Mobile eCommerce Security

David Hemsath, Chief Technologist, IBM Global Security Solutions, dhemsath@us.ibm.com

06 March 2002

SHARE 98, Session 3516

Disclaimer

The information contained in this document is distributed on an “as is” basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM’s licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

Trademarks

- IBM (IBM)
- WAP Forum, W@P Certified, and W@P (Wireless Application Protocol Forum Ltd.)
- Other company, product, and service names may be trademarks or service marks of others.

Abstract

In the last year, the term mCommerce or Mobile Commerce has been used more and more frequently. The term denotes that eCommerce is moving from the wired-only world into the exploding wireless world. Today's WAP-enabled phones and HDML-enabled PDAs can now access many kinds of web services. However, security in the mobile world is far more complex than in the wired environment, and the speaker will attempt to address these issues. Topics will include all aspects of wireless security, including user, device, message, end-to-end security, and centrally managed security through enterprise security tools. Come and see what is already possible – you will be impressed and reassured!

Note: WAP 2.0 was published last January. It will profoundly affect (improve) mCommerce security, but this session will focus on WAP 1.x due to latency of WAP 2.0 devices coming to market.

Contents

- Mobile Internet
- e-business security considerations
- Wired
- WAP 1.x
- WAP 2.0
- iMode
- Wired and wireless security
- Conclusions

Mobile Internet

Waves of Mobile Applications

- First wave early 2000
  Information services and entertainment
  - Email, news, weather, time tables
  - Targeted info services
  - Consumer entertainment

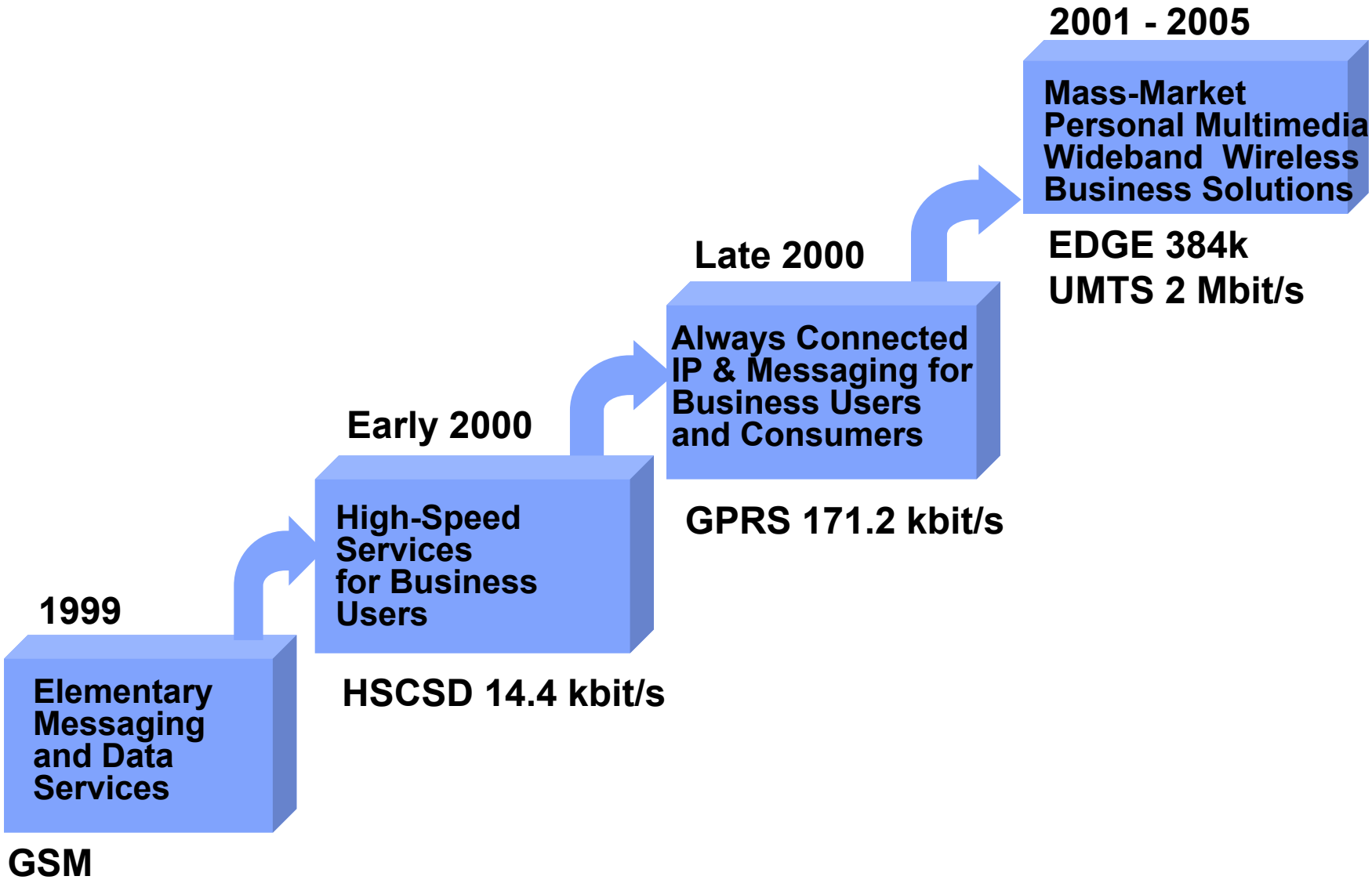
- Late 2000
  Mobile Intranet and Extranet
  - Email & Scheduling
  - Consumer services: Banking, Travel etc
  - WAP interfaces for Enterprise applications
  - Enhanced CRM and ERP systems

Waves of Mobile Applications

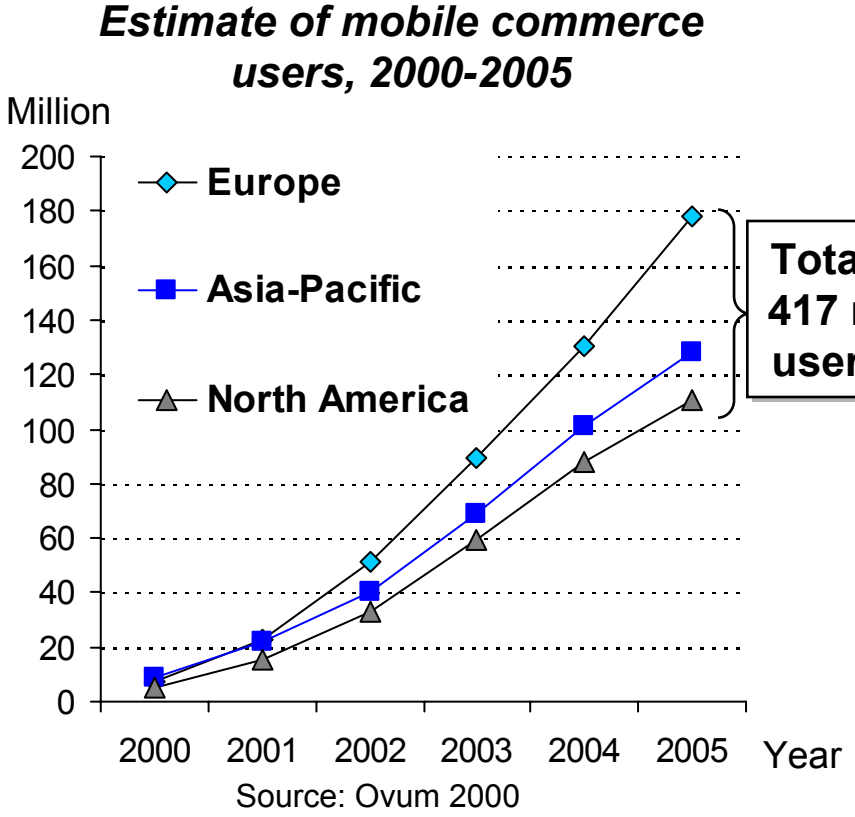
- Second Wave 2001
  Mobile eBusiness
  - Location-based services
  - Event-driven services
  - Mobility added to most eBusiness online services
  - Mobile phone becomes the 'Personal Trusted Device'
  - Emergence of Voice/Data Interfaces

