

Security Project Success Stories

High-quality, Innovative, and Reliable Secure Solutions from Leading Security Experts

Over the years, ObjectSecurity has successfully delivered many different projects. Our customers benefited greatly from the in-depth knowledge, innovation, flexibility, quality, and many years of experience our staff has. Some of our non-confidential success stories include:

Model Driven Security Accreditation Research Project for UK Ministry of Defence (UK, 2009)

ObjectSecurity was awarded a concept exploration project by the UK Ministry of Defence's Centre for Defence Enterprise (CDE), to outline ObjectSecurity's "Model Driven Security Accreditation" (MDSA) concept. MDSA applies model-driven security to assurance accreditation for agile, interconnected IT landscapes. Agile accreditation is a great challenge, and is currently often cited as one of the show-stoppers for the adoption of modern IT architectures (e.g. SOA) in mission critical domains.

ObjectSecurity's unique patent-pending Model Driven Security Accreditation (MDSA) approach automates large parts of the compliance and assurance accreditation management processes (e.g. Common Criteria). The benefits of MDSA are most significant for agile, interconnected IT "systems of systems" that are model-driven (potentially also business process-driven). MDSA automatically analyses and documents two main aspects:

- Does the actual security match with the stated requirements?
- Do any changes impact the current accreditation?

See www.modeldrivensecurity.org and www.objectsecurity.com for details.

OpenPMF / RTI DDS Integration for US Navy / Air Force (USA, 2007 / 2008)

"ObjectSecurity provides significant experience in security management." (for US Navy & US Air Force)

(Joe Schlesselman, Real-Time Innovations)

ObjectSecurity was contracted by Real-Time Innovations (RTI) to develop OpenPMF plug-ins for their Data Distribution Services (DDS) middleware. ObjectSecurity extended their OpenPMF policy manager with the features necessary for DDS, and

implements local plug-ins. ObjectSecurity also added OpenPMF to RTI's DDS demonstrator, so that secure RTI DDS can be demonstrated to the customer base.

The benefit for DDS end-customers is that they can manage security for large DDS environments centrally, flexibly, intuitively and with low effort. This makes RTI DDS the first DDS implementation in the world that includes security and model driven security management. RTI Data Distribution Service (formerly NDDS) is networking middleware that implements a real-time publish-subscribe communications model and allows distributed processes to share data without concern for the actual physical location or architecture of their peers. It includes support for best-effort and reliable communications (including reliable multicast), as well as client-server communications. RTI Data Distribution Service is an open-architecture, data-critical platform based on the Object Management Group's (OMG) Data Distribution Service for Real-Time Systems (DDS). The OMG is the same group that manages the CORBA and UML standards. OMG recognized the need to augment CORBA with a data-centric publish-subscribe specification. The DDS standard answers that need, and RTI is a primary author of the new specification. RTI Data Distribution Service is field-proven middleware that is currently used in a wide variety of time-critical applications. It is available with C, C++, and Java APIs.

Model Driven Security (MDS) for SOA study for QinetiQ for MoD (UK, 2007)

"ObjectSecurity supported QinetiQ's analysis of Service Oriented Architectures by providing a thorough and enlightening overview of the industry's history and best practice."

(Dr. Mark O'Dell, QinetiQ)

Defining security policies for complex, large IT environments is a difficult, cumbersome, and error-prone task. This is in particular the case for agile IT environments such as highly distributed component based systems and Service Oriented Architecture (SOA). We have shown that model-driven security, which allows the generation of security policies from the application models, helps build and maintain secure, agile IT environments. ObjectSecurity is the world leader for model driven security.

ObjectSecurity carried out a SOA model driven security study for QinetiQ (contracted by the UK Ministry of Defense). The project deliverable provides the definitive reference to model driven security, objectives, benefits, approaches, vendors, prior work, and

industry trends. It also outlines the concepts behind OpenPMF 2.0 as the leading model driven security solution in the world.

Model Driven Security (MDS) for SOA study & workshop for BAA Heathrow Airport (UK, 2007)

ObjectSecurity carried out a SOA security roadmap consulting project for BAA Heathrow Airport. The study discussed the benefits of model-driven security and OpenPMF 2.0 for agile SOA security in an airport IT environment.

Model Driven Security (MDS) for SOA study & workshop for large German software vendor (Germany, 2007)

ObjectSecurity carries out a SOA security training and consulting project for a large European enterprise software vendor. A whitepaper discusses the benefits of model-driven security and OpenPMF 2.0 for agile SOA security within the SAP software suite.

