DoS and Authentication in Wireless Public Access Networks

Daniel B. Faria, and David R. Cheriton, Stanford

WiSe'02 ACM September, 2002

林佑青 2002/10/18

Outline

- Introduction
- Access control framework
- Wireless security
- IEEE 802.11 and 802.1X
- Public-key based secure internet access
- SIAP、SLAP
- Other DoS attacks
- Conclusion

Introduction

- Every mechanism has the potential of creating a vulnerability or enabling denial of service (DoS) attacks.
- Less mechanism is better, restricting the provided services to the ones that are really essential to creating a secure solution.
- Secure association is an important service to provide.

Introduction (cont.)

- DoS attacks effective are made possible by the lack of implementation of essential services or wrong assumptions made about the environment.
- SIAP/SLAP can be used to implement a secure association service and avoid the DoS attacks.

An access control framework

- Mutual authentication
- Flexible authorization
- Access verification
  (message authentication code、replay detection)
- Interoperability
- Simple user interface
- Data confidentiality and integrity

An access control framework (cont.)

- Authentication protocol provides mutual authentication and sets up fresh session keys and parameters.
- Lower-layer protocol receives the parameters from the authentication protocol and use them to provide confidentiality, integrity.
- The scheme enforced the bond between the IP address and the session keys while eliminating specific attacks.

Wireless Security

- Access point authentication
- Association is the service used to establish access point/station mapping.
- Use an authentication server (AS) hidden behind the access points.
- The access control mechanism should provide the client with access point authentication.
- Authentication should be executed before association in order to eliminate DoS attacks.

IEEE 802.11 Authentication

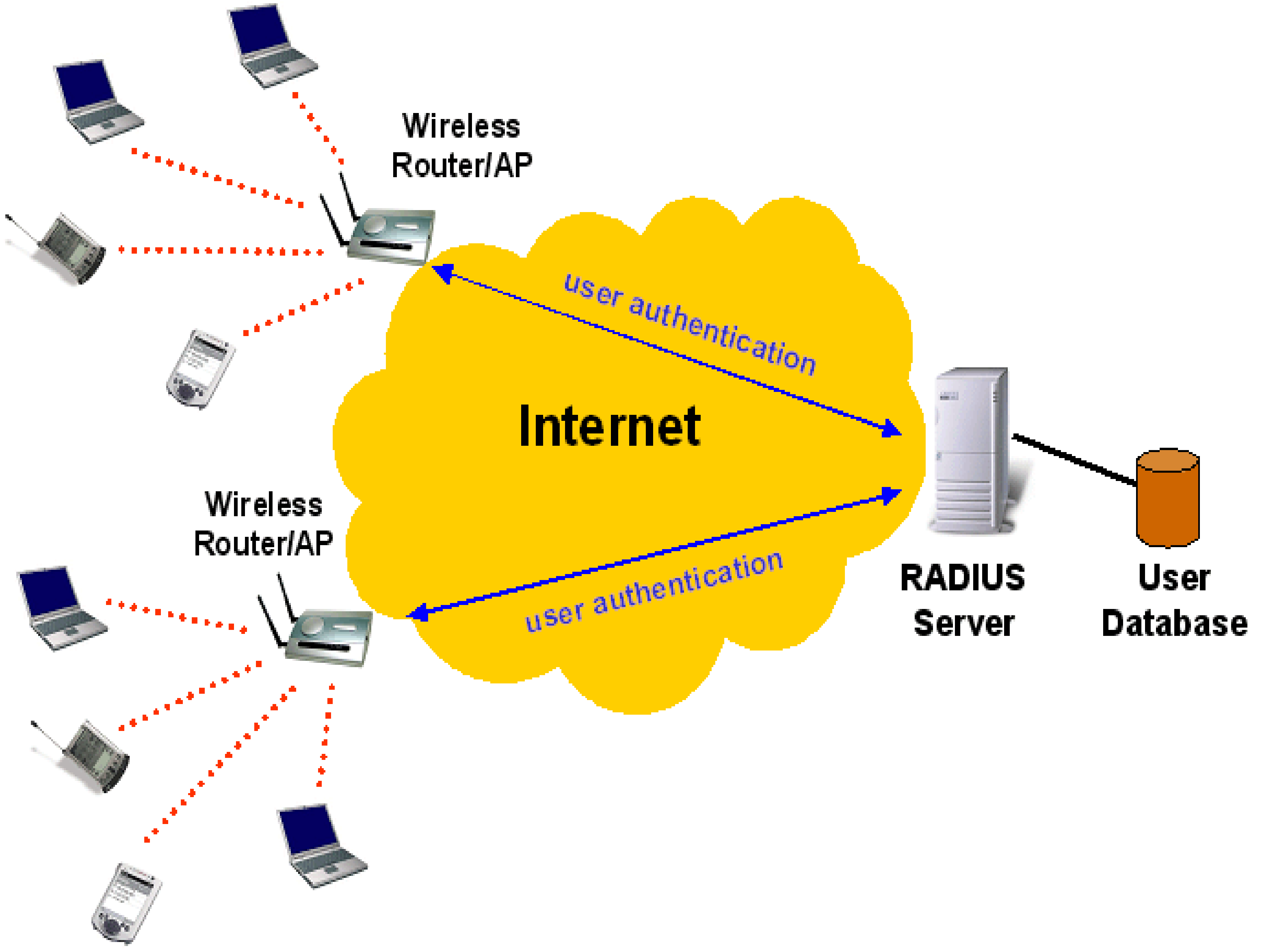
- The standard had very limited objectives when dealing with authentication and confidentiality.
- It defined an authentication protocol based on a shared key know by APs and client machines. A four-message handshake is performed in order to authenticate the client.
- The authentication mechanism is turned off when the protocol is integrated with the 802.1X framework.