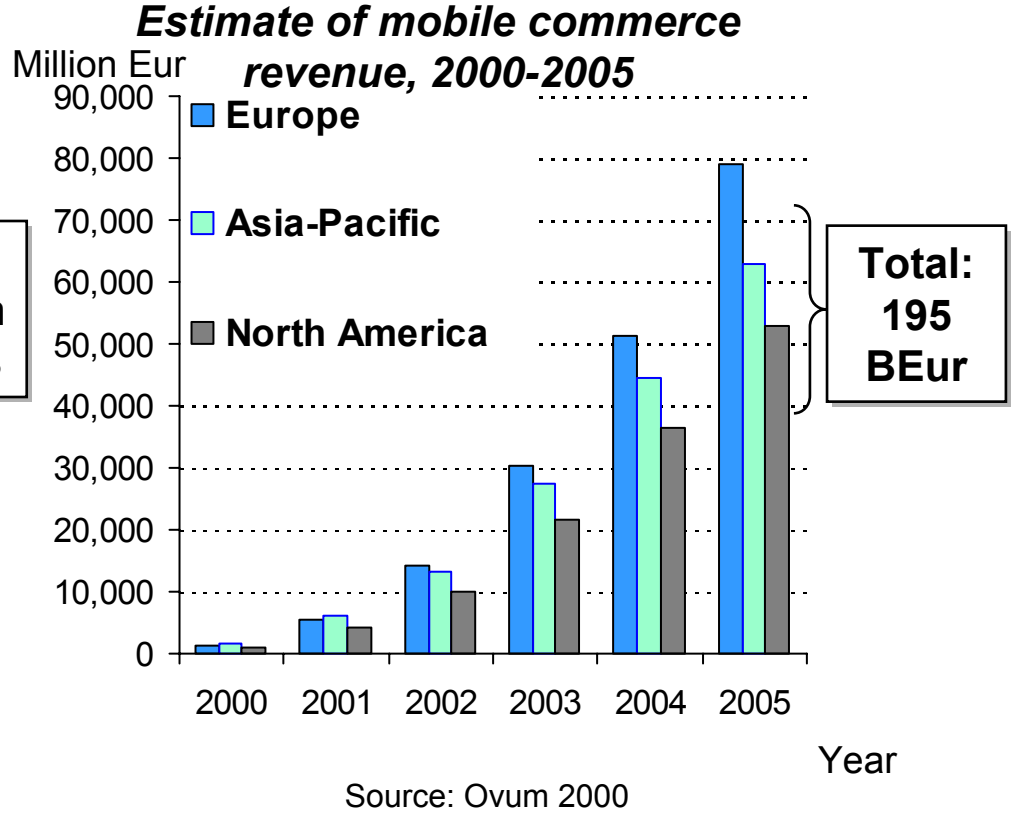
- Third Wave 2002
  Innovative Mobility Breakthrough Applications
  - Multimedia, seamless integration of voice, video and data
  - The mobile phone emerges as the primary transacting platform
    - Customer Relationship Management

Evolution of GSM Network



Mobile Commerce Opportunity

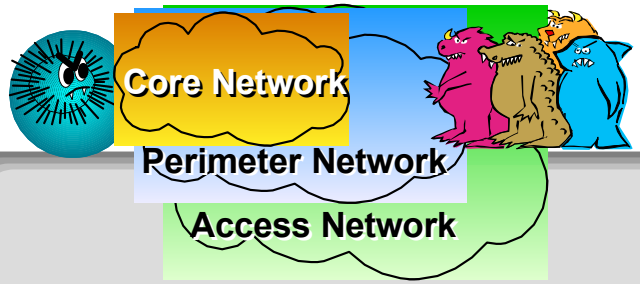




Europe, Asia-Pacific and North America total over 85 % of the mobile market opportunity.

e-business Security Considerations

The Security Challenge



"They're out to get you!"

- **Threats**
  - Viruses
  - The insider threat
  - Hackers, competitors, . . .
- **Risks**
  - Corporate image, public trust
  - Intellectual and/or financial capital
  - Privacy issues, litigation, . . .

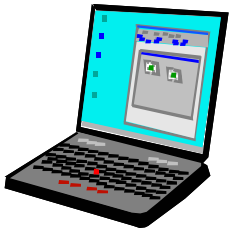
Orientation:
Keep intruders out!

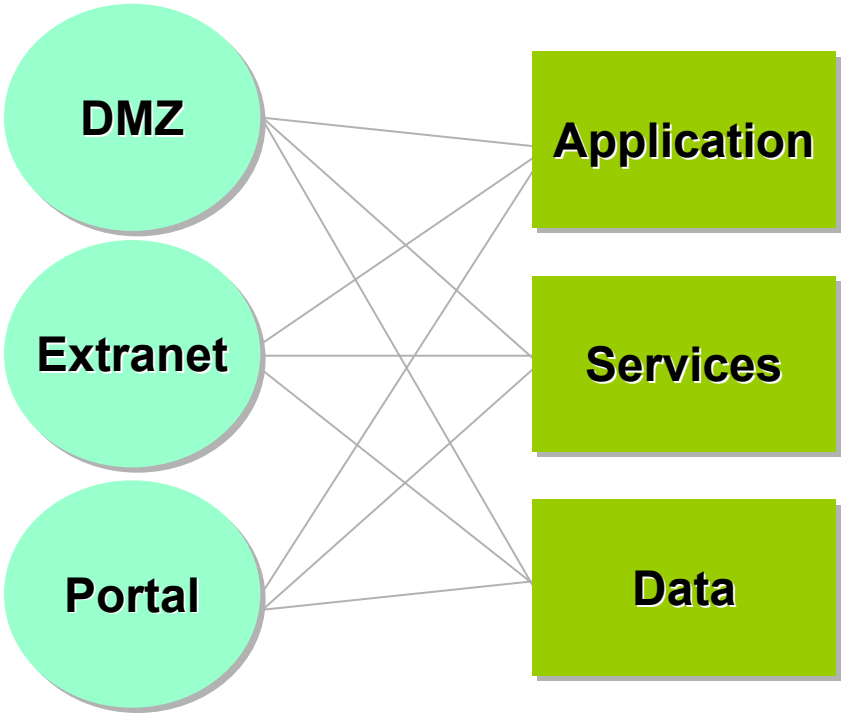
"Security as an enabler!"

- **Policy-driven security**
  - Centralized policy definition:
    - Eases administration
    - Eliminates application security impact
- **Security tightly linked to:**
  - Enterprise management
  - Enterprise directory
  - e-business resource availability

Orientation:
Allow authorized people in!

Key Questions for e-business Scenarios





1. ***Who is entering and how?***

2. ***What can they access, and how can they access it?***

Security Services

- User Authentication
- Authorization and Access Control
- Accountability
- Data Security

User authentication

- User Authentication: the process of identifying or authenticating an end user to a (distributed) computer system.

Authorization and Access Control

- Authorization: The security service which protects a system's resources against improper access
- Access Control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (ISO 7498-2)

Accountability

- Users should be accountable for their actions
  - Do not trust internal users unconditionally

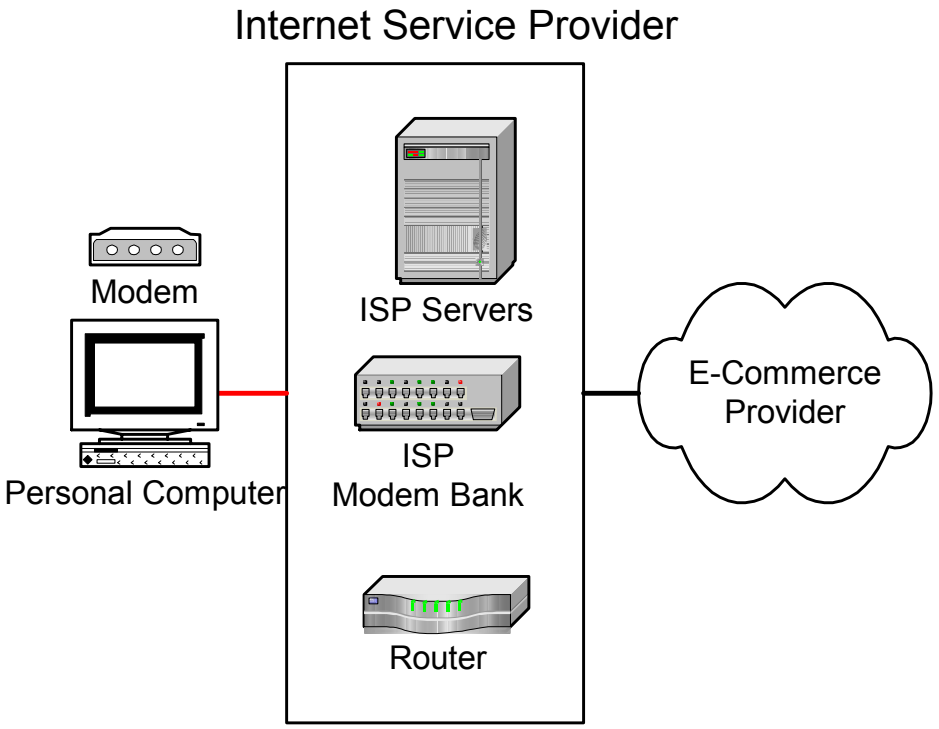
Data Security

- Data Authentication:
  - Data Origin Authentication: authenticating the sender of data
  - Data Integrity: assuring the integrity of data
- Data confidentiality (privacy):
  - Assuring data is not disclosed
- Non-repudiation
  - Proof towards independent third party

