ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Wireless Security

Sicurezza, Privacy e Audit delle reti Wireless

Giancarlo Castorina – CISA, CISSP

Giancarlo.Castorina@acm.org

INDICE DELLA PRESENTAZIONE :

- Pianificazione
  - Analisi dei rischi
  - Security Policy
- Implementazione
- Monitoraggio
  - Auditing

Analisi dei rischi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Intercettazione del traffico
- Accesso illecito alla rete
- Denial of Service
- Furto o perdita dei dispositivi mobili
- Access Point “impostori”
- Connessioni automatiche e indesiderate
- Gestione dei dispositivi

Contromisure

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Intercettazione del traffico
  - Giusta collocazione degli Access Point
  - Tipo e potenza delle antenne
  - Uso di crittografia (WPA) e/o VPN
- Accesso illecito alla rete
  - Autenticazione 802.1X
  - Qualità delle password e/o strong authentication

Contromisure

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Denial of Service
  - Prevenzione interferenze
  - Identificazione / risposta ad attacchi
- Furto o perdita dei dispositivi mobili
  - Cambiamento periodico di password / chiavi
  - Uso di crittografia per proteggere i dati

Contromisure

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Access Point “impostori”
  - Mutua autenticazione
  - Sistemi di rilevamento
- Connessioni automatiche e indesiderate
  - Disabilitare connessioni auomatiche
  - Disabilitare i dispositivi se non necessari
  - Personal Wireless Firewall
  - Evitare connessioni a reti non protette

Contromisure

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Gestione dei dispositivi
  - Modifica di account e password di amministrazione
  - Evitare connessioni non protette (http)
  - Gestione sicura degli alert (syslog, SNMP)

Wireless Security Policy

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Installazione e configurazione dispositivi
- Configurazione della rete Wireless ed integrazione con la rete Wired
- Modalità di accesso alla rete Wireless per utenti interni ed esterni
- Gestione credenziali di autenticazione
- Monitoraggio
- Educazione degli utenti

Wireless Security Policy

- Wireless Security Policy é raccomandata anche nei siti ove la tecnologia non è utilizzata
  - Vietare l'uso di dispositivi wireless connessi alla rete
  - Educazione utenti dotati di dispositivi che possano connettersi a reti wireless (laptop, palmari)

- Verifica funzionamento della rete (access points, wireless routers/gateways)
- Traccia degli accessi
- Identificazione Access Point impostori
- Controllo configurazione e utilizzo di autenticazione / crittografia
- Verifica cambiamento periodico di password / chiavi
- Gestione log ed integrazione con sistemi di analisi centralizzati

INDICE DELLA PRESENTAZIONE :

1. Introduzione alle tecnologie Wireless
2. Architettura reti IEEE 802.11 (Wi-Fi)
3. Sicurezza reti Wi-Fi

4. Gestione e auditing reti Wireless
5. Bluetooth
6. RFID

7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

Bluetooth

Bluetooth

- Tecnologia Wireless a corto raggio (10-100 metri)
- WPAN (Wireless Personal Area Network)
- Ideato da Ericsson
- Standardizzato come IEEE 802.15
- Supportato in svariati dispositivi (palmari, telefonini, laptop, stampanti, cuffie, ecc.)

Caratteristiche Bluetooth

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Dispositivi classe 3: fino a 1 metro
- Dispositivi classe 2: fino a 10 metri
- Dispositivi classe 1: fino a 100 metri

- Data rate: 1 Mbps (Version 1.2), 3 Mbps (Version 2.0 + EDR)

Piconet – La rete Bluetooth

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- I dispositivi bluetooth si localizzano automaticamente e si associano in una rete ad-hoc (piconet)
- Un dispositivo svolge il ruolo di *master*
- Gli altri dispositivi (sino a 7) svolgono il ruolo di *slave*

Architettura Bluetooth

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Bluetooth adotta un'architettura service-oriented
- Ciascun dispositivo espone dei servizi che possono essere rilevati tramite il *Service Discovery Protocol* ed utilizzati
- Il trasporto può essere asincrono (ACL) per i dati o sincrono (SCO) per la voce

Sicurezza Bluetooth

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Discovery
  - Un dispositivo può essere impostato come “nascosto”; esiste però la possibilità di individuarlo ugualmente
- Autenticazione
  - *Stored Link Key* o *pairing (PIN)*
  - Vengono autenticati i dispositivi

- Autorizzazione
  - Un servizio può essere bloccato in assenza di autenticazione o di autorizzazione
  - *Trusted devices* (relazione predefinita) possono accedere a qualunque servizio
  - 3 *Security Mode:*
    - *Security Mode 1*: nessuna sicurezza
    - *Security Mode 2*: a livello di servizio
    - *Security Mode 3*: a livello di link
- Crittografia

Vulnerabilità Bluetooth

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Perdita di informazioni
  - Dispositivi mal configurati possono permettere il trasferimento di informazioni riservate (ad es. rubrica)
  - http://www.thebunker.net/security/bluetooth.htm
- Utilizzo abusivo
  - Invio di SMS o MMS senza autorizzazione (a carico e sotto la responsabilità di altri)
- Tracciabilità
  - Possibilità di individuare e tracciare i movimenti di persone con indosso dispositivi Bluetooth
- Speciali antenne permettono di estendere il raggio della tracciabilità fino a 500m

Vulnerabilità Bluetooth

- Si tratta per lo più di vulnerabilità dovute a:
  - errori nella implementazione Bluetooth di produttori (firmware di telefonini o sistemi operativi di palmari)
  - Cattiva configurazione o utilizzo (mai accettare connessioni sconosciute!)