IEEE 802.11 Association

- A finite-state machine (FSM) in the standard defines three states for a client:
  - Unauthenticated/unassociated
  - Authenticated/unassociated
  - Authenticated/associated
- The FSM requires the client to run the authentication algorithm before it can associate with a AP.

IEEE 802.1X

- Port-based access control
- The standard uses the EAP (Extensible Authentication Protocol) protocol as a tunnel between client and server, passing through the access point.
- Between the AP and the authentication server, RADIUS (Remote Authentication Dial In User Service) is the option as the encapsulation protocol.


Wireless
Router/AP
user authentication
Internet
Wireless
Router/AP
user authentication
RADIUS
Server
User
Database

Limitations of IEEE 802.1X

- One of the limitations of 802.1X is that the authenticator, AP, is never authenticated by the client.
- 802.1X involves far too many protocols and encourages incompatibility between domains.
- Its integration with 802.11 is poor and has been shown to be vulnerable to various attacks.

Public-key-based secure Internet Access

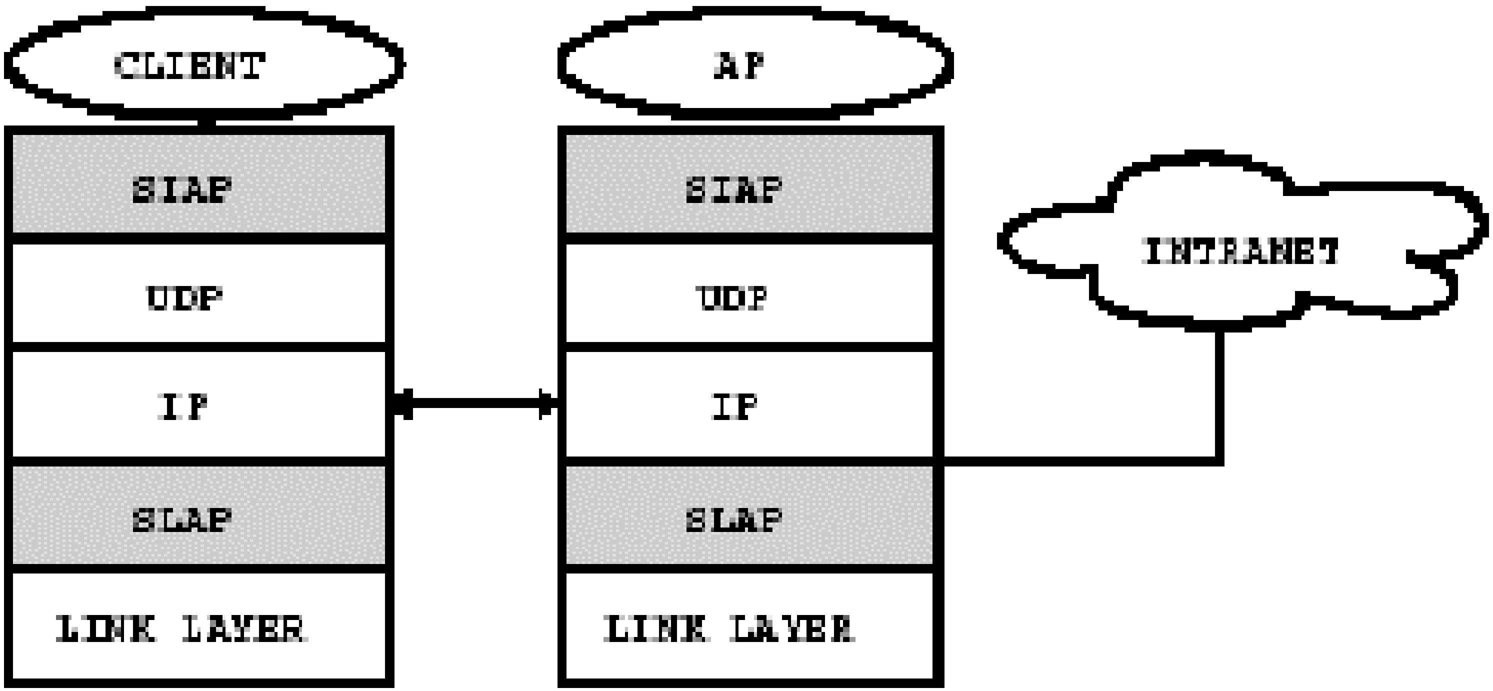


Figure 1: Protocol stack.

- Both protocol are implemented in the clients and access points.

SIAP (Secure Internet Access Protocol)

- SIAP client performing an authentication handshake with the SIAP server in the access point.
- The three-message handshake provides mutual authentication and supplies the client with fresh session keys, tied to a given IP address selected by the SIAP server.
- In SIAP, every client and access point has a public key signed by a known Certification Authority (CA).

