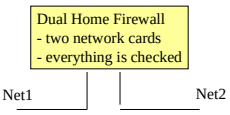
Security Solutions

•Network Security (Firewalls, VPN, IPSEC, SSL)

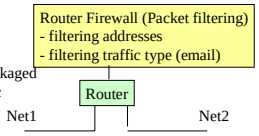
•Web and Application Security (SSL, Client Security, Server Security, Proxies, Security (security of wireless networks, apps, middleware)

Firewalls Overview

A) two networks are completely isolated
- Packets never transferred directly
- may be repackaged
- can run a proxy on the firewall machine



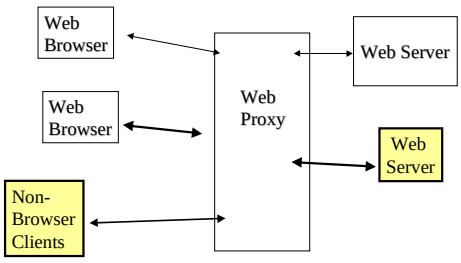
b) two networks are completely isolated
- Packets can transfer directly through router
- Some are sent to the firewall program e repackaged
- Firewall can run a proxy for repackaging, etc



Many commercially available firewalls: Altavista, Borderware (secure computing)

Proxies as Firewalls

•Proxies sit between clients and servers
•Act as a server to client and vice versa
•can be used for security, workload balance, etc

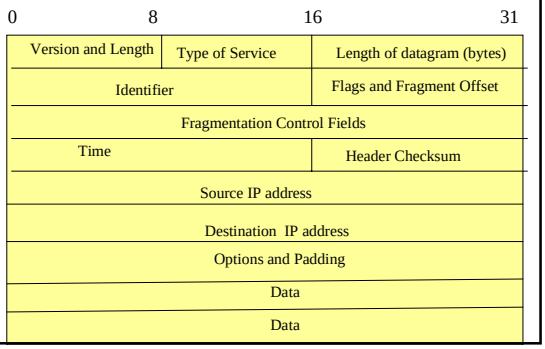


Proxies as Firewalls

- act on behalf of a server
- can be a front-end to many clients
- can handle security (used as a firewall) but can introduce security threat also (client not authorized but uses a proxy to fake authorization)
- can translate requests (web to non-web)
- can be used for caching
- can provide anonimity to clients or servers
- can be used for workload balance (more than one server)
- can be used to filter requests and responses
- Other uses?
  -

Packet Filtering Firewalls:

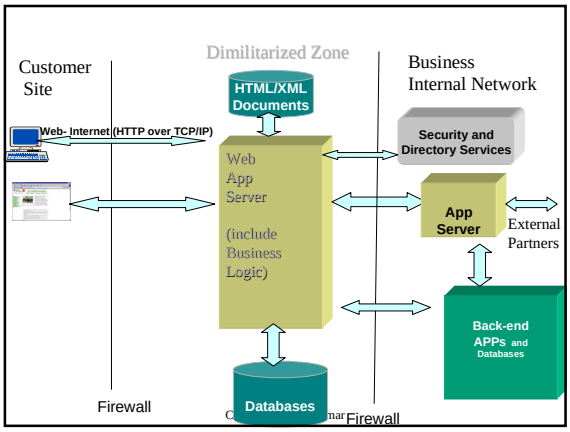
IP (v4) Packet Format



TCP Port Number Examples

Table Ethert Network Specifies System Assignments 1-1 Examples of Assigned TCP Port Numbers

Port No	Keyword	Description
0		Reserved
1-4		Not assigned
5	RJE	Remote job entry
7	Echo	Echo port
11	Users	No. of active users
13	Daytime	Daytime
15	Netstat	Network Status
20	FTP Data	FTP data send/receive
21	FTP	FTP session management
23	Telnet	Terminal logon/logoff
25	SMTP	Simple Mail Transport Protocol
53	Domain	Domain name server
80	HTTP	HTTP default port for Web

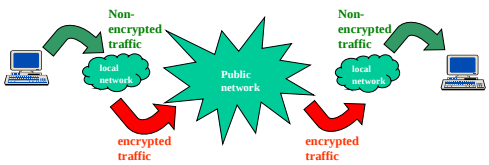


Firewall Policies and management

- Filtering versus applications
  - Filtering not strong enough for sensitive data (e.g., financial data)
  - Proxies must be controlled carefully
  - May need combination
- To use a DMZ or not
  - What should be in DMZ
- Firewalls policies need to be established and monitored carefully
- Firewalls only protect end-points
  - what about transmission network

