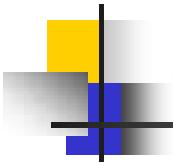
WLAN security with VPN

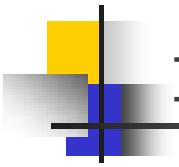
S-72.333

Postgraduate Course in Radio Communications



Contents

- Introduction
- Problems with WLAN security
- IPsec VPN based solution
- Possible authentication methods
- VPN vs. WEP / WPA
- Performance issues
- Conclusions



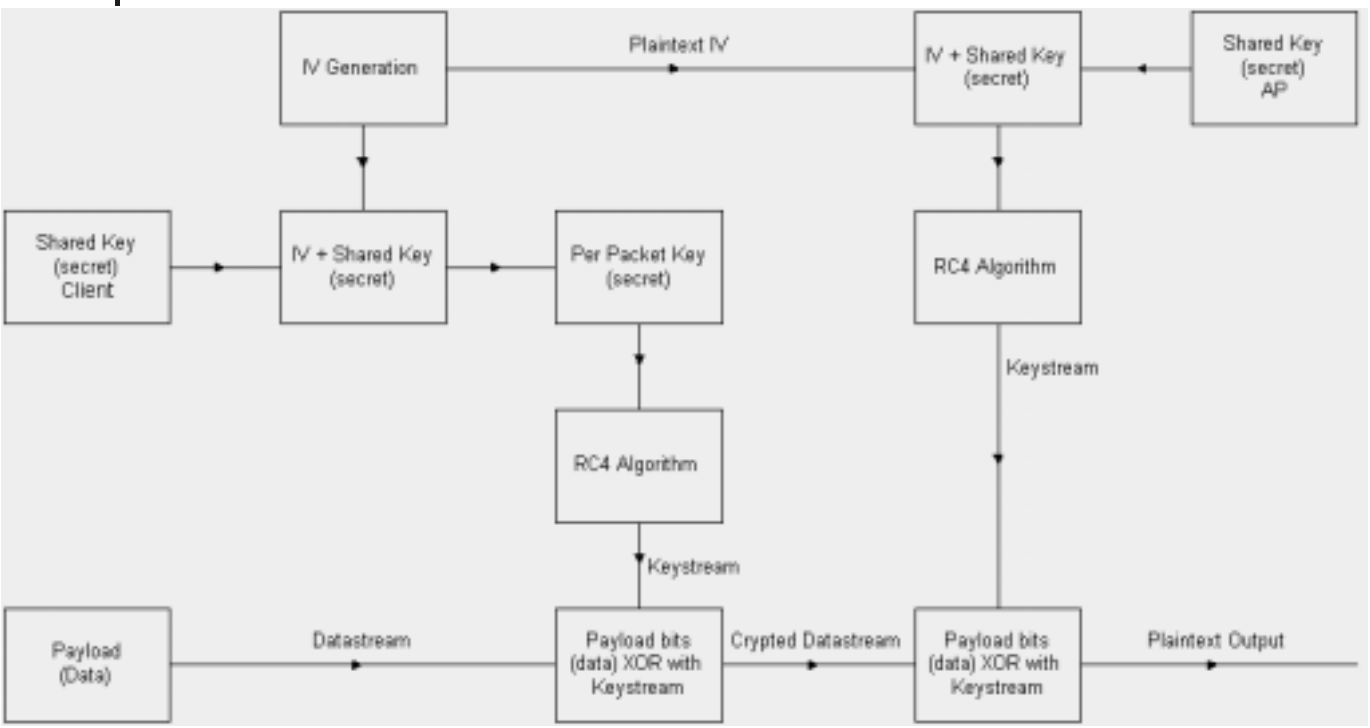
Introduction

- Wireless networks are vulnerable to attacks
- WLAN networks have some serious problems with security
- IEEE 802.11(b) based security methods are not suitable for large scale networks
- Well known standardized security methods are needed to secure wireless networks

Basic problems with IEEE 802.11(b) security

- WEP isn't secure enough for all environments
  - Effective key length is often too short
    - Official key length from 40- to 104bit
    - Effective key length often less than alleged
  - Shared secret leaks because of used initialisation vector implementation if WKA –support is not available
- Static shared secret is not usable in large scale networks
  - Hard to maintain and vulnerable to local attacks

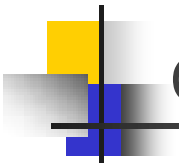
Logical operation of WEP protocol



Basic problems with WPA -security

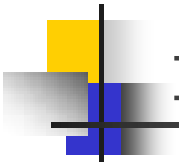
- WPA is not a real standard
  - Limited supportability
  - It will be replaced with IEEE 802.11i -standard
  - WPA is similar to IEEE 802.11i but not compatible

  => WPA has a rather short lifespan
- WPA offers some improvements compared to WEP but it also some new problems
  - Limited support for strong authentication
  - Password based PSK is vulnerable to attacks [8]



