WiFi SECURITY

Ivan Klimek
Ivan.Klimek@cnl.tuke.sk

PHENOMENOM WiFi

WiFi is everywhere: soho, enterprise, campus, ISP ...

- masive popularity because of cheap HW, easy to use, fast to deploy
- many organizations rely on weak or none security, ISPs too...
- basic know-how needed to break into a common WiFi network, attacker doesnt need to be a guru

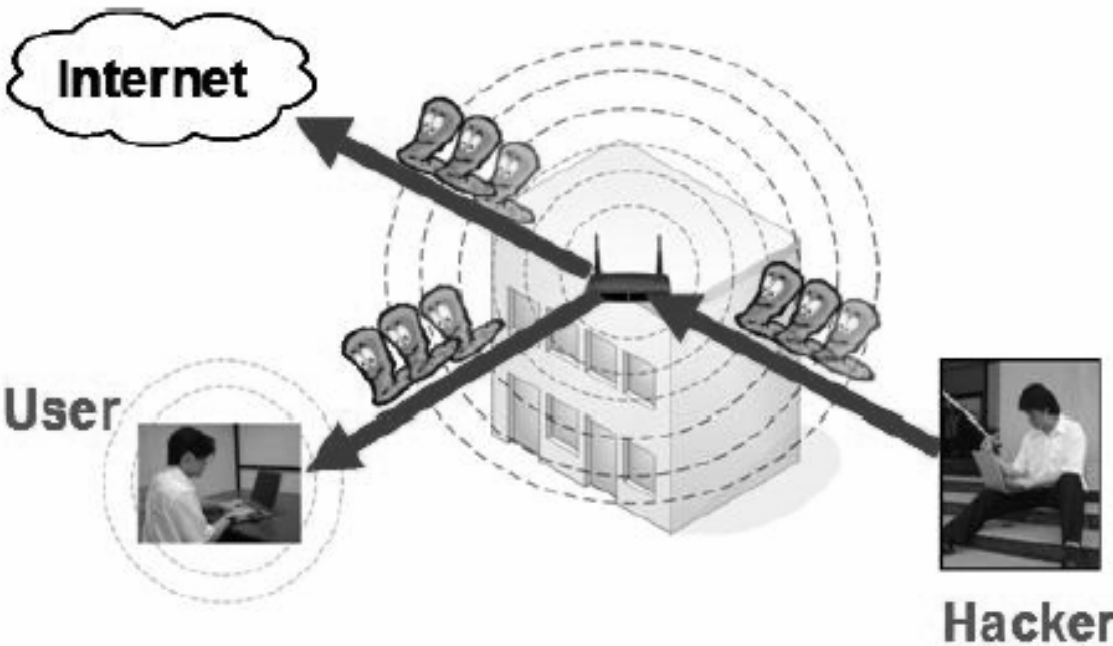
WLAN security threats

- Passive data sniffing
  - AiroPeek, Kismet
  - Username/password
  - Credit card number
  - Email messages
  - Company Info.

Stealth sniffer !

WLAN security threats

- Unauthorized access

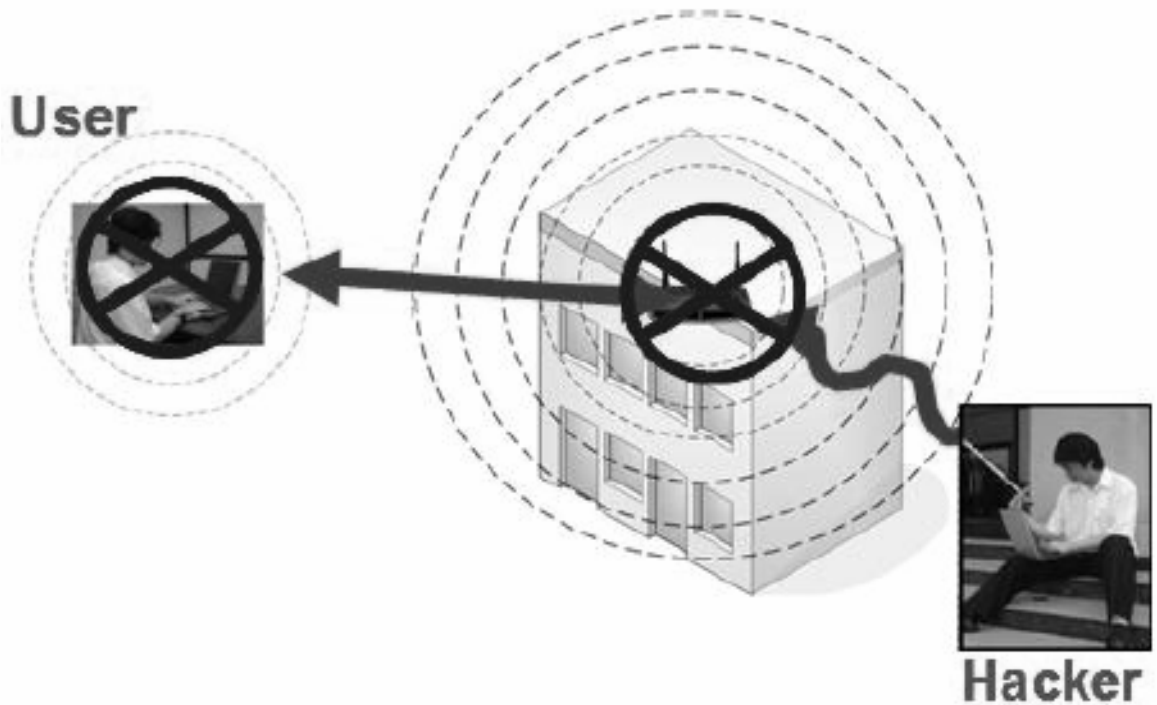


- Wardriving
- Internet attack
- MAC spoofing
- Company backdoor
- Client-to-client attack
- Spam mail

Stealth Attacker!

