- Cryptographic Execution Time for WTLS Handshakes on Palm OS Devices

Neil Daswani
neil@yodlee.com
September 21, 2000

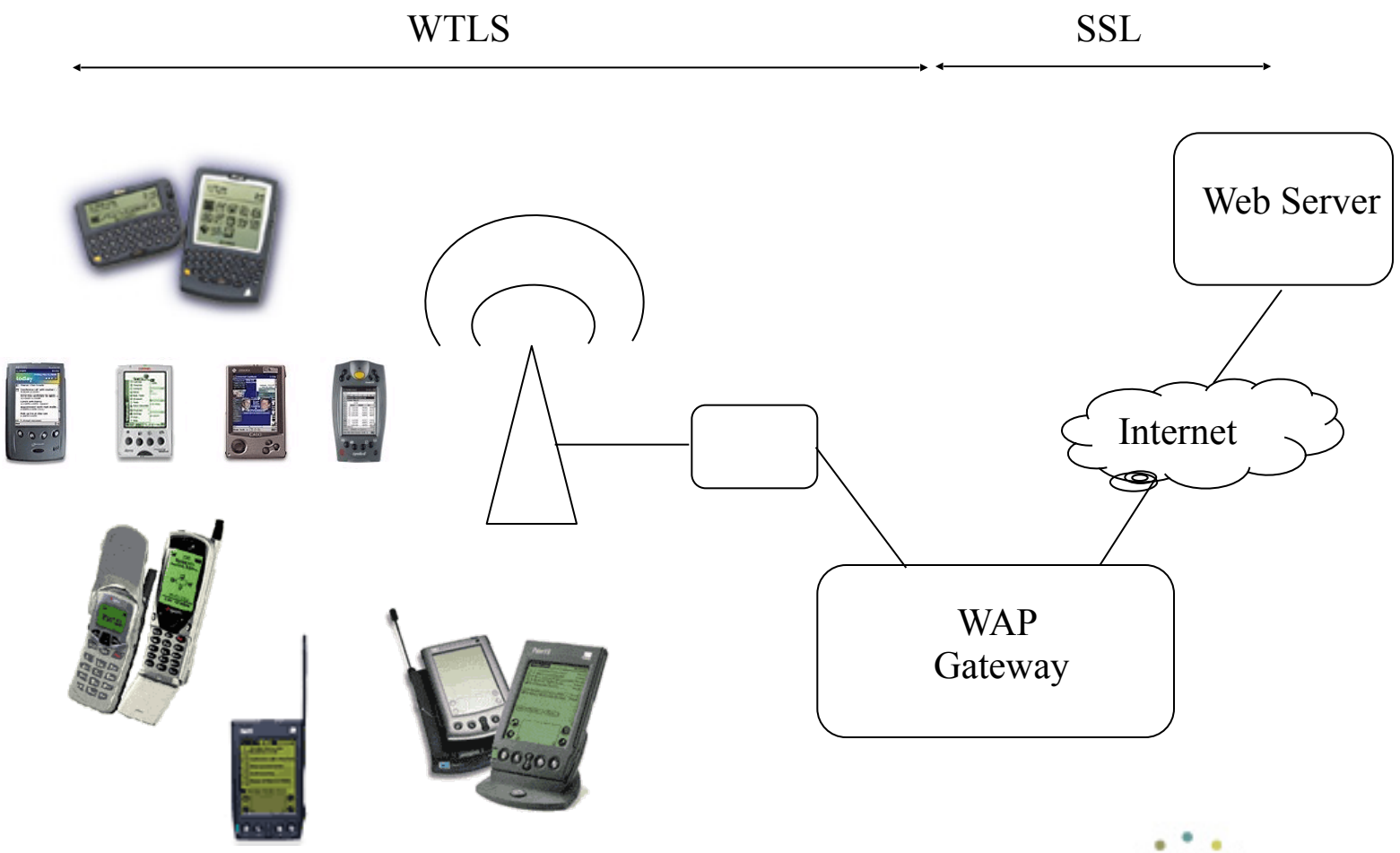
Overview

- WAP Browsers & Handhelds
- A Review of WTLS
- Benchmarking Experiments
- WTLS Handshake Timing Estimates
- Discussion of Results
- Summary / Conclusions

WAP Browsers & Handhelds: What is WAP?

- WAP: Wireless Application Protocol
- Created by WAP Forum
  - Founded June 1997 by Ericsson, Motorola, Nokia, Phone.com
  - 500+ member companies
  - Goal: Bring Internet content to wireless devices
- WTLS: Wireless Transport Layer Security

WAP Browsers & Handhelds: What is WAP?



