

# VPNs

Artur Hecker, ENST

# Outline

---

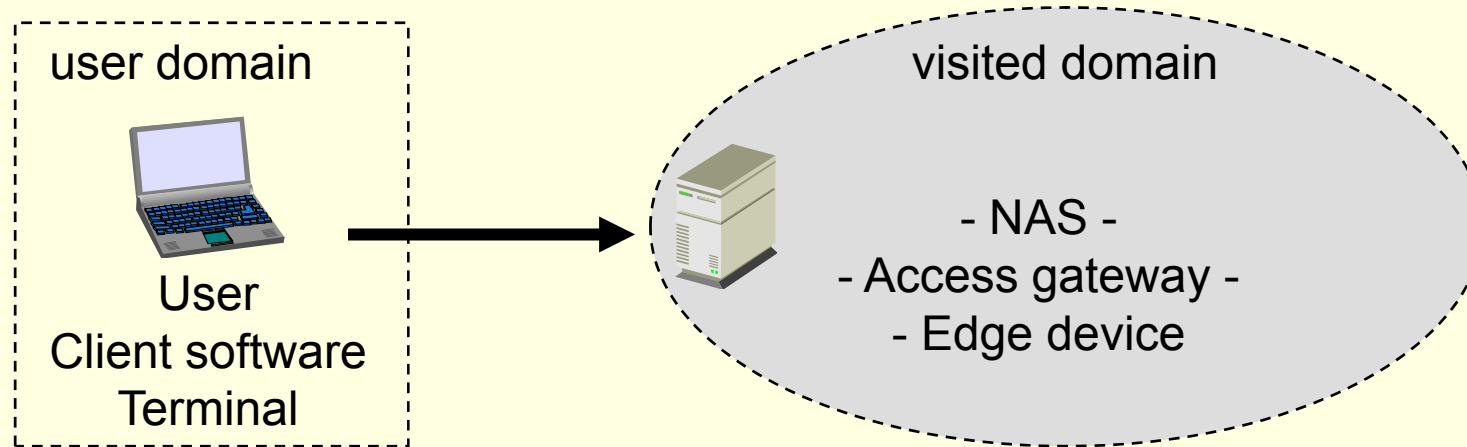
- Introduction
- VPNs
- VPNs in wireless
  - Adoption of the VPN techniques for wireless data security
- Conclusion

# Motivation

---

- Need for more network security
  - Increased danger from outside
  - Hacker/Cracker attacks
  - Cyber terrorism
- Need for more client security
  - More small operators through deregulation
  - No trust in visited networks
  - Demand for data privacy
- New standards, new flaws

# General network access model



- User access with their client software installed on the terminal the network's edge device implementing the corresponding access gateway software and thus acting as NAS
  - User/NAS in AAA definitions

# Access Control and OSI Layers

---

- PHY Layer
  - Hardware modifications in NAS & NIC for new authentication methods
  - Bug fixes are generally difficult
- MAC Layer
  - MAC layer changes required unless implemented in driver
  - Need network standard definitions and compliant devices
  - + No network access required before auth
  - + No firmware updates for new methods
  - + Independent of higher protocols
  - + Fast and inexpensive NAS available
- Higher Layers
  - Requires client software, app modifications
  - Partial network access prior to auth
  - How to find the access control server?
  - Higher = replication in every protocol
  - + Completely independent of the hardware/network standards
  - + Can be used as a uniform access protocol in heterogeneous networks

# VPN

Definition, classification, examples

# What is a VPN?

---

**Virtual Private Network** is

- an overlay over a public network, establishing secure (*private*) connections over a *public* infrastructure

# VPN features

---

- Provides a virtual, i.e. non-physical, data privacy on potentially unsecured networks
  - Access control (authentication, authorization)
  - Encryption
  - Integrity protection
- Can be used to securely interconnect distant subnets
  - Site interconnection
  - Single user interconnection
    - for network access



# VPN: advantages

---

- Overlays different technologies
- Accepted standards exist
- Widely deployed
- Typical clients often integrated in the OS
  - No special software required