WLAN security threats

- Jamming or denial of service attack

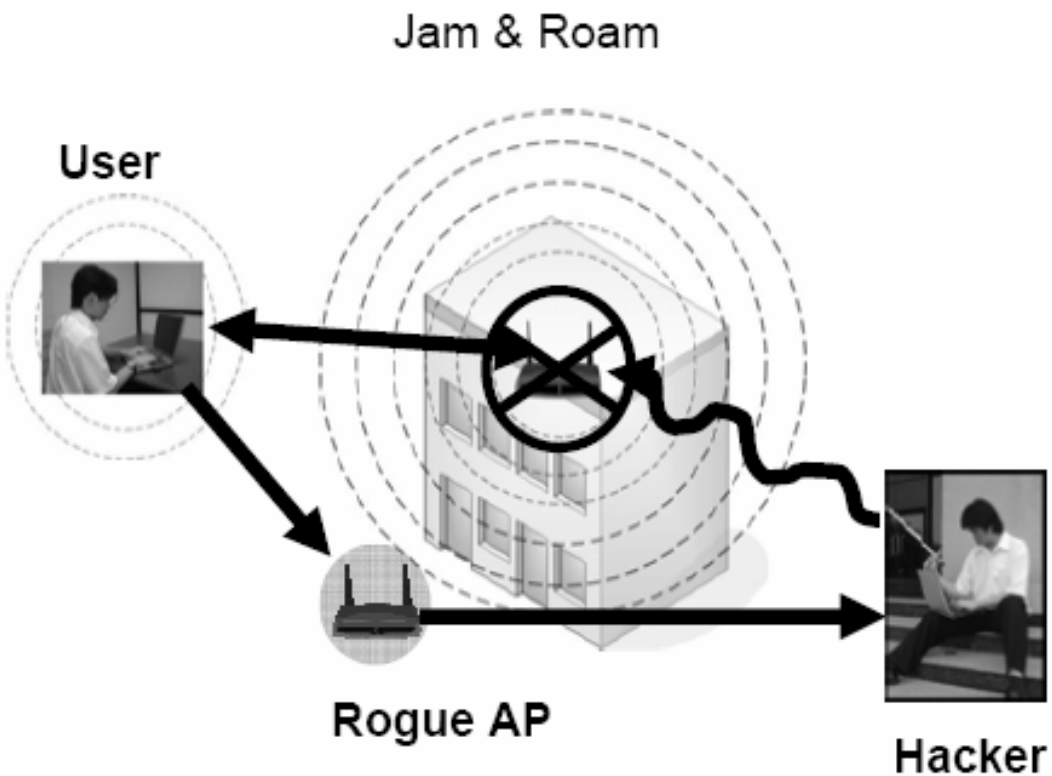


- 2.4 GHz RF jamming
- Packet flood

RF Jamming unsolvable!

WLAN security threats

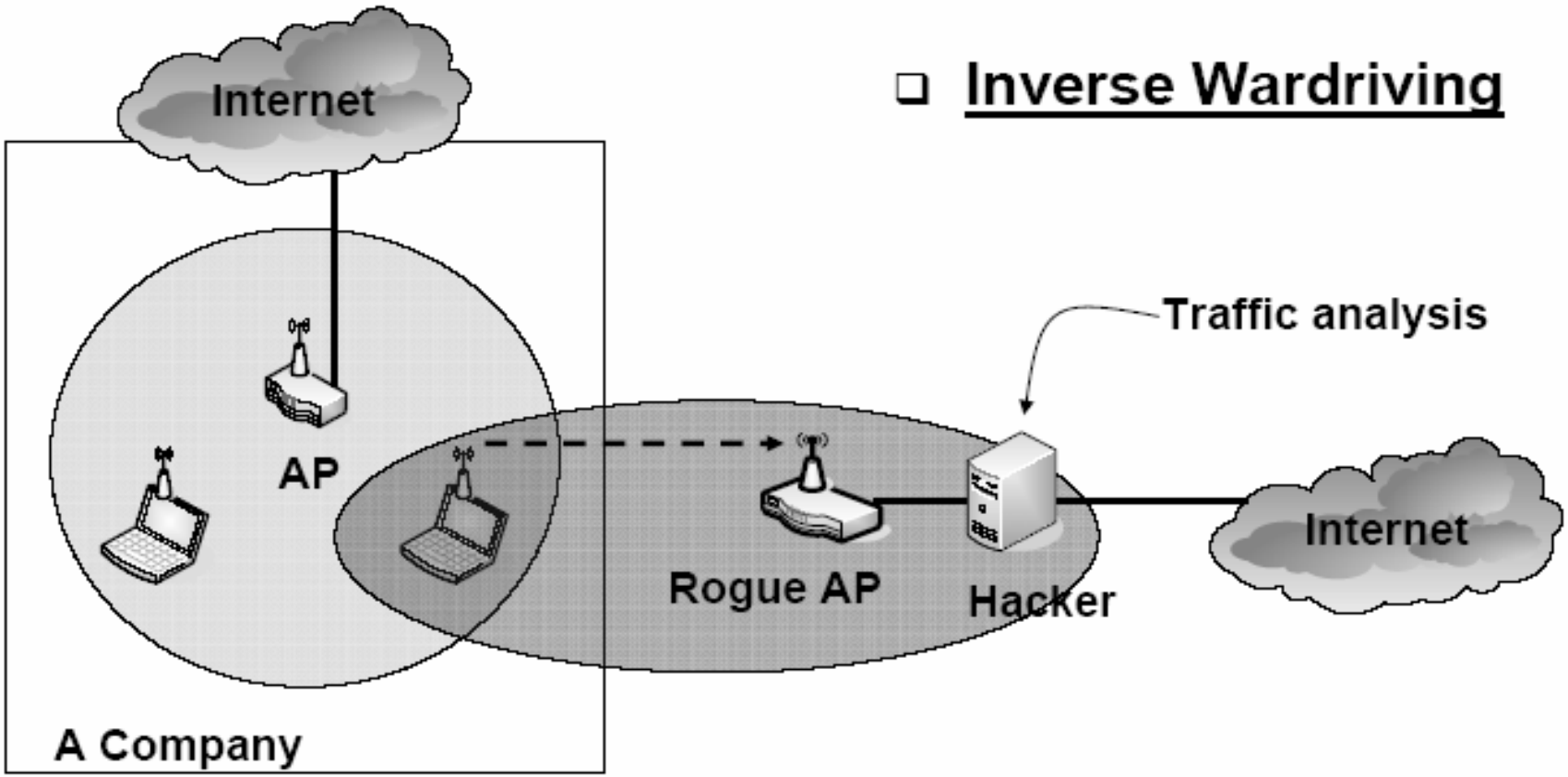
- User hijacking & Man-in-the-middle attack



