

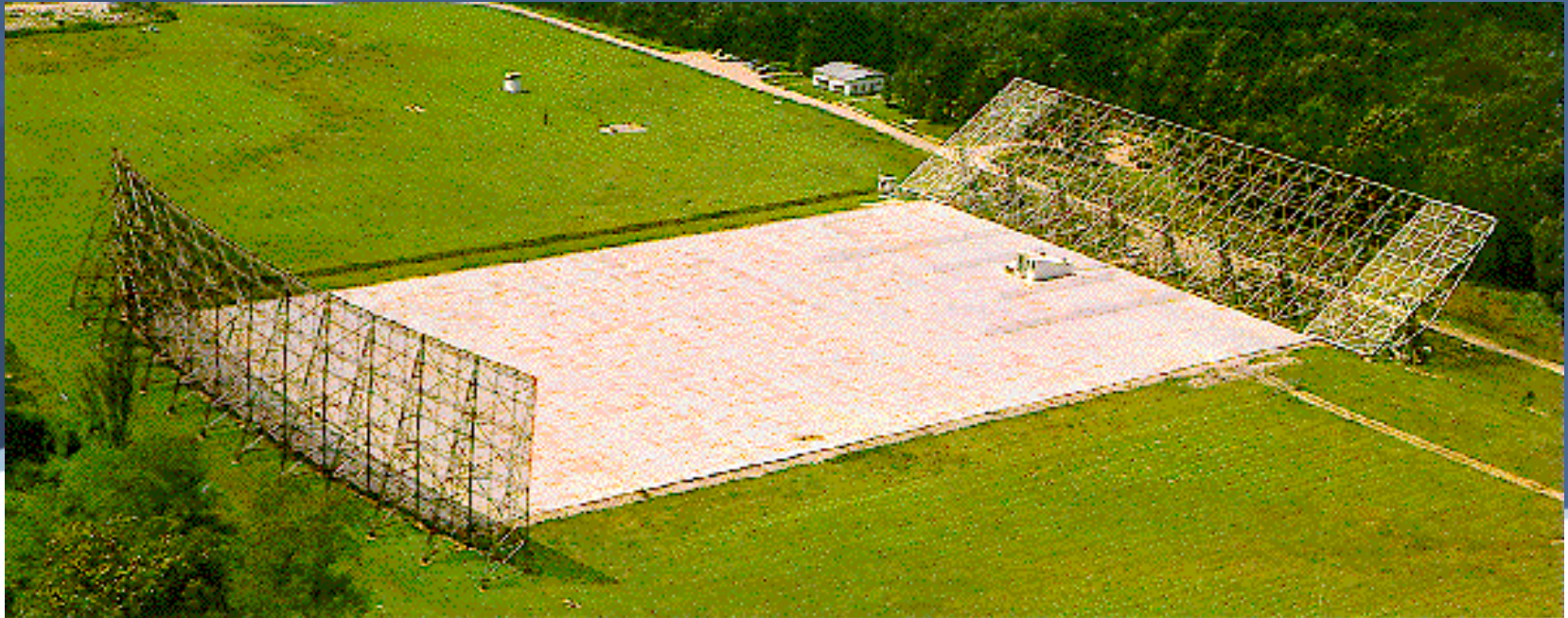


# The 5 P's of Secure Mobile Communications

Best Practices For Secure Wireless Roaming

Emil Sturniolo  
Chief Scientist, NetMotion Wireless, Inc.  
[emils@nmwco.com](mailto:emils@nmwco.com)