VPN

- Virtual Private Networks (VPN)
  - Data that is sent over public infrastructure needs to be secured
  - Virtual private networks are private networks (e.g. networks internal to corporations) that use public communication infrastructure
  - Encrypts the data before sending (symmetric key)



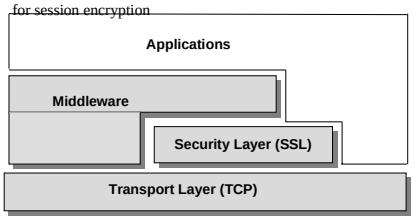
Internet Security Protocol (IPSec)

- Standard for VPN encryption (1992)
- Provides security at the packet level (IP), instead of security at application layer - Part of IPv6
- Encrypts and signs Headers and/or Data parts of IP Header
- Security handled without requiring changes to applications
- Issue:
  - If the entire packet is encrypted, how will the routers know where to send info (destination address)
  - destination headers are not encrypted or duplicated (encrypted, non-encrypted)

•Can authenticate machines but not users -- too low level

Secure Socket Layer (SSL)

- Runs on top of TCP/IP
- Manages secure messaging on the network
  - Client and server negotiate encryption scheme, key size (flexible)
  - Uses RSA Public encryption for key session negotiation, DSA for session encryption



Used heavily in Web
Web clients and servers agree on a "session" key

Availability Versus Security Tradeoffs in Corporate Networks

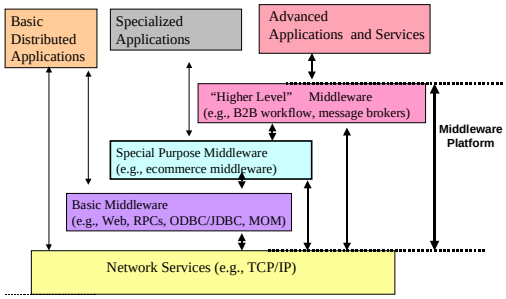
- Tradeoffs between security and availability must be considered while architecting a network security solution.
- Redundant network equipment can increase system availability but it also can introduce security exposures.
- For example, redundant routers, cables, and access points should be protected as diligently as the primary network equipments.
- Fragmentation, redundancy, and scattering (FRS) techniques employed to increase the security as well as availability of software by fragmenting the messages and then routing them on multiple paths

Web Security

- Web security Issues
- S-HTTP
- SSL
- Web Client side issues
- Web server side security
- SET (secure electronic transaction)

Middleware Security

- Different type of middleware services needed for different applications
- Advanced applications require several layers of middleware services
- Web presents high vulnerability (highly used, low protection)



Internet Security - Main Technologies

- Applications
  - SET (secure electronic transaction) and Cybercash: for electronic fund transfer
  - PGP and S/MIME: email security (encryption)
- Web:
  - S-HTTP; secure browsing
  - SSL: secure socket layer (TCP/IP level encryption)
  - TLS: transport level security (same as SSL)
- Network
  - IPsec: packet level encryption

Web-XML Security

- Many web security issues (client-side and server side)
- Web is used widely
- XML is very popular in many segments
- XML is relatively new, it has introduced several security concerns
- Intrusion of XML Schema can have serious impact
- Trading on the hubs that use XML can completely stop if the XML DTDs/schemas are modified to invalidate the transactions
- SSL (secure socket layer is the main approach)
- S-HTTP was a competitor

S-HTTP

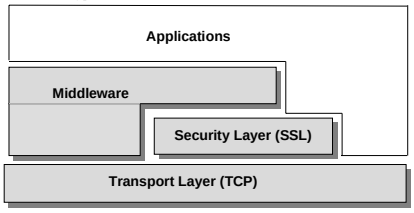
•Same type of cryptographic techniques as SSL
•Historical note:
  •SSL and S-HTTP came into existence roughly at the same time
  •SSL was free (with Netscape Browser)
  •S-HTTP was not (NCSA Mosaic)

•S-HTTP:
  •More oriented towards HTTP (uses HTTP headers)
  •Limited to HTTP only

•What to do with apps that do not run on top of HTTP (e,g,, ODBC)
•So far use has been rare
•May be brought back to life due to XML-Web services and .NET

Secure Socket Layer (SSL)

- Runs on top of TCP/IP
- Manages secure messaging on the network
  - Client and server negotiate encryption scheme, key size (flexible)
  - Uses RSA Public encryption for key session negotiation, DSA for session encryption