- Inverse Wardriving
- Sniff & Modify
- Fake server
- Https hack
- Password stealing
- “Phishing”

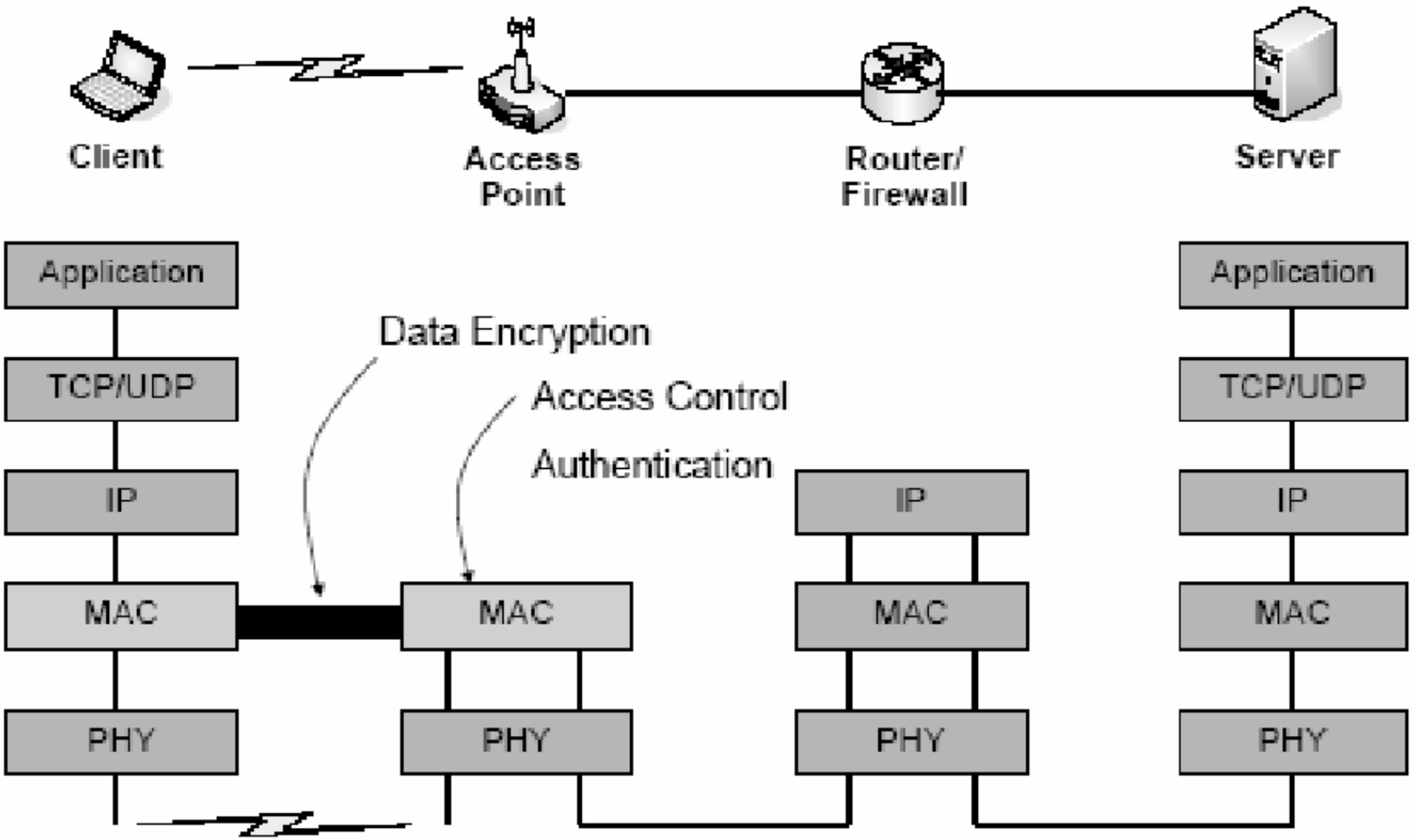
WLAN security threats

- Man-in-the-middle attack



- **Inverse Wardriving**

WLAN security technologies



Generations of WiFi security technologies

WEP (Wired Equivalent Privacy)

