The Responsibility Chain in End-to End Reconfigurable Systems

Klaus Moessner, CCSR, UniS, UK
Didier Bourse, Motorola Labs, ECR, France
Karim El-Khazen, Motorola Labs, ECR, France
David Grandblaise, Motorola Labs, France

1. Introduction

Reconfigurability, along with all the merits and advantages it offers introduces as well system design constraints on security and reliability. The fact that equipment could be configured to literally any setting and could potentially implement any radio interface, be it standardised or rogue, opens the door for any type of intended or unintended faulty system implementation.

Reconfigurable equipment, in particular terminals, may easily be circulated and may appear in areas where regulation or law prohibits the reconfiguration capability or even the possession of such equipment. The problem of how to prevent the unintentional incrimination of users arises, considering the future extended roaming capabilities of the reconfigurable equipment over the different regions.

The capabilities of reconfigurable equipment will facilitate cross air interface technology roaming, the ability to adapt to any (legacy and possible future) air interface available and to download and install new software implementations in both the home but also the foreign environment. The question of "what happens when a user wants to install software, obtained from a third party provider, on their terminal, which should operate in the network of another operator" arises. With respect to security, appropriate mechanisms are needed to verify the origin of program code prior to its integration into a reconfigurable device. Furthermore, it might be needed to supervise at runtime the functionality of specific program modules in order to ensure that downloaded code fragments do not perform unauthorized functions. Regarding reliability, appropriate techniques, mechanisms and procedures are needed to ensure that a reconfiguration action will not cause a running system to stop working correctly. This requires means for validation, fault diagnosing as well as error recovery procedures.

The implications of end-to-end reconfigurability scenarios [1], on top of all security, reliability and privacy issues, directly lead to the question of responsibility. One of the key questions to be answered will be the identification of the responsibilities for the compliance and fault-free functioning of reconfigurable equipment when reconfigured in (foreign) environments or administrative domains.

This paper aims to describe the chain and relations of actors involved in (re)configuration and to identify the possible threats and associated responsibilities. Furthermore, it aims to provide a framework (i.e. the "Responsibility Chain") that offers the possibility to clearly assign the responsibilities for reconfiguration processes.

2. The Concept of the Responsibility Chain

Historically, there was no problem with the assignment of responsibilities, equipment was manufactured implementing all layers according to the given standards and it was verified through an independent type approval process in test houses. The equipment configuration could not, or only in a long lasting and tedious procedure, be changed after the type approval, the responsibility for the functionality was with the test house. With the introduction of the R&TTE directive [2], the situation significantly evolved, manufacturers can now produce their equipment and can certify its standard compliance and when necessary they can introduce patches and upgrades in a rather short time. The responsibilities and liability in this case were shifted to the manufacturer. The regulatory approach for equipment (re)configuration is different within the regions [3].

Reconfigurability is opening the possibility for third party software vendors to provide software, and for many actors to change the HW/SW combination *after* the equipment has entered the market and to install or upgrade the configurations during equipment operation. The question of “who will and can be held responsible for the standard compliant function of the equipment” arises.

The settings and software combinations of equipment, even for non-reconfigurable technologies, are rather complex. The manufacturer installs the firmware, operating system and basic applications while the operator may include some tailored platform software and applications. All of these installations may have bugs and may require patching. While this can rather easily be done, to certain extent, in current terminals, such patching will be rather problematic when configuration software may be procured and installed even from/by third parties.

Lots of the flexibility and the value added by reconfigurability are based on software download and controlled installation/activation. This however may be at stake if downloads are not sufficiently secure and if the origin, download path, suitability and authenticity of the software downloaded are not asserted.

For the operators there are two major identified problem areas; if reconfigurations should cause any problems, the operator will be the main point of contact (and blame) for the user, thus failed reconfigurations can potentially harm the operators reputation. The second problem lies in the efficient use of the spectrum an operator has, thus reconfigurations may lead to inefficiencies or misuses and consequently resulting in revenue loss. The list of problems described is far from being complete, however the common theme appearing is the need for a common scheme to assign the responsibilities for reconfiguration.

The actors involved in reconfiguration procedures are not dealing in one single dimension; hence these actors, their tasks and their relations need to be identified. There are two dimensions in which the actors may operate: the first is the operational and the second the administrative. As depicted in Figure 1, from the system perspective, fifteen actors have been identified for end-to-end reconfigurable systems [3]: User, subscriber, network operator, equipment manufacturer, (value-added) service provider, content provider, software provider, service aggregator, regulator, reconfigurable equipment, reconfiguration manager, certification entity, security entity, pilot channel provider and spectrum manager.

Focusing on some specific actors, their roles in the operational dimension include:

- *Equipment Manufacturer*: provides the reconfigurable platform, firmware and software updates/new versions,
- *Network Operator*: owns the spectrum as well as the infrastructure, can also act as service provider,
- *Software Provider*: third party providing application software, but also low level configuration relevant software,
- Service Provider: provides the required/requested services, this may also imply the possibility that an end user may act as service provider,
- *Reconfiguration Support Service Provider* (e.g. Reconfiguration Manager): provides the basic services necessary for reconfiguration, including for example secure software download,
- *User/Subscriber*: uses the equipment and infrastructure, may request installation of new configuration of application software.