Wired

Wired

- User connects to ISP
- ISP routes requests to the Internet E-Commerce providers
- TCP/IP protocols



WAP Version 1.x

Wireless Application Protocol

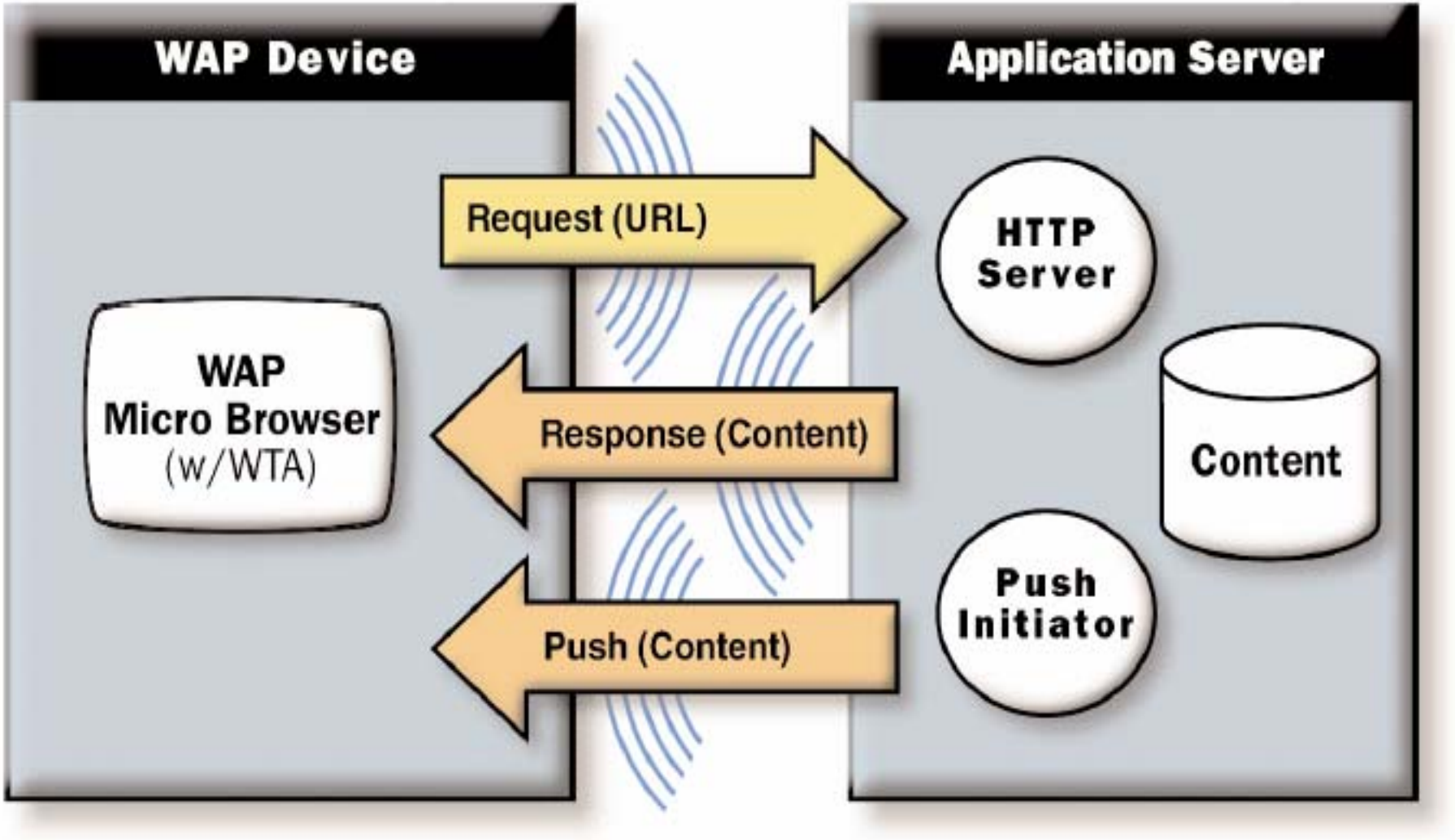
Motivations for WAP

- Enable data access from mobile devices
  - Pagers
  - Cellular phones, radios, etc.
- Characterized by
  - Limited network bandwidth (wireless)
  - High network latency
  - Limited computational power on client
  - Limited screen display size and capability
  - Limited user interface (no mouse, etc.)
- Proprietary solutions, no interoperability

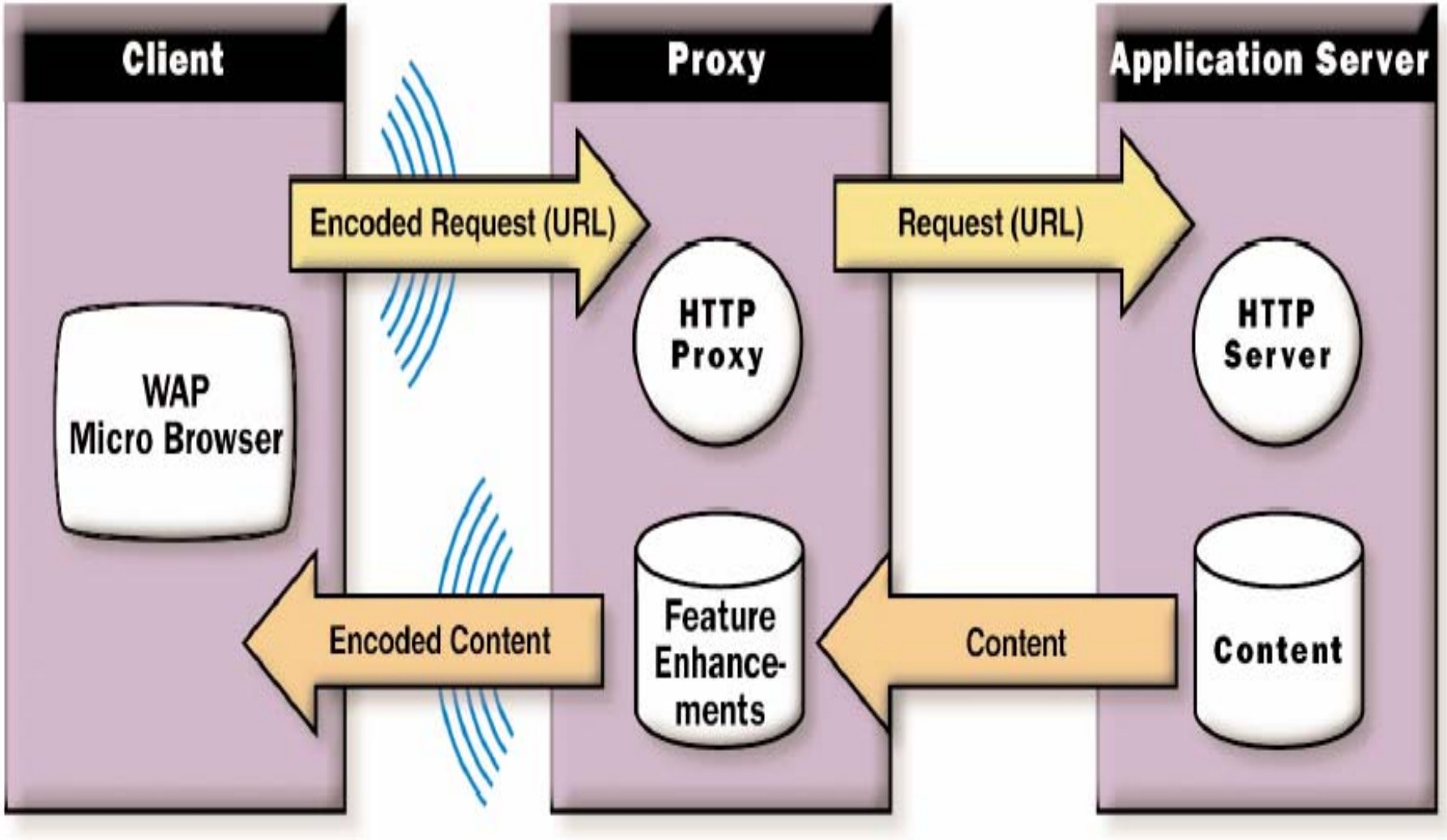
WAP – Wireless Application Protocol

- WAP Forum
  - Founded 9/97 by Nokia, Ericsson, Motorola, Unwired Planet (Phone.com)
  - Membership includes
    - Handset manufacturers
    - Telcos
    - IT/SW companies: IBM, MS
- Goal: Network protocol and data content standards for mobile devices
  - Version 1.2 standard issued in 2000
  - Version 2.0 standard issued January 2002