Conclusion about WLAN -security

- Security methods based on IEEE 802.11(b) standard are not secure enough in practical environments
- WPA is not a real alternative if high security level and long life span are important issues
- IEEE 802.11i is basically enhanced WPA, which is standardized
- Alternative security protocols are needed



IPsec VPN based solution 1/2

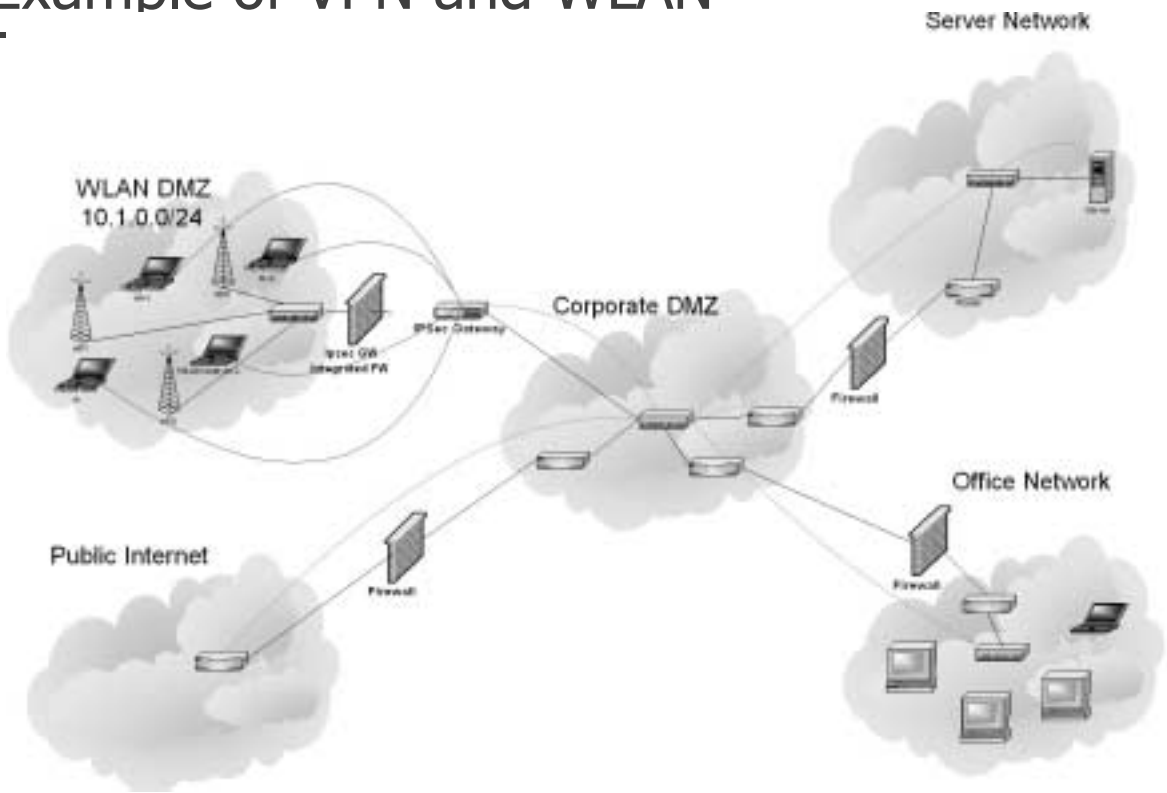
- IPsec VPN provides security services on top of IP –protocol
  - Connection independent operation
  - WLAN –network is used only as an transport layer
- IPsec VPN security is based on
  - Strong authentication (Secure ID, PKI…)
  - Strong encryption (AES, 3DES…)
  - Controlling traffic with firewalls (p. 10)

IPsec VPN based solution 2/2

- IPsec VPN is considered to be very secure when it uses AES, 3DES or some other strong encryption algorithm, but it isn't perfect [1]
- Most operating systems don't include usable IPsec support

  =>Additional software is needed especially when IPsec VPN is combined with PKI

Example of VPN and WLAN



Strong authentication (IPsec VPN/ IKE)

- IPsec VPN security needs strong authentication to prevent unauthorized persons to access corporate network
- IKE supports for example PSK and PKI
  - PSK is simple and secure but harder to maintain in large systems
  - PKI is more complex and costs more to build but it's also more flexible to use and easier to maintain
  - PKI suites well especially to large organisations
  - PSK is suitable mainly for small companies and home use

PKI authentication

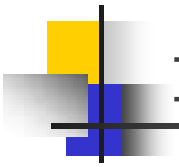
- Enables standardized method to authenticate both users and devices
- Scalable and flexible solution
- PKI/PKE can also be used for other purposes like secure email messages etc.
- Although PKI authentication is considered to be very secure and well supported it also has some disadvantages
  - High price compared to IEEE 802.11(b) or password based WPA (PSK)
  - More complex than for example WEP or VPN PSK

