SAPinsider

This article appeared in the Jan • Feb • Mar 2014 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Secure Your System Communications with **Unified Connectivity**

A Simple, State-of-the-Art Approach to RFC Security

by Dr. Thomas Weiss, SAP AG

Business processes are becoming increasingly integrated, both inside your company and across company borders. Seamless integration of business processes is a must, and often not only between the systems within your company, but also with the systems of partners and suppliers. In many cases, even end customers expect to read and write data in your company's systems via the internet, not to mention sales colleagues who expect to access ABAP-based back-end systems via OData-based apps.

From a process and communication perspective, this increased openness is a welcome development — it means seamless process integration, which speeds up these business processes, makes them more comprehensive, and enables end-to-end tracking. From a security perspective, however, every interface to the outside world, and even to other systems within your own company, is a potential security risk. The more access your systems offer, the greater the potential security risks: Somebody might intrude in your system and read or even write data.

To help you keep pace with ever-growing security challenges, SAP NetWeaver 7.40 includes a new framework — Unified Connectivity (UCON) — for securing Remote Function Calls (RFCs), which are a central communication technology of SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP and all ABAP-based systems. The RFC interface enables communication between systems by allowing remote-enabled function modules (RFMs) to be called between an SAP system and other SAP or non-SAP systems. To make these calls more secure, the UCON basic security scenario for RFC provides a simple process and toolset that dramatically reduce the number of RFMs that can be called from other clients or systems, which in turn dramatically reduces the potential attack surface.

How UCON Works

UCON uses a straightforward approach to make RFCs more secure on the server side: It simply reduces the overall attack surface that the RFMs of your ABAP-based systems expose to the outside world — that is, other clients of the same system or other systems — by completely blocking access to all RFMs in your systems that are not relevant for the connectivity scenarios you need. Most SAP customers run only a portion of the business and technical scenarios offered by SAP, and a large number of RFMs are needed only for load balancing and parallelization in the same client of the same system. RFMs that are unused or relevant only internally within a single client need not be exposed.

To make RFCs more secure, you simply have to find out which RFMs need to be accessed from other clients of the same system or from other systems to enable all the RFC scenarios you need, and then block access to all other RFMs that are not needed for your scenarios. A typical SAP customer's ABAP-based server system needs to allow external access to only a few hundred RFMs to support the scenarios needed. With 38,000 RFMs in an SAP ERP system (including SAP NetWeaver AS ABAP), for example, this approach can lead to a 95% reduction of the potential attack surface in terms of RFC communications.

Dr. Thomas Weiss (thomas.weiss@sap.com) has a Ph.D. in analytic philosophy and joined the SAP NetWeaver Product Management Training team in 2001, where his responsibilities included the e-learning strategy for ABAP. He later became a member of the SAP NetWeaver ABAP Product Management team, where his rollout activities covered the ABAP language, ABAP tools, and in particular the Switch and Enhancement Framework. By 2010, he was also responsible for the rollout of RFC and the RFC-based connectors. Since the beginning of 2012, he is the product owner of the SAP Core Connectivity Team, which develops Unified Connectivity.

To make the UCON RFC protection work in your system, you assign the RFMs that need to be accessed from the outside to a container called the default communication assembly (CA). RFMs that are not assigned to the default CA are protected by UCON and can no longer be accessed from the outside, but can still be accessed for load balancing and parallelization purposes from callers within the same client. In this way, UCON provides an additional security layer on top of the standard S_RFC authorization checks for RFC communications (see the sidebar "An Additional Security Layer for RFC").

A Process and Toolset for Securing RFC Communications

How do you find out which RFMs you need to expose for your business process and technical scenarios?

To help you determine which RFMs to expose and which to block, UCON provides a three-phase process and toolset. SAP has designed this process not only to help you identify the relevant RFMs and assign them to a default CA, but also to ensure that UCON protection does not interfere with or block your productive scenarios by making a required RFM inaccessible to external clients or systems.

Once you have set up and configured UCON (see the sidebar "UCON Setup and Configuration"), you step through a three-phase process, supported by the UCON toolset, in which you:

- Find out which RFMs you need to expose by deriving statistics for a defined time period from the system logs
- Ensure that you did not overlook or forget to expose any RFMs that you may need for your scenarios by evaluating the identified RFMs
- Activate the UCON runtime checks for a productive scenario

Figure 1 provides an overview of this process. Let's look at the phases in more detail.

Phase 1: Logging

In this phase, you determine which RFMs are accessed from the outside over a specified period of time. Choose a suitable length for this phase depending on your particular scenarios. For example, let's say that in your system all regular RFC scenarios run in a period of four months — this is the duration you would choose for the logging phase. To discover these RFMs, you use the UCON phase tool (transaction UCONPHTL) to show and filter the RFMs that have been called. Assuming that the identified RFM calls are part of legitimate scenarios, you assign all these RFMs to the default CA and then move them to the next phase by changing their status in the UCON phase tool.