Technical Support Contract for Lufthansa Systems (Germany, 2008-2009)

Lufthansa contracted ObjectSecurity twice to provide technical support for their MICO CORBA deployment.

Service Oriented Architecture (SOA) best practice analysis for QinetiQ (UK, 2007)

ObjectSecurity carried out an extensive review of a large analysis of Service Oriented Architecture (SOA) for the UK Ministry of Defense. The QinetiQ-led project was a study to assess the feasibility and benefits of SOA for MOD's CCII. ObjectSecurity's involvement was in the best practice analysis part where many widely-applicable recommendations were identified. ObjectSecurity also attended two QinetiQ-led SOA workshops with MOD, suppliers, and consultants and presented the best practice recommendations and ObjectSecurity's TrustedSOA approach to SOA security.

Service Oriented Architecture (SOA) security analysis for Cyber Security KTN (UK, 2008)

ObjectSecurity LLC Plug & Play Tech Center, 530 University Ave, Palo Alto, CA 94301, USA,
Tel. +1-650-515-3391, Fax +1-360-933-9591

ObjectSecurity Ltd St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS, United Kingdom
Tel: +44 (0) 1223 420 252, Fax: +44 (0) 1223 420 844

info@objectsecurity.com www.objectsecurity.com

In 2008, ObjectSecurity was contracted by the UK Cyber Security KTN to produce an in-depth study about the specific security challenges of SOA. This website www.secure-soa.org is the project online resource. The project includes a core document and numerous appendixes. An extended version that includes recommendations is commercially available.

SINS prototype demo for US Naval Research Lab (USA, 2006)

"ObjectSecurity has in-depth technical knowledge and industrial experience in the design and development of secure systems."

*Dr. Ramesh Bharadwaj,
U.S. Naval Research Laboratory*

ObjectSecurity partners with U.S. Naval Research Laboratory (NRL) to productize NRL's SINS middleware. The goal of the partnership is to complete the SINS prototype and bring it to a certified, ready-to-market product state. SINS is currently at a full prototype technology readiness level (TRL) and all concepts have been successfully validated. According to NRL's Dr. Ramesh Bharadwaj, who is responsible for the SINS project, and his colleague Jim Kirby, NRL intends to pursue several funding opportunities for their planned SINS commercialization strategy with ObjectSecurity.

SINS middleware supports the implementation of secure, distributed applications. It has some unique features that differentiate it from other middleware:

- Guaranteed Delivery vs. Best Effort
- Guaranteed Preservation of Global Properties
- Application Survivability
- Strong Information Security
- Model Based Application Development
- Support for Central Administration
- Certifiable Code Base
- Scalability
- Commercial Technical Support & Services

SINS consists of an infrastructure, a language, and a methodology. Software agents, defined in the Secure Operations Language (SOL), execute and communicate with one another and with services via the SINS infrastructure. The methodology guides the development of software agents and helps developers reuse existing patterns for their design. The SINS methodology, language, and infrastructure are multi-faceted. It has been our experience that a simple description of our framework is inadequate to expose all these facets.

ObjectSecurity LLC Plug & Play Tech Center, 530 University Ave, Palo Alto, CA 94301, USA,
Tel. +1-650-515-3391, Fax +1-360-933-9591

ObjectSecurity Ltd St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS, United Kingdom
Tel: +44 (0) 1223 420 252, Fax: +44 (0) 1223 420 844
info@objectsecurity.com www.objectsecurity.com

MICO Port for ESG for the HEROS-2/Lot 2 for the 1st German-Netherlands Corps (Germany, 2008)

ObjectSecurity was contracted by ESG to port their existing CORBA applications to the MICO open source CORBA implementation for the HEROS-2/Lot2 military command & control system. The success of this project shows ObjectSecurity's capabilities in mission-critical environments and in the defense industry, and also underscores the maturity of the MICO software.

"highly competent, well-managed and cost-effective technical support"

--- Steffen Pohle, ESG

SWIM-SUIT: ATC System Wide Information Management Supported by Innovative Technologies (EU FP6, 2007-2010)

