"Hotspot WiFi: considerazioni tecniche dedotte da un'esperienza di wardriving"

Ricerca condotta da CSP - SecureLAB

L'IEEE 802.11b Working Group, come noto, ha standardizzato l'algoritmo di cifratura WEP (Wired Equivalent Privacy) con l'obiettivo di:

- assicurare che i sistemi Wlan avessero un livello di privacy equivalente a quello delle reti wired;
- fornire un meccanismo di autenticazione all'interno della rete.

Sono tuttavia ben presto emersi problemi di sicurezza legati al WEP che, supportati da studi effettuati da note università americane, hanno dimostrato l'inefficienza di tale architettura di sicurezza.

In particolare, la pubblicazione dell'articolo "Using the Fluhrer, Mantin and Shamir Attack to Break WEP" di Adam Stubblefield, John Ioannidis e Aviel D. Rubin (Agosto 2001) ha stimolato l'interesse degli sviluppatori "underground" del mondo open source. In breve tempo sono stati creati una serie di tool automatici (Kismet, WepCrack, Airsnort, solo per citare i più famosi), liberamente disponibili su Internet, in grado di effettuare uno scan delle reti wireless presenti, di "sniffare" i dati in transito, capire l'indirizzamento della rete, ottenere informazioni sull'identificatore della rete (SSID), individuare il Mac Address dell'AP e di conseguenza il corrispondente vendor e, soprattutto, in grado di recuperare la chiave WEP in uso.

In America prima, ed in Europa in seguito, la facilità di utilizzo di questi tool, abbinata alla possibilità di ricevere e trasmettere segnali radio in modo diffuso ed al di là dei limiti imposti da connessioni wired, ha generato il fenomeno del WarDriving (cui hanno fatto seguito il WarWalking, WarBiking, etc.).

Il WarDriving consiste nell'individuazione dei punti di accesso presenti sul territorio attraverso l'uso di apparecchiature quali un dispositivo portatile, un'antenna omni-direzionale ed una scheda wireless, nel corso di spostamenti in automobile nell'area interessata (ad esempio in un'area urbana precisa). In America il fenomeno si è diffuso a tal punto che è possibile reperire su Internet delle vere e proprie mappe di interi stati, in cui vengono evidenziati tutti i punti di accesso wireless presenti e le loro caratteristiche di sicurezza.

Il Laboratorio permanente SecureLab di CSP, in linea con i propri obiettivi di studio e ricerca in tema di sicurezza delle reti wireless 802.11b, ha condotto un'attività di scanning delle reti wireless presenti nel territorio urbano torinese.
L'analisi approfondita dei meccanismi di sicurezza implementati dalle varie società presenti sul territorio non ha ovviamente avuto lo scopo di "attaccare" le reti wireless presenti nella città, bensì quello di comprenderne la diffusione, verificare lo stato dell'arte dei meccanismi di sicurezza implementati, e dare visibilità ai potenziali rischi ed alle possibili vulnerabilità cui tali reti sono soggette.

"CSP – Innovazione nelle ICT" s.c.r.l.
Via Livorno, 60 - 10144 Torino
Tel. 011/4815111 Fax 011/4815001
info@csp.it; www.csp.it

L'analisi di SecureLAB si è svolta nel pieno rispetto dell'anonimato delle reti individuate, limitandosi alla fase di "stumbling" (ovvero di ricerca) e senza attestazioni non autorizzate sull'infrastrutture rilevate.

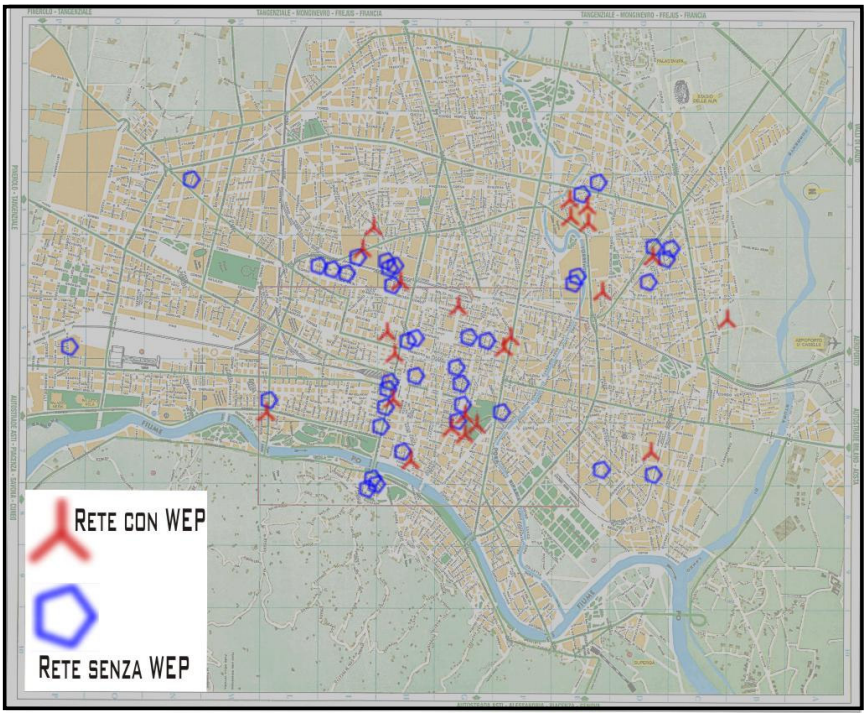
Il team, ha eseguito l'esperimento utilizzando le seguenti apparecchiature:

- N.° 2 power inveter per alimentare i notebook ed i palmari in auto
- N.° 2 notebook: uno equipaggiato con sistema operativo Linux ed uno con windows
- N.° 1 scheda Pcmcia Dlink Dwl650 + Antenna esterna 8.5 db
- N.° 1 scheda Pcmcia Cisco Aironet + antenna esterna 5 db
- N.° 2 rilevatori Gps

L'attività ha avuto la durata di 6 ore, durante le quali sono state analizzate le zone della città riportate nella tabella seguente:

MAPPA WLAN A TORINO			
ZONA	**# AP**	**AP con WEP**	**AP senza WEP**
Politecnico	10	3	7
Madonna di Campagna	7	2	5
Piero della Francesca	7	4	3
Porta Nuova	7	2	5
Centro Città	13	3	10
Crocetta	9	1	8
Mole Antonelliana	5	4	1
Porta Palazzo	3	2	1
Aree Industriali	6	2	4
TOTALE	**67**	**23**	**44**

I dati più significativi emersi dall'analisi riguardano l'alta percentuale di AP presenti sul territorio che non utilizzano cifratura WEP: fatta eccezione per contesti specifici (come aziende e zone ad alto densità di uffici) si è riscontrato che la maggior parte delle connessioni private sono sprovviste di qualunque tipo di sicurezza infrastrutturale.



L'assenza di cifratura WEP comporta per amministratori ed utenti un rischio elevato di subire intercettazioni del traffico in transito ed abusi della rete per finalità di qualunque genere (incluse attività illegali, con conseguenti implicazioni in termini di responsabilità).

TABELLA RIASSUNTIVA	
# Access point trovati	67
Reti ad hoc	6
Reti Infrastructure	60
Reti con WEP	23
Reti senza WEP	44
Reti a 22 Mbps	1
Reti a 54 Mbps	2
Reti che nascondono il SSID	9
Km percorsi	130
Area analizzata di Torino	40%

Dai dati emersi, inoltre, si riscontra una maggior densità di apparati Wi-Fi nel centro urbano e nelle zone notoriamente più portate a sperimentazioni tecnologiche vista la presenza di Università e centri ed aziende di settore.

Concludendo, il numero significativo di reti rilevate dall'analisi condotta sul territorio torinese è indicativo di un settore ICT fortemente ricettivo verso la sperimentazione e l'introduzione di nuove tecnologie per l'ottimizzazione dei processi aziendali e dei servizi agli utenti.
Parallelamente, lo scarso impiego di meccanismi di sicurezza, rilevato nell'indagine, evidenzia la necessità di dare avvio a campagne di informazione, rivolte ad amministratori di rete, con obiettivi di incremento della sicurezza delle infrastrutture e per ridurre il più possibile i rischi di intercettazione ed abuso.

SecureLAB: Laboratorio permanente sulla Sicurezza Informatica

SecureLAB è il laboratorio permanente di *CSP - Innovazione nelle ICT* s.c.ar.l dedicato agli aspetti di Sicurezza Informatica e costituito a gennaio 2001.
All'inizio del 2003 il CSP ha firmato un contratto quadro con il Dipartimento di Informatica e Automatica del Politecnico di Torino per la formalizzazione di un rapporto di collaborazione nelle attività di ricerca inerenti la Sicurezza Informatica, che vede la direzione scientifica del prof. Antonio Lioy.
Il laboratorio svolge, in tema di sicurezza, attività di sviluppo, sperimentazione, trasferimento tecnologico e progettazione.
Le attività del laboratorio si articolano secondo tre aree tematiche principali:

- Sicurezza Applicativa
- Sicurezza Infrastrutturale
- Sicurezza Mobile

La *Sicurezza Applicativa* è l'area tematica che raccoglie tutte le attività volte ad integrare funzionalità di sicurezza all'interno delle applicazioni, fornendo a queste ultime soluzioni allo stato dell'arte per le problematiche di integrità, autenticazione e riservatezza dei dati.
In dettaglio, le esperienze e il know-how maturato dal laboratorio in questo ambito riguarda i seguenti argomenti:

- Public Key Infrastructure (PKI) X.509 e servizi di CA
- Firma Digitale e Crittografia
- Smart Card e dispositivi crittografici
- Privilege Management Infrastructure (PMI) X.509v4

La *Sicurezza Infrastrutturale* è l'area tematica in cui vengono trattati gli aspetti di sicurezza delle reti e dei sistemi.
Le attività principalmente svolte riguardano attività di test di sistemi firewall commerciali con particolare riferimento al grado di compatibilità nella realizzazione di VPN (Virtual Private Network) con tecnologie IPSec.
Altre attività riguardano le nuovissime problematiche di firewalling in IPv6 e i sistemi di Intrusion Detection (IDS) su reti a larga banda (Gigabit).