The WAP Programming Model

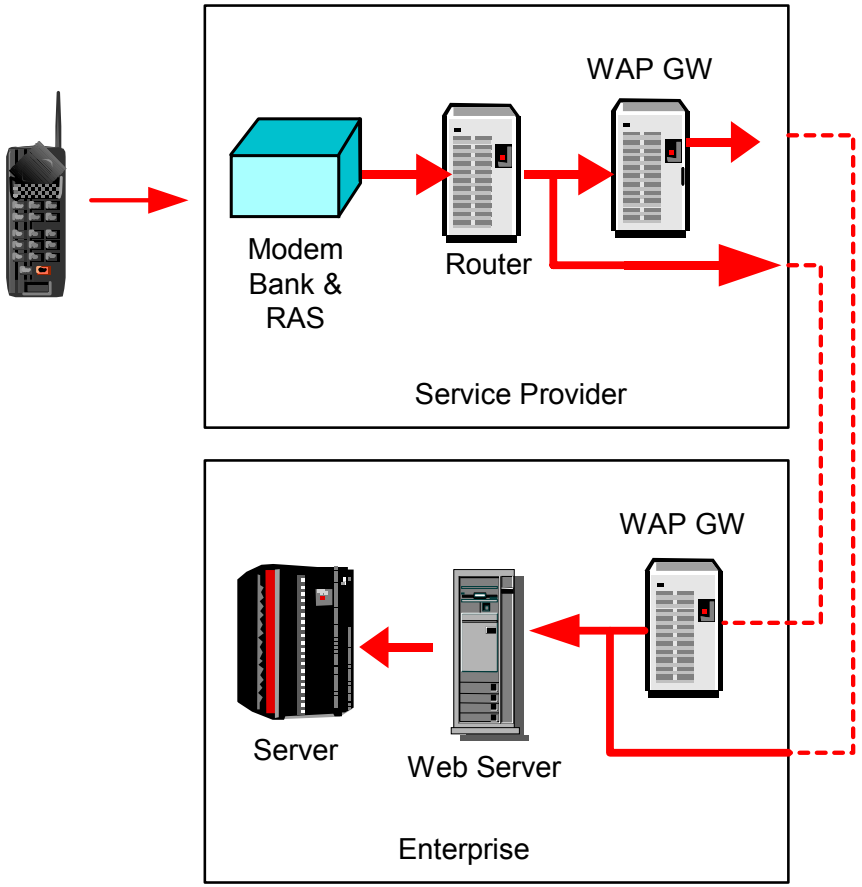


WAP's optional proxy model supports network-based optimizations



WAP 1.x – Wireless Application Protocol Version 1.x

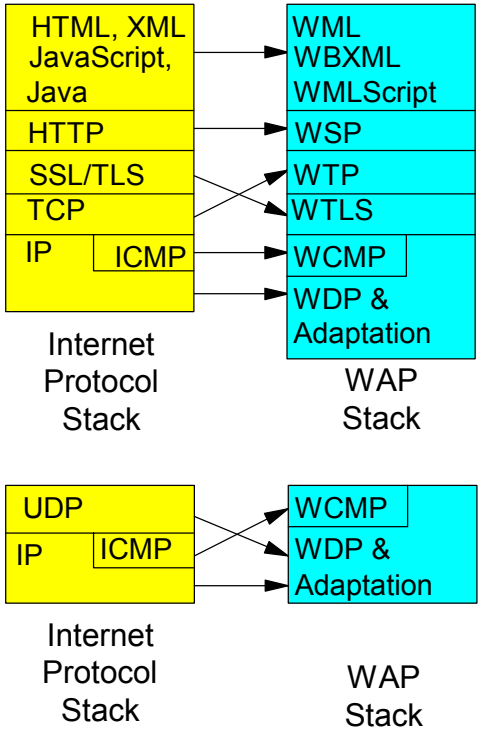
- Wireless Service Provider (WSP) equivalent to ISP
- Modem Bank receives incoming calls
- Remote Access Server (RAS) translates incoming calls from wireless to wired
- Router routes wired data
- WAP Gateways
  - Translate WAP to TCP/IP
  - Provide DNS services
  - Transcoding (HTML to WML)
  - Maybe at WSP or enterprise (or both)



WAP 1.x – Wireless Application Protocol Version 1.x

- WAP Specification
  - Wireless Markup Language (WML) with WMLScript
  - Microbrowser specification
  - Lightweight protocol stack
  - Provisioning service

WML: Wireless Markup Language
WSP: Wireless Session Protocol
WTP: Wireless Transport Protocol
WTLS: Wireless Transport Layer Security
WCMP: Wireless Control Management Protocol
WDP: Wireless Datagram Protocol



WAP 1.x: off to a strong start, despite bad press

- Financial industry has been a major early adopter
  - High customer value, low transaction cost
  - Mobile extension of Internet banking and brokerage, fits the multichannel strategy
  - Security good enough, and improving
  - Both operator-hosted and independent gateway models are being implemented

…the numbers are for real though

- 60 million internet capable phones shipped in 2000 (200 million in 2001)
- 40 million WAP phones shipped in 2000 (180 million in 2001)
- 23 million mobile Internet users in Japan
  - 15 million I-mode users in Japan (Oct. 2000)
  - 8 million WAP users in Japan (Aug. 2000)
- 849 WAP services listed on Yahoo Mobile (Nov. 2000)
- 636 industry members in WAP forum (Nov. 2000)
- 1999 the year when it started!

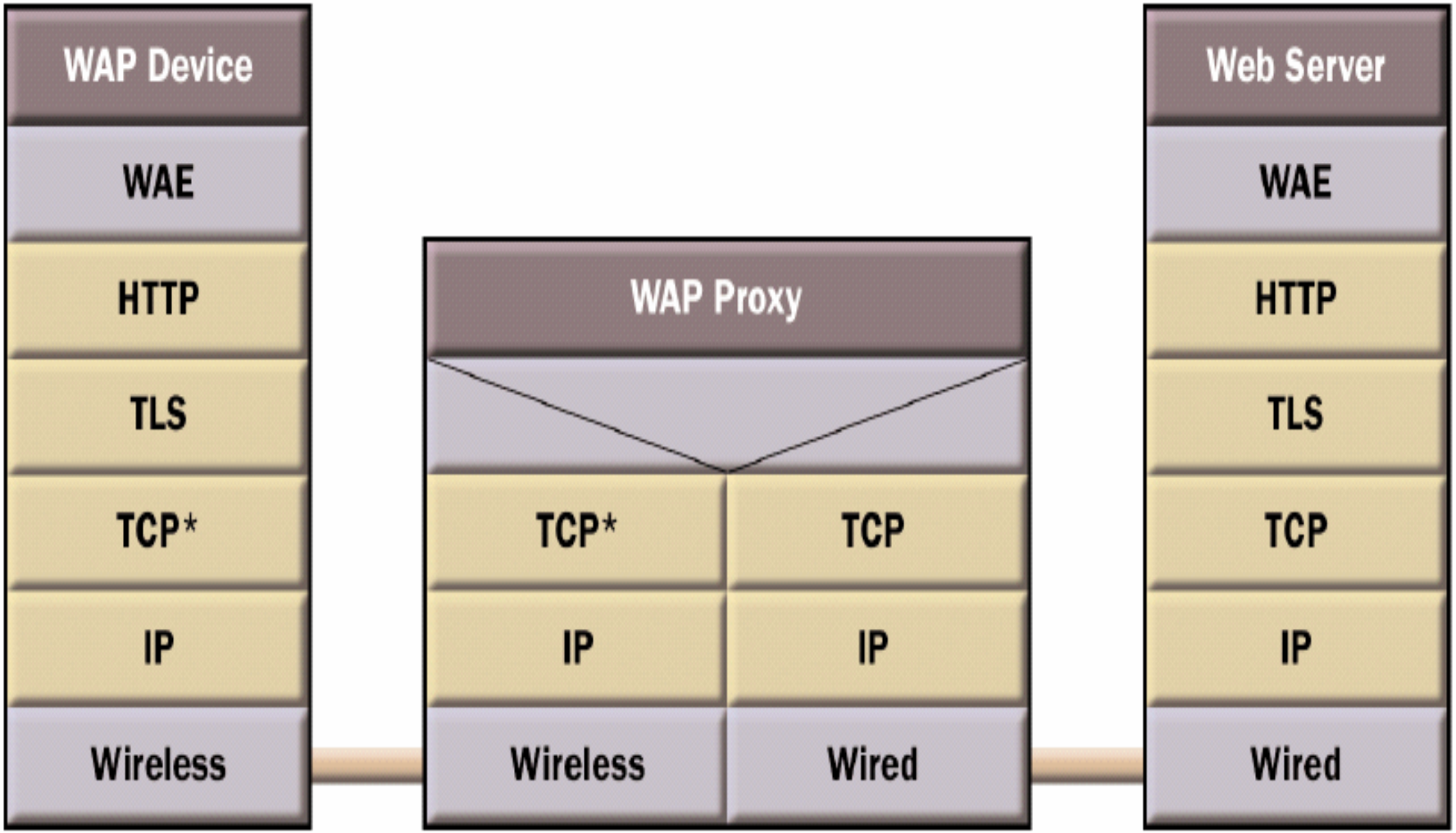
- Sources:
  - Nokia, Dec. 2000
  - Telecommunications Carriers Association TCA and NTT DoCoMo
  - Yahoo
  - WAP Forum

