



Raoul Chiesa
Chief Technical Officer

Maurizio Agazzini
Security Analyst

Divisione Sicurezza Dati
@ Mediaservice.net Srl

SEMINARIO CLUSIT

BROADBAND E WIRELESS
opportunità di business e sfide di
sicurezza per un mondo in movimento
Sessione Pomeridiana

Venerdì 27 Settembre 2002
Milano, Star Hotel Splendido



Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altro utilizzo o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

(C) 1997-2002 @ Mediaservice.net Srl

▶ **Agenda della sessione tecnica**

▶ **Relatori**

14.30 I - INTRODUZIONE AL WIRELESS

Raoul Chiesa

**15.15 II - WIRELESS: ANALISI DEI
PROBLEMI**

Maurizio Agazzini

16.00 Coffee Break


**16.15 III - WIRELESS: LE CONTROMISURE,
ANALISI E CONFRONTO**

Fabrizio Croce

**17.00 IV - WIRELESS ATTACKS:
DIMOSTRAZIONE PRATICA**

Maurizio Agazzini

17.15 Q&A, Contacts, Thanks



WIRELESS INTRO: Breve introduzione ai dispositivi senza fili

SEMINARIO CLUSIT

BROADBAND E WIRELESS
opportunità di business e sfide di
sicurezza per un mondo in movimento
Sessione Pomeridiana

Venerdì 27 Settembre 2002
Milano, Star Hotel Splendido





The Company

(a few words 'bout us)

- **System Integrator established in 1997**
- **D.S.D. (Data Security Division) since 1998**
- **Wide Background, Direct Experience**
- **Internal Tiger Team**
- **Specialized Focus**
- **Underground Security Vision**
- **Strong R&D**
- **Vendor Independent**

Cos'è il wireless

- Con il termine wireless viene inteso qualsiasi dispositivo in grado di comunicare con un altro senza l'ausilio di fili fra di essi.



Tipi di tecnologie wireless

- Radio Device
 - Basato su onde radio
 - Utilizzato da dispositivi di input come mouse e tastiere
- IrDA
 - Infrared Data Association
 - Basato su infrarossi e quindi conseguentemente su uno spazio visivo




Tipi di tecnologie wireless

- Bluetooth
 - Basato su onde radio
 - Primi dispositivi disponibili nel 2000
 - Spazio di utilizzo molto limitato
- IEEE 802.11 (1a Generazione)
 - Basato su onde radio
 - Velocità di 1-2Mb/s



Tipi di tecnologie wireless

- IEEE 802.11b (2a Generazione)
 - Velocità 11Mb/s
- IEEE 802.11g (3a Generazione)
 - Velocità 22Mb/s
 - Non è uno standard

A large, blurred image of a human eye, looking directly forward, occupies the upper half of the slide. The eye is rendered in grayscale and is out of focus, creating a sense of depth and mystery.

Sicurezza informatica in azienda

(le connessioni di ieri e di oggi)



Connettività aziendale

- Fino ad oggi
 - Broadband
 - ADSL (Asymmetric Digital Subscriber Line)
 - HDSL (High Bit-Rate Digital Subscriber Line)
 - R-ADSL (Rate-Adaptive Digital Subscriber Line)
 - SDSL (Symmetric Digital Subscriber Line)
 - VDSL (Very High Bit-Rate Digital Subscriber Line)
 - Fibra ottica
 - Il vecchio CDN
 - Il quattro fili
- Oggi
 - 802.11x



Problematiche di sicurezza

- Virus
 - Perdita di dati
 - Divulgazione di dati riservati
- Worm
 - Perdita di dati
 - Divulgazione di dati riservati
- Crackers
 - Perdita dei dati
 - Divulgazione di dati riservati
 - Vendita di informazioni ad attività concorrenti



HACKING: Classificazioni (1/3)

PROFILO PSICOLOGICO

Wannabe Lamer

(Vorrei essere hacker ma non ci riesco....)

