



# Introduction

---

- "Security Issues In Wireless Environments"
  - Introduction to WAP, WTLS
  - Differences between WTLS and TLS
  - The future: WAP-NG
- Dean Vogler
  - email: [vogler@labs.mot.com](mailto:vogler@labs.mot.com)
- Motorola Labs
  - Communication Systems and Technologies Labs
    - Security Technology Research Lab



# WAP Deployment

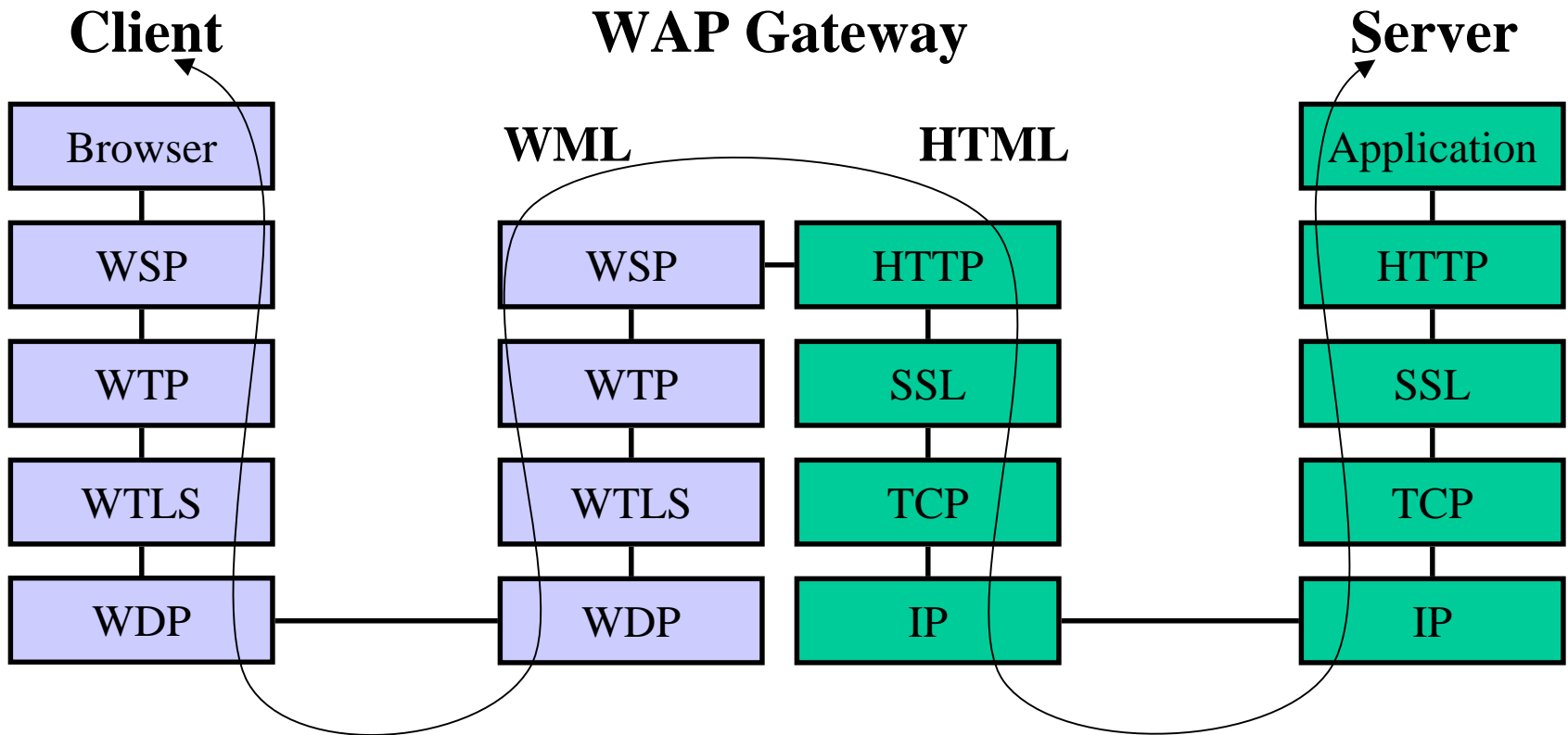
---

- 500+ member companies in WAP
- WAP Forum members represent:
  - over 90% of the global handset market
  - carriers with more than 100 million subscribers
- The number of wireless Internet users will exceed PCs on the Internet by 2002
- Wireless Web users increasing from 300 million last year to one billion in 2003