Used heavily in Web
Web clients and servers agree on a "session" key

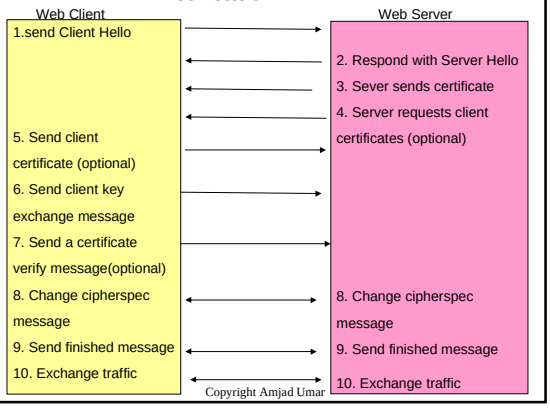
SSL (cont.)

- Not designed specifically for HTTP
- Gives many choices symmetric key: DES, triple Des,,,
  - asymmetric key (for authentication): RSA public key and certificates
  - Integrity: Message digest with MD5 or SHA algorithms
  - Various key lengths
- The choices known as “cipher suite” with different strength:
  - Example: DES-RSA-MD5 in SSL 3.0 (very high)
- Each web browser and server supports several cipher suites
- When an SSL client connects to a server
  - both negotiate a cipher suite that is strongest but available on both sides
  - Common problem: international web sites have smaller key lengths (40 bit) -- session uses 40 bit keys even though higher available
- SSL also provides built in encryption.

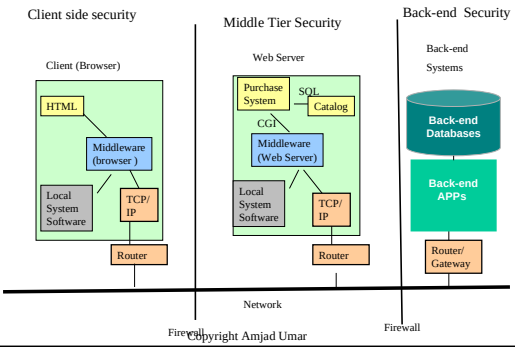
SSL (cont.)

- Once an SSL session is established, all web server to client traffic (both ways) are encrypted. This includes
  - URL of the requested document
  - Contents of the requested document
  - contents of any filled out forms
  - Cookies sent from client to server
  - Cookies sent from server to client
  - Contents of the HTTP header
- Cannot hide that a particular browser is talking to a particular server
  - can use a proxy for ananmity
- Screen appearance with SSL is very similar
  - use https instead of http (e.g., https://www.fedex.com)
  - lock appears in the bottom

SSL Session



Web-based application security Model

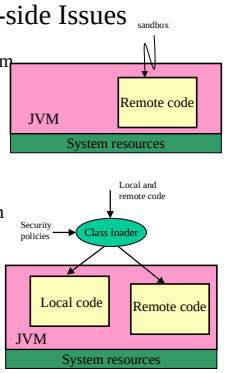


Client (Browser) Side Security

- Typical threats are based on active content
  - Helper applications and plug-ins
  - Java script and VB script
  - XML processing (XSL)
  - Java applets
  - ActiveX
  - CORBA clients
  - XML/SOAP clients
  - Cookies
- The role of PICS (Platform for Internet Content Selection)
  - intended for content type
  - being used for authorization (almost like HTTP headers)

Java Security - Client-side Issues

- Java1.1's security management system
  - All local code is trusted
  - All remote code is untrusted, unless it is digitally signed by a trusted source
  - Untrusted code runs in a "sandbox", and has limited access to local system resources
- Java 2's security management system
  - Local and remote code are checked by the same security management system
  - Fine-grained, flexible and easy-to-specify security and permission policies

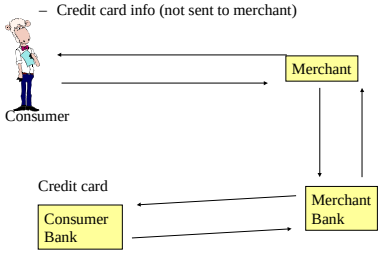


Web Server Security

- Many serious issues
  - HTML content
  - XML content
  - CGI
  - Servlets
  - JSPs
  - EJBs
  - ODBC/JDBC
  - Server logs
- Server side app issues
  - database access
  - transaction processing

SET (Secure Electronic Transactions)