INDICE DELLA PRESENTAZIONE :

1. Introduzione alle tecnologie Wireless
2. Architettura reti IEEE 802.11 (Wi-Fi)
3. Sicurezza reti Wi-Fi

4. Gestione e auditing reti Wireless
5. Bluetooth
6. RFID

7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

RFID

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Radio Frequency IDentification
  - Tecnologia per l'identificazione automatica di oggetti, animali, persone
  - Il sistema si basa sul leggere (o anche scrivere) a distanza il contenuto di un *tag*
  - Può essere visto come la nuova generazione di codici a barre
    - Codice di identificazione univoco
    - Lettura automatica senza intervento umano

RFID

- I campi di applicazione sono svariati
  - Etichettatura prodotti in vendita
  - Gestione del ciclo di vita dei prodotti
  - Token di autenticazione - antifurti
  - Telepass
- Standards
  - ISO 14443 – ISO 15693
  - EPCglobal Class-1 Generation-2

Tag RFID

- Tag passivi
  - Economici, senza batteria
- Tag semi-passivi
  - Dotati di batteria
- Tag attivi
  - Dotati di batteria, possono iniziare una comunicazione

Reader RFID

- Reader RFID (lettore e scrittore)
  - Emette segnali tramite un'antenna
  - "Attiva" ed interroga i tag
  - Conserva i dati o li propaga ad un'applicazione centralizzata

RFID e Privacy

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Tracciabilità
  - Possibilità di “seguire” gli spostamenti
  - Associazione tra un tag e un individuo
  - Profilazione di un individuo in base ai tag posseduti
  - Passaporti con tag RFID incorporati
- La distanza di intercettazione può essere molto superiore a quella nominale

RFID e Privacy

- Disattivazione (killing)
  - I tag possono essere disattivati, ad esempio al momento della vendita
    - Vengono persi i benefici post-vendita (restituzione senza ricevuta o identificazione lotto di appartenenza)
    - Non tutti i posti vendita potrebbero essere dotati di reader
- Tag di blocco
  - Proposta di aggiungere ai tag un bit di privacy e realizzare dei blocker tag che impediscano la lettura dei tag marcati come privati
- Protettori personali (proxy)
  - Alcune ricerche ipotizzano la possibilità di intercettare le richieste di letture e permettere le risposte solo in determinate situazioni

RFID e Sicurezza

- Autenticazione
  - Assenza di autenticazione
    - Un PIN può essere usato per la scrittura
  - Tags attivi possono utilizzare meccanismi crittografici
    - Il loro costo in molti casi ne scoraggia l'utilizzo
    - Non sono esenti da problemi
  - Possibilità di clonazione
    - http://www.rfidanalysis.org
  - Scarsa integrità dell'identificazione
    - Attacco "a staffetta" (relay) http://www.cl.cam.ac.uk/~gh275/relay.pdf

RFID: Analisi dei rischi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- L'adozione di tecnologie RFID deve avvenire a seguito di un'adeguata analisi dei rischi e dei costi/benefici valutando i requisiti di:
  - Confidenzialità
  - Integrità
  - Robustezza dei protocolli di sicurezza
  - Locazione fisica

INDICE DELLA PRESENTAZIONE :

- Wi-Fi (IEEE 802.11)
  - IEEE Standards
    - http://standards.ieee.org/getieee802/802.11.html
  - Wi-Fi Alliance
    - http://www.wi-fi.org

- WEP
  - Walker J., “Unsafe at any key size: an analysis of the WEP encapsulation”
    - http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip
  - Borisov, Goldberg, Wagner “Intercepting Mobile Communications: The Insecurity of 802.11”
    - http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
  - Arbaugh, Shankar, Wan “Your 802.11 Wireless Network has no clothes”
    - http://www.cs.umd.edu/~waa/wireless.pdf

- WPA
  - Moen V., Raddum H., Hole K. "Weaknesses in the Temporal Key Hash of WPA" *ACM Mobile Computing and Communications Review Vol 8, 2*
    - http://portal.acm.org/citation.cfm?id=997132&dl=GUIDE&coll=GUIDE
  - Moskowitz R. "Weakness in Passphrase Choice in WPA interface"
    - http://wifinetnews.com/archives/002452.html

