Securing a Global CORBA-based Logistics Support System at Volkswagen

Gerald Brose, Jörg Bartholdt, Olaf Haase

Xtradyne Technologies AG  Volkswagen AG
Roadmap

- GLOBUSS
  - Enterprise-wide tracking and tracing system
- Requirements
  - Architecture
  - Security
- System Architecture
  - Security Technology
  - Integration
- Lessons Learned
Global Unit Supply Survey

- GLOBUSS -

- GLOBUSS
  - supports tracking and tracing of items between sites

- Complex logistics interrelationships between sites
  - Global exchange of materials with long shipping times
  - Enable short-term reaction to market changes and avoid bottlenecks or over-storing
  - requires precise control of the flow of goods

- Project partners:
  - Volkswagen, gedas (Volkswagen IT subsidiary)
  - Xtradyne
GLOBUSS functionality

- Displays part shippings within Volkswagen
  - Disposition information
    - „Do I have enough of part xyz? Is supply under way?“
    - „How long will it take until abc arrives?“
    - „Where are empty containers for shipping part #4711“
  - Manual bookings (where integration with other systems incomplete)
    - Shows deviations from projections
- Supports access from world-wide sites
GLOBUSS integrates data from different sources

Process Flow based on time schedule

Delivery order

Supplier Order System

Packing Service System

Export Port System

Import Port System

Deconsolidation Area

VW Plant System

Order

Container

Box

Invoice

Status

Order

Container

Vessel

Container

Container Box / Parts

ORDER-ENTRY

Packing Invoice Out

Terminal Port Out

PORT IN

Terminal Gate Out

DC IN

VDA 4905

VDA 4913

VDA 4906

EDIFACT IFTSTA

= Tracking points

DOCsec 2002
Architecture Requirements

- Browser-based, but complex GUI
  - Applet clients rather than HTML-based GUI
- Internet access for sites without intranet access:
  - Certain foreign branches, external service providers
- Interoperability and Performance concerns
  - Potentially narrow-band internet connections
  - IIOP rather than XML-based protocols
- Outsourcing of server infrastructure
  - operated + managed by ASP (gedas)
- World-wide deployment, control over client software
  - Applets designed and maintained by Volkswagen
Overall Application Architecture

- App Server
  - Business Objects
- Web Server
  - HTML
  - JAR
- Database
- Internet
  - HTTP
- Applet Client
- VDA's
  - EDI
  - FACT
- RVS
- EDI Converter
- Volkswagen intranet
- IIOP
Customer Security Requirements

- Focus on Perimeter Security
  - Retain security in internal and ASP networks
  - Several separated segments
- IIOP Firewall Traversal
  - Well-known problem, ASP won’t simply open port ranges in its firewalls
  - Use of Network Address Translation (NAT)
  - Filter GIOP requests
- System complexity must be kept low
  - Minimize potential for software errors
  - Simplify administration
  - Minimize impact on applications
Security Requirements contd.

- Encrypt Internet communications
  - Prevent fake bookings or corruption
  - Keep transport information private

- Authentication
  - Perform authentication in the DMZ
  - Strong Server authentication
  - Strong Client authentication

- Audit
  - Write Audit logs for operations and trigger alarms for invalid messages
  - Perform audit on separate log host
Selected Technologies

- Server authentication & transport encryption
  - SSL
- Client authentication
  - RSA SecurID, already in use at Volkswagen
  - No corporate PKI available
- ORBs
  - Signed Client-side applets on JacORB + SSL libs
  - C++ server on BEA WebLogic Enterprise
  - Communicates with back-end Oracle DB
Selected Technologies (contd.)

- Application-level gateway: Domain Boundary Controller (DBC)
  - secure IIOP firewall traversal
    - ORB-neutral
    - transparent to applications
  - provides IIOP/SSL: no SSL in servers required!

- Client Authentication
  - DBC supports RSA SecurID

- Auditing
Lessons Learned

- IIOP over the Internet does work
  - Secure firewall traversal with good performance possible
  - Complex applications can be deployed
- Integration of different ORBs using IIOP/SSL
  - not always easy
  - Open Source ORB (JacORB) proved stable and mature
- Mutual authentication requires client modification
  - Potentially more than one user input/message necessary for SecurID
- Security Gateway approach simplifies matters
  - Integrates well with existing packet filters
  - No changes to servers