Software for secure wireless e-business

Vaughan Harper
Tivoli EMEA Security Product Manager
Software for secure wireless e-business

- Why Wireless e-business?
- Approach to Wireless e-business
- IBM Products
- Case Study
Motivation for Wireless Client Support

Pervasive Devices Will Become the Dominant Means of Information Access

Installed Base (Millions)

10000
1000
100
10
1


Note: Does not include cars with driver information systems (approximately 8% of 150 million in 2006)

Sources: ResearchPortal.com, Semico, EE Times, Gartner, Reuters, Ericson, . . .
Europe, Asia-Pacific and North America total over 85% of the mobile market opportunity.
Software for secure wireless e-business

- Why Wireless e-business?
- Approach to Wireless e-business
- IBM Products
- Case Study
"They’re out to get you!"

- **Threats**—viruses, hackers (crackers) competitors, insiders, . . .
- **Risks**—Corporate image, public trust, intellectual/financial capital, privacy, litigation, . . .

**Orientation:**
Keep intruders out!

"Security as an enabler!"

- **Policy-driven security**
  - Centralized policy definition:
    - Identify e-business participants
    - Determine their access rights
- **Security tightly linked to:**
  - Enterprise management/directory
  - Risk management
  - e-business resource availability

**Orientation:**
Allow authorized people in!
How to make wireless e-business a reality?

- Security involves balancing costs...

  It needs to be easily implementable
Software for secure wireless e-business

• Why Wireless e-business?

• Approach to Wireless e-business

• IBM Products
  – Tivoli Policy Director 3.8
  – Tivoli Risk Manager 3.8
  – IBM WebSphere Everyplace Server R2

• Case Study
Tivoli Policy Director
Policy Director - Web Access Control

- Policy Manager
- Object/ACL Database
- User Registry (LDAP)
- Virtual Web Namespace
- Internet
- WebSEAL
- Object/ACL Replica
- SSL
- Wireless Gateway
- Netscape
- Domino
- MS IIS
- IBM Wireless e-business
Policy Director - Broad Scope

Define security policy centrally

Privacy Applications
- Dynamic roles
- Personally-identifiable information

MQSeries
- Store-and-forward applications

UNIX Servers
- UNIX system resources

Web/URL
- URLs
- CGI programs
- HTML files
- Java servlets
- Java class files

WebSphere and other Web/application servers, via standardized interfaces
- Java 2 / JAAS
- The Open Group’s Authorization API (aznAPI)

PCs
- NetVista A40p and other PCs with the embedded security chip

Easily Extend

Policy Director

Easily Extend

Policy Manager

User

ACL

ACL
Network Dispatcher balances traffic across multiple WebSEAL proxies

WebSEAL balances traffic among multiple Web Servers
What Does Policy Director Do?

- **Maintains a central user registry**
  - Users and groups
  - Authentication information
- **Maintains a model of the Protected Objectspace**
  - Hierarchically organised
- **Defines permitted actions on objects**
  - Uses Access Control List templates
  - These are attached to entries in objectspace
- **Provides an API for making Authorization queries**
  - And provides a number of ‘blades’ that use it
Authentication versus Authorization

- **Authentication**
  - Who is the user?

- **Authorization**
  - Determining if a given user or entity has permission to perform an action on a protected resource... or “what is that user allowed to do”?
Delegated Enterprise Administration

Requirements: Align security admin with organization and business relationships (departments, dealerships, branch offices, partnerships, suppliers, distributors...)

- Multiple levels of delegation
- User administration
- Group and role administration
- Security administration
- Browser-based for ease of deployment/operation
WAP Support Architecture

WAP Phone 1

WAP Device 2

REMOTE ACCESS SVR

WTLS

Mobile Commerce Provider (MCP)

WAP Gateway

WTLS

SSL

SSL

PD Proxy

PD Proxy

Telco

WebSEAL or WebSphere Caching Proxy

Internet

SSL
Policy Director WAP Support

How Does It Work?