Strong encryption

- Strong encryption is needed to protect information from outsiders
- IPsec VPN uses typically AES - or 3DES algorithm for encryption
  - DES is often supported as an fallback option
  - IPsec VPN can also be used with out encryption but it not secure
- Both AES and 3DES are symmetrical encryption algorithms
  - Symmetrical encryption is typically much faster than PKE
  - IKE is used to exchange secret encryption keys

Controlling network traffic

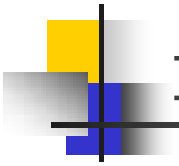
- Only authenticated and encrypted traffic should be allowed from wireless network to and from corporate network (p. 10)
- Also user devices should control incoming traffic to prevent security attacks against user equipment (p. 10)



IPsec VPN + PKI vs. WKA enabled WEP

- Standardized
- Connection independent
- Strong and flexible authentication based on PKI
- Usable also in system that require high security
- High scalability
- Moderate – high cost

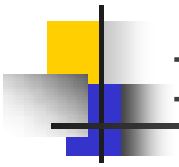
- Based on defacto standard
- Only for WLAN networks
- Authentication is based on shared secret
- Usable in systems that require only moderate security
- Poor scalability
- Inexpensive



IPsec VPN + PKI vs. WPA

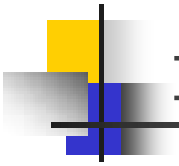
- Standardized
- Connection independent
- Strong and flexible authentication based on PKI
- Usable also in system that require high security
- High scalability
- Moderate – high cost

- Based on defacto standard
- Only for WLAN networks
- Authentication is normally based on password (PSK)
- Usable in systems that require only moderate security
- Good scalability
- Inexpensive



IPsec VPN Performance issues 1/2

- IPsec VPN doesn't effect to WLAN performance in practice
  - A little more overhead because of extra headers
  - Modern computers can make AES/3DES crypto operations without any problems
    - For example PIII933 laptop can encrypt/decrypt (AES) much more than 100Mbit/s traffic flow
    - 3DES encryption is about 50% slower than AES encryption
- Hardware based IPsec VPN –solutions are scalable



IPsec VPN Performance issues 2/2

- Software based IPsec VPN –solutions like FreeS/WAN can handle even 1Gbit/s full-duplex links at full speed if encryption accelerators are in use
- Biggest problem with performance issues with software solutions it that for example FreeS/WAN can handle simultaneously only hundreds of users (or less)

Conclusions

- IPsec VPN offers well supported, standardized method to secure WLAN networks
- PKI offers a scalable, standardized solution to authenticate users and exchange secret keys
- Although IPsec VPN combined to PKI offers superior security and scalability compared to WPA and WEP, it is also much more expensive to use than WEP or WPA

Acronyms 1/2

- 3DES Triple DES
- AES Advanced Encryption Standard
- AP Access Point
- CA Certificate Authority
- CRL Service Revocation List
- DES Digital Encryption Standard
- IKE Internet Key Exchange
- IPsec IP security
- NAT-T Network Address Translation - Transversal

Acronyms 2/2

- PKE Public Key Encryption
- PKI Public Key Infrastructure
- PSK Pre-Shared Key
- VPN Virtual Private Network
- WEP Wired Equivalent Privacy
- Wi-Fi Wireless Fidelity
- WKA Weak Key Avoidance
- WPA Wi-Fi Protected Access

References

[1] N. Ferguson and B. Schneier, "A Cryptographic Evaluation of IPsec", http://www.macfergus.com/pub/IPsec.pdf .

[2] Scott Fluhrer, Itsik Mantin ja Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", http://downloads.securityfocus.com/library/rc4_ksaproc.pdf .

[3] EEMA Unified Messaging Interest Group, "Best Practice for Wireless Networks", https://www.eema.org/All_R1.asp?FirstParam=118 .

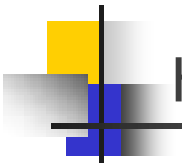
[4] AT&T Labs Technical Report TD-4ZCPZZ, "Using the Fluhrer, Mantin and Shamir attack to Break WEP Revision 2", http://www.cs.ucsb.edu/~vigna/courses/CS279/13_WirelessSecurity/stubblefield01-using_fluhrer.pdf .

[5] FreeS/WAN documentation, http://www.freeswan.ca/

[6] Richard E. Smith, "Authentication From Password to Public Keys".

[7] Intel Information Technology White Paper, "Wireless 802.11b security in a corporate environment", http://www.intel.com/business/bss/infrastructure/security/vpn_wep.pdf

[8] Robert Moskowitz, "Weakness in Passphrase Choice in WPA Interface", http://wifinetnews.com/archives/002452.html .



Homework

- Explain (shortly) what following concepts mean and how/where they are used.

  AES

  IKE

  IPsec VPN

  PKE

  PKI

  PSK