

Mircea-Radu-Serban Dobrau

Distributed Enterprise

Applications Report

by Mircea-Radu-Serban Dobrau

FILE	2787_MIRCEA-RADU-SERBAN_DOBRAU_MIRCEA-RADU-SERBAN_DOBRAU_DISTRIBUTED_ENTERPRISE_APPLICATIONS_REPORT_113620_1263333027.DOCX		
TIME SUBMITTED	04-MAY-2018 11:50PM (UTC+0100)	WORD COUNT	1209
SUBMISSION ID	88431596	CHARACTER COUNT	7363

Mircea-Radu-Şerban Dobrău

P147987

Web Development (BSc)

Distributed Enterprise Applications

(M6X01094)

Tim Bashford

Abstract

Knowledge of major concepts, principles and practices of WCF as well as distributed systems in general is essential towards designing distributed software components for use in enterprise services. Additionally, comprehensive knowledge and understanding of complex client/server concepts, principles and tools is essential towards successfully evaluating software components inside the scope of scalable, distributed applications. This report starts with concepts necessary towards understanding security principles, as well as the options WCF provides the developer towards successful implementation of these concepts. Next, the principal modes of WS-Discovery, WCF's SOAP-based protocol for probing and communication between endpoints, are brought forth: ad hoc and alternatively managed mode, along the clients' and the services' properties unique to each scenario. Finally, the report ends with a discussion on how the software may be deployed as part of a commercial distributed system.

Table of Contents

WCF	4
Security	4
Transmission	6
Deployment as part of a commercial distributed system.....	7
References	8

WCF

Security

When it comes to securely transmitting data, WCF presents a few [1, pp. 316–317] [2, Ch. 10] [3, pp. 220–221] important concepts:

- **Authentication:** Authentication represents the process of establishing the identity of a user using the service. As such, authentication can be usually done by asking for a username-password pair already present in the service's users database.
This concept is implemented by WCF with the use of either **certificates, Windows accounts or groups**.
- **Authorization:** The next step in the security process is establishing the allowed actions of the calling party e.g. the user. It has to be noted that authorization is not strictly dependent on authentication. For example, anonymous users can be authorized access to the service but only with a limited sub-set of normal functionality.
This process in turn can be implemented through custom service code, native or custom authorization providers, as well as ASP.NET roles. Alternatively, Windows groups, Active Directory and Authorization can be used as well as other methods of implementation.
- **Confidentiality:** Confidentiality represents the concept of preventing other users from reading the information that is sent between the caller and the service.
Usually this is implemented through encryption, however other various mechanisms are present in WCF for establishing this.
- **Integrity:** Finally, the integrity concept assures that the data that was transmitted has not been tampered with and/or modified during the transmission. This attribute can be verified by either through digital signatures or having the receiver validate that the hash of the received message matches the original generated hash by the sender.

A few over-arching features [3, pp. 220–245] of WCF present with the scope of assuring security of data transmission is as follows:

- **Bindings:** Bindings define one or more WCF-supported WS-* protocols. Each binding addresses two aspects of messaging: “Encoding” the method in which messages are to be serialized and “Transport” the mechanisms required for getting the messages from the caller to the callee.
Additionally, the “ProtectionLevel” property of bindings allow the user to enforce either signing, encryption, or both signing and encryption of the message.
- **Credentials and Claims:** Credentials are entities compatible with XML which aid the Windows Runtime in properly identifying the user. Credentials consist of one or more claims which can either be a username, a digital certificate or a custom token specifying the user’s right towards accessing the application.
Several “claim sets” are available in WCF such as usernames, certificates, Kerberos tickets etc. which are in turn mapped to the standard internal claim set in the WCF runtime.
Credentials can be presented in two ways: at the **transport** level or the **message** level.
Under the **transport-level**, the transport-level protocols will verify the credentials with the Windows runtime and establish a secure session between the client and the service. However, the messages may be exposed to malicious hackers the moment they exit the destination’s SSL gateway.
Under the **message-level**, the credentials are embedded within the message. This method however is slowed due to a larger amount of encryption involved. Once the receiver has received the message he a special key known only to the receiver is used to decrypt the message.