SAP recommends assigning RFMs to the default CA after the phase expires, which you can find out by checking CCMS Monitoring

Note: CCMS Monitoring (transaction RZ20) includes a monitoring set called SAP Unified Connectivity Monitor Templates for monitoring UCON settings, the number of RFMs with an expired logging and evaluation phase, and the status of the batch job that gathers the RFM statistics records during the three phases.

An Additional Security Layer for RFC

The Unified Connectivity (UCON) approach to Remote Function Call (RFC) security enhances protection by adding a layer of access checks independent of users and roles to the standard authorization checks provided by the S_RFC authorization object.

When an outside user tries to access a remote-enabled function module (RFM) on a UCON-protected system, the framework checks if the RFM is included in the default UCON communication assembly (CA), which is a grouping of RFMs that are designated as externally accessible. If the RFM is not in the default CA (not exposed), the RFC session is terminated with an informative message, and the access is denied. If the RFM is in the default CA, and, consequently, the access is granted, the usual user-dependent S_RFC checks are then performed.

UCON means an additional security layer on top of the existing S_RFC authorization layer, and it is also less time-consuming to set up and maintain this layer because the question of whether a particular RFM should be exposed is completely user-independent. It takes far less time to determine whether an RFM is needed for your scenarios with a role- and user-independent approach than it does to build roles and authorizations and assign them to each relevant user who might need to access that RFM.

(transaction RZ20). CCMS Monitoring includes a UCON monitoring functionality that issues a warning when the logging phase is expired — and also when the evaluation phase expires, but not the final phase, which does not expire — so there is no need to check the UCON phase tool frequently to see if the logging or evaluation phase of some RFMs has expired.

To learn more about the relevant RFMs that were called — for instance, to decide whether to allow access to these RFMs in the future — you simply drill down into the details (such as calling system [SID], calling client, or server-side user) shown in the UCON phase tool.

Phase 2: Evaluation

To ensure that UCON does not interfere with productive customer scenarios by blocking external access to required RFMs, this phase simulates the UCON runtime checks to evaluate whether you have exposed all needed RFMs. Again, choose a suitable duration for this phase in the UCON phase tool. It is recommended that the logging and evaluation phases should cover a period in which all connectivity scenarios in your company have run at least once, and that the annual closure should be part of this plus some safety margin, so that at the end of the evaluation phase, you can be sure that all the RFMs needed to run your scenarios are assigned to the default CA.

To determine whether you have forgotten any RFMs you need to expose, in the simple selection screen of the UCON phase tool (see **Figure 2**), select the RFMs for which the evaluation phase is expired and that have been called but are not yet part of the default CA. Add these overlooked RFMs to the default CA. Again, as in the logging phase, SAP recommends assigning RFMs to the default CA after this phase expires (which you can find out in transaction RZ20).

Finally, move all of the RFMs for which the phase is expired to the next phase by changing the phase status in the UCON phase tool. Be sure to change the phase to final for all RFMs for which the phase is expired, not just for the RFMs identified as overlooked.

Phase 3: Activation

After you have set the RFMs to the final phase (to do this, change the phase assignment in the

UCON Setup and Configuration

It is simple to set up and configure Unified Connectivity (UCON):

1. Set the UCON profile parameter UCON/RFC/ACTIVE to 1 to enable UCON runtime checks for RFMs in the final phase.
2. Run the UCON setup to generate a default communication assembly (CA) and other required entities.
3. Schedule the batch job SAP_UCON_MANAGEMENT that selects and persists the RFC statistic records that are needed by the UCON phase tool on the database.

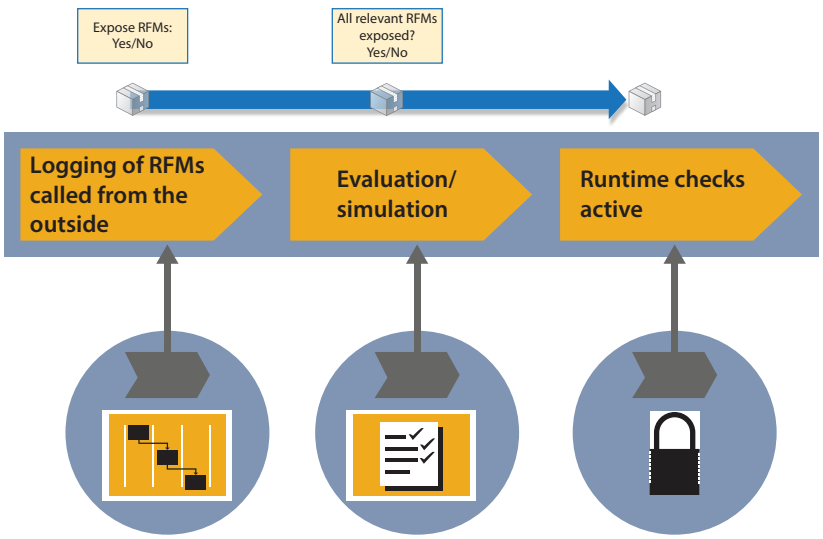

FIGURE 1 ▲ UCON provides a three-phase process for determining which RFMs to block from external access and which to expose