# Why is **Security** important?

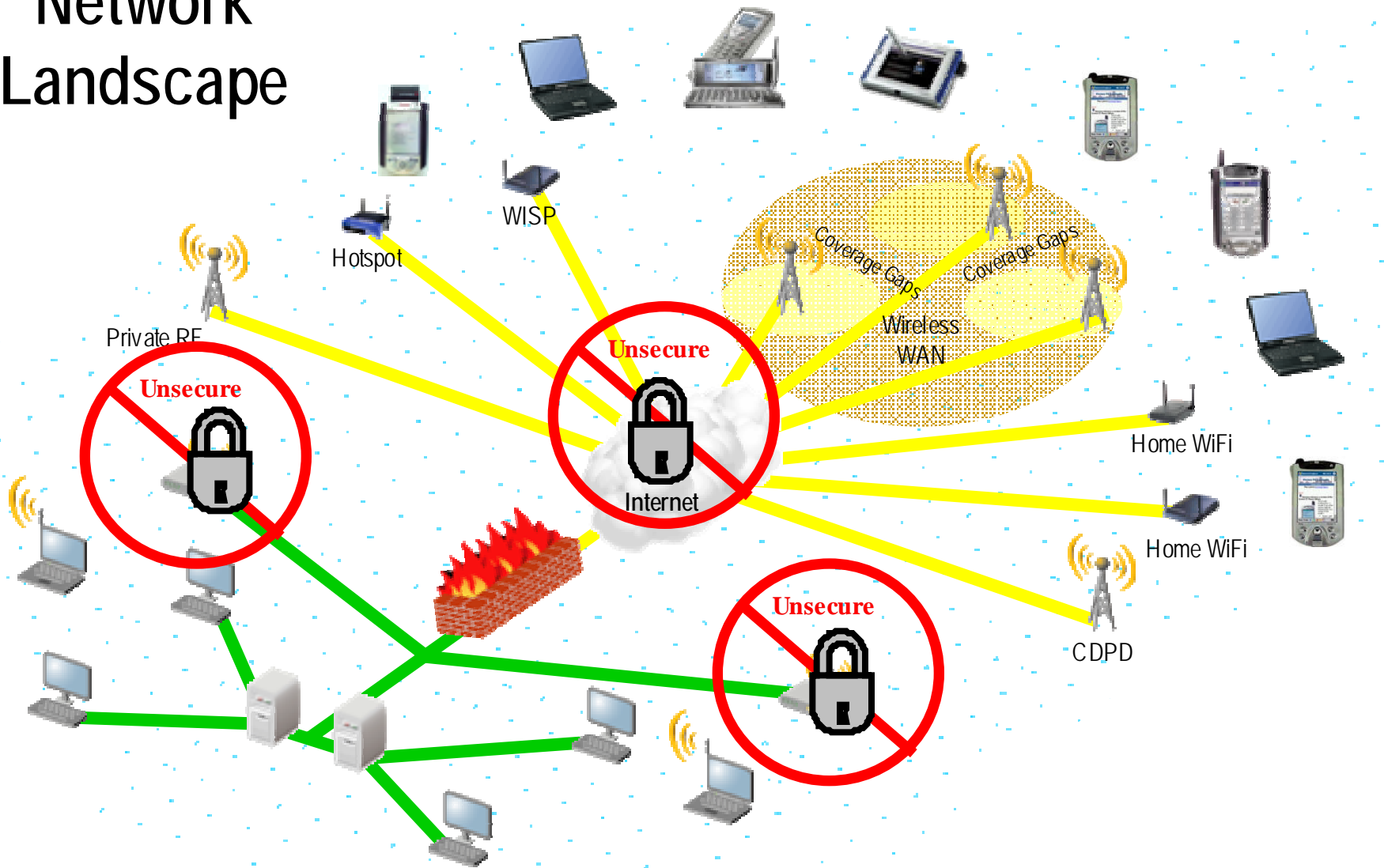


**My what big ears you have!**

## Sometimes its Government Mandated (Healthcare industry)

- « HIPAA requires healthcare organizations to secure all patient related data traveling over a wired or wireless network
  - Be careful if you are a health care organization. Some software/hardware companies have said that using their product will make your organization “HIPAA certified.” Technically this is incorrect as organizations outside of healthcare practices are not governed by HIPAA and there are no “certification tests” for them.

# Network Landscape



# Multi-Networking Environments

## « Healthcare: Marshfield Clinic

- Clinicians require seamless roaming among:
  - Wide area networks
  - Hospital wireless LANs
  - Campus wireless LANs



- Network manager needs to ensure all data is encrypted in a roamable VPN



## « Public Safety: Aurora Police Department

- Police officers need to seamlessly roam among GPRS, Private RF and Wi-Fi networks (local & wide area)
- Network manager only wants bandwidth intensive applications to be used on high-speed Wi-Fi networks

# Who's listening ?

*National Security Agency (NSA) for one*

**According to ABC news (Nightline)**

“...With satellites, listening posts, spy ships, planes, you name it, they can listen to just about anything. One listening post can reportedly pick up about two million phone calls and emails an hour...”

## Who can listen?

### *Hacking with a Pringles tube*

"...Empty cans of Pringles crisps could be helping malicious hackers spot wireless networks that are open to attack.

Security company i-sec has demonstrated that a directional antenna made with a Pringles can significantly improves the chances of finding the wireless computer networks ..."



<http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm>

# Internet Engineering Task Force

## *RFC 1045 (1988)*

“... Without security at the transport level, a transport level protocol cannot guarantee the standard transport level service definition in the presence of an intruder. In particular, the intruder can interject packets or modify packets while updating the checksum, making mockery out of the transport-level claim of ‘reliable delivery’...”

# Internet Engineering Task Force

## *RFC 2448 (1998)*

“... Data encryption at the physical and/or link layers can provide secure communication over satellite channels. However, this still leaves traffic vulnerable to eavesdropping on networks before and after traversing the satellite link...”

# Internet Engineering Task Force

## *RFC 2316 (1998)*

### *Report of the IAB Security Architecture Workshop*

“... In general, relying on the security of the infrastructure is a bad idea; it, too, is under attack. ...”