While in the administrative dimension, the following actors have their roles as defined:

- *Regulator*: sets the framework for use of reconfigurable equipment, allocates the spectrum to lease holders and governs (using policies) the usage of the spectrum and the circulation of reconfigurable equipment,
- *Reconfiguration Controller* (e.g. Certification Entity, Security Entity, Spectrum Manager): verifies that intended reconfigurations will comply with given standard or that the equipment is prevented from implementing an intended configuration. This controller also implements functions like spectrum management according to given policies and certifies the intended configurations of the reconfigurable equipment,
- *Equipment Manufacturer*: arranges and initiates (performs) software (firmware) updates and patch installation,
- *Software Provider*: provides third party system, protocol and application software,
- *Service Provider*: may request the reconfiguration of equipments to enable the provision of its services,
- *Reconfiguration Support Service Provider* (e.g. Reconfiguration Manager): provides the control and security features for the reconfiguration procedure, independent of who may have initiated the reconfiguration process,

- *Network Operator*: provides the radio resources, mobility management and fixed capabilities to switch, route and handle the traffic associated with the services offered to users,
- *User/Subscriber*: may initiate, allow or decline a reconfiguration.

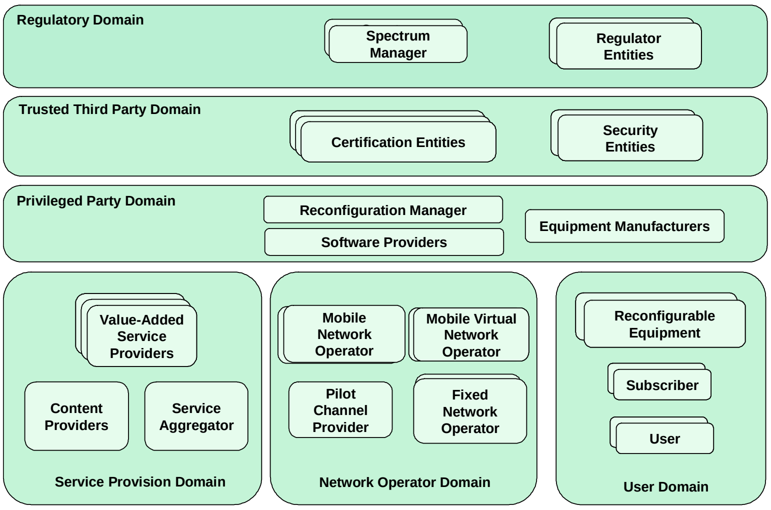

Figure 1: Actors in an End-to-End Reconfigurable Environment

3. The Responsibility Chain

End-to-end reconfigurable system, focusing on the administrative roles of its actors, is depicted in the Figure 2. Former sections outlined the problem of responsibility assignment, while this figure shows, in the context of the end-to end-system, the main points of interference identifying where actors would have to take responsibility for the system state. There are a number of sensitive areas (indicated by the stars in the figure) in a reconfiguration procedure. *Issue 1* highlights the question of the actor who takes the responsibility for third party software and who vouches that such software can be used to implement a radio protocol on the platform built by a specific manufacturer. *Issues 2* and *3* tackle the same situation but in these cases the software would be provided by the equipment manufacturer or operator, respectively, and the configurations would be used in a different administrative domain. *Issue 4* tackles the matter about permitting (reconfigured) terminals to access/use an operator's Radio Access Technology (RAT), while *Issue 5* deals with the biggest problem of who can (and will) take the responsibility if a terminal is being reconfigured. *Issues 4* and *5* include the prevention of misuse of spectrum (e.g. in the Cognitive Radio Approach, when a user does not releases the spectrum) as well as the spectrum control.

To tackle these problems, a clear understanding of the relationships between the actors in end-to-end reconfigurable environment has to be established. The introduced responsibility chain concept will provide an overview of the different responsibilities and aim to show their relationships. This chain will also be related to the value chain of mobile telecoms, with the aim to outline possible approaches for the assignment of responsibilities in reconfigurable radio systems. The responsibility chain defines a model where the accountability for reconfigurations can be assigned to the different actors within end-to-end reconfigurable systems. Connected to the concept of value chain in the definition of the business models for end-to-end reconfigurable systems, the responsibility chain will identify the dynamic interactions between actors encompassing information data, control data and money flow. Moreover, as illustrated in Figure 3, the money flow of the responsibility chain will include the penalty payments to recover damages created by faulty reconfiguration.