ObjectSecurity joined the already running EU FP6 SWIM-SUIT project as a middleware and modeling security specialist partner. It supports the development of technologies for System Wide Information Management (SWIM) for the future SESAR air traffic management system. This STREP with a total budget of 11,8 M€ provides vital input into SWIM for SESAR, the next generation air traffic management system across Europe. The main objectives of the project is a feasibility study of a System Wide Information Management (SWIM) implementation: Specification of the requirements for the SWIM prototype, validation of the technologies identified as enablers of the SWIM concept, and assessment of the organizational, legal and financial implications. The demonstrator will consider middleware and communication architectural layers. It will not consider air/ground data link issues and operational requirement definition activities at this stage. In addition to ObjectSecurity, the project partners include: SELEX Sistemi Integrati S.p.A., THALES ALENIA SPACE FRANCE SAS, ADVANCED RESOURCES, AIR FRANCE CONSULTING SAS, ATMB, ALITALIA S.p.A., BOEING RTE, Direction des Services de la Navigation Aérienne du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer de la République Française, FREQUENTIS GmbH, NAV Portugal, ENAV S.p.A, QINETIQ Ltd., SELEX COMMUNICATIONS S.p.A., SEA S.p.A., SECTOR SA, Consorzio SICTA, UNIVERSITY OF ZILINA, EUROCONTROL, INTEGRA.

AD4: Secure distributed application platform for air traffic management (EU FP6, 2005-2007)

We were the security specialist in the 2-year duration EU AD4 project (EU FP6 IST R&D project), which builds a next-generation air traffic management system with innovative visualization concepts. The aim of the project is to develop a virtual airspace management system that offers benefits in terms of clear and transparent visual representation with strong security and easy interoperability with other systems including internet-based ones. Thus great emphasis is attached to the use of open, standards-based interfaces.

We were working on the secure communications infrastructure and security management, based on MICO, Qedo and OpenPMF. The other project partners are: Fraunhofer Fokus, NEXT Ingegneria dei Sistemi SpA, ENAV Italian Air Navigation Services; Vitrociset, SICTA, ESI (European Software Institute), Digital Video Spa, Space Application Services, Middlesex University's Interaction Design Centre (IDC).

New dimensions in air traffic control – The enormous growth of air traffic is a great challenge for air traffic control because controllers have to handle more flights while preserving a high level of safety. There are essentially two approaches to achieve this - the better overall optimization of air traffic and the improvement of individual air space sectors. The maximum number of aircraft movements that can be simultaneously controlled inside a single sector is a major limitation factor. This is where the AD4 Project – the 4D Virtual Airspace Management System – comes in: Improving the efficiency of controlling sectors by better visualization of airspace.

4D Virtual Airspace Management System – Currently, air traffic controllers receive intensive training based on two-dimensional representations of planes on a Controller Working Position (CWP). The controllers then map this 2d display to a 3d representation of airspace in their mind, and calculate future separations of the planes. This is a very complex mental task that requires a lot of concentration, esp. in crowded sectors. In AD4, we are moving this complex mapping process from the controller to an improved CWP. Instead of the usual two-dimensional visuals, air traffic controllers are now supported by a complex 4D representation of airspace. This can be best imagined by thinking of three-dimensional modeling of current air traffic, e.g. the positions of planes, and adding a simple visual representation of the speed of the planes and their expected trajectories to show future separations.

Technical Background – In AD4, ObjectSecurity provides the overall system security and large parts of SecureMiddleware, the platform used for the development of the visualization system and the integration of the existing ATC simulation systems providing the air traffic data, Eurocontrol's Escape and ATRES. SecureMiddleware is jointly developed by ObjectSecurity and Fraunhofer Fokus and consists of an implementation of the CORBA Components Model with improved security support, the OpenPMF Security Policy

Management Framework, the ObjectWall IOP firewall and an MDA Tool Chain.

SecureMiddleware allows a rapid development of complex and secure distributed applications for mission critical domains. MDA enables modeling of the target system, both the functional and non-functional aspects like security, on a high level of abstraction without any need for in-depth knowledge of the SecureMiddleware. With a MDA Tool Chain, this abstract system description can be transformed into CORBA Component Models (CCM) and high assurance security policies, which are then enriched with business logic and deployed on the SecureMiddleware runtime infrastructure.

COACH Secure Distributed Telecoms Service Platform (EU FP5, 2002-2004)