YODLEE

WAP Browsers & Handhelds: Gaining Steam

- Palm OS
  - AU Systems
  - 4th Pass kBrowser
- Windows/PocketPC
  - EZOS EzWAP
- Psion
  - Purple Software/
    Dynamical Systems Research
- RIM
  - Neomar

WAP Browsers & Handhelds: Security & Performance

- Secure Connections:
  - Too long -> affects usability
  - Shorter keys -> too risky
- How long does the crypto take?
  - Using different crypto. algs.
  - Using different authentication methods

A Review of WTLS: WTLS Goals

- WTLS Goals
  - Authentication
  - Privacy
  - Data Integrity
- Authentication: Public-Key Crypto (CPU intensive!!!)
- Privacy: Symmetric Crypto
- Data Integrity: MACs

A Review of WTLS: Crypto Basics

- Public-Key Crypto
  - RSA (Rivest-Shamir-Adelman)
  - ECC (Elliptic Curve)
- Certificates
- Authentication
  - None, Client, Server, Mutual

A Review of WTLS: Server-Authentication

- Server-Authentication Only

```
ClientHello                 ---------->
                                                ServerHello
                                                Certificate
                            <----------         ServerHelloDone
```

1. Verify Server Certificate

```
ClientKeyExchange
ChangeCipherSpec
Finished                    ---------->
```

2. Establish Session Key

```
                            <----------         Finished

Application Data            <---------->        Application Data
```


YODLEE

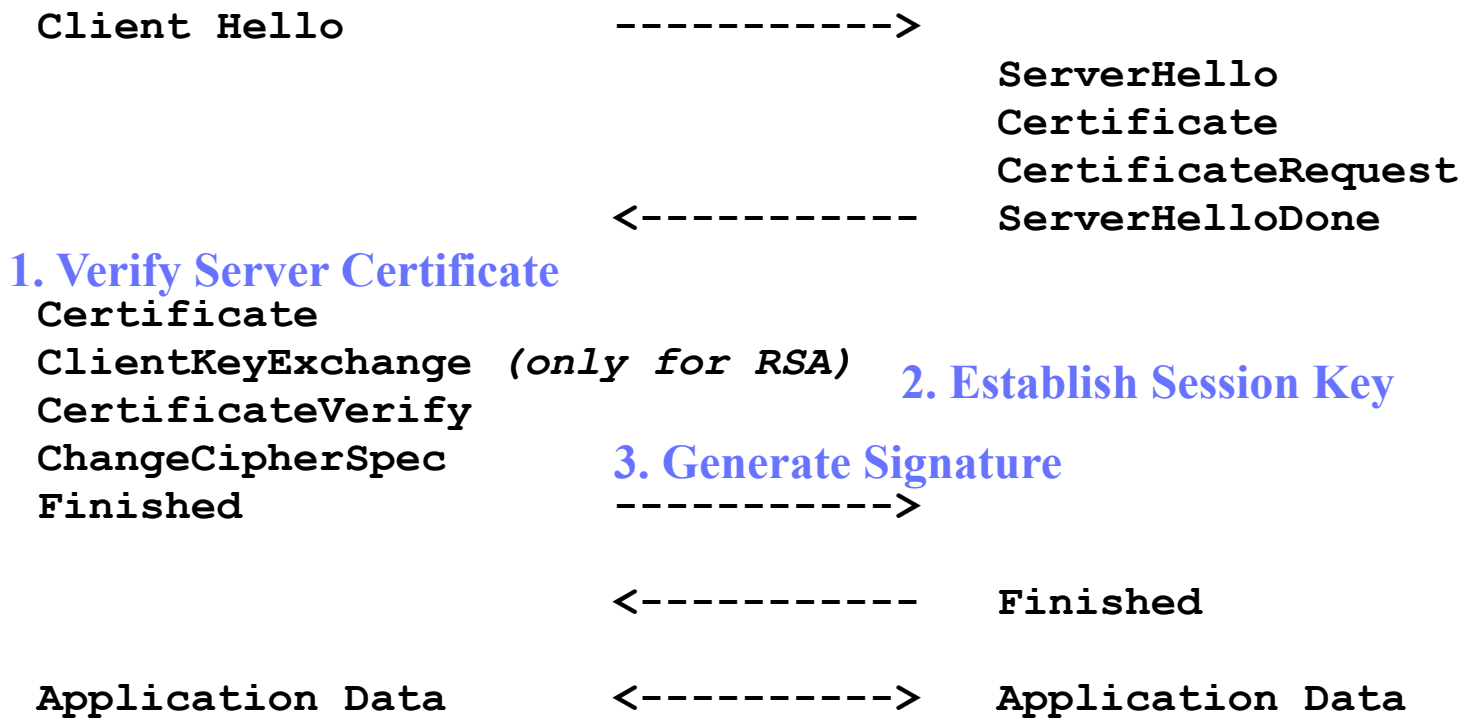
A Review of WTLS: Server-Authentication

1. Verify Server Certificate
   - ECC & RSA: Verify Signature

2. Establish Session Key
   - ECC: Generate ECC-DH Key Pair & Multiply
   - RSA: Encrypt w/ Server Public Key

A Review of WTLS: Mutual-Authentication

- Mutual-Authentication



YODLEE

A Review of WTLS: Mutual-Authentication

1. Verify Server Certificate
   - ECC & RSA: Verify Signature
2. Establish Session Key
   - ECC: Generate ECC-DH Key Pair & Multiply
   - RSA: Encrypt w/ Server Public Key
3. Verify Client Certificate
   - ECC & RSA: Signature Generation