WAP Version 2.0

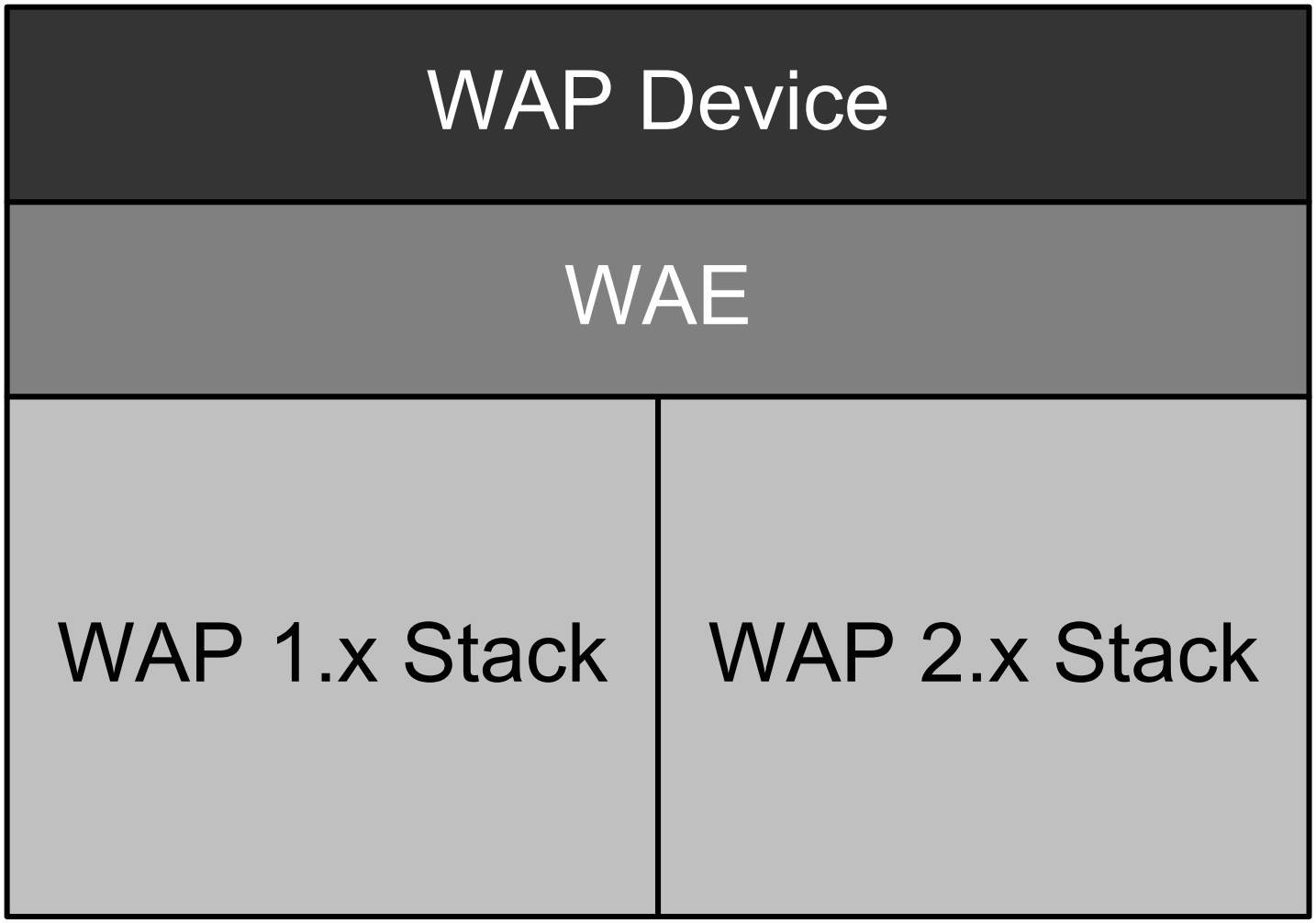
WAP 2.0: Bringing Wireless Closer to the Internet

- Objectives:
  - Add support for the standard Internet communication protocols, e.g., IP, TCP and HTTP.
    - Environment that permits wireless devices to utilize existing Internet technologies
  - Permit applications/services to operate over all existing and foreseeable air interface technologies/bearers, incl. new, higher-speed technologies known as General Packet Radio Service (GPRS) and 3rd Generation (3G) cellular.
  - Rich application environment
  - Address unique characteristics of wireless devices
  - Minimized device processing power, optimized network resources
  - Enable a variety of user interface (UI) designs