# Classification of VPNs

---

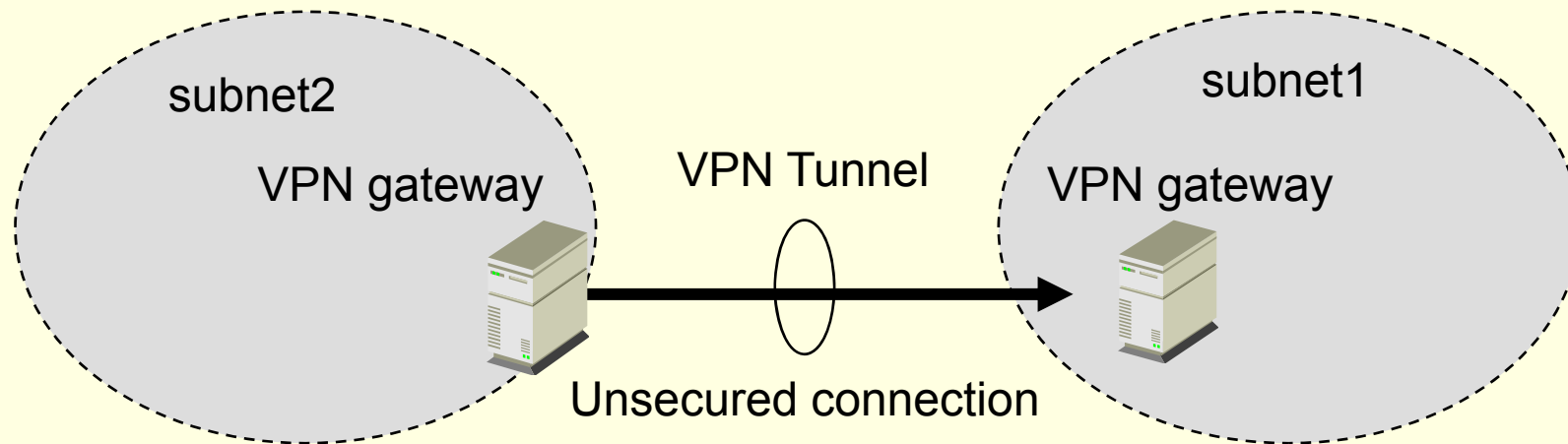
- How and on which OSI layer does it transport the data?
  - Define  $\text{layer}_x$
- From which layer are these data originally?
  - Define  $\text{layer}_y$
- Session signaling (connect, disconnect, change options)
- Typically,  $\text{layer}_y \leq \text{layer}_x$ 
  - Since otherwise there is no real encapsulation/tunneling
- Example:
  - An example of a typical VPN:
    - Public network = Internet
    - The data are transported in secured IP tunnels (L3)
      - Authentication, encryption
    - The data are also IP packets (L3)
    - Minimal signaling defined by the VPN protocol

# Classification of VPNs (2)

---

- Authentication
  - What is authenticated
    - Port
      - Minimal State (close/open)
    - Machine
      - Filter non-authorized machines
    - User
      - Need to distinguish different users on the same machine
      - Filter non-authorized flows
  - How is it authenticated
    - Trust relationships, trust representation (certificates, passwords)
- Encryption
  - Quality
  - Limitations