Benchmarking Experiments

	New Palm VII (Dragonball-EZ, 20MHz, PalmOS v.3.2.5) (ms)	Palm V (Dragonball-EZ, 16.6MHz, PalmOS v.3.3) (ms)	Old Palm VII (Dragonball, 16.6MHz, PalmOS v. 3.1) (ms)
ECC Benchmarks (163-bit)			
Key Generation	372.4	514	556
Key Expansion[1]	254.8	350	378
Diffie-Hellman Key Agreement	335.6	462	500
ECC-DSA Signature Generation	514.8	713	773
ECC-DSA Signature Verification	1254	1740	1885
RSA Benchmarks(1024-bit)[2]			
Signature Generation	21734	27808	29628
Sig Verify (e=3)	598	758	790
Sig Verify (e=65537)	1482	1860	1966
RSA Encrypt	622	798	834

WTLS Handshake Timing Estimates

- Server-Authenticated Only: RSA

Operation	Cryptographic Primitive(s)	Time Required (ms)
Server Certificate Verification	RSA Signature Verification (Public decrypt, e=3)	598
Session Key Establishment	RSA Encryption (Public encrypt)	622
TOTAL		1220

WTLS Handshake Timing Estimates

- Server-Authenticated Only: ECC

Operation	Cryptographic Primitive(s)	Time Required (ms)
Server Certificate Verification	CA Public Key Expansion	254.8
	ECC-DSA Signature Verification	1254
Session Key Establishment	ECC Key Generation (DH Ephemeral Key)	372.4
	Server Public Key Expansion	254.8
	Key Agreement	335.6
TOTAL		2471.6

The cryptographic execution time for server-authenticated 1024-bit RSA handshakes is up to 2 times as fast as the cryptographic execution time for server-authenticated 163-bit ECC handshakes on the Palm VII.

WTLS Handshake Timing Estimates

- Mutual-Authentication: RSA

Operation	Cryptographic Primitive(s)	Time Required (ms)
Server Certificate Verification	RSA Signature Verification (Public decrypt, e=3)	598
Session Key Establishment	RSA Encryption (Public encrypt)	622
Client Authentication	RSA Signature Generation (Private encrypt)	21734
TOTAL		22954

WTLS Handshake Timing Estimates

- Mutual-Authentication: ECC

Operation	Cryptographic Primitive(s)	Time Required (ms)
Server Certificate Verification	CA Public Key Expansion	254.8
	ECC-DSA Signature Verification	1254
Session Key Establishment	Server Public Key Expansion	254.8
	Key Agreement	335.6
Client Authentication	ECC-DSA Signature Generation	514.8
TOTAL		2614

The cryptographic execution time for mutually-authenticated 163-bit ECC handshakes is at least 8.64 times as fast as the cryptographic execution time for mutually-authenticated 1024-bit RSA handshakes on the Palm VII.

Discussion of Results

- Strictly CPU time
- Optimizations
  - Store Expanded Keys
- Mutually authenticated handshakes could be too expensive for 1024-bit RSA on constrained microprocessors.
- Issue: who will sign ECC certificates?

Discussion of Results

PDA	Microprocessor	Speed
Palm, Handspring	Motorola Dragonball	16.6 – 20 MHz
RIM Interactive Pager	Intel 386	10 MHz
Compaq Aero 1530	NEC/VR4111 MIPS RISC	70 MHz
HP Jornada 820	Intel/StrongARM RISC SA-1100	190 MHz
Casio Cassiopeia E-100	NEC/VR4121 MIPS	131 MHz
Psion Revo	ARM 710	36 MHz
Psion Series 5	Digital/Arm 7100	18 MHz

Summary / Conclusions

- Cryptographic Execution Time for WTLS handshakes on wireless devices is significant.
- Server-Authenticated 1024-bit RSA can be 2x as fast as 163-bit ECC
- Mutually-Authenticated 163-bit ECC is at least 8x as fast as 1024-bit RSA

References & Acknowledgements

- References:
  - WAP Forum, Wireless Application Protocol Specification Version 1.1, 4.30.1998
  - WAP Forum, Wireless Transport Layer Security Specification Version 1.1, 11.2.1999
  - AU-Systems WAP Browser Home Page, http://www.wapguide.com/wapguide/browser.html
  - EZOS EzWAP Browser Page, http://www.ezos.com/
  - Psion WAP Browser Beta Page, http://wap.psion.com/
  - Neomar RIM WAP Browser Page, http://www.neomar.com/
  - Neomar Press Release, http://www.neomar.com/press/00.05.23certicom.html
- Acknowledgements:
  - Tim Dierks, Rob Lambert, Chris Hawk (Certicom)
  - Nagendra Modadugu (Stanford)