Example WAP 2.0 HTTP Proxy with Profiled TCP and HTTP



Optional Dual WAP Stack Support



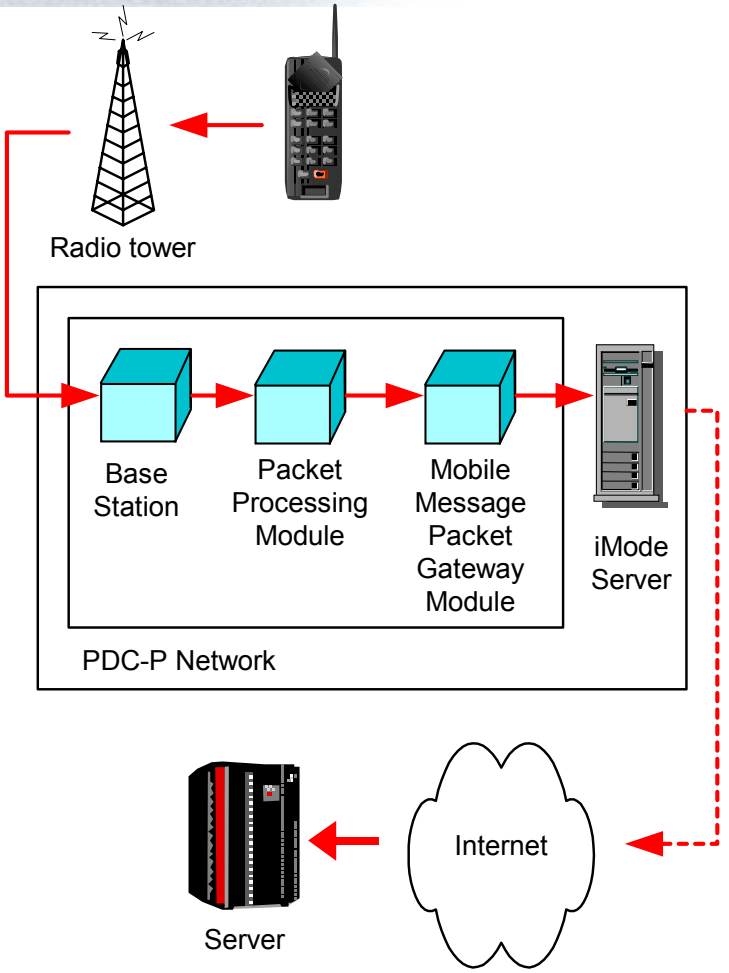
iMode

iMode

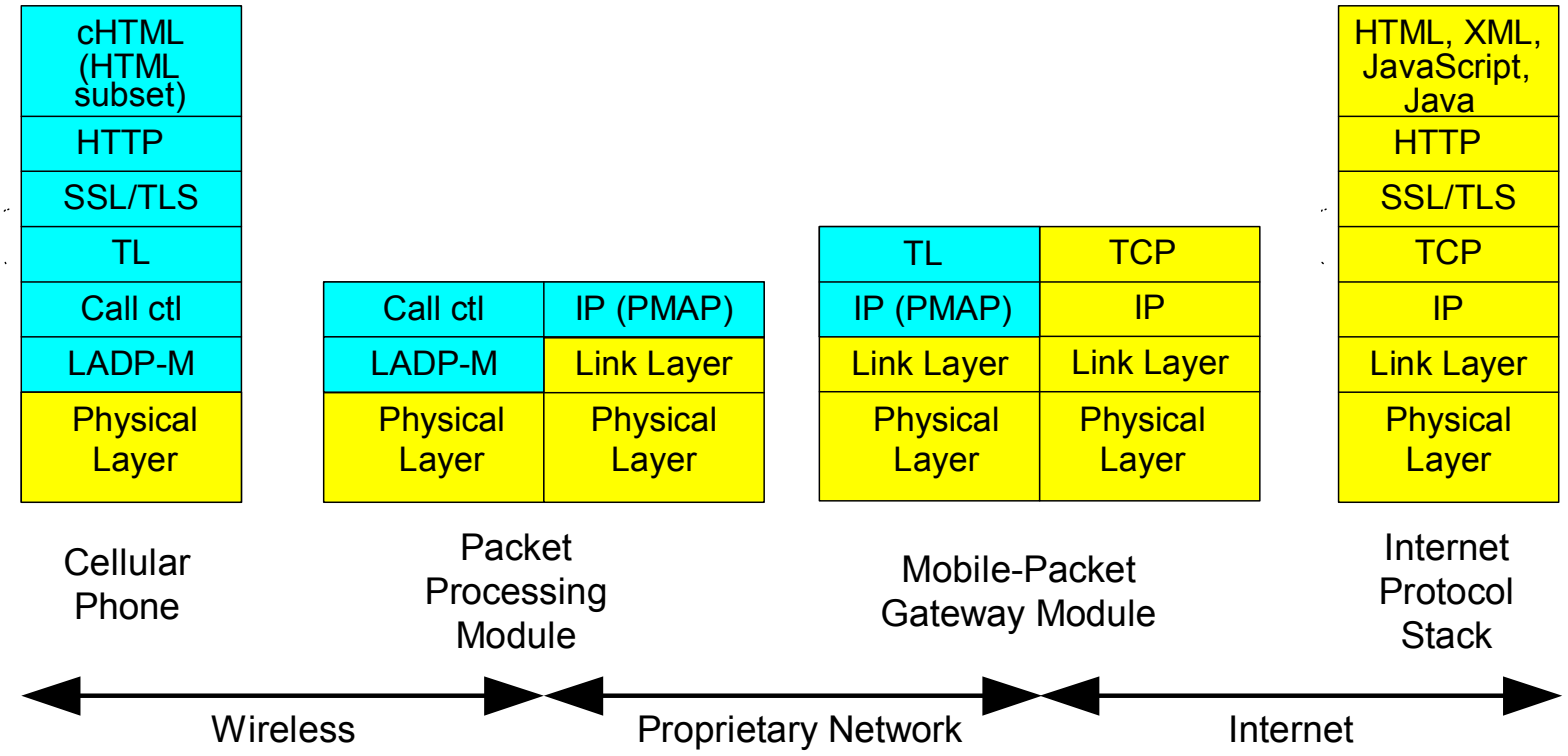
- Proprietary protocol of NTT DoCoMo
  - Information availability is limited
  - We have learned about iMode from testing with it and from at IETF and RSA conference
- Currently only available in Japan (some trials in Europe and US now)
- Phones support downloading Java Applets and cHTML
- Some TCP/IP protocols right to handset
- Example iMode web sites
  - http://www.kyoto-bauc.or.jp/i
  - https://kabu.com (SSL enabled site)

iMode

- Wireless Service provider
  - Base station
  - Packet Processing Module
  - Mobile Message Packet Gateway Module
- iMode server is standard web server



iMode


cHTML (HTML subset)
HTTP
SSL/TLS
TL
Call ctl
LADP-M
Physical Layer
Call ctl
IP (PMAP)
LADP-M
Link Layer
Physical Layer
Physical Layer
TL
TCP
IP (PMAP)
IP
Link Layer
Link Layer
Physical Layer
Physical Layer
HTML, XML, JavaScript, Java
HTTP
SSL/TLS
TCP
IP
Link Layer
Physical Layer
Cellular Phone
Packet Processing Module
Mobile-Packet Gateway Module
Internet Protocol Stack
Wireless
Proprietary Network
Internet

Wired and Wireless Security

Wired, WAP, iMode

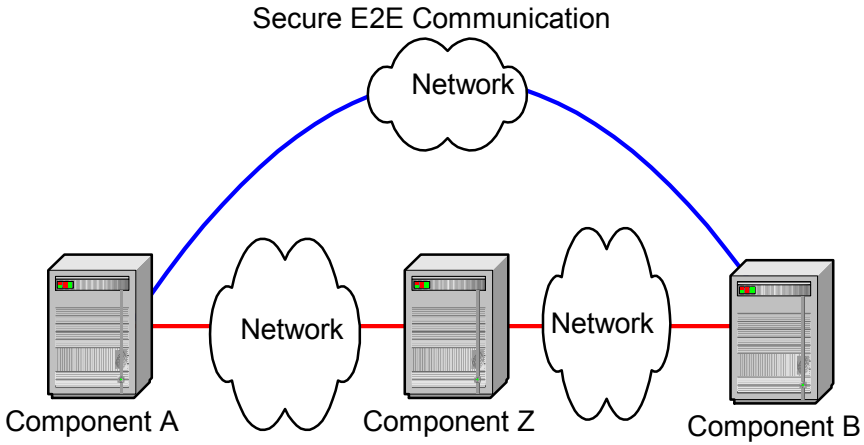
Wired Security

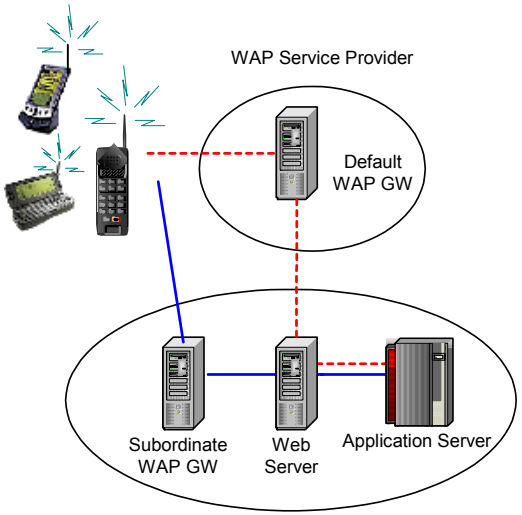
- TCP/IP
- Security by SSL
- Data Authentication/Confidentiality
- Server Side Authentication
  - Server has certificate signed by recognized CA
  - Links (server's) name to public/private key pair
- (Optional) Client Side Authentication
  - Client has certificate signed by recognized CA –perhaps the enterprise that they are authenticating to
  - Unlock of private key in browser or smart card
  - Not as common – user's tend to authentication with username/password
- Non-repudiation possible based on digital signatures
  - User needs smart card reader
  - Plug-in / applet / JavaScript needed at browser

Security in e-business Today (Wired)

- Uses the SSL protocol Data Security
- Username/password User Authentication
- No non-repudiation
  - Only enablement building blocks
- Plethora of authorization solutions
- Still considered a success

WAP 1.x “Security GAP”