SIAP Handshake

Handshake

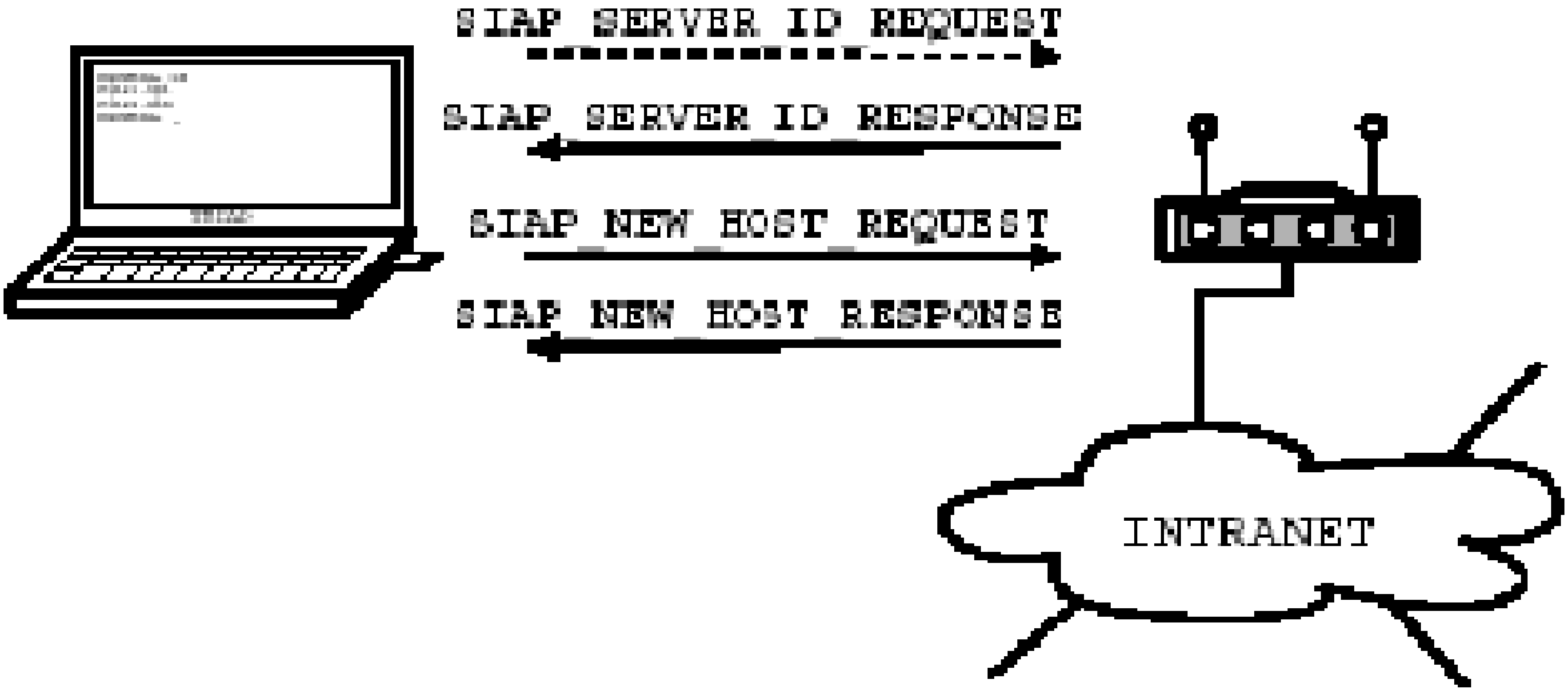


Figure 2: SIAP handshake.

SLAP (Secure Link Access Protocol)

- Located above the link layer, intercepting and processing all incoming and outgoing frames.
- SLAP can be seen as SIAP’s agent over link-layer frames, providing confidentiality, sender authentication, integrity, and replay detection.

SLAP

- After the client is authenticated, the generated keys are passed from SIAP to SLAP.
- All frames receive the SLAP header and can be encrypted and authenticated after the security state is set in both client and AP.

Encryption and Authentication

- SLAP uses AES in counter mode to encrypt the SLAP packet.
  - → fast implementation in both hardware and software.
- SLAP uses HMAC-MD5 as the authentication algorithm.
  - → fast implementation as it is based in the MD5 hashing function.

AES (Advance Encryption Standard)

- Select the "Rijndael" cryptographic algorithm for the proposed AES.
- Support 128,192,256-bit keys and block size.
- AES-CTR mode provides high parallelism, each plaintext block can be encrypted independently.

Authenticate and Associate

- The association handshake is modified to use a key shared between client and AP and provide mutual authentication.
- Before a client gets associated with an AP, it needs to set up an association key by executing the SIAP handshake.
- SIAP messages destined to the AP are not processed by the SLAP module.