- In WAP scenarios, WebSEAL¹ is 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)
- WebSEAL¹ uses the WAP gateway for authentication:
  - WML form
  - In the near future: WAP Identification Module (WIM) module for client-side, certificate-based authentication
- WAP gateway sends information to WebSEAL¹ via:
  - HTTP header
  - Cookie
- WebSEAL¹ maps phone’s ID into an internal Policy Director identity
- Authorization performed by WebSEAL¹ using Policy Director identity
- The solution should work with any WAP Gateway
  - Nokia and IBM’s WebSphere Everyplace Suite (single SSL)
  - Tantau (Multi SSL)
- i-mode phones work with NTT GW
- Cookie proxy supports i-mode phones that don’t handle cookies
- PD proxy can be the Edge Server Caching Proxy or WebSEAL
- WebSphere Transcoding Publisher (WTP) handles Web sites that haven’t been designed for i-mode (e.g. compact HTML)
Benefits of Common Security Services

Old Way
- Security coded into each application
- Update user access policy? Multiple places!
- Individual sign-on to each application

With Policy Director
- Common security services, separate from application
- Consistent, delegatable admin
- Single sign-on
- Personalized user experience
IBM is delivering the industry's first secure access management software, Tivoli Policy Director, that can deliver a consistent security policy across both WAP and i-mode applications.
**Platforms**

- AIX 4.3.3
- Solaris 7, 8
- Windows NT 4.0, SP6a
- Windows 2000 Advanced Edition
- HP-UX 11.0
- RedHat Linux 7.1 (x86)
  - PD RTE and AuthADK only

**Languages/Translation**

- English, French, Italian, German, Spanish, Korean, Brazilian Portuguese, Japanese, Simplified Chinese, Traditional Chinese

Single byte and double byte character support.

**Crypto**

- Single world-wide product (128-bit)
Secure Web portal environment for GM/supplier applications
30,000 suppliers—critical to prevent info access cross-over!

Customized delegated administration
Interfaces to Microsoft Exchange

Quickly moved from pilot to production

Authorization for easyPAY e-business (Pay at the Pump) application
Other applications—commercial partners and customers check accounts

Reached 1 million users April, 2001
82 applications; 35K logins/day
Help desk calls down 61% since PD has been in production
Policy Director - Customer Examples - Europe

BRITISH AIRWAYS

The Reliable Airline KLM

IBM Wireless e-business
Tivoli Risk Manager
Risk Manager

IBM Research

Network Scanner

ISS RealSecure System Agent
Tivoli Host IDS for Windows, AIX and SUN Servers

ISS RealSecure Network Engine
Cisco Secure IDS
Tivoli Network IDS

Symantec Norton AntiVirus for Desktops

Tivoli SecureWay
Risk Manager 3.8

Tivoli Web IDS for WebSphere, Microsoft IIS, Domino, Apache, Netscape Web Servers

CheckPoint FW-1
Cisco PIX Firewall

Cisco Routers

* Technology Preview

IBM Wireless e-business
<table>
<thead>
<tr>
<th>Time Received</th>
<th>Class</th>
<th>Repeat count</th>
<th>Severity</th>
<th>Status</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>RMV_VirusFound</td>
<td>0</td>
<td>Critical</td>
<td>Open</td>
<td>VIRUS: smithnt1 [smithnt1.NA =&gt; ... Virus: Nuke/NukeIt.gen Typ...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>RMV_VirusFound</td>
<td>0</td>
<td>Critical</td>
<td>Open</td>
<td>VIRUS: jonesnt1 [jonesnt1.NA =&gt; ]... Virus: Nuke/NukeIt.gen Typ...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_WEP_Open</td>
<td>0</td>
<td>Harmless</td>
<td>Open</td>
<td>SECPOLICY: tv1 (N/A =&gt; tv1)    WSA: State wep-open Desc...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_WEP_Shared</td>
<td>0</td>
<td>Harmless</td>
<td>Open</td>
<td>SECPOLICY: tv2 (N/A =&gt; tv2)    WSA: State wep-shared D...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_WEP_Shared</td>
<td>0</td>
<td>Harmless</td>
<td>Open</td>
<td>SECPOLICY: tv3 (N/A =&gt; tv3)    WSA: State wep-shared D...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_WEP_Associated</td>
<td>0</td>
<td>Warning</td>
<td>Open</td>
<td>SECPOLICY: tv4 (N/A =&gt; tv4)    WSA: State wep-associate...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_Open</td>
<td>0</td>
<td>Critical</td>
<td>Open</td>
<td>SECPOLICY: tv5 (N/A =&gt; tv5)    WSA: State open Desc:...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_Open_Associated</td>
<td>0</td>
<td>Critical</td>
<td>Open</td>
<td>SECPOLICY: tv6 (N/A =&gt; tv6)    WSA: State open-associate...</td>
</tr>
<tr>
<td>01-Oct-01 6:36:48 AM</td>
<td>WSA_Open_Associated</td>
<td>0</td>
<td>Critical</td>
<td>Open</td>
<td>SECPOLICY: tv7 (N/A =&gt; tv7)    WSA: State open-associate...</td>
</tr>
</tbody>
</table>
New wireless network vulnerability management capabilities have been added to Tivoli Risk Manager for wireless security event correlation and analysis (Available Oct. 10)