- WTLS only reaches WAP GW
- WAP GW has to decrypt WTLS and re-encrypt into SSL

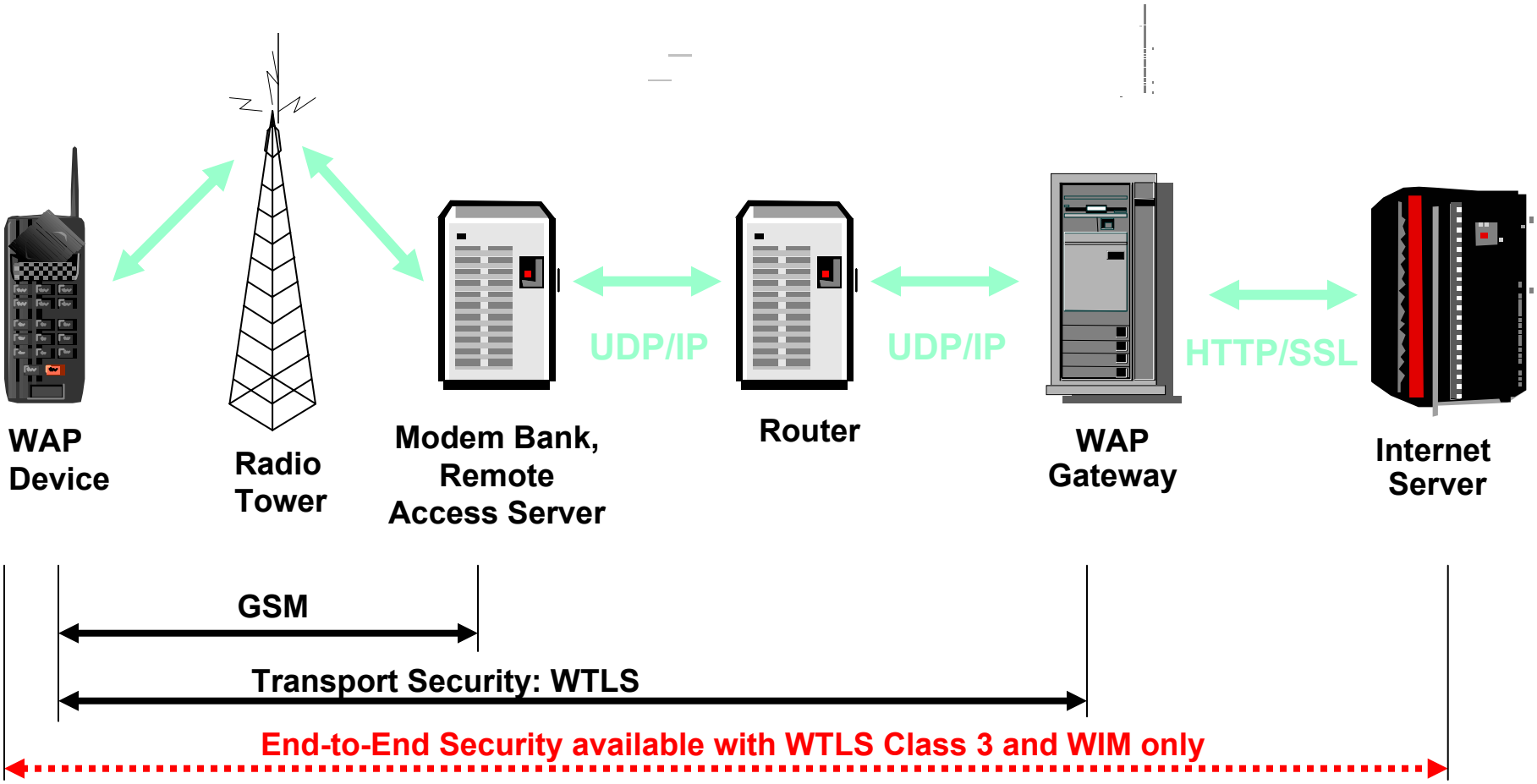
Mitigating the WAP 1.x GAP

- Push the GW into the Mobile Application Provider's control
- GW does NOT require telecom skills!

WAP 1.x GAP is not the problem!

- Bad reputation
- Current available WAP phones suffer from other shortcomings

Introduction to WAP 1.x Security



WAP 1.x Security

- WTLS
  - Class 1
    - Unauthenticated Diffie-Helman key exchange for negotiation of a secure session
  - Class 2
    - Server-side authentication based on public-key certificates
  - Class 3
    - Mutual authentication with client-side certificates

WAP 1.x Security

- WAP Identity Module (WIM)
  - WTLS
  - Application level security functions (e.g., signText in next slide)
  - Store and process information needed for user identification and authentication.
- Example of a WIM implementation is a smart card
  - SIM
  - SWIM
- Tamper-resistant
- Support for public key cryptography embedded (either RSA or Elliptic Curve Cryptography)
- PIN is prompted for every private key operation

WAP 1.x Security – signText

- WMLscript is the scripting language used in the WAP environment.
- One of the extensions allows for providing application level security by digitally signing a message string (text).
- Although WTLS provides client authentication for the duration of a WTLS session, it does not provide non-repudiation for transactions.
- To support this requirement, the WAP browser provides a WMLScript function, Crypto.signText, that asks the user to sign a string of text.
- It is recommended to use special signature keys that are distinct from authentication keys used for WTLS.
- A WIM module may be used for private key storage and signature computation.

Security Services & WAP 1.x Primitives

- Data Confidentiality: WTLS
- User Authentication: WTLS Class 3, WIM
- Data Authentication
  - Data integrity: WTLS Class 2-3
  - Data origin authentication: WTLS Class 2-3
- Data Non-Repudiation: WIM, signText

iMode Security

- Based on TCP/IP
- HTTP and SSL to handset
  - Data authentication/confidentiality
  - Server certificate authentication supported (only Baltimore and VeriSign acceptable as CAs)
  - Client certificate authentication NOT supported
- Suffers the same security gap as WAP
  - Can be similarly overcome by place iMode server at enterprise
- Non-repudiation not currently possible
  - iMode investigating smart cards for similar function to WIM

Analysis & Conclusion

Current* WAP 1.x Limitations

- Limitations of mobile commerce solutions based on pre-WTLS Class 3 WAP
  - Weak client authentication
  - No ability to handle client certificates
  - Lack of end-to-end security: the GAP!
  - Does not support non-repudiation

* Note that this presentation has not been completely refactored for WAP Version 2.0.

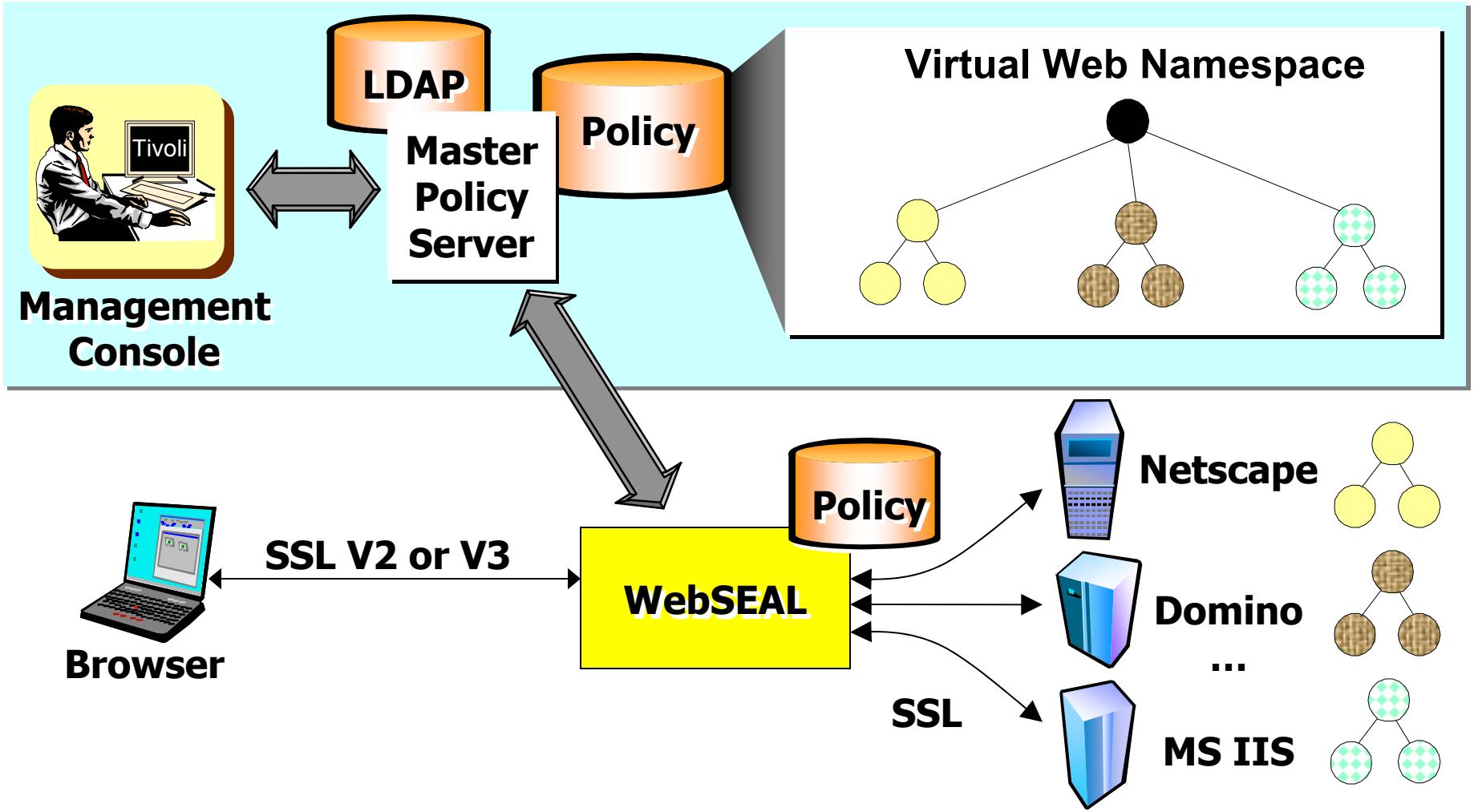
WAP 1.x Solution

- This is remediated with WTLS Class 3 and WIM Cards
  - WTLS Class 3 “duplicates” TLS
  - WIM enables strong user authentication and non-repudiation
- Actual deployment also requires an authorization solution such as Policy Director