- IEEE 802.11 -> 1999
- WEP encryption -> shared secret key cryptography, RC4 algorithm, encrypt data directly
- WEP authentication -> open authentication (no security) or shared key authentication
- key managment -> share the same key for both sender / receiver, static key, key size of 60 / 104 bits
- weak initialization vector (24 bits), can be used to gain the WEP key
- can use MAC addres filtering

Generations of WiFi security technologies

WPA (Wi-Fi protected acces)

- Interim draft of IEEE 802.11i -> 2002
- TKIP (Temporal Key Integrity Protocol) is a modification of WEP to defend against currently known attacks (WEP + four patches for key mixing, message integrity, re-keying and initialization vector protection)
- WPA Personal – uses preshared key
- WPA Entarprise – use of RADIUS (Remote Authentication Dial In User Service) server
- capable of AES (Advanced Encryption Standard)

Generations of WiFi security technologies

WPA2

- intended to bring WPA in-line with IEEE 802.11i standard

- backward compatible with WPA

- uses AES-CCMP (Advanced Encryption Standard – Mode Cipher Block Chaining Message Authentication Code Protocol) just like 802.11i

- support for fast-roaming: stations are pre-authenticated to neighboring access-points in addition to the one they are communicating

Generations of WiFi security technologies

IEEE 802.11i

- this draft standard includes:
  - the Advanced Encryption Standard (AES) and 802.1x Port-Based Network Authentication standard for WLAN user authentication and key managment
  - AES mode used: AES-CCMP
  - AES is the most secure and prefered encryption method today, it replaced DES and 3DES

- 802.11i Cipher Negotiation: devices advertise their encryption capabilities, used to set up policies for the network, for example allow only stations capable of AES to associate

- 802.1x framework is based on Extensible Authentication Protocol over LAN (EAPoL) messages, requires use of a RADIUS server, there are a number of EAP authentication algorithms that may be used

EAP types

EAP-TLS (Transport Layer Security):

- build in Windows XP
- requires certificates on both sides client / RADIUS server

LEAP (Leightweight EAP):

- Cisco propietary
- dont use certificates, uses passwords to authenticate
- not all clients support this protocol, requires special software

EAP-FAST (Flexible Ath. via Secure Tunnel):

- Cisco propietary
- follow-up of LEAP, more secure than LEAP because of setting up a secure tunnel before client sends sensitive data

EAP-TTLS (Tunneled TLS) & PEAP (Protected EAP):

- supported by wide range of companies
- uses certificates only on server side
- **protocols used for “wired“ user authentication (MS-CHAPv2) can be layered over PEAP**