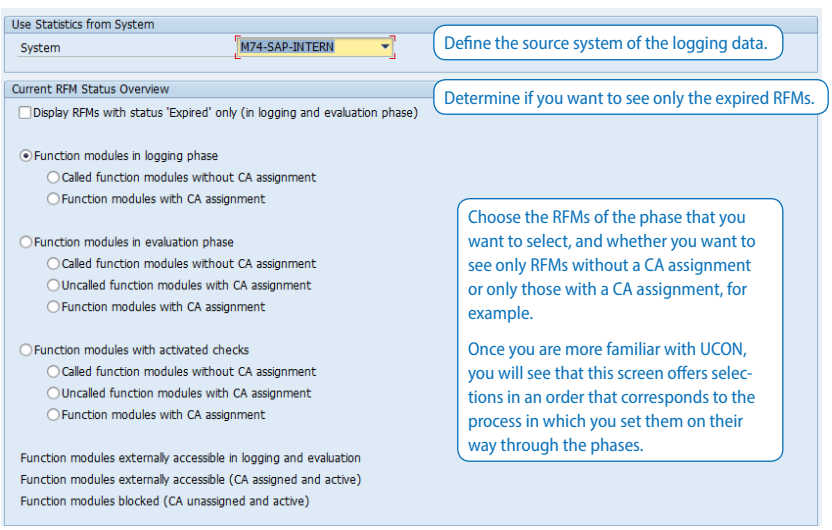

FIGURE 2 ▲ The simple selection screen of the UCON phase tool

UCON phase tool accordingly), the UCON runtime checks become operative for these RFMs, which means:

- Only RFMs in the default CA are accessible from outside the system
- RFMs that are not in the default CA are now protected against any access from outside the system

With the UCON checks operative, less than 5% of the RFMs in a typical customer system are exposed, resulting in a massive reduction of RFC attack surface for the average customer system — from 38,000 RFMs in an SAP ERP system to only the few hundred actually needed for a productive customer connectivity scenario, for instance.

Note: The UCON runtime check is operative for RFMs only in the final phase. During the logging or evaluation phase, RFMs can be called from other clients or systems regardless of whether they are in the default CA.

Consistency and Adaptability Across Your Landscape

Once all the RFMs in your system have gone through the three-phase process, each RFM is either exposed (part of the default CA) or protected (blocked because they are not part of the default CA). However, there are two crucial boundary conditions in almost every customer SAP system:

- Most ABAP-based systems do not live alone, but rather in a landscape, typically with development, test, and production systems. Can the content of the default CA be transported through a landscape to other systems?
- New RFMs will constantly come into a system after the initial UCON security setup via support packages, enhancement packages, new add-ons, and so on. Does the three-phase process also cover new RFMs that come into the system after the initial setup?

The answer to both questions is, "Yes." UCON is fully life-cycle management enabled to handle both conditions.

Support for Transports

Using the standard SAP transport program R3trans, you can transport the default CA from your development system through your landscape, so that all systems expose exactly the same RFMs.

You can also log incoming RFC calls in the production system, export the statistics using the UCON phase tool, transport that log file (with the called RFMs and their properties) back to the development system, make the CA and phase assignments in the development system, and then transport the content of the CA back to the production system.

Support for New RFMs

When new RFMs arrive in your system, UCON automatically assigns them to the logging phase to begin the process of moving them through the three phases mentioned previously. Because the phase assignment is a property of each RFM, you can have many RFMs in your system that are already in the final phase (and therefore protected or exposed), while others are in the logging or evaluation phase.

As described earlier, check transaction RZ20 to find out when the logging or evaluation phase for an RFM expired and use the UCON phase tool to add any needed RFMs to the default CA and to change the phase assignment of these RFMs accordingly.

Summary

With increasingly integrated environments, securing your RFC scenarios can seem like a daunting task. The UCON framework offers a simple, straightforward approach to enhancing the security of your RFCs by minimizing the number of RFMs on ABAP-based servers exposed to other clients and systems, and in turn reducing the available attack surface in your RFC communications.

With a three-phase process and supporting toolset, UCON not only enables you to determine which RFMs to expose and which to protect, it also helps make sure that you don't inadvertently block access to any required RFMs.

UCON is also fully life-cycle management enabled to ensure consistent RFC security across your landscape, from development to test to production systems, and it covers all new RFMs that arrive in your systems via support packages or enhancement packages, for instance.

Looking ahead, current plans for future functionality include a simple approach for building suitable roles for external RFC users using UCON logging and the UCON phase tool — continuing SAP's commitment to ensuring that your system communications remain secure. ■