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

• 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

Client
- Browser
- WSP
- WTP
- WTLS
- WDP

WAP Gateway
- WML
  - WSP
- HTML
  - HTTP
  - SSL
  - TCP
  - IP

Server
- Application
  - HTTP
  - SSL
  - TCP
  - IP

Internet Protocols

October 12, 2000
# Handshake Message Flow

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientHello</td>
<td>ServerHello</td>
</tr>
<tr>
<td>Certificate*</td>
<td>Certificate*</td>
</tr>
<tr>
<td>ServerKeyExchange*</td>
<td>CertificateRequest*</td>
</tr>
<tr>
<td>Certificate*</td>
<td>&lt;-------- ServerHelloDone</td>
</tr>
<tr>
<td>ClientKeyExchange</td>
<td></td>
</tr>
<tr>
<td>CertificateVerify*</td>
<td></td>
</tr>
<tr>
<td>[ChangeCipherSpec]</td>
<td></td>
</tr>
<tr>
<td>Finished</td>
<td>--------&gt; Finished</td>
</tr>
<tr>
<td></td>
<td>[ChangeCipherSpec]</td>
</tr>
<tr>
<td>Application Data</td>
<td>&lt;-------- Finished</td>
</tr>
</tbody>
</table>

- 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
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**

- 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 $F2^n$ ECC curves as defined in WTLS spec. RSA using 1024 bits with client using small public key exponent.

**WTLS Class 3 Memory Size Comparison**

---

October 12, 2000
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
<table>
<thead>
<tr>
<th></th>
<th>2G</th>
<th>3G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>5 MIPS</td>
<td>20 MIPS</td>
</tr>
<tr>
<td><strong>Flash Memory</strong></td>
<td>100 KB</td>
<td>20 MB</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>100 KB</td>
<td>1 MB</td>
</tr>
<tr>
<td><strong>Minimum Bandwidth</strong></td>
<td>100 bps</td>
<td>14.4 kbps</td>
</tr>
<tr>
<td><strong>Maximum Bandwidth</strong></td>
<td>9.6 kbps</td>
<td>384 kbps</td>
</tr>
</tbody>
</table>
## End to End Performance Modeling

<table>
<thead>
<tr>
<th>System / Protocol</th>
<th>Server Auth.</th>
<th>Server &amp; Client Authentication</th>
<th>Application Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>ECC</td>
<td></td>
</tr>
<tr>
<td>3G &amp; TLS</td>
<td>1365 msec</td>
<td>3851 msec</td>
<td>2050 msec</td>
</tr>
<tr>
<td>2G &amp; WTLS</td>
<td>1886 msec</td>
<td>9660 msec</td>
<td>2440 msec</td>
</tr>
</tbody>
</table>

- 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