## Wireless LAN community

*Jessie R. Walker – Intel Corporation*

“... Increasing the WEP key from 40 to 104 or 128 bits does nothing to increase WEP's resistance to attack. This is because the deficiencies are related to *how WEP uses cryptography, not the key size. WEP's design attempts to adapt RC4 to an environment for which it is poorly suited, with potentially catastrophic consequences for its intended users...*”

# Wireless LAN community

## *Wi-Fi Network News (November 2003) on WPA*

“...Wi-Fi Protected Access (WPA) has a weakness: poorly chosen short human-readable passphrases can be cracked with a robust dictionary attack offline and without access to the network...”

<http://wifinetnews.com/archives/002452.html>

## LEAP Cracked!

- « In August 2003, Joshua wrote a tool called asleep for Linux systems to exploit a weakness in the Cisco LEAP authentication protocol. Using this tool, *an attacker can actively compromise Cisco LEAP networks by mounting an offline dictionary attack against weak user passwords*. In his testing, Joshua was able to search through large dictionary files very quickly for user passwords (~45 million passwords per second on meager hardware).

<http://www.securiteam.com/tools/5TP012ACKE.html>

## Some Potential Solutions

- « Secure Socket Layer (SSL/TLS)
- « Traditional Virtual Private Network (VPN)
- « IPSec
- « Layer 2 Encryption

*None are designed with mobility in mind!*

# *Technical Challenges!*

# SSL/TLS/WTLS

Pros	Cons
Encrypts only application data - - interoperable in all IP network environment	Applications may need to be modified to take advantage of its features.
Defacto standard for Web based access	Depending on O/S architecture it may not secure all network application
	May cause increased network overhead (reduced performance and increased latency)
	Both peers need to support protocol

# Traditional Virtual Private Networks

Pros	Cons
Secures all application data that traverses the tunnel	Extra steps needed to establish connectivity
Applications do not need to be modified	May not be able to roam between networks without reestablishing link
	Causes increased network overhead (reduced performance and increased latency)
	May not operate in all IP network environments

# IPSec

Pros	Cons
Insures integrity of application data to peer	Separate session for each peer, thus not interoperable with all peer systems
Applications do not need to be modified	May not be able to roam between networks without reestablishing link – Not designed for mobility
Encrypts entire message, including transport headers	May not be interoperable behind some policy enforcement equipment or NATs
	Causes increased network overhead

## Layer 2 Encryption

Pros	Cons
Encrypts all data traversing the first hop	May require private interconnect to ensure integrity and privacy back to corporate network (\$\$\$)
May off load processing from main system (better performance)	Not able to roam between networks mediums or to networks not under administrative domain
Encrypts entire message, including transport headers	Credentials normally base on device not user- (Lost device = breech)
	Point solution – Only available on specific network

*The 5 P's to remember  
when considering a  
mobile security  
solution.*

# Privacy

- ⌂ **Security in depth**
  - Employ all that are available
  - Buy solutions that are compatible and complimentary to other security technology
- ⌂ **Between the mobile device and your trusted computing base**
  - Solution is application agnostic
    - Does not require reconfiguration or modification of the application(s)
  - Should be independent of access technology
- ⌂ **Publicly scrutinized ciphering algorithms**
- ⌂ **Automatic rekeying**
  - Insist on Perfect Forward Secrecy
- ⌂ **Size does matter**
  - Make sure key length is sufficient for both asymmetric and symmetric keys
    - RFC 2409
    - draft-orman-public-key-lengths-05.txt

# Persistence

- ⌋ Out of range conditions
  - Coverage gaps
  - Suspend/Resume
- ⌋ Roaming
  - Layer 2
  - Layer 3
- ⌋ Other power management issues
  - Network disconnects
- ⌋ Network address translation
  - Traversal
  - Keep alive issues

# Performance

- « **Considers bandwidth challenged links**
  - Compression
- « **Reduce overhead**
  - Link optimizations
  - Minimize encapsulation
- « **Cognizant of power management**
  - Standby/Hibernate
  - Network induced

# Protection

- ⌋ Identification
  - Which device
- ⌋ Authentication
  - Who
- ⌋ Authorization
  - What
- ⌋ Policy
  - How
  - When
- ⌋ Cooperative enforcement
  - Enforce on both ends of the connection

# Productivity

- ⌋ **Unencumbered user experience**
  - Small learning curve if any
  - Can not inhibit the user's experience
    - *If it gets in the way, people will try to subvert it !*
- ⌋ **Easily deployable**
  - Works with existing infrastructure
- ⌋ **Centrally administrable**
- ⌋ **Allows for migration path as standards progress**
  - Fork-lift upgrades not acceptable
- ⌋ **Information Technologist and End-users are not RF engineers**
  - Solution needs to fit the needs of both groups.
- ⌋ **Remember, Security is only the beginning of mobility**

## Continuous Secure Connectivity



***“Nothing in this world can take the place of persistence.”***

***- Calvin Coolidge***