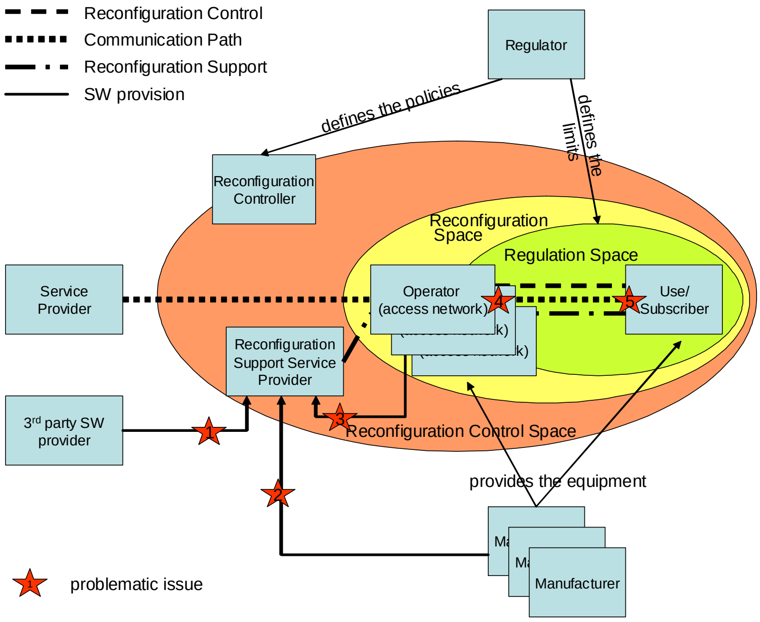

Figure 2: Actors of the Administrative Dimension and their Involvement

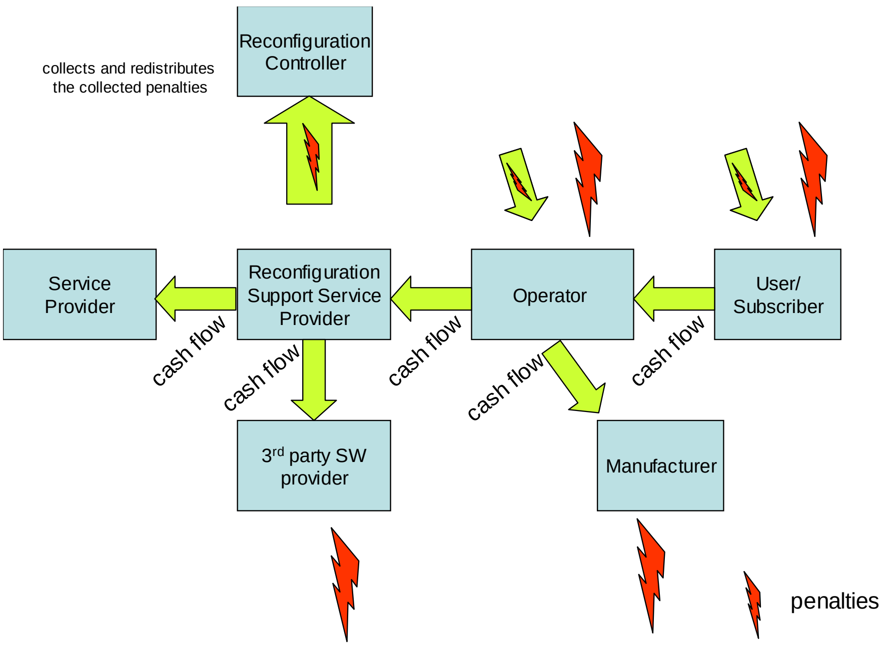

Figure 3: Revenue and Penalty Flow

Main assumption in this model is that regulation defines for the RATs the policies and the limits that are to be applied in defined geographical area and timeframe. The second assumption is that equipment can not be altered without consent from the controller of the reconfiguration space (as depicted in Figure 2).

4. Conclusion

Questions regarding the actors' responsibilities in an end-to-end reconfigurable environment arise when addressing security, reliability and privacy issues. In order to ensure compliance and fault-free functioning of reconfigurable equipments in this heterogeneous environment, it is necessary to clearly describe the chain and relations of the actors involved in reconfiguration, identifying the possible threats and associated responsibilities.

Taking the responsibility for reconfiguration of radio equipment may appear to be a burden, but it also opens new commercial possibilities. The classical communications value chain remains being in place, but, on top of this, a scheme to charge for violations of reconfiguration policies is being introduced. The responsibility chain enables the provisioning of security and reliability in the reconfiguration procedures, which is of crucial importance in order for end-to-end reconfigurability technology to gain market acceptance.

Acknowledgment

This work has been performed in the framework of the EU funded project E^{2}R. The authors would like to acknowledge the contributions of their colleagues from E^{2}R consortium.

References

[1] IST-2003-507995 FP6 Project E²R, http://www.e2r.motlabs.com

[2] R&TTE Directive, http://europa.eu.int/comm/enterprise/rtte/

[3] Walter Tuttlebee, "Software Defined Radio: Origins, Drivers and International Perspectives", Wiley, March 2002

[4] S. Hope, F. Marx, M. Arndt, A. Delautre, E. Buracchini, P. Goria, A. Trogolo, M. Stamatelatos, N. Alonistioti, A. Kaloxylos, G. Vivier, K. El-Khazen, M. Alvarez, "End-to-End Reconfigurability System Scenarios", Wireless World Research Forum, June 2004