Transmission

WS-Discovery [3, pp. 38–39], the SOAP-based protocol which helps find the location of endpoints of the service is used for probing the service endpoints, after which their endpoint address is used to call the WCF service.

In this manner, WS-Discovery supports **Ad hoc** and **managed** modes, which in turn are based on two types of transmission: **unicast** and **multicast**.

- **Unicast transmission** represents the process of sending a message to a single network, in turn identified by a unique address. In other words it can be thought of as a “one-to-one” connection between the service and the client.
- **Multicast transmission** on the other hand a message or data is sent to multiple destinations simultaneously in a single transmission.

During **ad hoc** mode, the service is probed by the client through the sending of multiple multicast messages. Next, services which respond to the probe answer back to the client using a unicast transmission method.

Some characteristics of ad hoc **clients** include:

- The client is responsible for listening to any type of multicast message possible by the service.
- The client sends a “Probe” message in a multicast manner with the scope of locating a service
- A service can be found by the client through the sending of a “Resolve” message under a multi-cast manner, in the circumstance that service endpoints change.

Ad hoc **services**, on the other hand:

- Send multicast messages upon joining or leaving a network
- Respond back to a “ProbeMatch” or “ResolveMatch” message using unicast transmission whenever it matches a “Probe” or “Resolve” message respectively.
- Accept and respond to any “Probe” messages sent in a unicast fashion

With **managed mode**, clients and services interact with each other indirectly, through a “discovery proxy” situated between them. As such, services send event notifications to the discovery proxy whenever it joins or leaves the network. The client in turn can probe for a service through a unicast message sent to the discovery proxy, after which the response is sent back in the same fashion.

Managed mode **clients** may have the following properties:

- Responsible for unicast messages sent by the discovery proxy
- Sends a "Probe" message with unicast transmission to the discovery proxy towards locating the service
- Finds messages using the "Resolve message" sent in a unicast fashion under the circumstance that service endpoints have changed

Services on the other hand:

- Optionally send a unicast message to the discovery proxy whenever it joins the network, and a multicast message whenever it leaves the network
- Accept and respond to any type of unicast Probe messages

Deployment as part of a commercial distributed system

The software would be hosted on IIS, as it boasts several useful features. [4, pp. 3–19]

References

- [1] S. Resnick, R. Crane, and C. Bowen, *Essential windows communication foundation: for .net framework 3.5*. Addison-Wesley Professional, 2008.
- [2] J. Lowy and M. Montgomery, *Programming WCF Services: Design and Build Maintainable Service-Oriented Systems*. O'Reilly Media, Inc., 2015.
- [3] N. Pathak, *Pro WCF 4: Practical Microsoft SOA Implementation*. Apress, 2011.
- [4] K. Schaefer, J. Cochran, S. Forsyth, D. Glendenning, and B. Perkins, *Professional Microsoft IIS 8*. John Wiley & Sons, 2012.

Mircea-Radu-Serban Dobrau Distributed Enterprise Applications Report

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

27 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

GRADING FORM: SMU GENERIC_GJ

MIRCEA-RADU-SERBAN DOBRAU

27

RESEARCH-INFORMED LITERATURE

 An acceptable number of high-quality sources.
Some material, however, taken directly from them
without adequate paraphrasing. **2**

KNOWLEDGE AND UNDERSTANDING

 Some good knowledge and understanding evident
from the report - though too brief overall. **12**

ANALYSIS

 Unfortunately, code is unfinished to the point that it
was barely started. This massively limits the marks I
can give in this and other sections. **4**

PRACTICAL APPLICATION AND DEP.

 Very little to mark. **3**

SKILLS FOR PROFESSIONAL PRAC.

 A reasonably well-written and presented report. **6**