

Wireless Security: sempre i soliti problemi

Danilo Bruschi

Università degli Studi di Milano

Dove sono i problemi?

- Sistemi wireless (portatili, PDA, cellulari)
- Protocolli di comunicazione wireless (IEEE 802.11x)

Sistemi: PDA-Windows CE

- Sono stati recentemente individuati i seguenti problemi:
 - DoS per evitare la sincronizzazione tra PDA e PC via rete (TCP port 5679)
 - KOD (kiss of death) individuato nei sistemi W98/2000 nel 1999, blocca la connettività del PDA
 - Trivial TCP initial sequence number (1985)

Protocolli di comunicazione (1)

- Primi anni '80
 - Ethernet (poi IEEE 802.3) si diffonde come standard de facto, tra i protocolli di comunicazione per LAN basate su canale di comunicazione multi-accesso
 - Ethernet poggia le sue radici su Aloha protocollo per comunicazioni tra radio stazioni

Protocolli di Comunicazione (2)

- Fine anni '80 fanno la loro apparizione nell'ambito delle reti Ethernet i primi programmi per:
 - Sniffing
 - MAC – address spoofing
- Sino all'introduzione dello switching, le Lan restano il “parco giochi” degli hacker

Protocolli di comunicazione (3)

- Fine anni '90
 - Si diffonde il protocollo IEEE 802.11 per le comunicazioni wireless
- Al fine di evitare i problemi riscontrati con il protocollo 802.3 vengono adottati:
 - SSID (Service Set Identifier)
 - MAC address Restrictions
 - WEP (Wired Equivalent Privacy)

Protocolli di comunicazione (4)

- Immediatamente si scopre che:
 - SSID viaggia in chiaro e può essere facilmente intercettato
 - I MAC address sono a loro volta intercettabili ed usati con tecniche di spoofing
- Nel 2001 vengono scoperti banchi implementativi di WEP

Protocolli di Comunicazione

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP

AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001

Authors

[Adam Stubblefield](#)

[John Ioannidis](#)

[Aviel D. Rubin](#)

Abstract

We implemented an attack against WEP, the link-layer security protocol for 802.11 networks. The attack was described in a recent paper by Fluhrer, Mantin, and Shamir. With our implementation, and permission of the network administrator, we were able to recover the 128 bit secret key used in a production network, with a passive attack. The WEP standard uses RC4 IVs improperly, and the attack exploits this design failure. This paper describes the attack, how we implemented it, and some optimizations to make the attack more efficient. We conclude that 802.11 WEP is totally insecure, and we provide some recommendations.

Text

[PostScript](#)

[PDF](#)

Conclusioni

- Premesso che gli esempi precedenti sono l'ennesima conferma delle seguenti affermazioni:
 - Per fare sicurezza non è sufficiente essere consapevoli del problema
 - Saper fare sicurezza non è cosa semplice
 - Nella sicurezza non è vero che “sbagliando si impara” ma piuttosto “chi sbaglia persevera”

Conclusioni

- **IL LAVORO CHE CI ATTENDE E'
DAVVERO TANTO**
(speriamo che qualcuno lo sappia apprezzare)