- Primarily for credit card processing
- Dance between four players
- Purchase transaction separated in two parts:
  - Purchase info (sent to merchant)
  - Credit card info (not sent to merchant)



Availability Versus Security Tradeoffs in Distributed Applications

- Redundant application software can increase system availability but it also can introduce security exposures.
- Redundant copies must be protected as diligently as the primary copies.
- Fragmentation, redundancy, and scattering (FRS) techniques can be employed to increase the security as well as availability of distributed applications.
- For example, you can fragment the account information and scatter it around the network in such a fashion so that even if a hacker can access a fragment, he/she cannot understand it.
- Implies that the applications that access the fragmented and scattered information can properly understand the fragments.
- Some packages, such as Oracle 8i and later, allow fragmentation of Oracle databases.

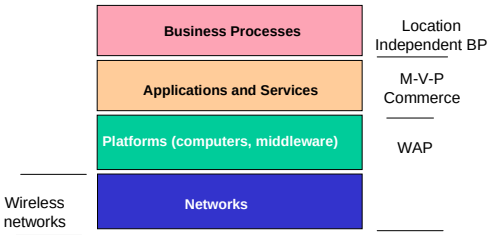
Wireless security

•Wireless Networks and wireless network security

•Wireless middleware and middleware security

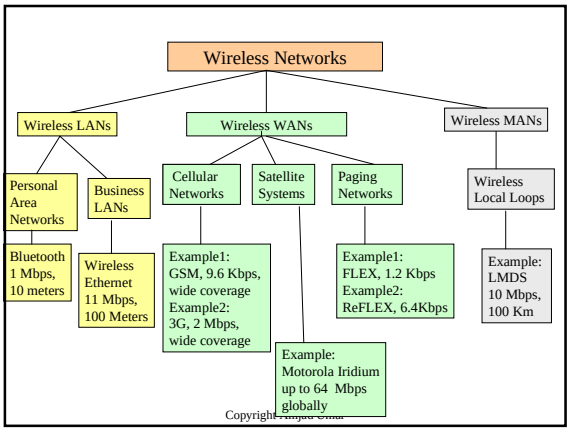
•Wireless applications and wireless applications security

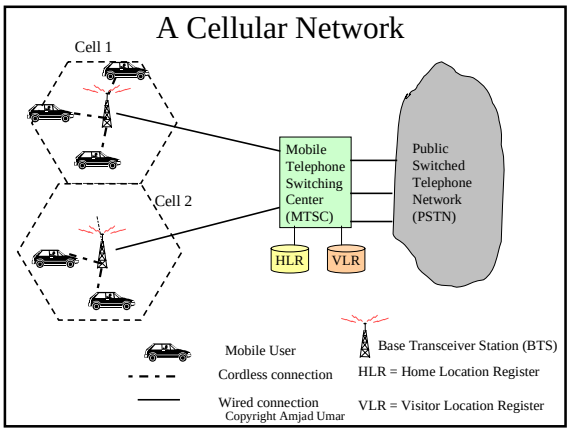
Security Mobility Issues at Various Levels

