Secure wireless access in a mobile world

Giuseppe “Gippa” Paternò
Senior Solution Architect and Security Evangelist
Visiting Researcher
Trinity College Dublin

Fàilte

(welcome)

Who am I

- Visiting Researcher at Trinity College Dublin
- Currently Solution Architect and EMEA Security Expert at a premier software company
- Previously Security Solution Architect in Sun and also in IBM
- Certifications: RHCA, RHCDS, RHCSS, CCNP/CCNA, Nortel, Array Networks and Cyberoam
- Part of the italian security community *sikurezza.org*
- Published books and whitepapers
- Forensic analisys for local govs
- More on:
  - http://www.scss.tcd.ie/Giuseppe.Paterno/
  - http://www.gpaterno.com/
  - http://www.linkedin.com/in/gpaterno

New devices

- We are facing the increasing number of mobile devices that are getting more and more popular:
  - Smartphones based on Windows Mobile
  - Apple iPhone
  - Netbooks (Linux/Windows)
- We're more and more connected (“always on”):
  - UMTS/HDSPA (3g, 3.5g), Wi-Fi and Wi-Max (4g)
- More and more users are requesting access to corporate data through these new devices

New security challenges

- Integrating the mobile devices into our company:
  - Accessing Groupware/PIM systems (Exchange, ...)
  - Accessing database systems
  - Accessing web services
  - Integration with geo-localization services
- New services and new “always on” needs
- Ensure data security:
  - Intentional or unintentional loss, es: thieft organized by competitors or a simple loss.
  - Issues on users' privacy

… old problems

- Default configurations
- No perception of end-user about data privacy
  - End-users usually “trusts” technical stuffs
- Companies pays low/no attention to security
  - The usual sentence is: “it have to work, we'll implement security later”
- Attacks are getting more and more sophisticated
- Minimum security not implemented:
  - Do you keep your home door unlocked?

Type of attacks

- Radio attacks:
  - WEP and some WPA networks (based on TKIP) are insecure by design. Attackers can avoid cryptography easily.
  - Radio Jamming (Denial of Service).
  - Fake Access Point injected to capture users' data.
- Corporate/internal network
  - Traditional attacks (exploits/XSS) to access corporate data
- Wireless clients
  - Misuse of clients (PDAs, netbooks, laptops) as a “bridge” to the internal network.