# General VPN model



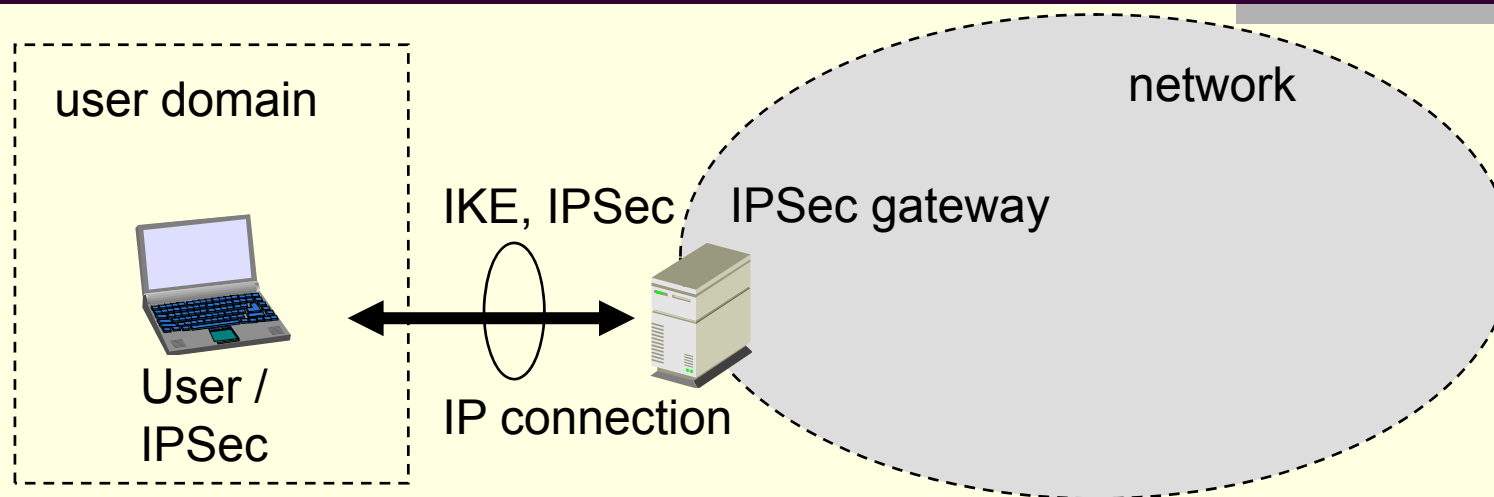
- Site interconnection:
  - Usually IP tunneling by IPSec
- User interconnection:
  - Typically, PPP (L2) is tunneled over the underlying network (typically IP)
  - Examples: PPTP (Microsoft), L2TP (RFC2661 08/1999, since 06/2000 also Ethernet tunneling, L2TPv3 work in progress)

# VPNs on different OSI layers

- Application layer VPN (and above)
  - Secure application layer protocol between two instances forwarding data securely
  - Example: TCP port forwarding over SSH
- Session layer VPN
  - Usage of a common secure session layer
  - Example: usage of SSL for data privacy, e.g. by using `stunnel`
- Transport layer VPN
  - Data transport in TCP or UDP
  - Example: CIPE, secure IP in UDP tunneling
- Network layer VPN
  - Data forwarding through IP tunneling (GRE, IP-IP, etc.)
  - Usually uses IPSec for the transport security (e.g. L2TP)
  - But can use some other security suite (e.g. MPPE in PPTP)
  - Example: the most existing VPNs
- Link layer VPN
  - “Distributed switch”
  - Example: MPLS marking in trusted infrastructures for the establishment of virtual links between remote subnets

