposta è si, in relazione all'esempio riportato nell'articolo "SSID: Alice-12345678, MAC: 00:23:8E:01:02:03 e SN: 67902X0587411", potete fare letteralmente "copia e incolla" di quello che avete inserito nel campo "dati" per ottenere il codice hash "b1d5d0dc8f3a2132d7872641250f998d53e58824ecb9118e046a943239bf1220"?

Se la risposta è no, ho capito che necessito di un programma di programmazione ma, se non chiedo troppo, è possible avere lo script (mi sembra d'aver intuito che sia questo il nome) da scrivere nel programma e, visto le difficoltà nel quote, anche la modalità di inserimento dei dati?

Di nuovo grazie.

temp1

April 13, 2012 at 8:08 am Reply

Scusate, ma ho una curiosità. Per aggiungere righe al file config.txt, se io conosco già la wpa del mio router alice ed il mio SSID, posso risalire a tutti i dati mancanti cioè SN e MAC ?
Saluti.

luca

April 25, 2012 at 8:42 pm Reply

programma alice wpa console

https://rapidshare.com/files/1033618168/Alix_console.rar

FaMa

August 5, 2012 at 1:15 pm Reply

> **raiden :**
> ciao e tutti.. ho un problema con alice AGPF:
> -trovato il magic number 52420689
> -trovato il Seriale 67903X0212845
> -trovato il MAC 00255339DBB9
> -realizzato l'algoritmo sha256() (che funziona, attraverso varie prove fatte anche su siti web ho dedotto de cripta in sha256)
> come devo comporre
> sha256(5242068967903X0212845 00255339DBB9) ?? trasformare in binario il magic e il mac?
> grazie

QUALCUNO RISPONDE???? non voglio la pappa pronta ma questo passaggio è davvero un buco nero!!! Ho addirittura fatto un brutalforce che tenta la combinazione dei tre dati in varie forme ma niente non da mai il risultato sperato (sia ben chiaro uso i dati dell'esempio!!!)…
DELUCIDAZIONI???

Berto

August 6, 2012 at 12:10 pm Reply

PRIMO non urlare, secondo, il magic number non lo devi trovare perché è sempre lo stesso.

FaMa

August 6, 2012 at 12:54 pm

Lo so!!! Il brutalforce tenta tutte le combinazioni tra maiuscole minuscole decimali, sono poche decine di combinazioni… so qual'è il magic number (ALIS) ma come diavolo vanno messi per far corrispondere i risultati???? e che nessuno risponda ALIS+SN+MAC perchè lo so!!!
Voglio sapere:
ALIS deve essere in formato byte… cioè??? esadecimale???
Maiuscolo??? minuscolo??? altro???
SN in formato stringa… Tutto? solo una parte? prima c'era scritto che d'ora in poi SN si sarebbe riferito alla parte dopo la x… vale ancora??? se non vale più e l'sn va messo tutto la x maiuscola?? minuscola???
il MAC di nuovo in formato byte… non mi ripeto… stesse domande di prima…
E comunque se nel messaggio precedente ho scritto 3 parole in maiuscolo non vuol dire che ho urlato vuol dire che volevo far risaltare quelle parole nel messaggio!!! (e che nessuno dica che nei forum il maiuscolo vuol dire urlare perchè lo so!)

cmq sono più di due anni che c'è quest'articolo e nessuno che spiega meglio questa cosa… non voglio l'algoritmo gia fatto ma solo una spiegazione più dettagliata su questo passaggio… grazie in anticipo… e che nessuno se la prenda…

Berto

August 6, 2012 at 12:34 pm Reply

Mi sembra che il forum sia morto (e in preda ai vari bimbominchia che postano l'SSID e vogliono la password), ma in ogni caso provo a condividere una mia riflessione. Analizzando la formuletta con cui si ricava la seconda parte del seriale (quella dopo la X) balza subito all'occhio che la parte numerica dell'SSID non può essere arbitraria. Infatti, se l'unico vincolo che la parte numerica dell'SSID deve avere fosse la lunghezza (8 cifre al massimo), in alcuni casi il seriale sarebbe un

numero frazionario. E poiché l'SSID dipende direttamente dal MAC, significa che non tutte le schede ethernet possono essere usate per costruire questi router. Mi spiego meglio con un esempio. Più in alto sono stati postati dei dati di esempio:

ESSID: Alice-37588990

MAC: 00:23:8E:29:51:FE

SERIAL: 67902X0339534

K: 13

Q: 33175048

Applicando la formula SN=(SSID-Q)/K ovvero SN=(37588990-33175048)=339534 si ottiene la seconda parte del seriale. Ma ipotizziamo di essere nella catena di montaggio del router. Il router prodotto prima di questo avrebbe la scheda di rete con MAC 00:23:8E:29:51:FD e di conseguenza con SSID Alice-37588989. Ma se provassimo a calcolare il seriale otterremmo SN=(37588989-33175048)=339533,923076923. Discorso simile per le schede di rete 00:23:8E:29:51:FC 00:23:8E:29:51:FB 00:23:8E:29:51:FA etc. La prima scheda "utilizzabile" tra quelle precedenti sarebbe 00:23:8E:29:51:F1. Insomma, la Telecom potrebbe produrre router utilizzando solo una scheda di rete su tredici (se k=13) o ogni 8. La cosa non mi sembra molto sensata, anche ammesso che la Pirelli/Telecom si producano da soli le schede. ringrazio chi ha avuto la pazienza di leggermi: il mio ragionamento si chiude qui. Per ora non porta da nessuna parte, spero che ispiri chi è più "smaliziato" di me nel trovare un algoritmo che collega direttamente il MAC al seriale.

mareeee

August 27, 2012 at 8:05 pm Reply

Ragazzi sto cercando password alice-76613613 wpa se trova il mio skaype rachid.rachid180

Alexandr

October 5, 2012 at 5:02 pm Reply

aiutate per favore a trovare la wpa del 32628817… mac — 64:87:D7:E5:E8:F4 ….programmi e liste che ci sono su internet non mi aiutano.. per la serie 32xxxxxx non c'e' nulla.. email: alexandr.vendetta@gmail.com

FaMa

October 6, 2012 at 10:37 am Reply

So qual'è il magic number (ALIS) ma come diavolo vanno messi per far corrispondere i risultati???? ALIS+SN+MAC lo so ma
ALIS deve essere in formato byte… cioè??? esadecimale??? Maiuscolo??? minuscolo??? altro???
SN in formato stringa… Tutto? solo una parte? prima c'era scritto che d'ora in poi SN si sarebbe riferito alla parte dopo la x… vale ancora??? se non vale più e l'sn va messo tutto la x maiuscola?? minuscola???
il MAC di nuovo in formato byte… non mi ripeto… stesse domande di prima…
non voglio l'algoritmo gia fatto ma solo una spiegazione più dettagliata su questo passaggio… grazie in anticipo…

Lili

October 17, 2012 at 3:50 am Reply

Non mi funziona. mi trovereste la pass di Alice-90703630 per favore? MOLTO Grazie

Simone

November 28, 2012 at 5:20 pm Reply

Qualcuno mi sa dire come reversare il bin del firmware con Ida pro ,
ho capito che il processore è un brodcom ed è un MIPS ….quando vado ad importarlo

non viene reversato …o meglio rimane esadecimale senza xref ecc.
Grazie

audzine.com

December 13, 2012 at 7:15 am Reply

Image 06. Re-gifting is a flawlessly satisfactory strategy to minimize waste following a principle with the Three or more Urs (Re-use, Decrease and Recycle) – provided those items you're re-gifting bring a few benefit to the people you intend to give the crooks to. Lessen your Carbon Impact: Travel, Purchasing & Holiday Cards – Minimizing the co2 presence is probably the very best actions during the holidays –especially with all the current vacation along with time you generally devote within vehicles, educates or aircraft.

nico

December 18, 2012 at 6:13 pm Reply

raga aiutatemi alice-32741993

Monstsa

January 4, 2013 at 3:29 pm Reply

Guys i need help please the router only sais Alice-Wlan67 please help how do i get the rest of the ssid.

murad resurgence promo code

January 14, 2013 at 6:08 am Reply

hello!,I really like your writing very a lot! percentage we keep in touch more approximately
your post on AOL? I need an expert in this house to resolve my problem.
May be that's you! Looking ahead to see you.

daniela

February 14, 2013 at 12:30 pm Reply

Alice-11728126
MAC: 00:17:C2:44:54:6E
Se qualcuno mi trova questa wpa pago 10 euro! (paypal o ricarica telefonica)
Grazie!

KevinMitNicl

March 27, 2013 at 4:48 pm Reply

> **????** :
> Avete provato l'algoritmo ragazzi?
> Di 4 ssid in mio possesso(serie 56xxxxxx e 96xxxxxx) non corrisponde neanche una chiave(e le wpa sono quelle di default!!!)…Mmha…

Infatti questi si credono dei veri e proprio hacker/cracker quando invece sono dei veri e propri troll… Il mondo fa schifo!

weight loss tips

June 30, 2013 at 9:04 pm Reply

Heya i'm for the primary time here. I found this board and I in finding It truly

useful & it helped me out much. I hope to give one thing back and help others like you aided me.

hi

August 8, 2013 at 12:04 am Reply

Piece of writing writing is also a excitement, if you know afterward you can write otherwise it is complex to write.

yakuza82

September 27, 2013 at 2:33 pm Reply

Alice 71791185……..mac wifi…02.21.00.13.b8.43..mi aiuta qualcuno con wpa ..???..grazzie!!