La *Sicurezza Mobile* raccoglie tutte le attività inerenti le problematiche di sicurezza nelle reti mobili. Si tratta di un ambito di interresse nuovo che è iniziato nel 2002 con una attività di ricerca sulle problematiche di sicurezza in ambito wireless 802.11b.
Nel corso dell'anno si è anche caratterizzata da una attività di trasferimento tecnologico che ha permesso di effettuare uno studio delle problematiche di sicurezza in ambito GSM/GPRS e UMTS.
Da pochi mesi è stata anche avviata una attività volta alla sperimentazione su aspetti di sicurezza nelle architetture satellitari e in particolare quelle basate sugli standard DVB (Digital Video Broadcasting) e DVB-RCS (DVB with Return Channel System).
Altre attività di interesse svolte in questo ambito riguardano la sicurezza delle trasmissioni multicast (alla base delle reti satellitari) e le soluzioni di DRM (Digital Rights Management) per la protezione dei diritti d'autore sui contenuti digitali.

Sicurezza delle wireless LAN – Attività in corso

In questi ultimi anni si è potuto assistere ad un crescente interesse da parte della società dell'informazione per tecnologie di accesso alle risorse di rete che siano in grado di supportare la mobilità degli utenti.
Le wireless LAN (basate sullo standard 802.11b) rappresentano la tecnologia più diffusa per questo tipo di applicazioni.
A fronte di tale interesse, è emersa l'esigenza di garantire anche agli utenti mobili un adeguato livello di sicurezza per le trasmissioni radio, che di per sé utilizzano un mezzo trasmissivo intrinsecamente condiviso e pervasivo, quindi a maggior ragione potenzialmente vulnerabile.
SecureLAB ha avviato nel 2002 una attività di ricerca il cui scopo è stato quello di delineare lo scenario tecnologico e lo stato dell'arte in merito alle soluzioni di sicurezza in queste tipologie di reti. Inoltre sono state effettuate diverse tipologie di attività sperimentali:

- Realizzazione di attacchi informatici documentati verso una rete sperimentale
- Test di robustezza condotti su un campione di schede wireless disponibili sul mercato
- Attività di war-driving per il censimento delle reti wireless presenti nella città di Torino

SecureLAB partecipa al progetto denominato "Wireless Campus". Si tratta di una iniziativa congiunta tra *CSP – Innovazione nelle ICT* e *Environment Park* (Parco scientifico e tecnologico per l'ambiente, che accoglie aziende ed Enti di ricerca nei settori dell'innovazione tecnologica e dell'eco efficienza) finalizzata alla progettazione e messa in opera di una rete wireless. Il progetto è volto a fornire connettività wireless alle diverse aziende presenti nel campus, mantenendo un livello di sicurezza tale da fornire accesso controllato e riservatezza dei dati.

"CSP – innovazione nelle ICT" è un centro di eccellenza per la ricerca, sviluppo e sperimentazione di tecnologie informatiche e telematiche. Società consortile di diritto privato, ne fanno parte sia organismi della Pubblica Amministrazione che istituzioni universitarie e rappresentanti del mondo imprenditoriale piemontese.
CSP opera sia nel panorama nazionale che internazionale, agendo da facilitatore fra la pubblica amministrazione, il mondo delle imprese e le istituzioni universitarie e della ricerca.

Un forte rapporto con il mondo della ricerca
CSP mette a disposizione dei propri clienti e partner competenze qualificate, che spaziano dalla progettazione e sperimentazione tecnologica di sistemi IT e infrastrutture di telecomunicazione, al supporto strategico progettuale in ambito di Nuovi Media, promozione dell'Information Society, Community e ICT-based Professional Networks, allo sviluppo prototipale di servizi evoluti.
Professionisti di alto profilo, supportati da collaborazioni consolidate con rappresentanti del mondo accademico attraverso laboratori congiunti (WTLab, InLab, SecureLab e M3Lab), fanno di CSP un centro in grado di individuare gli scenari evolutivi del mondo delle ICT e di trasferire le tecnologie ai processi.

"CSP – Innovazione nelle ICT" s.c.r.l.
Via Livorno, 60 - 10144 Torino
Tel. 011/4815111 Fax 011/4815001
info@csp.it; www.csp.it