- Monitors output of the Wireless Security Auditor
- Sends events to the Tivoli Risk Manager event correlation engine and management console
- Combining these security events with firewalls, intrusion detection systems, servers and other security checkpoints--giving administrators a broad view of e-business security exposures, attacks and vulnerabilities
WebSphere Everyplace Server R2
WebSphere Everyplace Server R2

- **Everyplace Wireless Gateway**
  - Support for SMS and I-Mode
- **WebSphere Transcoding Publisher**
  - Transforms content into a form that can be presented on a device - XML -> HTML, cHTML, WML …
- **Tivoli Personalized Services Manager (TPSM)**
  - A comprehensive set of management services including
    - Content personalization, Enrollment, Self care, Customer care, Interfaces to billing systems…
- **WebSphere Edge Server**
  - Highly scalable caching functions on a server to reduce bandwidth costs and improve response times
- **TPSM user management will manage Policy Director users**
  - Mapping of TPSM user collections (realms) to Policy Director groups
  - Use of ACLs to control groups/realms access to deals (e.g. $19.95 for 1000 minutes/month) and premium content services (e.g. Doppler Radar service)
  - User self enrollment:
    - User written to TPSM database
    - User written to TPSM/PD LDAP
    - User added to groups
  - Self management via TPSM
  - User’s personalized home page can be provided via
    - TPSM API
    - Policy Director aznAPI “entitlements” service

- **WES and Policy Director can share common LDAP user/group information**

- **Edge Server with WebSEAL Lite can be used as an alternative to WebSEAL**
  - WebSEAL Lite:
    - Provides authentication (username/password only) to LDAP
    - Provides aznAPI calls for authorization decisions
    - Provides SSO via LTPA
Software for secure wireless e-business

- Why Wireless e-business?
- Approach to Wireless e-business
- IBM Products
- Case Study
Wireless/Wired Portal

- Customer is big European telco
- Wanted to provide portal services to both their wired and wireless customers
- Solution using Tivoli Policy Director and WebSphere Everyplace Server
The Approach...

- **Policy Director**
  - Authentication and Access control for web resources
- **TPSM**
  - Enrollment, self-care and device management
  - Registered users can use the self-care application (update their preferences, password and service selections)
- **Wireless Gateway**
  - Translation from WAP (or other) to TCP/IP
- **Transcoding Publisher**
  - Transforms content as required to device

- **Optimum Combination of IBM Products**
Physical Architecture

Internet

DMZ

Wireless Gateway

Network Dispatcher

Policy Director WebSEAL Proxy

WTE Proxy

Policy Director WebSEAL Proxy

TPSM Servers

Self Care

Enrollment

Device Manager

Intranet

LDAP Server

Radius Server

TPSM Servers

TPSM DB

TPSM Servers

Self Care

Enrollment

Device Manager

Web Application Server

Web Application Server

TP

TPSM DB

TPSM Servers

InternetDMZIntranet
Recognized Leadership

Tivoli • Software Portfolio Wins Information Security Excellence Award

Reader’s Choice Award for Enterprise Security, Authorization & Centralized Administration Presented to Tivoli at InfoSec World

Market Engineering Leadership Award for Security

FroST & Sullivan

Market Engineering Award Recipient

2001

IBM Wireless e-business
Conclusion

• Wireless e-business can be a reality

• IBM provides the ideal software/services to make wireless e-business a reality - now!