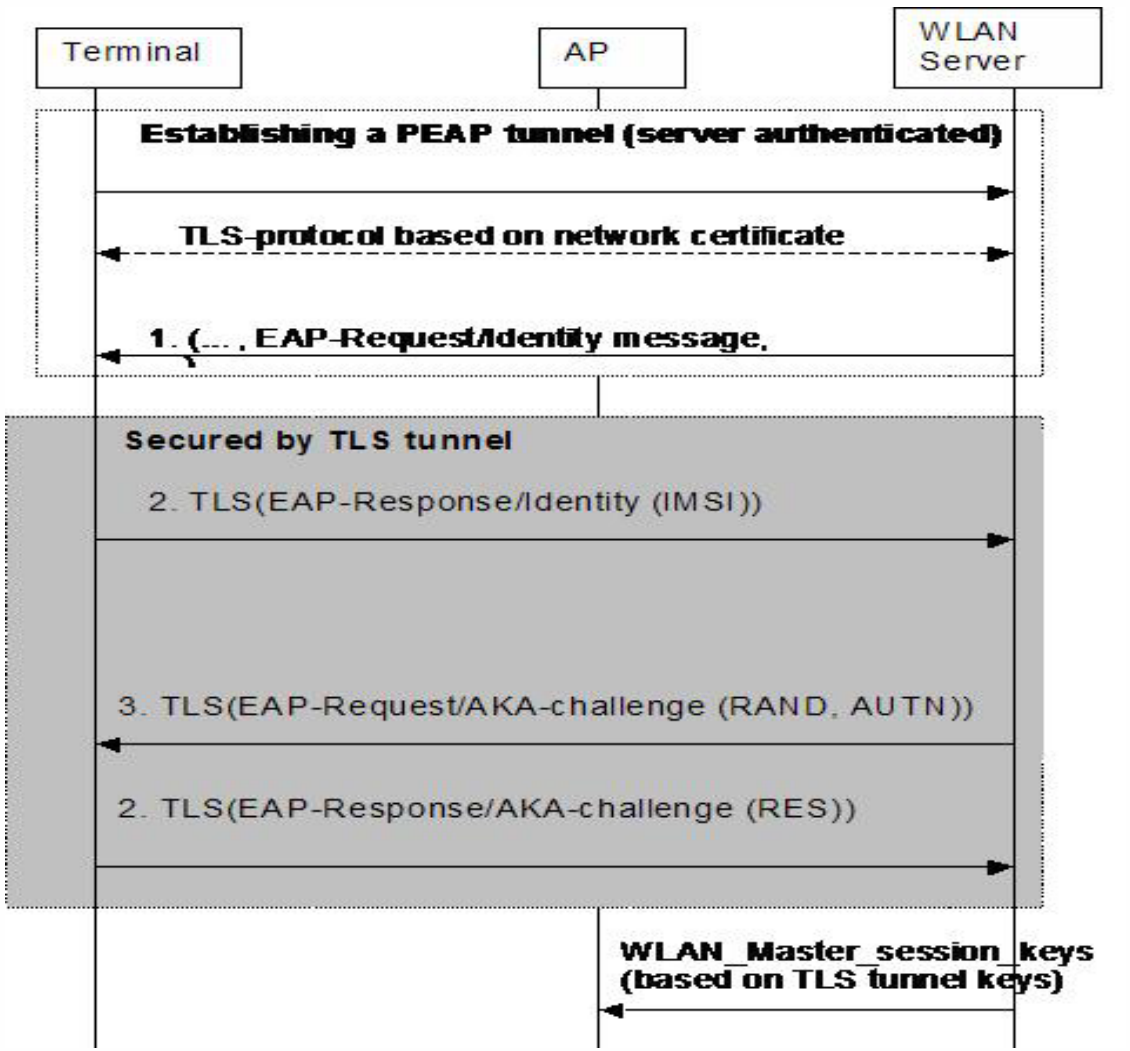
What do we use

- WPA2 (AES), MS-CHAPv2, PEAP – all of these are available in Windows XP SP2 by default, no special software / drivers needed
- first design used LEAP, currently for transition reasons we run both LEAP and PEAP, (asleap used to hack weak LEAP passwords)
- open source RADIUS server (Freeradius) can be used for PEAP and LEAP, quite hard to get it running for PEAP but it is possible (a howto about that is available at my website)
- Freeradius can be configured to use default build in certificates, or you can buy one or create yourself one, or as we do it for now – exist without it
- Freeradius can autenticate user against any DB server or LDAP server, we use the second mentioned
- for user managment we use a special web portal writen by our member Mr. Peter Fecilak

Is our design secure ?

- NO, but there is nothing more secure ....
- AES is currently the best choice for encryption, but can be BROKEN
- PEAP is used because of its wide range of supported clients
- every EAP type is vulnerable to MITM (man in the middle atacks) (a theoretical study about that exists), and to Injection of fake EAP/Success (or Failure) packets (Arbaugh attack), but because PEAP uses TTLS it is more secure than other possibilities
- the network can use the most up-to-date technologies, but when there is another hole in the security all this is useless, so do not think you are secure, because you are not, every day there are new exploits, software / firmware / drivers updating is a MUST

PEAP – How it works



PEAP with MS CHAPv2 operation

PEAP part 1: Creating a TLS tunnel:

1. After creating a logical link the AP sends a EAP-Request / Identity message to the client

2. The client responds with EAP-Respond Identity (username)

3. The EAP-Respond message is send to the RADIUS server, from that point the AP is only a pass-through device

4. The RADIUS server sends an EAP-Request / Start message to the client

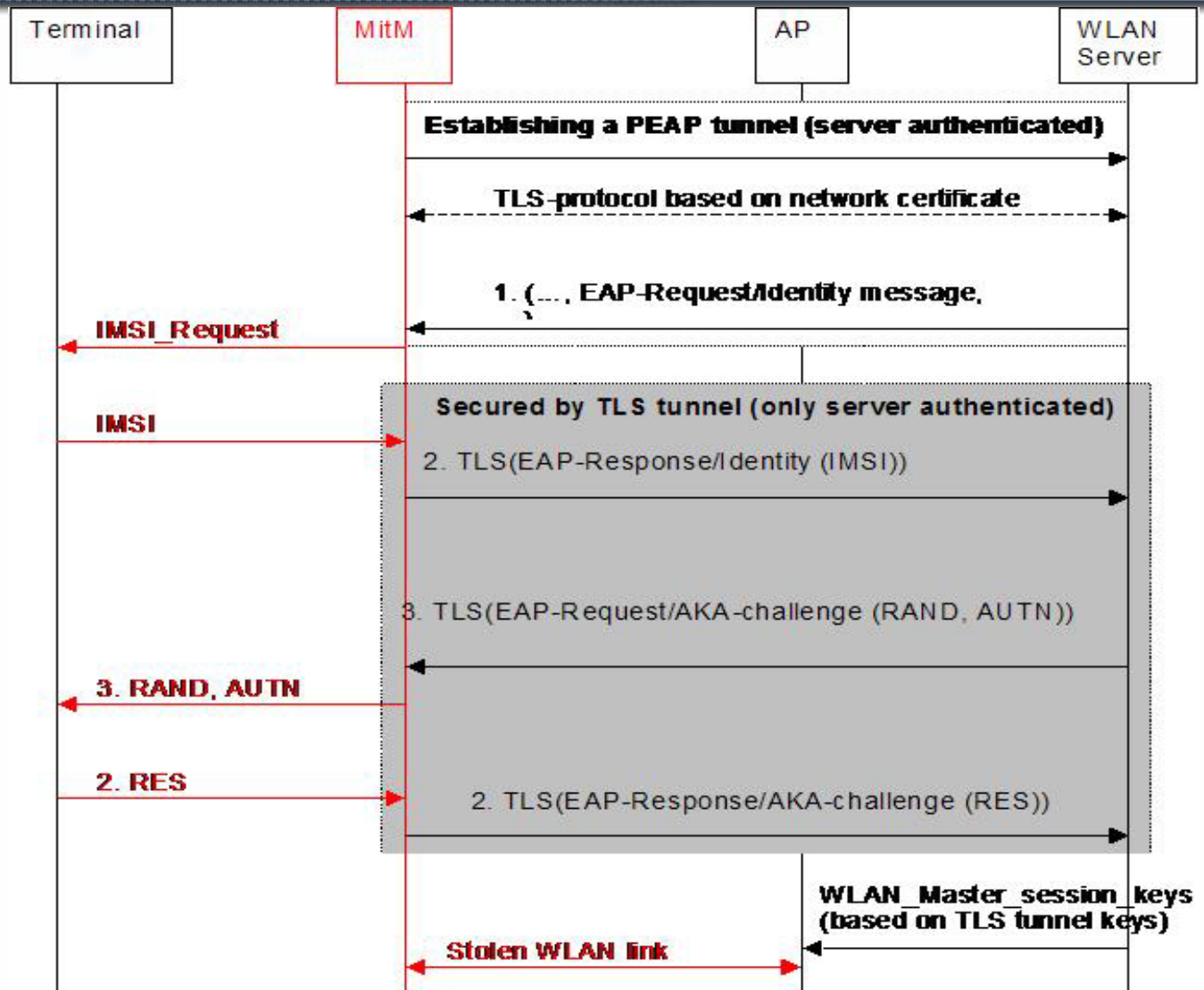
5. A series of TLS messages are exchanged, the cipher suite is negotiated and the RADIUS server sends a certificate for its authentication to the client

