

# High Assurance Security For Embedded, Distributed Systems

Bill Beckwith  
Objective Interface Systems, Inc.  
+1 703 295 6500  
[bill.beckwith@ois.com](mailto:bill.beckwith@ois.com)  
<http://www.ois.com>  
OMG Real-time and Embedded Workshop  
July 2002

## Embedded Security Initiative



- Terms
- Motivations
- Issues
- Trust Model
- Proposed Solution Space



## Terms

- Authentication
  - Verifying that the accessor of data or sender of a message is authentic
- Access Validation
  - Providing application developers with APIs to validate that an accessor can access information
- Confidentiality
  - Third parties cannot access information
  - Encryption commonly used
- Encryption
  - Scrambling data
  - Allows transmission of information through untrusted areas



## More Terms

- Integrity
  - Assurance that third parties have not modified information
- MAC - Mandatory Access Control
  - Access controls that prevent a user from making information available arbitrarily
  - As opposed to discretionary access controls like the ACL mechanism
  - Typically implemented with information *labeling*
- TCB - Trusted Computing Base
  - “The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy.” – TCS Eval Criteria

## Viewpoint: Why are we doing this?



- Address customer need for a security architecture that is:
  - Standards-based
  - High-performance
  - Lightweight
  - Economical
  - MAC-capable
  - Cross-platform
  - Distributed
  - With minimal trusting model

## Motivations



- Existing O/S security architectures
  - + Don't require trusting the application code
  - Inconsistent support across O/Ses
  - Don't distribute
    - Creates huge hole in TCB when IP is used
  - Most don't support MAC (Mandatory Access Control)
  - Aren't extensible
- Existing distribution security architectures
  - CORBA Security
    - + Independent standard
    - + Distributes well (delegation)
    - Requires trust of ORB, application, and transport (i.e. ORB, application, and transport are part of TCB)
    - No MAC

## Motivations 2

- Existing distribution security architectures (cont.)
  - Banking/ATM
    - Visa Security Module
      - Cryptoprocessor
      - Protect PINs transmitted over ATM networks
      - Requires specialized, proprietary hardware
      - High performance was not a design goal
  - ???
    - Trusted RDBMS?

## Motivations 3

- Budding applications & security architectures
  - Information enabled warfighter
    - DoD: Joint Tactical Radio System, connected intel, ...
    - Air Force: JSF, F-22, UAVs, ...
    - Army: Objective Force, Land Information Warfare Activity, ...
    - Navy: Aegis, DD-21, ...
  - Digital entertainment content protection
    - 5C
  - Home automation security
    - Honeywell GHS
  - TV set top boxes
    - AOL TV
    - TiVo

## Embedded Security Issues

- Performance Concerns
  - Slower kernel operations
  - Potential source of jitter
- Footprint Concerns
  - Larger kernels
    - Authentication
    - Authorization
    - Encryption
    - Auditing
  - Larger applications
    - Access checks
    - Error handling
    - Maintaining levels

## Trust Model

- Application Trusting Model
  - Applications part of TCB
  - Scope of trust includes:
    - Application programmer
    - Tools vendors
    - O/S vendors
    - Hardware vendors
- Kernel Trusting Model
  - Applications must obey security system
  - Existing kernel based trust models are ignorant of distribution
- Hardware Trusting Model
  - Kernel and applications must obey security system



## Distributed Security

- General standards
  - CORBA Security
    - + Independent standard
    - + Multiple implementations exist
    - + Robust model for building trusted applications
    - Requires trust of ORB, application, and utility libraries
    - Trust is transitive
    - Large implementations
    - Existing implementations introduce large overhead to ORB
  - SSL, SSH, RSA, Triple-DES
    - + Content protection
    - Large implementations
    - Heavy computational requirements
    - Incomplete security model
    - No provision for Mandatory Access Control (MAC)



## Proposed Solution Space

- Extensible security architecture
- Security system is pluggable
- Kernel security hooks
- Application access validation API
- Labeled messaging protocol and API



## Kernel security hooks

- Allow third-party installation of
  - Access validation
  - Auditing
  - Authentication
  - Authorization
  - Encryption
  - Information Labeling



## Application access validation API

- Used by application developers
- Consistent API between
  - Security system and
  - Application

## Labeled, messaging protocol and API



- Below-the-middleware technology
- Integral with kernel security plug-ins
- Potential uses:
  - Intersystem communications
    - Not limited to just IP
    - Provides for assurance, authentication, identification, confidentiality, integrity, etc. of messages
  - Peripheral communications
    - Disk storage of secure data

## Venue for specification



- Options
  - Open Group?
  - OMG?
  - ISO, ANSI, ...
- Chose
  - Open Group
  - More O/S vendor involvement



## Further Information

- Open Group Real-Time and Embedded Systems Forum, Security Working Group
  - <http://www.opengroup.org/rtforum/>
- Real-time and embedded CORBA discussion forum, security discussion
  - [http://www.realtime-corba.com/ultimatebb.cgi?ubb=get\\_topic&f=6&t=000001](http://www.realtime-corba.com/ultimatebb.cgi?ubb=get_topic&f=6&t=000001)
- Information about CORBA for Real-Time, Embedded, and High Performance Applications
  - <http://www.ois.com/resources/corb-1.asp>