ObjectSecurity participated in the very successful and well-received 2-year IST project COACH (Component Based Open Source Architecture for Distributed Telecom Applications) as a work-package leader and a significant contributor. As part of the project, two complete CORBA Component Model (CCM) tool chains were developed in Java and in C++, and demo applications from the telecom domain are implemented. Also, testing of distributed component-based systems was covered by the project. ObjectSecurity contributed a new and innovative security framework for distributed systems that is inspired by model-driven software engineering and a formal calculus for security. In addition, ObjectSecurity contributed to several security-related OMG standards and ensured that the C++ ORB used in COACH, MICO, met the requirements of the CCM implementers and users. As part of the project, we also contributed a state of the art security analysis. During the project we worked extensively with Deutsche Telekom T-Systems on secure service platforms. As a part of Deutsche Telekom's Secure CORBA project, ObjectSecurity developed MICOsec, the first Open Source implementation of the CORBA security services and one of the first implementations of the CSIV2 protocol. In addition to internal projects at Deutsche Telekom and ObjectSecurity (a secure platform for mobile applications and research in CCM security) MICOsec is used in academic and industrial projects. Since 2002, ObjectSecurity is the official maintainer and main contributor of the Open Source CORBA ORB "MICO". The cooperation with Deutsche Telekom has continued in several projects in CORBA security, Open Source software, mobile secure computing and ubiquitous computing. As part of the project, we also did a comprehensive CORBA security analysis. This work was continued in the EU IST COACH project, where ObjectSecurity, Humboldt University, Fraunhofer Gesellschaft FOKUS and T-Systems jointly developed a Secure Parlay platform based on MICO, Qedo and OpenPMF.

ObjectSecurity LLC Plug & Play Tech Center, 530 University Ave, Palo Alto, CA 94301, USA,
Tel. +1-650-515-3391, Fax +1-360-933-9591

ObjectSecurity Ltd St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS, United Kingdom
Tel: +44 (0) 1223 420 252, Fax: +44 (0) 1223 420 844

info@objectsecurity.com www.objectsecurity.com

The key objective was to build a component framework that is well integrated with state of the art software engineering techniques like the OMG's Model Driven Architecture. The framework can rapidly transform models, architecture and design level components, as well as policies to execution level and deploy them efficiently and securely on distributed hardware platforms. This allows the developer to concentrate on the business logic instead of reinventing technical infrastructure and to reuse existing components, which increases software quality and greatly reduces development costs and time to market.

The consortium included T-Systems (coordinator), Lucent, Thales, Intracom, ObjectSecurity, Fraunhofer FOKUS, Humboldt University Berlin, University Pierre & Marie Curie Paris, and CNRS/USTL/LIFL Lille

The main focus of COACH is on telecommunications applications, but the results are also directly applicable to other large scale and mission critical applications, such as traffic management and navigation, defense, or financial applications. The COACH framework is language and platform neutral and allows a secure interoperability between heterogeneous systems, from mobile devices to mainframes. The entire development of the component framework was realized as Open Source using standard Open Source licenses and Open Source software development methodologies. It is composed of an OMG IDL 3.0/PSDL/CIDL compilation and code generation tool chain, a packaging/assembling/deployment tool chain, and of a flexible runtime environment integrating means to describe the components (Network Management and Service Platforms). This allows to build applications by components assembly and to efficiently deploy the components manually or automatically over the network. Furthermore, COACH provides a framework for component testing that allows developers to rigorously test CCM components using a variety of test tools and a new security architecture for CORBA and CCM that allows the flexible enforcement of consistent enterprise-wide security policies. Finally, two relevant telecommunication applications were implemented to evaluate the suitability of the COACH framework and the CCM for the development of complex distributed applications.

- The following issues were addressed within the COACH project:
- Elaborate the state of the art of component architectures.
- Identify specific requirements for the Telco domain.
- Develop specifications to complete the CCM and to extend it according to requirements for the Telco domain.
- Develop a model driven security architecture, which meets the requirements of the CCM and the Telco domain.
- Implement a complete Open Source CCM platform.
- Implement the deployment and configuration architecture according to existing specifications.
- Provide modeling support for CCM.

- Specify, design and implement Telco specific components to validate the Telco specific CCM.
- Specify and implement a component test environment to support component development.

Secure Wireless Telecoms Service Platform for T-Systems (Germany, 2001)

ObjectSecurity has ported Secure MICO onto a wireless Linux based handheld computer as a prototype project for a pervasive CORBA based telecoms application platform. On top of this platform, we built a secure geographical information system (GIS) that uses ObjectSecurity's secure CORBA infrastructure.

The widespread use of mobile phones with value-added services indicate that there is a heavily expanding market for wireless applications in the near future. Rapid application development will be critical to stay ahead of the game in this highly fluctuating market, and to maximize the return of investment as early as possible. Today, security is also one of the prime requirements, especially for mobile electronic commerce application – customers will simply not use insecure services for financial transactions.

In a project with T-Systems Deutsche Telekom, the biggest German carrier, ObjectSecurity has ported their secure CORBA infrastructure onto a Linux based PocketPC, the most advanced pocket computer available at that time. In line with the middleware philosophy, the resulting mobile device had to be transparent to the application developer so that mobile clients can be seamlessly integrated into the entire CORBA middleware environments. Conformance with the well-established CORBA middleware standard provides interoperability, portability, flexibility, scalability, and transparency.