Script Kiddie

(Il ragazzo degli script)

Cracker

(Terra bruciata, il Distruttore)

Ethical Hacker

(L'Hacker "Etico")

Quiet, paranoid, skilled hacker

(L'hacker taciturno, paranoico, specializzato)

Cyber-Warrior

(Il mercenario, hacking a pagamento)

Industrial Spy

(La spia- Spionaggio industriale)

Government agent

(L'agente governativo, CIA, Mossad, FBI, etc..)

LIVELLO DI PERICOLOSITA'

NULLO

BASSO

ALTO

MEDIO

MEDIO

ALTO

ALTO

ALTO



HACKING: Classificazioni (2/3)

PROFILO PSICOLOGICO

Wannabe Lamer

Script Kiddie

Cracker

Ethical Hacker

Quiet, paranoid, skilled hacker

Cyber-Warrior

Industrial Spy

Government agent

REATI

Nessuno

Nessuno/615 ter

635 bis/615 ter,quater,quinquies/420 c. 2

615 quater/615 ter

615 quater/615 ter/ (635)

615 quater,ter/640 ter Frode informatica

come sopra + eventguali aggravanti

come sopra + eventuali aggravanti



HACKING: Classificazioni (3/3)

PROFILO PSICOLOGICO

Wannabe Lamer

Script Kiddie

Cracker

Ethical Hacker

Quiet, paranoid, skilled hacker

Cyber-Warrior

Industrial Spy

Government agent

TARGET

End-User

PMI/vulnerabilità specifiche

Grandi aziende/P.A./Finance/Telco

Vendor/System Integrator/Telco

Grandi aziende/P.A./Finance/Telco

Multinazionali “simbolo”

Multinazionali, ICT

Multinazionali/Government



... possibili soluzioni

- Firewall
- DMZ (De Militarized Zone)
- xIDS (Intrusion Detection System)
- Formazione di base agli impiegati
- Aggiornamento continuo dei sistemi

WIRELESS NETWORK, 802.11b: Analisi dei Problemi

SEMINARIO CLUSIT

BROADBAND E WIRELESS
opportunità di business e sfide di
sicurezza per un mondo in movimento
Sessione Pomeridiana

Venerdì 27 Settembre 2002
Milano, Star Hotel Splendido





Analisi delle problematiche tecniche

Broadcast network

- “Tutto arriva a tutti” (FM Radio :)
- Il campo di azione non è controllabile
- Algoritmi di cifratura deboli e mal implementati



Il WEP (Wired Equivalent Privacy)

- Basato su RC4
 - Ron Rivest (<http://theory.lcs.mit.edu/~rivest/>)
 - Tenuto segreto per 7 anni
 - Divulgato da anonimi in circostanze misteriose
 - Algoritmo molto semplice
 - Conseguentemente gli algoritmi di decrypting possono raggiungere alte velocità



Il WEP (Wired Equivalent Privacy)

- Utilizzo di chiave simmetrica
 - Stessa chiave sia per il mittente che per il destinatario
 - Tutti i PC utilizzano la stessa identica chiave
 - Impossibilità di cambi chiave soventemente
 - Coloro che hanno accesso ai pc hanno accesso alla chiave



Il WEP (Wired Equivalent Privacy)

- Errori di implementazione dell'algoritmo di cifratura (quindi progettuale a livello di definizione dello standard)
 - Alcuni errori di implementazione delle chiavi permettono di riuscire ad intuire alcune parti della chiave
- Utilizzo di chiavi deboli (40 e 128 bit)
 - Lunghezza delle chiavi ormai ritenute deboli
 - Dovuto allo studio del protocollo alcuni anni fa, ma diffuso ed implementato solo ora



Generazione di chiavi “sicure”

- Una chiave wep di solito viene generata grazie ad una passphrase o una semplice password
 - L’implementazione del WEP ha problematiche con alcuni tipi di chiavi
 - La generazione non deve essere fatta in questo modo ma in un modo sicuro
 - Utilizzo di tools specifici



Accessi non autorizzati

- Possibili intrusioni casuali
 - Hackers curiosi (ingenuous hacking)
 - Censimento reti wireless in una città
 - Script Kiddies
- Possibili intrusioni non casuali
 - Terrorismo, Company resources Abuse
 - Spionaggio industriale (malicious hacking)