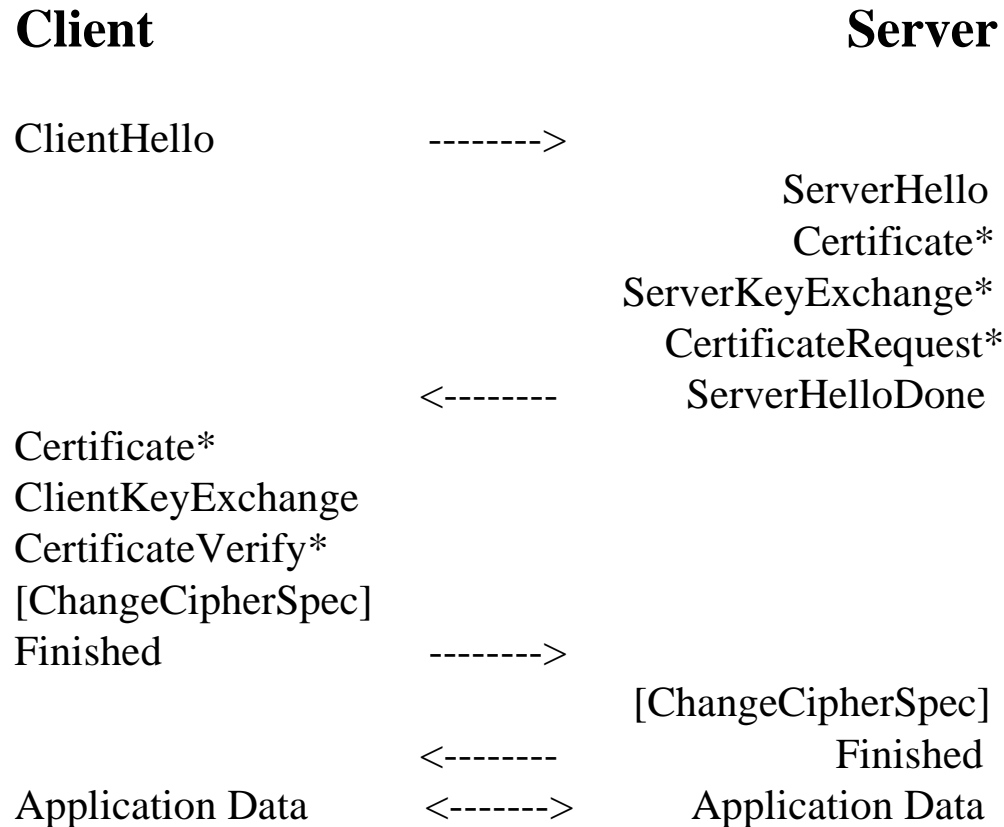
# Mobile Phone Secure Session

WAP Protocols

Internet Protocols



# Handshake Message Flow



\* Indicates optional or situation-dependent messages that are not always sent.

# WTLS Class Definition

## Class 1 WTLS Implementation

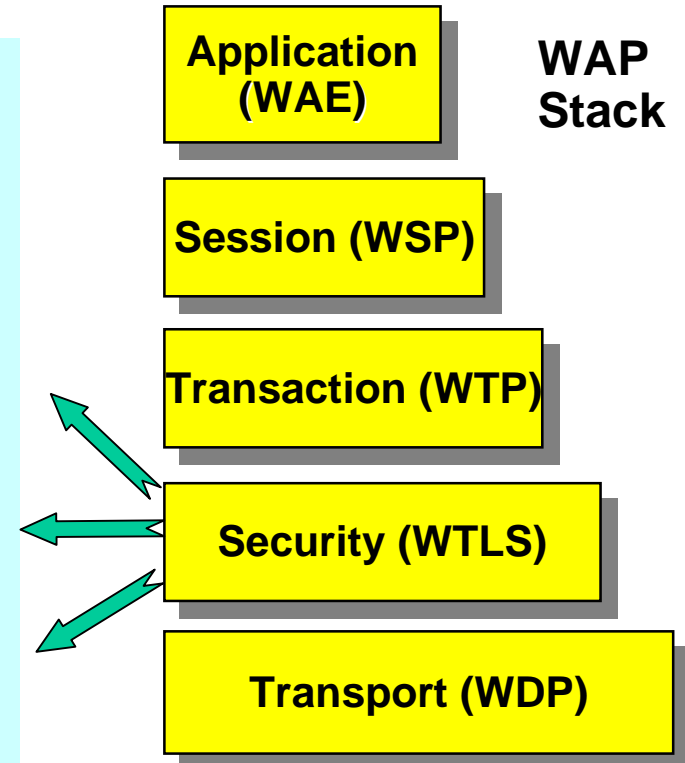
- No certificates exchanged in secure negotiation
- Client and Server setup secure tunnel anonymously
- Secure session created, but who is talking to who?

## Class 2 WTLS Implementation

- Server certificate sent to client during handshake
- Client authenticates server
- User (client) obtains server's identity before wireless transaction (e.g. shopping with credit card)

## Class 3 WTLS Implementation

- Server & client certificates exchanged
- Client authenticates server
- Server authenticates client
- High security transactions (e.g. wireless banking) need client & server authentication