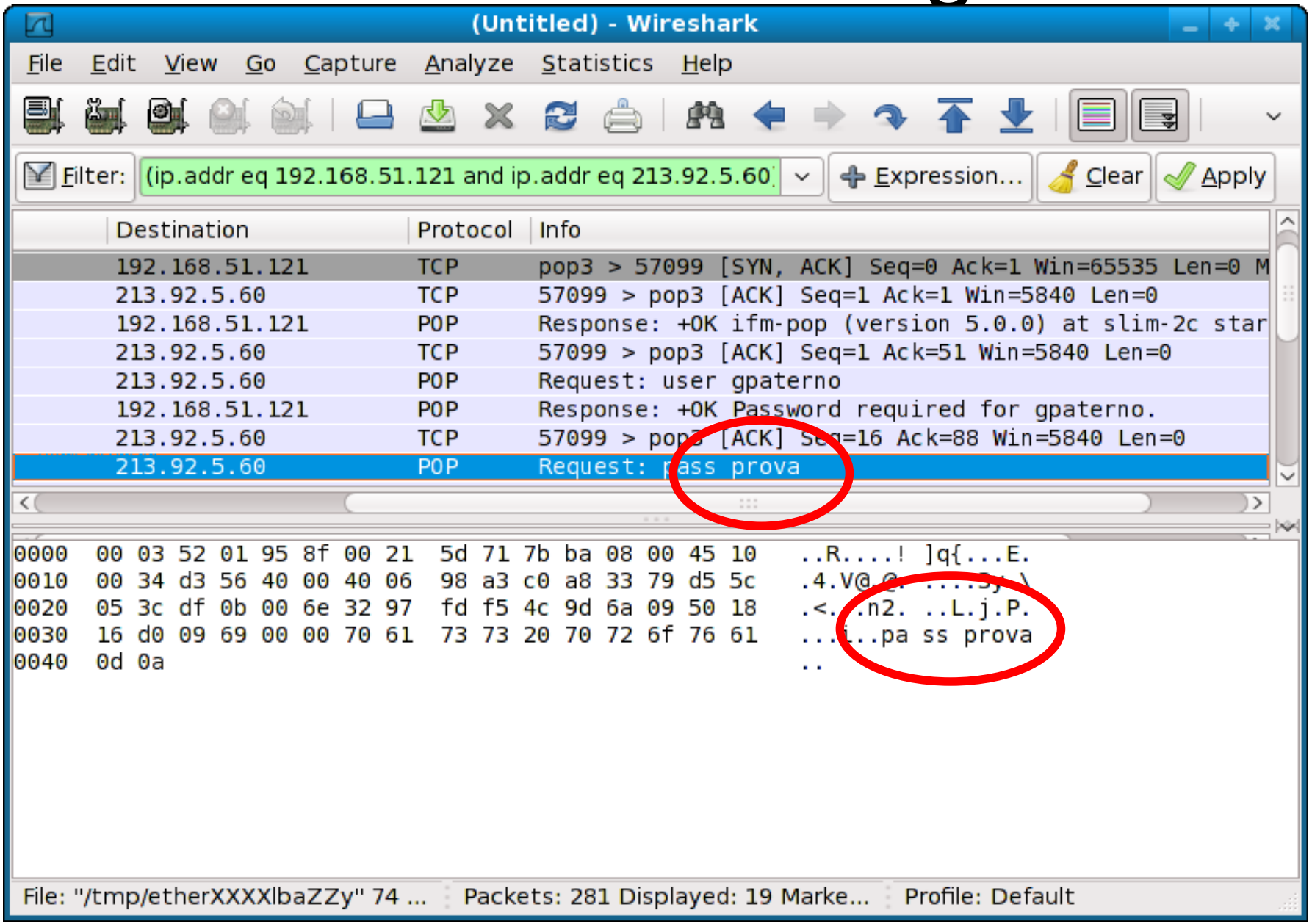
WPA issues

- We all know about WEP issues and the solution was WPA
- Some ethical hackers demonstrated the relationship between some providers' ESSID and the WPA default key
  - Some Italians and foreign providers give the end user a Wi-Fi router with the ADSL/voice subscription. It is possible to guess the WPA key (research of Muris Kurgaš)
  - In some router it is not even possible to change the WPA PSK (Pre-Shared Key, i.e. the password)

WPA issues

- Packet decode is possible if TKIP is used in WPA
  - Issue discovered in November 2008
  - The same type of attack is used in WEP: TKIP is a temporary WEP key that is changed every 3600 seconds (as default)
- Although WPA exists also with an AES encryption back-end (WPA2), how long will it last before another research "break" it?
- In an **enterprise** scenario, always use "*WPA Enterprise*"
  - Leverage RADIUS (see my previous research on OTP)
  - Key is generated **random**

Session Sniffing



SQL Server data replication

- One of the most popular database
- Widely used in a mobile world:
  - APIs makes it simple to add replication to Windows Mobile Applications
- SQL server encapsulate replication over HTTP
  - It is **very easy** to capture user data, user logins and domain information
- **Never** interconnect the replica server with Internet
  - Use a VPN and ensure that HTTPS is used