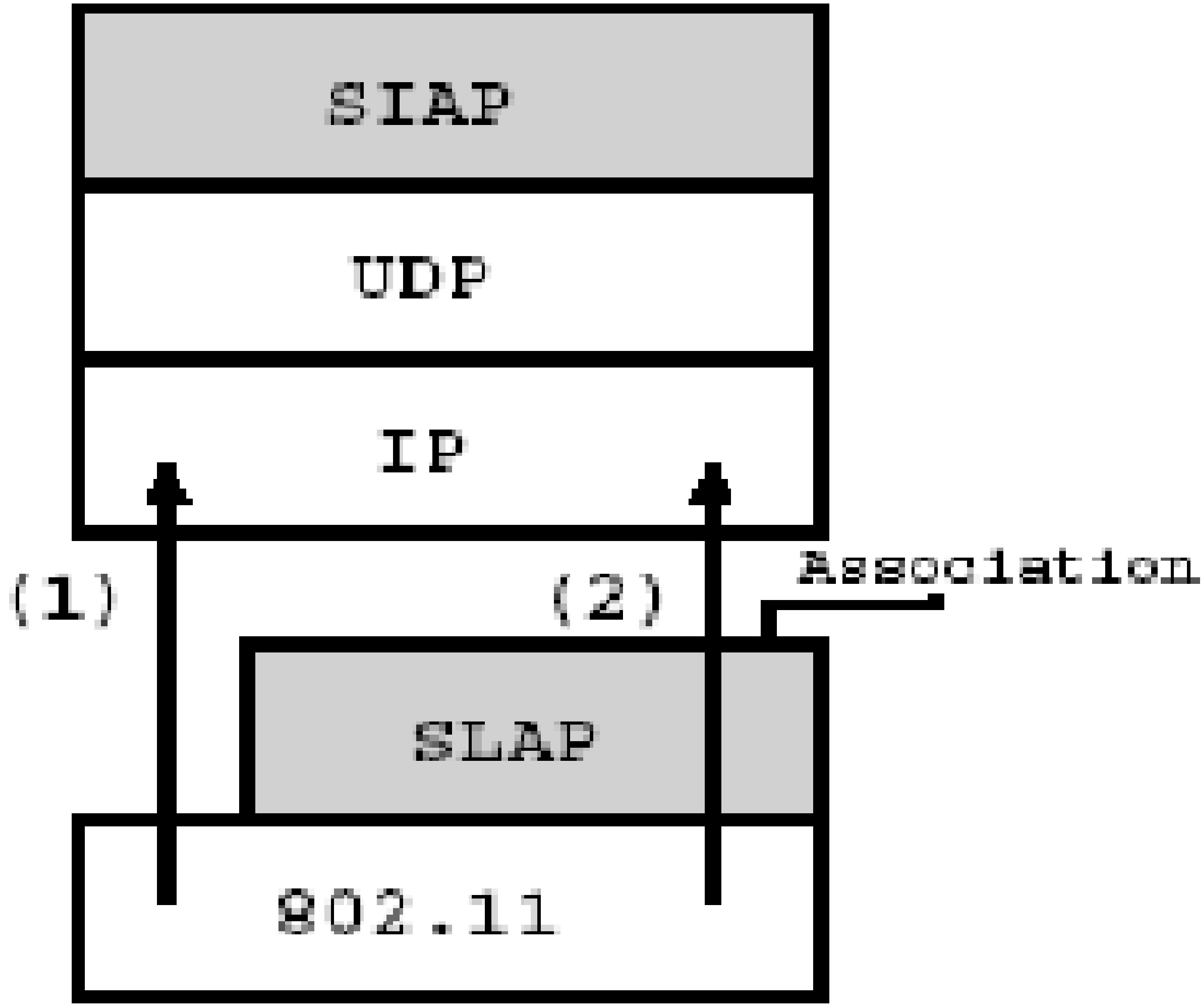


Figure 5: SIAP and SLAP integration.

Flexibility

- By making SLAP link-layer independent, the architecture can be used in non-802.11 networks.
- As the encryption performed by WEP is part of the link-layer protocol, the access points are necessarily the other endpoint of the secure channel.