PEAP with MS CHAPv2 operation

PEAP part 2: Authenticating with MS CHAP v2:

1. The RADIUS server send a EAP-Request Identity message
2. The client responds with EAP-Respond Identity (username)
3. The RADIUS server sends an EAP-Request /EAP-MS-CHAP-v2 Challange message that contains a challange string
4. The wireless client responds with an EAP-Response/EAP-MS-CHAP-V2 Response message that contains both the response to the RADIUS server challenge string and a challenge string for the RADIUS server
5. The RADIUS server sends an EAP-Request/EAP-MS-CHAP-V2 Success message, which indicates that the wireless client response was correct and contains the response to the wireless client challenge string
6. The wireless client responds with an EAP-Response/EAP-MS-CHAP-V2 Ack message, indicating that the RADIUS server response was correct
7. The RADIUS server sends an EAP-Success message

PEAP – How it can fail



AES – it is truly unbreakable ??

Cache-timing attacks on AES

Abstract. This paper demonstrates complete AES key recovery from known-plaintext timings of a network server on another computer. This attack should be blamed on the AES design, not on the particular AES library used by the server; it is extremely difficult to write constant-time high-speed AES software for common general-purpose computers. This paper discusses several of the obstacles in detail.

Daniel J. Bernstein *

Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
djb@cr.yp.to

Can we make it better ?

- PEAP uses certificates for network -> client authentication, but it can be run with default build-in certificates or with self-created ones, or in password only mode

- certificates bought from a CA (Certificate Authority) are a effective and secure mean of authentication of a network to a client, but they are quite expensive, several hundreds dollar a year

- you can become your own CA, for example CESNET is

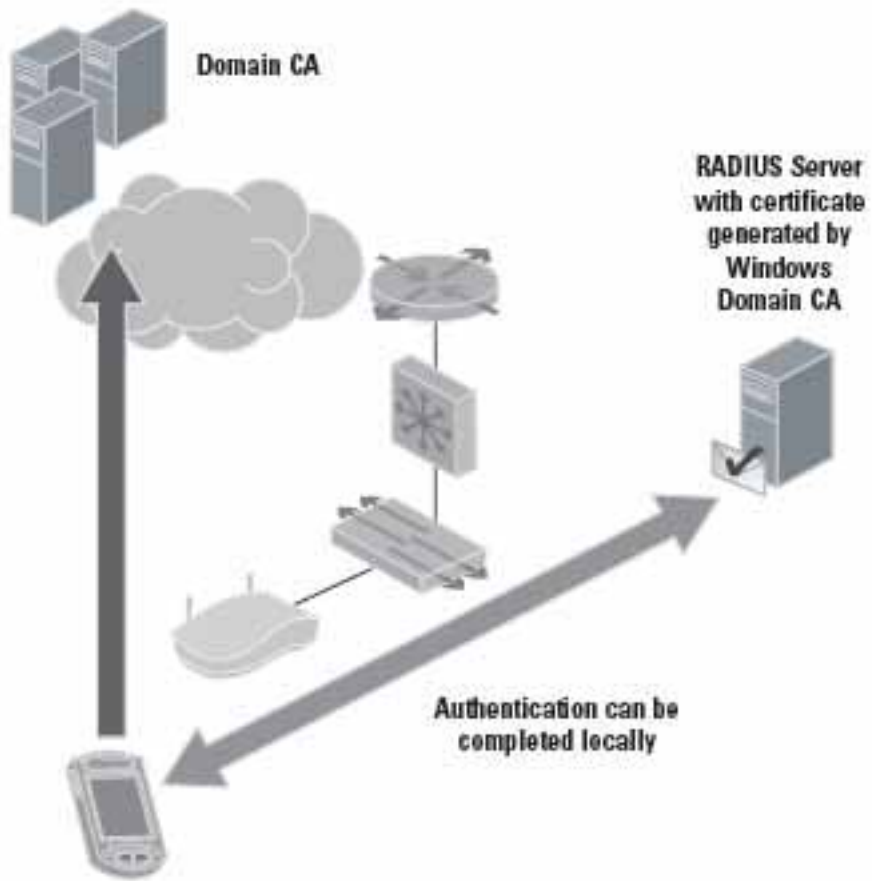
- there is a another possibility, as far only in my head, but it is ☺ , the use of a asymetrical encryption algorithm, something like Public-key cryptography for the network -> client authentication would effectively prevent any MITM perimeter attack, without the need for a secure certificate, which you would need to pay, or making yourself a CA what is not the right thing for every organization, with my idea every user would only need his user name, password and a network public key