Metodi di intrusione

- Utilizzo di schede wireless, modificate e non, in maniera da rintracciare Access Point anche a distanze non normali, grazie a speciali antenne
 - WarDriving
 - Utilizzo di una vettura come copertura e per lo spostamento
 - WarWalking
 - Non si utilizza nessun mezzo di trasporti
 - War* (biking, public bus,)



DHCP

(Dynamic Host Configuration Protocol)

- Il DHCP è un protocollo il quale si occupa di assegnare gli indirizzi ip della rete. Questo avviene tramite un server che si occupa della gestione degli indirizzi già assegnati e tramite richieste di ARP (Address Resolution Protocol) “speciali”

DHCP

- Rende più semplice i possibili attacchi
 - Grazie ad una richiesta di ARP viene assegnato un ip valido
 - Questa non è una reale problematica, è solo questione di tempo, intercettando traffico si può comunque capire quali sono i range di ip utilizzati nella rete: rallenta il TTA (Time To Attack)



Problematiche dell'utilizzo di onde radio

- L'utilizzo di onde radio non permette di controllare l'esatta propagazione del segnale
 - Il segnale non essendo controllato si diffonde nell'ambiente circostante, e arriva anche a distanze molto maggiori, seppur molto debole
 - Grazie a speciali antenne è possibile amplificare il segnale in entrata e in uscita annullando così la debolezza



Tipi di infrastrutture

- BSS
 - Un Access Point al quale una o più schede wireless si collegano
- IBSS (Bridged Architecture)
 - Un'insieme di Access Point collegati fra loro che formano una grande rete, alla quale una o più schede wireless si collegano

Tipi di infrastrutture

- Ad-Hoc
 - Non esistono Access Point, la rete è fatta solo ed esclusivamente da schede wireless che comunicano fra di loro.



Unauthorized Bridges

- Con il termine “Authorized Bridge” intendiamo la simulazione completa di un Access Point in modo che il secondo Access Point ci veda come AP pre-esistente e quindi autorizzato

Sicurezza Fisica

- Perché la sicurezza fisica infierisce con quella informatica
 - Il potere della “Console”
- Cosa può voler dire un'intrusione fisica
 - Le Password con i post-it sui monitor
- Formazione di base sulla sicurezza informatica mirata a tutti i dipendenti (security awareness)

WIRELESS ATTACKS:

Dimostrazione Pratica

SEMINARIO CLUSIT

BROADBAND E WIRELESS

opportunità di business e sfide di
sicurezza per un mondo in movimento

Sessione Pomeridiana

Venerdì 27 Settembre 2002
Milano, Star Hotel Splendido



Le schede wireless

- Utilizzo di schede wireless con uscita per antenne esterne, o modificabili. Si preferiscono le più diffuse per il supporto driver su tutti i sistemi operativi
 - DLINK (PRISM II)
 - CISCO (Aironet)

Le antenne

- Le antenne sono un componente di base, più l'antenna è potente e ben fatta più la distanza di trasmissione è maggiore
 - Antenne comprate
 - Alto costo
 - Antenne “fai da te”
 - Basso Costo
 - Prestazioni migliori in alcuni casi



Il Sopralluogo

- La ricerca del segnale
- Il posizionamento dell'antenna in maniera da capire dove si trova l'Access Point
- La ricerca di un posto tranquillo per poter sferrare un attacco

L'attacco

- Reti in chiaro
 - Autenticazione sull'Access Point
 - Analisi della rete
- Reti in criptato
 - Cracking del WEP
 - Autenticazione sull'Access Point
 - Analisi della rete



Target maggiormente a rischio

- Reti WiFi “in test”
- Privati (PSTN, ADSL ->BB)
- Strutture pubbliche
- Università
- P.A.



@ Mediaservice.net Srl

Divisione Sicurezza Dati

WIRELESS (in)Security

27 settembre 2002, Milano

Relatori

Raoul Chiesa

Maurizio Agazzini

Riferimenti

<http://@Mediaservice.net>

info@Mediaservice.net (general)

dsd@Mediaservice.net (the tech guys)

...and the old phone is still there: +39-011-32.72.100



Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altro utilizzo o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

(C) 1997-2002 @ Mediaservice.net Srl