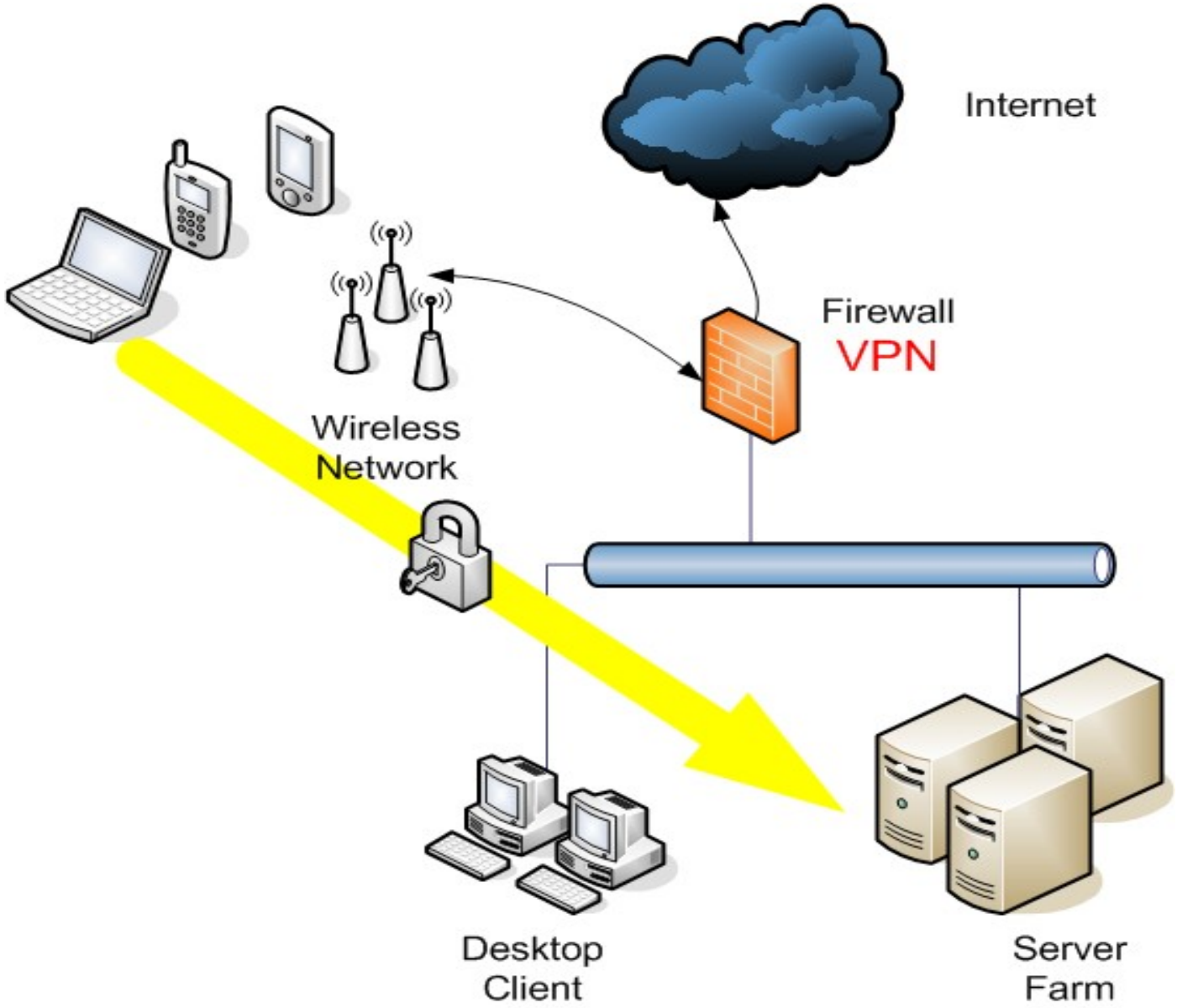
Protecting netbooks

- Netbooks should be handled like a standard laptop
- Leverage Operating Systems security feature
  - If Windows, use a firewall and antivirus
  - Hardening of the OS
  - Use central policies
- Use disk cryptography (whole disk or data only)
- Use two-factor authentication
- Do not trust wireless networks
  - Both Wi-Fi and 3G

Protecting Smartphones/PDA

- Both Windows Mobile and Apple iPhone have built-in security feature
  - Plan a wiping strategy
  - Use two-factor authentication
  - Do not trust external wireless networks (Wi-Fi and mobile operators' 3G)
  - Use cryptography in both internal and external storage, ex: Secure Digital (SD, microSD, ecc..)
  - Ensure that the application implement secure access to corporate data (HTTPS)

Use VPNs!


Internet
Firewall
VPN
Wireless
Network
Desktop
Client
Server
Farm

Thank you!!

Giuseppe “Gippa” Paternò
Visiting Researcher
Trinity College Dublin

paternog@cs.tcd.ie
http://www.scss.tcd.ie/Giuseppe.Paterno/
http://www.gpaterno.com/