Using certificates in WLANs

Using certificates from a CA is secure

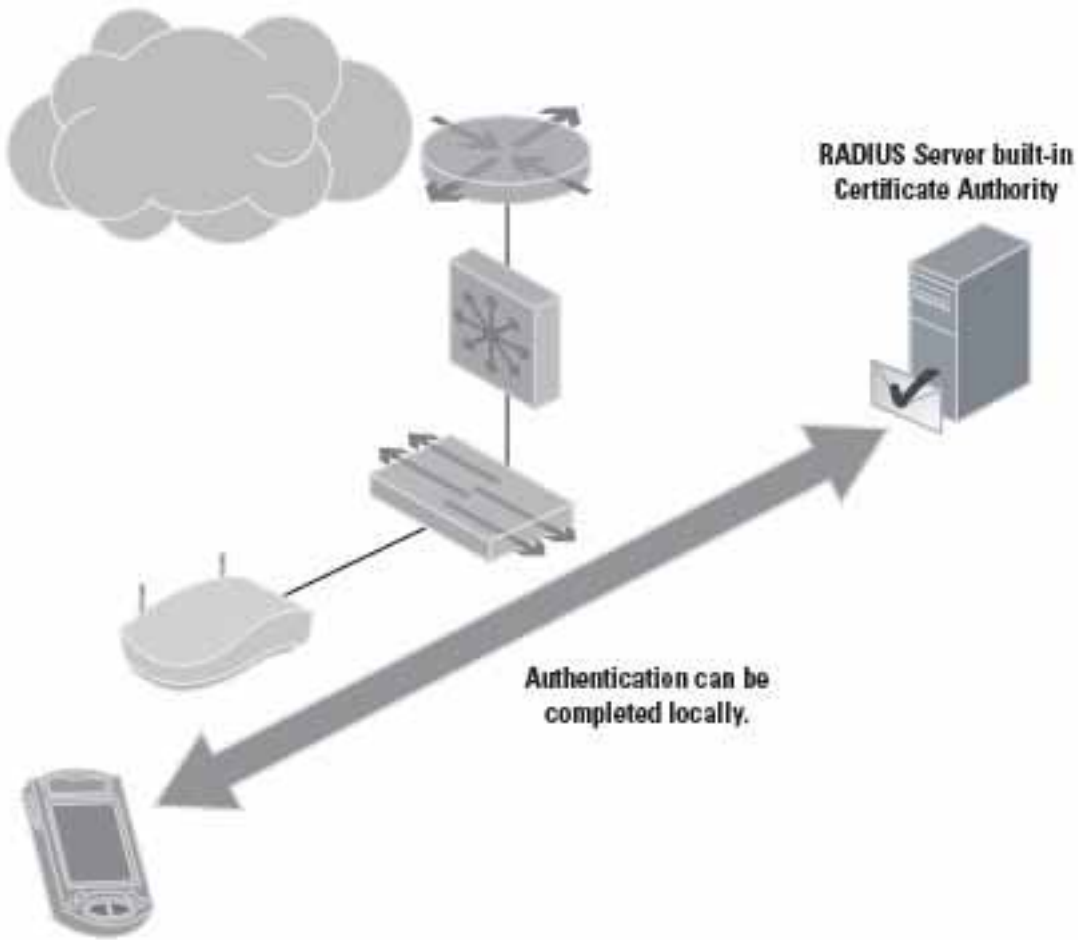
This can be a problem, because the client has no connectivity to the Internet in this phase of authentication

The certificate can be validated only localy against the root certificates the client has stored



