

# Security, as a built-in feature in Autonomic Systems

Y. Rebahi, R. Chaparadza

Autonomic networks are known to be networks that self-configure, self-heal, self-protect, self-optimize themselves using self and context awareness in accordance with the policies governing the system. This concept is often discussed within the context of Networks of the Future (or Future Internet) especially that in the latter, autonomicity and self-management are among the main characteristics. Securing Internet users is a major issue that has been discussed and addressed by both research and industry communities. The concerns raised by these communities include: ensuring users privacy, building trust among users, and protecting the infrastructures from worms, attacks and intrusion. Unfortunately, the solutions suggested to deal with the mentioned issues, in particular cryptographic techniques and access control can not be applied directly to Networks of the Future and in particular to autonomic systems. In the following part, we will discuss the main security challenges that have to be addressed by autonomic systems.

## *Flexibility*

Today, the communications world includes particularly,

- Different access technologies: Mobile, wireless, Ethernet, DSL and Cable
- New networking paradigms: ad hoc, Peer to Peer (P2P), sensor networks
- sensitive applications such as e-commerce and e-business
- Different providers: network, content and service providers

This wealth in the communication is unfortunately faced with a dramatic increase in complexity that autonomic systems try to overcome. In traditional communication networks, security is usually treated as a static component in system design. This means the security policies are pre-configured and cannot be easily adjusted to new constraints. On the other side, this “one size fit all” security is unable to cope with the diversity in the communications world today. As autonomic systems are expected to deal with a constantly changing environment, they should not, for instance, rely on signature based intrusion detection achieved through signatures noticed by administrators.

Self-configuration, which is one of the most important characteristics of autonomic systems, can play a primordial role in achieving the requested flexibility. For instance, reconfiguring security services according to the current context, will give the security system the flexibility to deal with any emerging situation. As an example, if the security dimension “authentication” is reconfigurable, it can deal with device characteristics such as hardware configuration, battery and CPU, or with user preferences namely, preferred modes and location specificities.

### ***Context-awareness***

Self-protection in autonomic networks can be achieved only through self-reconfiguration, which, in turn, heavily relies on the data collected from monitoring (context-awareness). Being aware of service requirements and potential threats, the system can adjust itself in a timely manner according to the network policies. In this case, the system will be able to provide the right service at the right time to the right user, detects attacks and misuse and takes actions to protect the network. For instance, if some keys are used for encryption and an attack is detected, the system will enhance the current security level by enforcing longer keys, strict access control and revocation of malicious nodes. Once the attack is over, the system may either come back to the normal security level or keep the new level.

### ***Autonomicity***

Autonomic security is an advanced step comparing to “reconfigurable” security. The former means adding more automation in the entire reconfiguration process and make the security system self-responsive. Similarly to autonomic systems, this can be achieved only through a control loop that monitors, analyzes and reacts.

An autonomic system is supposed to have enough knowledge about the overall network (trusted and non-trusted components, the neighbors’ capabilities and availability, etc), this information is collected and aggregated and before any reconfiguration is triggered, an analysis taking into account factors such as, overhead, complexity, and impact on the running applications is performed. As an example, if the network has detected a flooding attack targeting a certain component, the reaction might vary from the simple case where this component is switched off or the traffic reaching this component is dropped or to more complex situations where only a part of the traffic reaching this component is dropped based on some selection criteria. Dropping packets without taking into account the related running applications can harm more that help. This is for instance the case, if the running application are related to banking or e-commerce.