Get Your Foods Dried

January 18, 2014 at 10:53 pm Reply

Clean the frame with soap and water, rub mineral oil onto the frame to seal it, and then stretch cheese cloth, or 100 percent cotton material, around the frame and secure with a stapler.
A legend recommends that Roman militsry gain a flavor while stationed in Roman engaged Palestine and
urbanized a parallel food after recurring house.
A food dehydrator is being recognized as the catalyst that can
not only meet religious requirements butt allow one person to
effectively feed a mutitude with healthy, preserved, nutritious
food.

film seram jepang

March 7, 2014 at 12:57 pm Reply

Link exchange is nothing else however it is just placing
the other person’s website link on your page at suitable place and other person will also
do similar in support of you.

solar hot water heater kits

March 24, 2014 at 8:48 am Reply

You explained this superbly.

ropa bebe

May 14, 2014 at 3:38 am Reply

That is a really good tip particularly to
those new to the blogosphere. Short but very precise information… Appreciate your sharing
this one. A must read article!

solar hot water brisbane

October 17, 2014 at 11:48 am Reply

This information is worth everyone’s attention. How can I find out more?

Amazon Books

April 8, 2015 at 7:14 pm Reply

Microsoft and Unity technologies are working hard together to bring both the deployment options to developers using Unity as soon as possible. Various Friskies treats bounce around the screen and when touched by your cat, break into even more delicious treats, until 5 have been captured. As such, they are playable through any of the system’s browsers.

Marco

September 21, 2015 at 12:06 pm Reply

Io conosco l’algoritmo dei Telecom… ma non ve lo dico… eh eh eh!

Antoshkago

August 17, 2018 at 12:47 pm Reply

WEB-студия KONSULTANTE

rachelbi18

September 6, 2018 at 9:38 am Reply

Revitalized network invent:
http://edward.forum.telrock.net

Kate

October 15, 2018 at 8:30 am Reply

I’m Kate, girl, bisexual. I want to view a partaker without complexes. If I’m interested in you – Add me

p.s. my handle – katekitten

mobile

December 9, 2019 at 8:00 pm Reply

Thanks to my father who informed me regarding this weblog, this webpage is truly amazing.

#uristonline

December 20, 2019 at 11:41 am Reply

Привет
Увлекательная статейка про бизнес и реальные способы заработка, для тех кто хочет работать по совместительству или открыть свой бизнес
у кого мало опыта в бизнесе или хочет просто сменить место работы посмотрите на досуге https://moneymams.blogspot.com/

skiNauz

June 6, 2010 at 7:45 pm Reply

Ci mancava anche lo script pronto adesso….cosi’ anche i mega-lamer possono divertirsi(ed e’ la peggior razza)

skiNauzFucc

June 7, 2010 at 8:33 pm Reply

guarda tu con sto nick non puoi che andare a pascolare nei prati,
il fatto è che si fanno delle affermazioni, in più si mostra del codice, viene la voglia ed il gusto di verificare le cose…

skiNauz

June 7, 2010 at 8:47 pm Reply

Non so a cosa tu tu riferisca,ma questo nick l'ho inventato al momento,sicuramente non deriva dal fatto che sono nazista….anzi….casomai il contrario…capra!,comunque e sempre stato specificato di non postare script…ma qualcuno lo ha fatto lo stesso…..se volevano postare uno script lo avrebbero gia' fatto gli autori di questo blog…non pensi?..anche io ho fatto i miei bei script..ma me li tengo per me come la maggior parte delle persone qui penso…capito??? ….dimenticavo….SOOOOOKA!!!!

Freedom

June 14, 2010 at 1:43 pm Reply

Fuckin' nazi, continua a fare soffocotti invece di rompere a chi condivide informazioni!!

silvio

December 10, 2010 at 10:36 pm Reply

perche ce ? :))

skiNauzFucc

June 7, 2010 at 9:06 pm Reply

pascola pascola…
questo articolo non è full-disclosure… o fai una divulgazione come si deve o te ne stai zitto che fai più bella figura.
baci

ballard

June 7, 2010 at 9:20 pm Reply

Cos'e'… ti si e' incantato il disco(probabilmente nel culo):
o fai una divulgazione come si deve o te ne stai zitto che fai più bella figura.
Adesso l'ho detta io!!
E i baci mandali a tua sorella(la sufflonatrice)

skiNauzFucc

June 7, 2010 at 9:24 pm Reply

ahahh sei proprio un bimbominchia come il tuo compare.. la finisco qua per non dare corda ai troll…

Leave a Reply

Enter your comment here...

Telsey Fastweb: vulnerable!
Pirelli Fastweb – Free Access!

Top