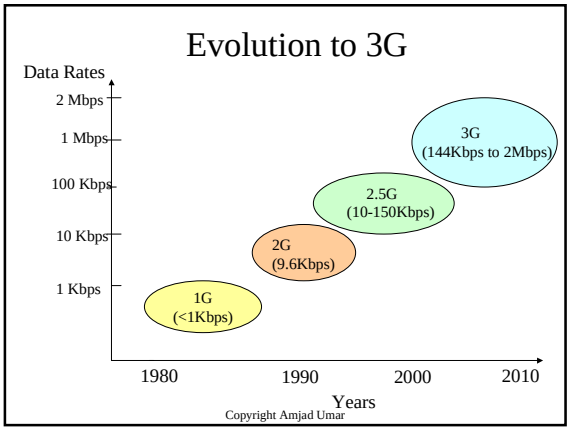


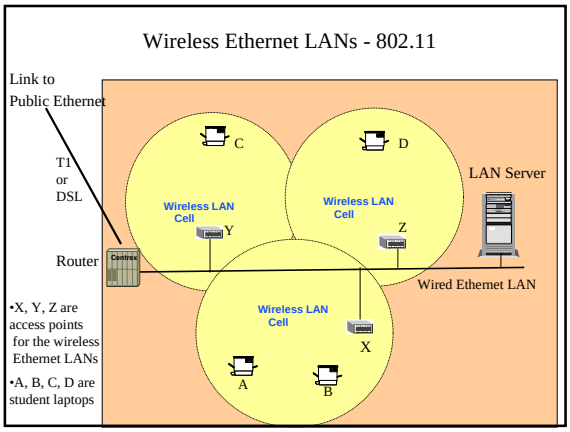
WIRELESS Security Issues

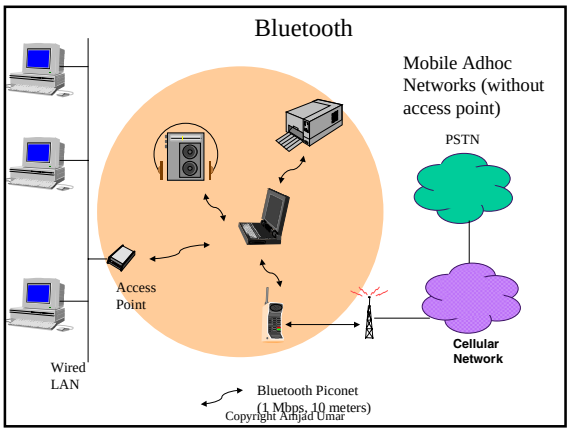
- Information transmitted over wireless networks
  - Wireless LANs
  - Bluetooth
  - Other wireless networks
    - Paging
    - Public packet networks: Mobitex and Ricochet
    - Satellite systems
    - Fixed Wireless
- Main issue: information transmitted over common medium (air)


Wireless Networks
Wireless LANs
Wireless WANs
Wireless MANs
Personal Area Networks
Business LANs
Cellular Networks
Satellite Systems
Paging Networks
Wireless Local Loops
Bluetooth 1 Mbps, 10 meters
Wireless Ethernet 11 Mbps, 100 Meters
Example1: GSM, 9.6 Kbps, wide coverage Example2: 3G, 2 Mbps, wide coverage
Example: Motorola Iridium up to 64 Mbps globally
Example1: FLEX, 1.2 Kbps Example2: ReFLEX, 6.4Kbps
Example: LMDS 10 Mbps, 100 Km
Copyright Amjad Umar


A Cellular Network
Cell 1
Cell 2
Mobile Telephone Switching Center (MTSC)
Public Switched Telephone Network (PSTN)
HLR
VLR
Mobile User
Cordless connection
Wired connection
Base Transceiver Station (BTS)
HLR = Home Location Register
VLR = Visitor Location Register
Copyright Amjad Umar


Evolution to 3G
Data Rates
2 Mbps
1 Mbps
100 Kbps
10 Kbps
1 Kbps
1G (<1Kbps)
2G (9.6Kbps)
2.5G (10-150Kbps)
3G (144Kbps to 2Mbps)
1980
1990
2000
2010
Years
Copyright Amjad Umar





Wireless Network Security

- Security concerns are more serious
- Many areas of vulnerability
  - Location services (HLR/VLR) are privacy concerns
  - the current wireless access points present a large security problem.
  - Mobile adhoc networks are concerns
  - Several products use un-authenticated Diffie-Hellman (DH) algorithm which suffers from a well-known *man in the middle* attack.
  - The Wired Equivalent Privacy (WEP) algorithm, part of the IEEE802.11standard for wireless LANs, is designed to protect wireless communication from eavesdropping.
  - Several weaknesses of WEP have been demonstrated
- Suggested approach:
  - encrypt the wireless traffic
  - heavily protect the resources accessed through wireless

WAP(Wireless Application Protocol)

•Intended for data entry/display on cellular phones
•"An open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly." *www.wapforum.org*
•Complete protocol stack similar to Internet protocols but optimized for wireless information pull and push transport layer and above; across multiple wireless technologie

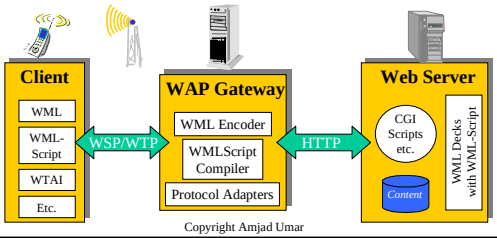
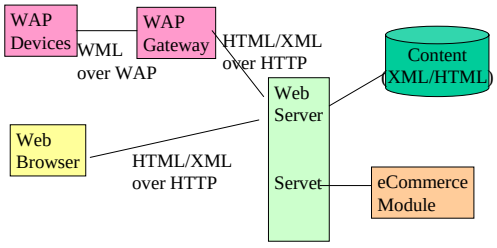


Figure 2: WAP Prototype



WAP Security

- WAP specification ensures that a secure protocol is available for transactions on a wireless handset.
- WAP uses Wireless Transport Layer Security (WTLS) protocol
  - WTLS ensures data integrity, privacy, authentication and denial-of-service protection.
  - WTLS does not support non-repudiation.
  - Some WTLS messages can be sent without authentication of origin
- WAP components can be attacked at several levels.
  - WAP clients and servers
  - WAP gateway
  - WAP messages
- Intrusion of WAP Gateway can have a very high impact on the WAP users.
- It is important to secure the WAP Gateway through high levels of security. It should also be replicated.