Widely deployed

# IPSec



IPSec (RFC2401), IKE (RFC2409) - IP security architecture

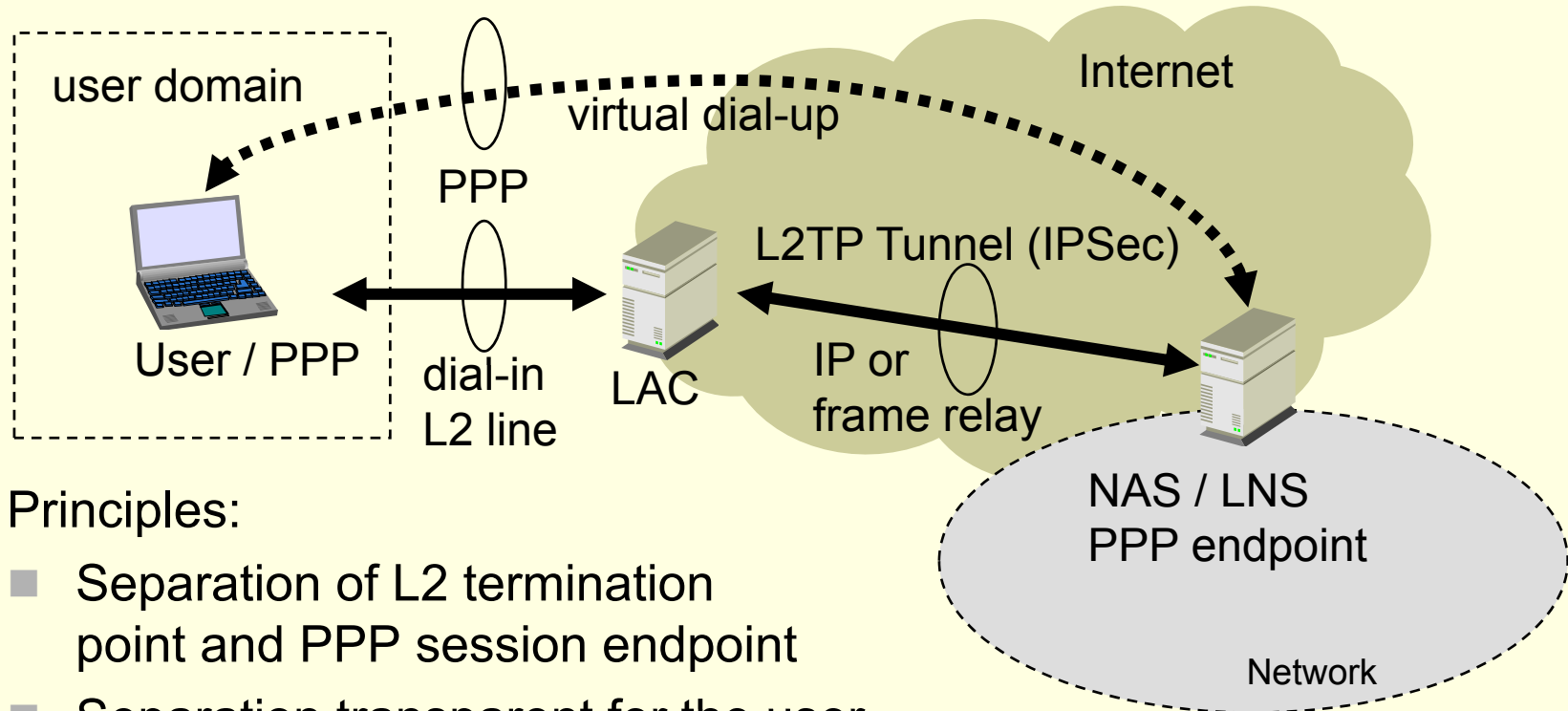
- Identity, authentication, key exchange over IKE
- Adds integrity protection and/or encryption header to every IP frame
- Can be used in transport and tunnel modes
- Security parameters:
  - Identity is an IP (machine level authentication, shared secret or certificate, based on the public key cryptography)
  - Encryption is negotiable (typically symmetric, authentication bound with perfect forward secrecy properties).

# IPSec

---

- Generally, IPSec is not a VPN protocol
- But an important brick for a VPN
  - IKE can be seen as VPN related signaling protocol
  - Transport over IP (L3)
  - Transports IP packets (L3)
- IPSec in a tunnel mode builds a VPN
  - often used for secure remote subnet connection to the main network

# L2TP



## Principles:

- Separation of L2 termination point and PPP session endpoint
- Separation transparent for the user
- LAC and user may be co-located
  - Using a virtual PPP link



# L2TP

---

- Includes the necessary signaling primitives
  - Call establishment, session control, etc.
  - Transports data in GRE tunnels over IP (L3)
  - Transports PPP data (L2)
- Designed for call cost minimization during remote modem access
  - Billed call goes from the user to the LAC but the virtual dial up is from the user to the LNS