### Bearers:

**GSM:** SMS, USSD, CSD, GPRS

**CDMA:** SMS, CSD, Packet

**TDMA:** SMS, CSD, Packet

**iDEN:** CSD, Packet

**PHS, PDC:** CSD, Packet

**Others:** CDPD, ReFlex



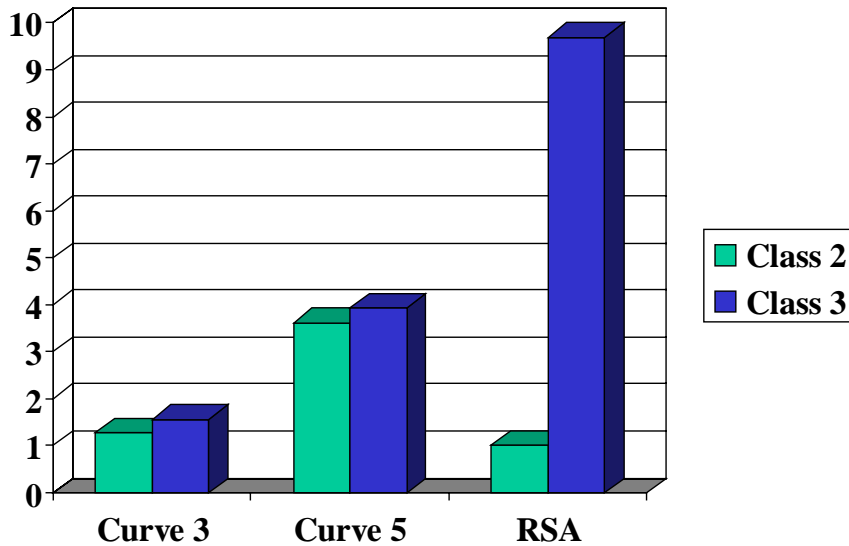
# Key Differences Between WTLS and TLS

---

- Key refresh for long-lived connections
- Optimised handshaking
- Compact certificate (WTLS certificate)
- Shorter parameters
- Client certificate URL
- Algorithms (ECC)

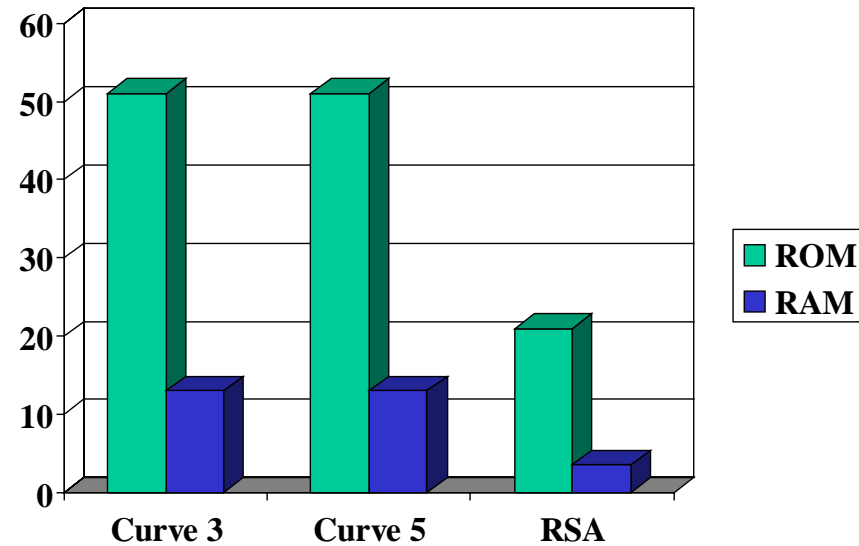
# RSA & ECC

## WTLS Client Execution Time Comparison



## WTLS Class 3

## Memory Size Comparison



- Total execution time for class 3 security functions can range from < 1 sec for ECC to > 10 sec for RSA implementation under weak signal conditions
- Comparison is from Motorola Labs using the best implementation available from several toolkits
- Curve 3 & 5 are 163-bit  $F_2^n$  ECC curves as defined in WTLS spec. RSA using 1024 bits with client using small public key exponent



# WAP Next Generation (NG)

---

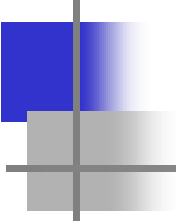
- Convergence with W3C and IETF Internet standards
- Support for 3G wireless devices and networks
- http, html, TLS, TCP/IP to the handset
  - But wireless friendly versions of these protocols



# Characteristics of 2G and 3G Devices and Networks

---

	<u>2G</u>	<u>3G</u>
CPU	5 MIPS	20 MIPS
Flash Memory	100 KB	20 MB
RAM	100 KB	1 MB
Minimum Bandwidth	100 bps	14.4 kbps
Maximum Bandwidth	9.6 kbps	384 kbps



# End to End Performance Modeling

System / Protocol	Server Auth.	Server & Client Authentication		Application Data
	RSA	RSA	ECC	
3G & TLS	1365 msec	3851 msec	2050 msec	617 msec
2G & WTLS	1886 msec	9660 msec	2440 msec	982 msec

- Application Data is 850 bytes of a request/reply example
- RSA used for client verify -- RSA & ECC reported for client signature
- Analysis done with typical values for system bandwidth, latency, processor performance & resource sharing



# Future Areas Of Research

---

- Current WAP/WTLS work items
  - End-to-end security (handset to end-server)
  - Application-level mechanisms for encryption and signing/verification
- Other WAP security issues
  - WAP public key infrastructure (WPKI)
  - Wireless Identity Module (WIM), Smartcards
- Public key algorithm performance (Elliptic curve, RSA)
- Bluetooth security