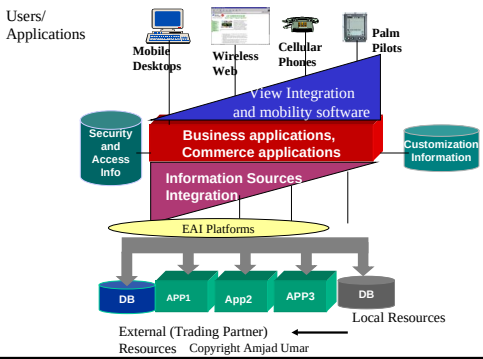
WAP Summary

- WAP is becoming an important element of the wireless and mobile middleware space
- WAP penetration is greater in Europe and Far East than US and elsewhere -- but gaining ground rapidly
- Some questions:
  - How many content providers will generate WAP/WML content? How well will automatic HTML/WML translators work?
  - Will existing Internet technology mature fast enough to reduce impact of WAP?
  - Will sophisticated e-commerce services for mobile users (e.g. stock purchase, transactions etc.) really become a significant market?

Mobile EB/EC Applications

- Mobility of:
  - Customers
  - Suppliers and Businesses
  - Employees
- Mobility applications in EB/EC
  - Mobile ebusiness applications (MEBAs), e.g., M-CRM, M-portal
  - Mobile ecommerce (M-Commerce)
  - Positional commerce *(p-commerce)* .
  - Voice commerce (v-commerce).
  - Television commerce (T-Commerce)
- Issues in building mobile applications
  - Network speed (wireless networks slower and unreliable)
  - Display features (increased voice usage)
  - "Roaming support"
- Two views:
  - Mobile applications are fundamentally new applications.
  - Mobility is another dimension of the existing EB/EC applications

Mobile Architecture



Mobile Agents in Ecommerce

- Simply stated: Agent: something that works on your behalf
- Typical agents are mobile, autonomous, intelligent

Many applications of mobile agents in Ecommerce (eMarkets)

- Personal agents to collect and present information to you in the way you want it
- shop bots: agents that go around and shop on your behalf
- Brokers and traders can be agents that act on your behalf
- Collaborative agents can perform collaborations
- Mobile agents to support mobile ecommerce
  - wireless devices may not be always connected
  - mobile agents hop around finding their way over a wireless network
- Multi-agent systems for large scale trading and brokering
  - Many local agents
  - Local agent managers handle local agents
  - multi-agent systems handle multiple local agent managers

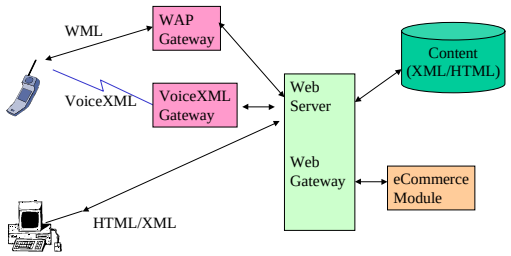
P-Commerce

- E-Business using global positioning systems (GPS)
- Possible usage
  - find shops close to his/her current location
  - guide cars to less congested routes
  - link up with maps and GIS for computation or measurement
  - co-relate with data associated with entities that occupy a location (e.g. house)
  - auto select a carrier for a call with least costs or certain feature based on the calling location

V-Commerce

- E-Business using voice interfaces
- Why?
  - access for your customers who are not yet on-line
    - voice devices more popular than data devices
    - voice interface is easier to learn than web interface
    - mobile devices mostly voice
- Typical uses
  - transaction-based services
  - self-service
  - workforce productivity

Voice Prototype



Mobile Application Security

- Mobile ecommerce is a potential area of growth
- Mobile agents are security risks
- Positional commerce raises some privacy issues
- Mobile application gateways must be protected (firewalls)

Some sites

- Wap forum (www.wapforum.org)
- www.mobileinfo.com
- www.ericsson.com
- www.nokia.com