# L2TP VPN

---

- Serves as VPN protocol, when used with a co-located LAC
- Is an IETF generalization of the original PPTP idea
- Is originally meant to transport PPP frames only. Newer versions are capable of other transports
  - L2TPv3 in an IETF draft version
    - defines an arbitrary payload transport
  - “Pseudo-Wire” discussions in the IETF
    - E.g. L2 subnet interconnection over Internet links

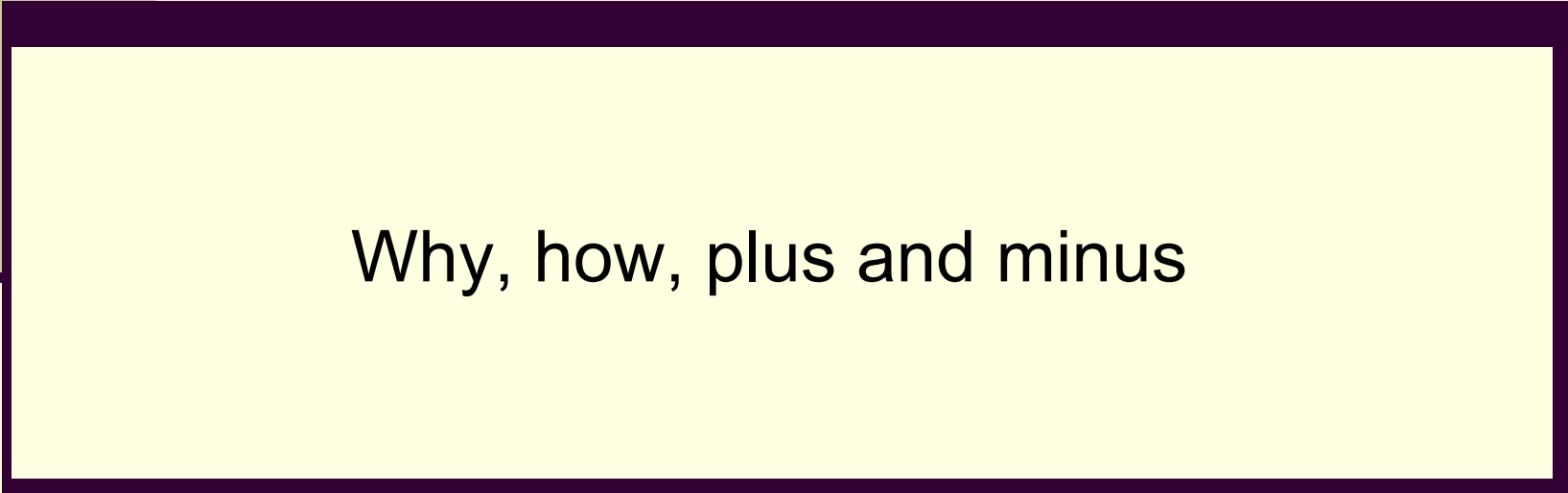

# VPN & firewalls

---

- Problem: VPNs dig holes in the firewalls
  - By defining trusted traffic
  - Tunneled & encrypted and thus unreadable
- VPN: “Boomerang effect”
  - Easy to secure one gateway, but how to secure all the clients?
  - Who/what enforces the local security policy at remote clients?
    - Need for a “host firewall” or similar solutions
  - If the clients are vulnerable how can their traffic be trusted?
  - Need of a second perimeter \*after\* the VPN gateway
  - Need for application level filtering, IDS, antivirus, etc.
- Evolution of firewalls:
  - 1G: Separate VPN / firewall
  - 2G: Proxies, application gateways
  - 3G: Stateful packet inspection (SMLI)
    - User profile snapshots
    - Policy and sanity checks
    - Integrated intrusion detection systems (IDS)



# VPNs & Wireless



Why, how, plus and minus

# Motivation

---

- Security problems in wireless
  - General security problems
    - Naturally broadcast
      - Passive snooping attacks
    - No trusted connecting physical medium
      - You know who is connected to the other end of the cable
    - Indeterministic wave propagation
      - No clear network limits
    - High bit error rates
  - Standard specific security problems
    - Security problems in 802.11
      - Authentication worthless
      - No integrity function
      - WEP broken
- Security in wireless
  - A “must be”
  - But harder