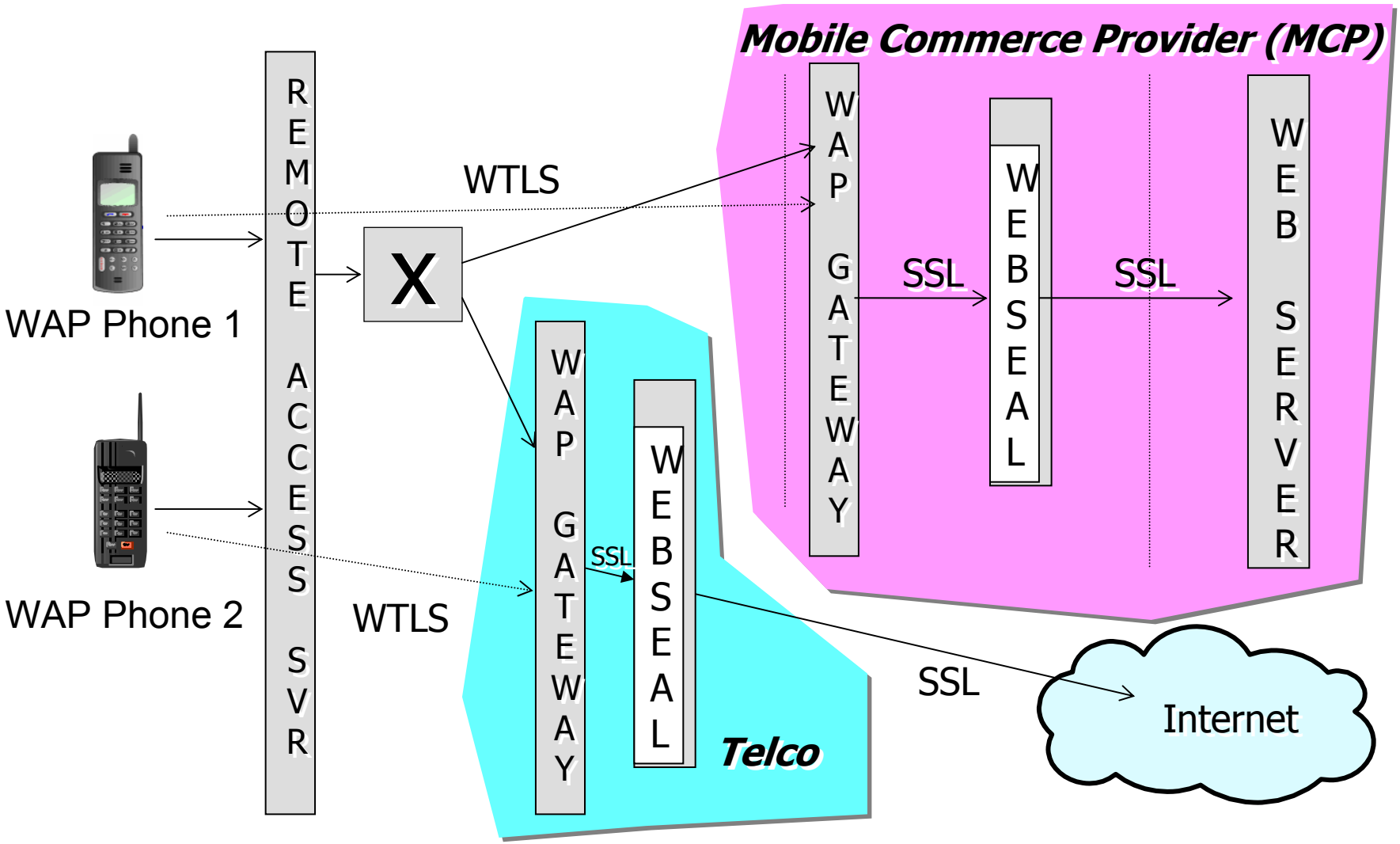
Policy Director Components—WebSEAL

- Web Access Control
- Web Single Sign-On
- Design for High Availability
- Supports Multiple Authentication Models
  - User ID/Password
  - PKI
  - SecurID,
  - …

WebSEAL—Web Access Control



PD 3.7.1 – WebSEAL Enhancements – WAP 1.x Support – Architecture



WebSEAL for WAP — How Does It Work?

- In WAP scenarios, WebSEAL can be dedicated to use in authorizing WAP flows (trusts WAP gateway to have done the authentication)
- A WTLS session is set up between the WAP phone and the WAP gateway (at the MCP or at the Telco)
- WebSEAL can use the WAP gateway for authentication: e.g.
  - Caller ID
  - WAP Identification Module (WIM) module for client-side, certificate-based authentication
  - Or can authenticate the user through WebSEAL supported authentication mechanisms (no client certificate or BA)
- WAP gateway sends information to WebSEAL via:
  - HTTP header
  - Cookie
- WebSEAL maps phone's ID into an internal Policy Director identity
- Authorization performed by WebSEAL using Policy Director identity
- The solution should work with any WAP Gateway, out of the box support for:
  - Nokia
  - IBM

WebSEAL for WAP 1.x – Directions

- Working on business agreements with WAP gateway providers to OEM Policy Director
  - Already incorporated in IBM's WebSphere Everplace Suite (WES)
- Integrate with e2e solution(s) based on WML Script (e.g. using signText to authorize a transaction)

Other IBM/Tivoli Products Supporting the Mobile Web

WebSphere Transcoding Publisher

WESee

Tivoli Internet Services Manager

Tivoli PKI

TPSM

MQe

DB2e

Tivoli Policy Director

WebSphere Portal Server

Mobile Services for Domino

Conclusion

- The security provided by WAP 1.x or iMode enabled transactions is equal to what can be achieved in current wired environment
  - WAP 2.0 a major improvement
- WAP 1.x is a step ahead
  - Specification of public/private key pairs in WIM
  - Built in crypto.signText function
  - Easier to provide non-repudiation service
- Hence using WAP or iMode shouldn't be a decision based on security
- Issues such as usability and openness should determine future use

A brief word about 802.11 “Wi-Fi” wireless networks

- Treat them as totally insecure!
  - Hang wireless access points (WAPs) *outside* the firewall
  - Use VPNs
  - Hope that 802.1X gets it right
  - Check out Tivoli Risk Manager’s Wireless Security Auditor (WSA)

Acknowledgements

- Paul Ashley, Ph.D.
- Heather Hinton, Ph.D.
- Mark Vandenwauver, Ph.D.

For more information

- http://www.tivoli.com/security
- http://www.ibm.com/security
- http://www.wapforum.com

Glossary

- **Client** – a device (or application) that initiates a request for a connection with a server.
- **Content** – subject matter (data) stored or generated at an origin server. Content is typically displayed or interpreted by
- a user agent in response to a user request.
- **Content Encoding** – when used as a verb, content encoding indicates the act of converting content from one format to another. Typically the resulting format requires less physical space than the original, is easier to process or store and/or is encrypted. When used as a noun, content encoding specifies a particular format or encoding standard or process.
- **Content Format** – actual representation of content.
- **Device** – a network entity that is capable of sending and receiving packets of information and has a unique device address. A device can act as both a client or a server within a given context or across multiple contexts. For example, a device can service a number of clients (as a server) while being a client to another server.
- **JavaScript** – a *de facto* standard language that can be used to add dynamic behaviour to HTML documents. JavaScript is one of the originating technologies of ECMAScript.
- **Resource** – a network data object or service that can be identified by a URI or URL. Resources may be available in multiple representations (e.g., multiple languages, data formats, size and resolutions) or vary in other ways.
- **Server** – a device (or application) that passively waits for connection requests from one or more clients. A server may
- accept or reject a connection request from a client.
- **Terminal** – a device providing the user with user agent capabilities, including the ability to request and receive information. Also called a mobile terminal or mobile station.
- **User Agent** – a user agent is any software or device that interprets WML, WMLScript, WTAI or other resources. This may include textual browsers, voice browsers, search engines, etc.
- **WMLScript** – a scripting language used to program the mobile device. WMLScript is based on ECMAScript and loosely based on the JavaScriptÔ scripting languages.

- **CGI** Common Gateway Interface
- **EFI** External Functionality Interface
- **HDML** – Handheld Device Markup Language
- **HTML** HyperText Markup Language
- **HTTP** HyperText Transfer Protocol
- **IP** Internet Protocol
- **MMS** Multimedia Message Service
- **OTA** Over The Air
- **PDA** Personal Digital Assistant
- **PKI** Public Key Infrastructure
- **SSL** Secure Sockets Layer
- **TCP** Transmission Control Protocol
- **TLS** Transport Layer Security
- **UDP** User Datagram Protocol
- **URI** Uniform Resource Identifier
- **URL** Uniform Resource Locator
- **W3C** World Wide Web Consortium
- **WAE** Wireless Application Environment
- **WAP** Wireless Application Protocol
- **WDP** Wireless Datagram Protocol
- **WIM** Wireless Identity Module
- **WML** Wireless Markup Language
- **WPKI** Wireless Public Key Infrastructure
- **WSP** Wireless Session Protocol
- **WTA** Wireless Telephony Application
- **WTAI** Wireless Telephony Application Interface
- **WTLS** Wireless Transport Layer Security
- **WTP** Wireless Transaction Protocol
- **WWW** World-Wide Web
- **XHTML** Extensible Hypertext Markup Language
- **XML** Extensible Markup Language