Research proposal evaluation and project review for BMVIT (Austria,2007-2009)

ObjectSecurity's Dr. Lang was contracted several times as proposal evaluator and project reviewer by Austria's government agency Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) FIT-IT - Research, Innovation, Technology - Information Technology.

Research proposal evaluation and project review for European Commission (Belgium, 2010)

ObjectSecurity LLC Plug & Play Tech Center, 530 University Ave, Palo Alto, CA 94301, USA,
Tel. +1-650-515-3391, Fax +1-360-933-9591

ObjectSecurity Ltd St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS, United Kingdom
Tel: +44 (0) 1223 420 252, Fax: +44 (0) 1223 420 844

info@objectsecurity.com www.objectsecurity.com

ObjectSecurity's Dr. Lang was contracted as proposal evaluator by the European Commission for the 7th Framework Programme (FP7).

GIS prototype platform for T-Systems (Germany, 2001)

We built a secure geographical information system (GIS) that uses our secure CORBA infrastructure and runs on a PDA. To achieve this, we had to port our entire secure CORBA infrastructure to a Linux based PocketPC. This project was a prototype deployment of our secure mobile CORBA infrastructure.

CORBA development for T-Systems (Germany, 2000-2002)

We have developed many useful additions to the MICO CORBA open source implementation as part of our projects with T-Systems.

Secure CORBA design and development for T-Systems (Germany, 2000-2002)

We have built a complete implementation of a secure CORBA infrastructure. It was initially based on the CORBA security standard, but was enhanced considerably.

Technical security audits for telecommunications etc. (Germany, 2000-2002)

We delivered security audits for several large organizations, involving both IT and non-IT aspects. In particular, we successfully analyzed network and distributed systems security.

MICO Technical Support Contracts for Intel, ESG, FutureTek, Agilent, General Electric, ... (2000-2009)

Due to demand from the telecoms industry, we provide technical support, consulting, and development for MICO/MICOsec CORBA.

Technical security audit for telecommunications etc. (Germany, 2000-2002)

We delivered security audits for several large organizations, involving both IT and non-IT aspects. In particular, we successfully analyzed network and distributed systems security.

Technical support for distributed systems technologies (2000-ongoing)

Due to demand from the telecoms industry, we provide technical support, consulting, and development for MICO/MICOsec CORBA.

Secure distributed IT infrastructure in the financial services sector (UK, 2000)

We carried out a substantial technical security analysis and risk analysis as an independent third party at a large bank in London, UK. In addition, we integrated firewalls with CORBA security and a 3-tier distributed application.

Book publishing (USA, 2001)

ObjectSecurity's founders published a well-received book "Developing Secure Distributed Applications with CORBA".

Lectures on distributed systems security (UK, 2001)

ObjectSecurity gave 3-hour tutorials about their field of expertise for the MSc in Information Security at Royal Holloway, University of London.

Web portal development and maintenance, incident monitoring (UK, 2004)

We were responsible for extending and maintaining a complex customer management web portal.

Evaluation of security technologies (UK, 2000)

We provided in-depth evaluations of firewalls, cryptographic systems, Web browser security, access control, intrusion

ObjectSecurity LLC Plug & Play Tech Center, 530 University Ave, Palo Alto, CA 94301, USA,
Tel. +1-650-515-3391, Fax +1-360-933-9591

ObjectSecurity Ltd St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS, United Kingdom

Tel: +44 (0) 1223 420 252, Fax: +44 (0) 1223 420 844

info@objectsecurity.com www.objectsecurity.com

detection, single sign-on systems etc. as part of several banking projects.

Secure "shrink-wrapped" third party software development (Germany/Switzerland, 2000)

We designed, developed, and supported a tool to allow encrypted files to be emailed without key exchange and with maximum usability.

Basic research and development (2000-ongoing)

Over the years, our specialists have explored new ways of improving integrated policy management in heterogeneous distributed systems, distributed systems security and middleware security in general, and security of CORBA, CORBA Components, Enterprise Java Beans, and .NET in particular (in collaboration with the Security Group at the University of Cambridge Computer Laboratory and the Information Security Group at Royal Holloway University of London).

www.objectsecurity.com

ObjectSecurity LLC Plug & Play Tech Center, 530 University Ave, Palo Alto, CA 94301, USA,
Tel. +1-650-515-3391, Fax +1-360-933-9591

ObjectSecurity Ltd St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS, United Kingdom
Tel: +44 (0) 1223 420 252, Fax: +44 (0) 1223 420 844

info@objectsecurity.com www.objectsecurity.com