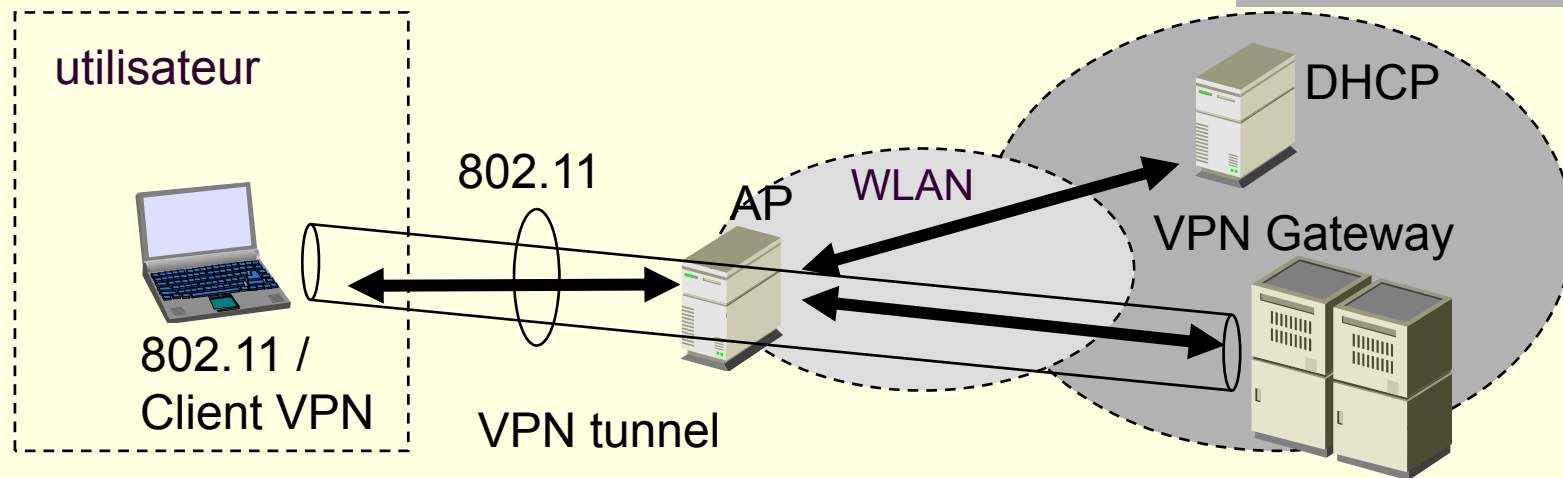
# VPNs & Wireless

---

## ■ Advantages

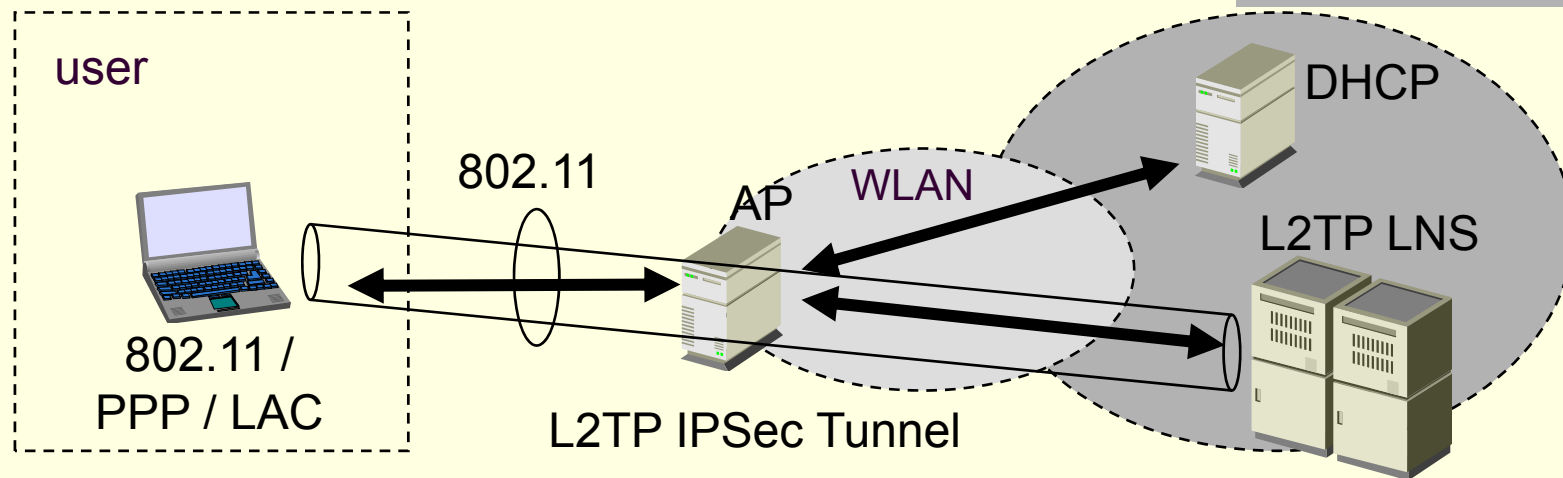
- Largely deployed, available technique
  - Well-known, understood, robust
- Independent of the specific standard
- Can correct integrated standard flaws
  - E.g. in 802.11
- Easy to deploy
  - Can be added on top of the existing physical network
  - Needs a gateway and client software

# VPN with Wireless LAN

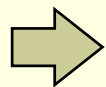


- Client has free access to the WLAN
  - Only DHCP and VPN services
- Client gets a DHCP address
- Client uses his VPN client to authenticate to the VPN gateway
  - E.g. IPSec
  - PPTP (Microsoft), L2TP with a co-located LAC

# Example: L2TP & Wireless LAN



1. Client connects to the WLAN
2. Client obtains an IP address over DHCP
3. Client has a preconfigured L2TP client with the address of the LNS and a user/secret combination
4. Client uses L2TP signaling to authenticate to LNS
5. Client uses the co-located LAC to encrypt data which traverses the wireless link



PPP frames are sent to the LAC, are encapsulated there and arrive at the LNS where they are decapsulated and bridged to the local network