- IEEE 802.1X
  - 802.1XPort Based Network Access Control
    - http://grouper.ieee.org/groups/802/1/pages/802.1x.html
  - Congdon P. “IEEE 802.1X Overview”
    - http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

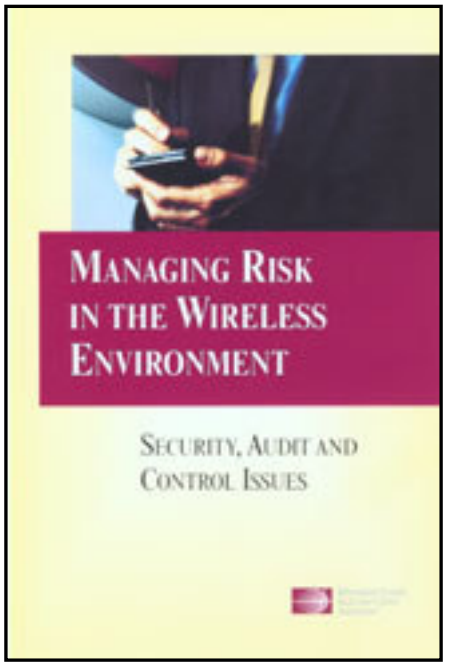
- IETF RFCs
  - RFC2865 Remote Authentication Dial In User Service (RADIUS)
    - http://www.ietf.org/rfc/rcf2865.txt
  - RFC2869 RADIUS Extensions
    - http://www.ietf.org/rfc/rcf2869.txt
  - RFC3579 RADIUS Support for EAP
    - http://www.ietf.org/rfc/rcf3579.txt
  - RFC3748 Extensible Authentication Protocol (EAP)
    - http://www.ietf.org/rfc/rcf3748.txt
  - Internet Draft Protected EAP Protocol Version 2
    - http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-10.txt

- Bluetooth
  - Bluetooth Special Interest Group
    - http://www.bluetooth.com
    - http://bluetooth.com/Bluetooth/Apply/Technology/Research/Bluetooth_Security_White_Paper.htm
  - IEEE 802.15.1
    - http://www.ieee802.org/15/pub/TG1.html
  - Jakobbson M., Wetzel S. Security Weaknesses in Blootooth
    - http://www.informatics.indiana.edu/markus/papers/bluetooth.pdf
  - http://www.thebunker.net/security/bluetooth.htm

- RFID
  - EPCglobal
    - http://www.epcglobalinc.org
    - Standards
      - http://www.epcglobalinc.org/standards_technology/ratifiedStandards.html
  - Juels, A. RFID Security and Privacy: A Research Survey
    - *IEEE Journal on Selected Areas in Communications, Vol 24, 2*
  - Garfinkel S., Juels, A., Pappu R. RFID Privacy: An Overview of Problems and Proposed Solutions
    - *IEEE Security & Privacy, Vol 3, 3*
  - RFID Viruses and Worms
    - http://www.rfidvirus.org/index.html
  - Analysis of the Texas Instruments DST RFID
    - http://www.rfidanalysis.org/
  - A practical Relay attack on ISO 14443 Proximity Cards
    - http://www.cl.cam.ac.uk/~gh275/relay.pdf

- ISACA eBook:
  Managing Risk in the Wireless Environment: Security Audit and Control issues

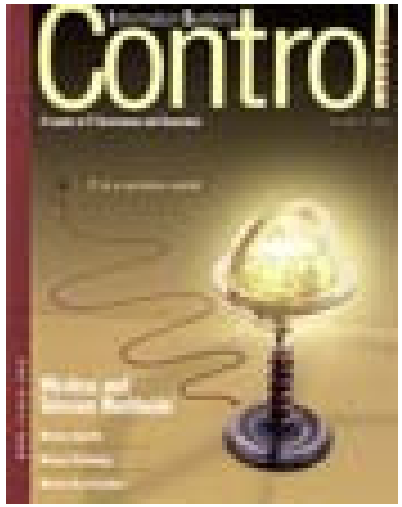
Disponibile online presso ISACA bookstore



- Information System Control Journal:

  Volume 3, 2004

  Wireless and Telecom Worldwide



- Altri articoli:

http://www.isaca.org/Template.cfm?Section=Article_Index1&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=67&ContentID=19103

- NIST SP 800-48 "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices" (Nov 2002)
  http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
- NIST SP 800-97 "Guide to IEEE 802.11i: Robust Security Networks" (draft)
  http://csrc.nist.gov/publications/drafts/Draft-SP800-97.pdf
- DISA "Wireless Security Technical Implementation Guide Version 4 Release 1"
  http://csrc.nist.gov/pcig/STIGs/wireless-stig-v4r1.pdf

Certificazioni

- Certified Wireless Security Professional
  http://www.cwnp.com

- GIAC Assessing Wireless Network
  http://www.giac.org