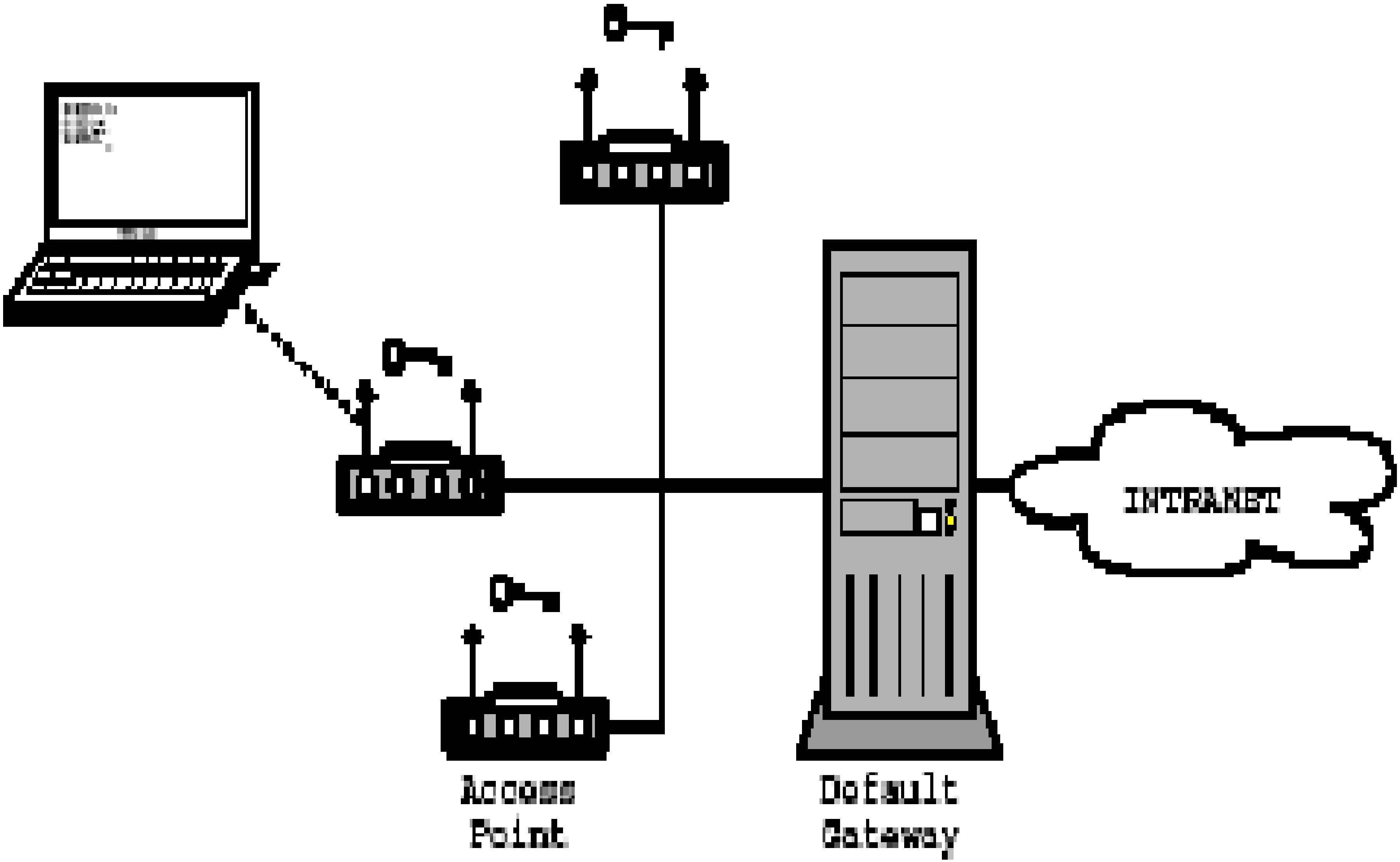


Figure 6: SIAP and SLAP in a wireless network.