# VPN weaknesses

---

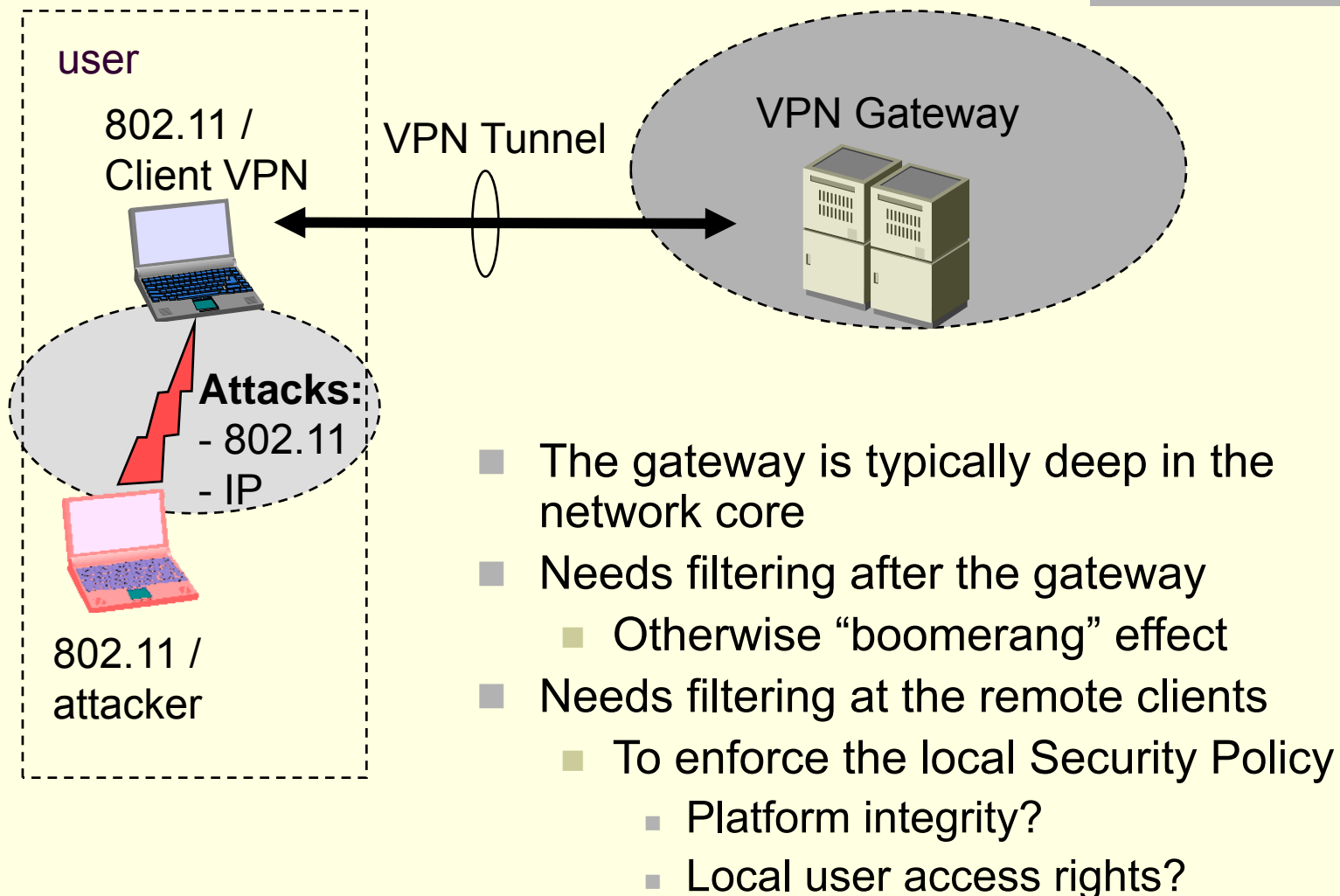
- No infrastructure protection
  - WLAN completely open
  - Attacks possible between the clients
    - At the WLAN layer (L2)
    - But also at any superior layer (e.g. IP)
  - DoS attacks possible through the WLAN at the IP-layer
- Pure software solution
  - Can be costly (e.g. for the PDAs, ->Wireless security processing gap)
- Adds some protocol overhead
  - Wireless resources - bandwidth - are scarce
- One gateway for the whole network
  - Scaling?
  - Single point of failure
  - Needs redundant gateways – costly!

# VPN weaknesses (2)

---

- Dilemma: bandwidth vs. performance
  - If the bandwidth is limited, the VPN protocol overhead becomes a critical issue
  - Else in a high throughput network (WLAN), the central VPN gateway becomes a bottleneck
- Example: 802.11g WLAN with 10 access points
  - Worst case scenario: 300Mbps of data to treat in real time
  - The gateway would need special hardware
    - Costly
  - Multiple gateways make the thing even worth
    - Equipment costs, management...

# Illustration of weaknesses



# Conclusion

---

- VPNs are a reliable ready-to-use technique
  - Well suited for remote access to enterprise networks
    - Over dial-up, ADSL, etc.
- VPNs do not protect the infrastructure
  - Are often infrastructure- and technology-independent
- VPNs provide data privacy (C.I.A.)
  - Flexibly: on-demand, per-service, per destination, etc.
  - Blindly: no adaptation to offered service properties and/or limitations
- VPN over wireless can be problematic:
  - Either it implies overhead
  - Or it cannot handle the incoming traffic
  - Is implemented in software: computation overhead
    - Battery, weak terminals...