Security in WAP 1.x and WAP 2.0

Seminararbeit

Ruhr-Universität Bochum
Zhang chen

Sommersemester 2007

Overview

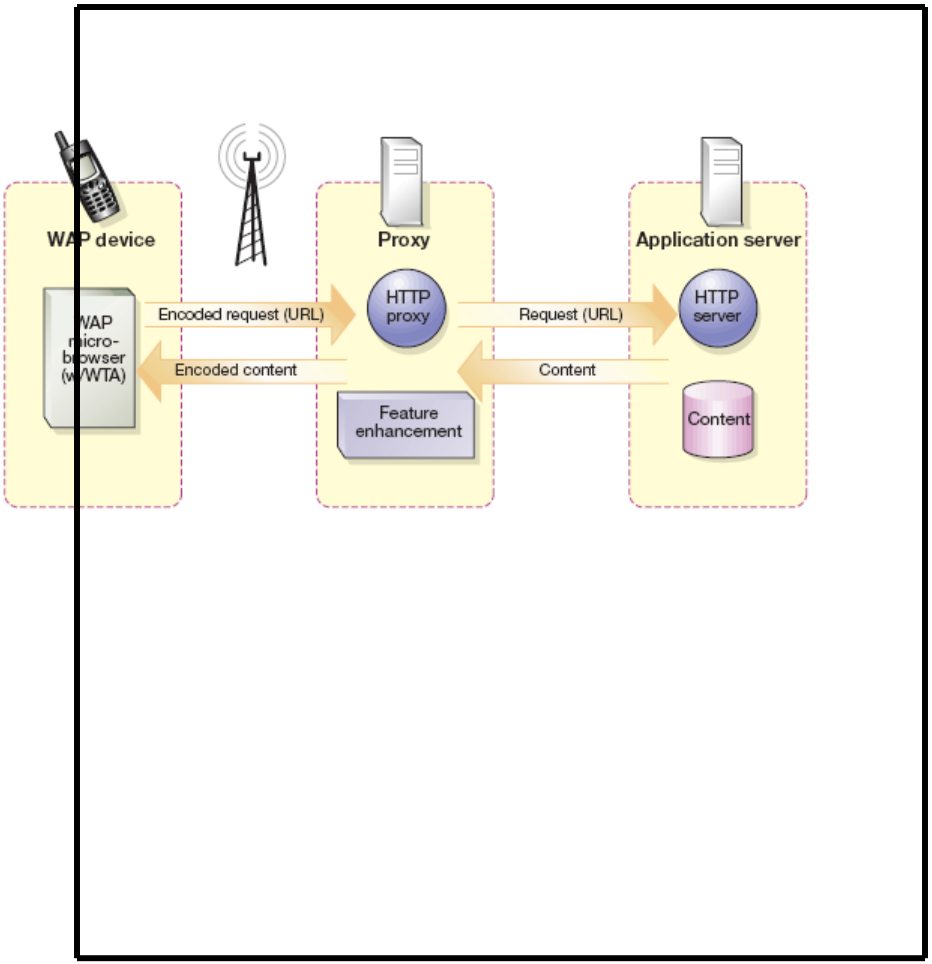
2. WAP1.x and WAP 2.0
3. Security problems with WAP

Introduction

WAP:

- protocol stack for wireless communication
- Internet access from mobile phone or PDA.

WAP 1.x



WAP 1.x architecture:

- WAP browser
- WAP gateway
- application server.

Wireless Transport Layer Security (WTLS)

WTLS: wireless variant of the SSL/TLS protocol, to secure the communication between the mobile phone and the gateway.

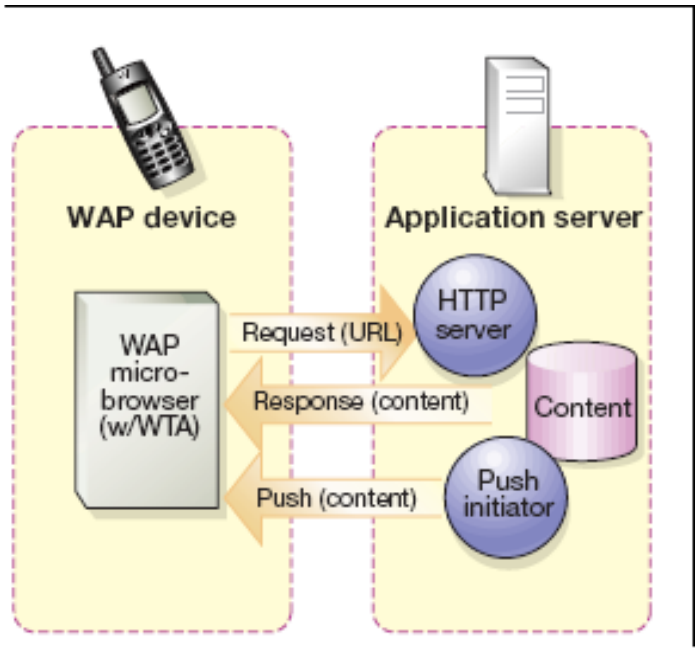
- Privacy

  Symmetric cryptography
- Data integrity

  Message Authentication Codes (MAC)
- Authentication

  Certificates

WAP 2.0


WAP device
Application server
WAP
micro-
browser
(w/WTA)
Request (URL)
Response (content)
Push (content)
HTTP
server
Content
Push
initiator

Transport Layer Security (TLS)

WAP 2.0:

use TLS 1.0 between mobile terminals and application server (end-to-end security!)

5. TLS Handshake Protocol
   - authenticate server to client
   - agree on encryption algorithm and cryptographic keys
6. TLS Record Protocol: provide connection security
   - private: Symmetric cryptography
   - reliable: Keyed-MAC

Security

- Gateway security problem
- WTLS security problem

WAP gateway security problem

- Only in WAP 1.x architecture
- Data is decrypted and again encrypted in WAP gateway
- No end to end security => man-in-the-middle-attack

Security problem with WTLS

- Predictable IVs
- The weak XOR MAC
- 35-bit DES encryption
- Unauthenticated alert messages
- The RSA PKCS #1 attack
- Plaintext leaks
- Probable plaintext attacks

Predictable IVs lead to chosen-plaintext attacks against low-entropy secrets

- CBC mode

Need new IV for encrypting each packet

- Linear IV computation

New IV: the sequence number of the packet xor the original IV

- Each keypress as individual packet
- Oracle: check if the guessed password letter correct

The weak XOR MAC and stream ciphers

- 40-bit XOR MAC
- Provide no message integrity protection if stream cipher are being used, regardless of the key length.

35-bit DES encryption

- 40-bit DES key
- The effective key only 35 bit, each byte has a parity bit

Unauthenticated alert messages

- Alert message are used to notify the client if a problem in sending the datagram.
- Some of alert message are sent in plaintext and not properly authenticated→ an attacker replace an encrypted datagram with an unauthenticated plaintext with the same sequence number.

The RSA PKCS #1 attack

- The protocol includes an oracle that tells whether a given packet has a correct PKCS #1 version 1.5 padding.
- RSA messages can be decrypted with approximately 2^20 chosen ciphertext queries

Plaintext leaks

- Eavesdropper can determine the initial IV of each packet under exportable from the Hello messages and the sequence number alone

Probable plaintext attacks

- Brute force on a symmetric encryption
- The correct key recognized with trial decryption of one or more blocks

WAP 2.0 with TLS

- No gateway security problem: end-to-end security