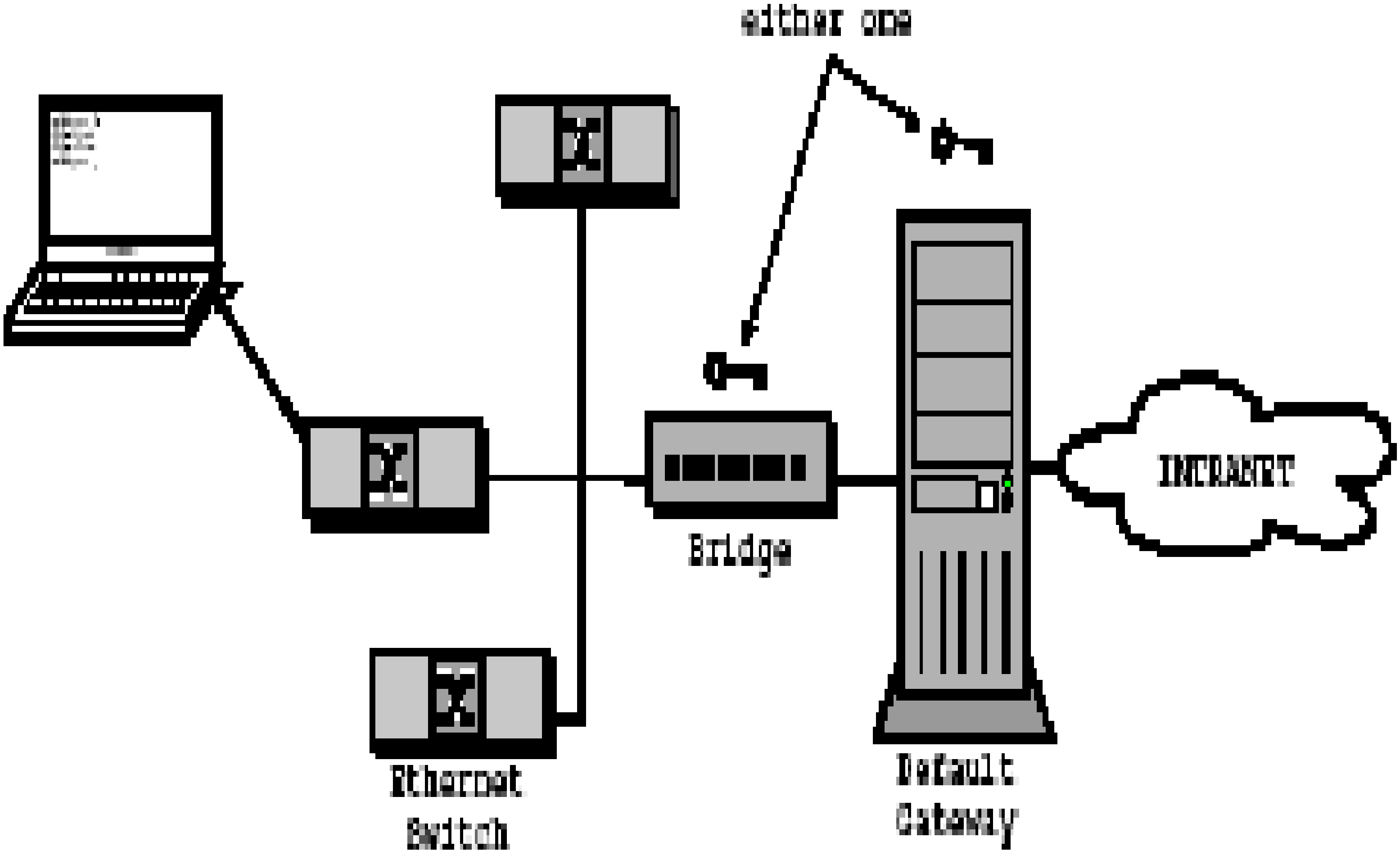


Figure 7: SIAP and SLAP in an Ethernet network.

Other DoS attacks

- Pre-authentication attacks

Some security architectures require the client to execute some configuration steps before it can go through the authentication process.

- Attacks on authorization

Giving the same key to multiple clients can be considered a flaw in authorization and is insecure.

- Attacks on verification

Based on the lack of important services, such as replay detection or sender authentication.

Preliminary results

- SLAP overhead: 50 μs ~ 330 μs (client)
  10 μs ~ 170 μs (AP)
- The overhead has little effect over representative TCP connections.
- The SIAP handshake was measured to terminate in hundreds of milliseconds, mainly due to the private key operations incurred by SIAP.

Conclusion

- Most of the attacks are caused by the lack of important services, such as replay detection and access point authentication.
- The architecture, composed of the SIAP and SLAP protocols, that solves the problem by coalescing essential services in a secure way.