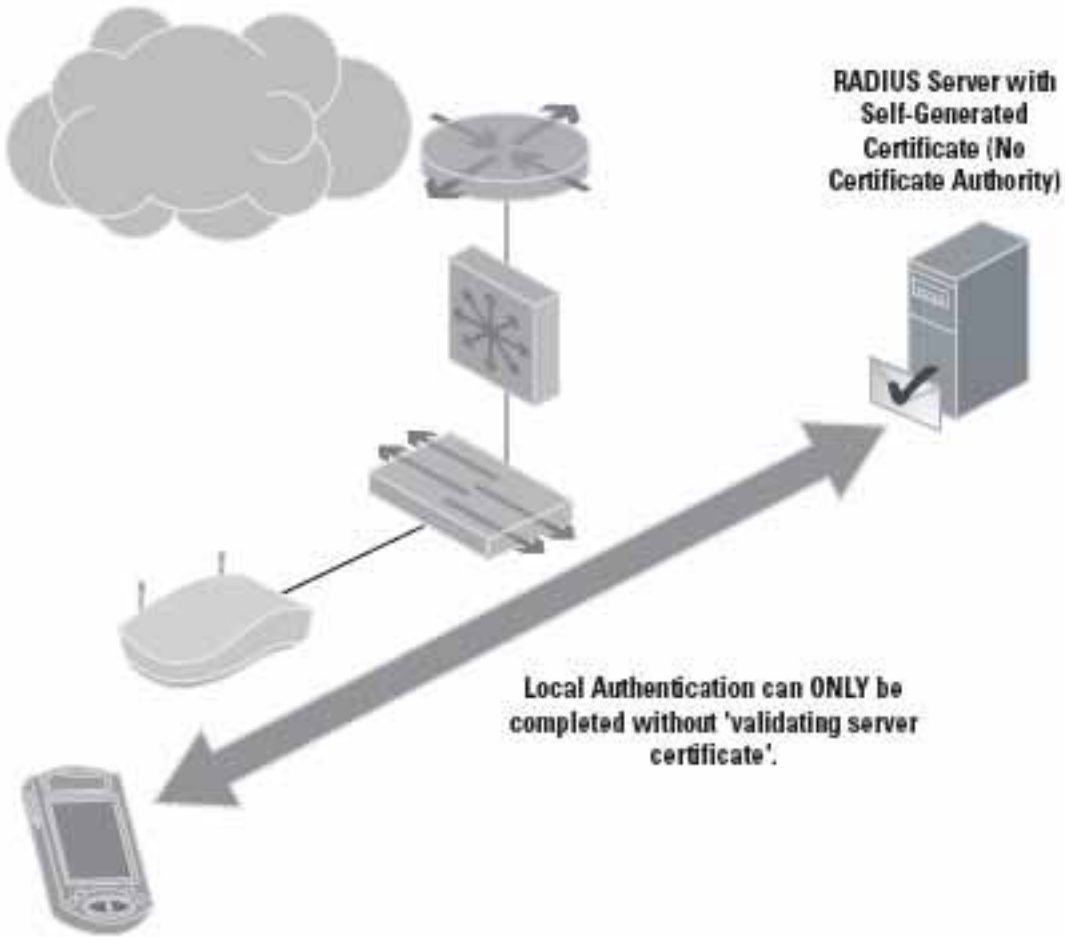
Using certificates in WLANs

The RADIUS server can be its own certificate authority



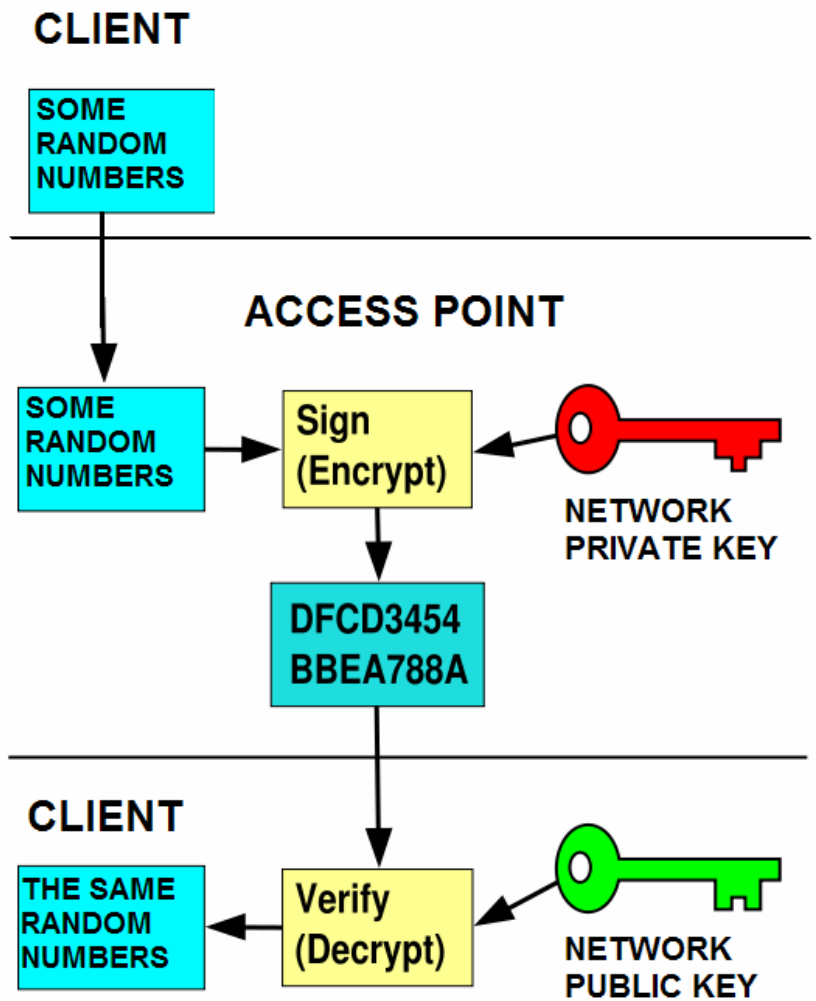
Using certificates in WLANs

Or any CA at all



How could it be done without certificates ?

- The process could look like this:
  - client chooses a network, it thinks it has the correct keys to, and should have access
  - client send a auth. request to the AP containing random numbers
  - AP responds with the random numbers sent from user encrypted using the NETWORK PRIVATE key
  - client uses the NETWORK PUBLIC key to decrypt the message, if the message is the same as it has send, the network is legitime, and can begin the association process



Can we make it even more better ?

- I am long-time experimenting with native IPv6 in WLANs (no dual-stack, no tunneling)
- this would provide end-to-end security because of the IPsec build-in IPv6
- more effective client auto-configuration
- no address space problems
- QoS features and much more ....
- because most of the Internet is still running IPv4, as a transitionary solution. I choosed TRT (Transport Relay Translation)

Q & A

Sources:

www.cisco.com
www.microsoft.com
www.cert.org
www.us-cert.org
www.nectec.or.th
www.ietf.org
www.cybersiencelab.com
www.freeradius.org
www.wikipedia.org
http://cs.byu.edu
http://eprint.iacr.org
www.berkeley.edu

Computer Networks Laboratory
Department of Computers and Informatics
Faculty of Electrical Engineering and Informatics
Technical University of Košice
Letná 9
042 00 Košice
Slovakia

VoIP @ Lab	www.cnl.tuke.sk/voip
VirtualLab @ Lab	www.cnl.tuke.sk/vlab
Video @ Lab	www.cnl.tuke.sk/video
VRVS @ Lab	www.cnl.tuke.sk/vrvs
Synets @ Lab	www.cnl.tuke.sk/synets
QoS @ Lab	www.cnl.tuke.sk/qos