ABSTRACT

Critical infrastructure (CI) services are constantly consumed by the society and are not expected to fail. A common definition states that CIs are so vital to our society that a disruption would have a severe impact on both the society and the economy. CI sectors include, amongst others, electricity, telecommunication and transport. CIs can be mutually dependent on each others services and a failure in one of these elements can cascade to another (inter)dependent CI. CI security modelling was introduced in previous work to enable on-line risk monitoring in CIs that depend on each other by exchanging risk alerts expressed in terms of a breach of Confidentiality, a breach of Integrity and degrading Availability (C,I,A). While generally providing a solid basis for risk monitoring, there is no way of evaluating if a risk alert received from an external CI is accurate. In this paper the authors propose a solution to this problem by adding a trust based component to the CI security model in order to improve its accuracy and resilience to inconsistent or inaccurate risk alerts provided by (inter)dependent CIs, allowing to evaluate the correctness of the received alerts. The proposed approach is validated on a realistic scenario by evaluating a dependency between the computing and the telecommunication sectors in the context of the Grid’5000 platform.

Keywords: Critical Infrastructures (CI), Information and Communications Technologies (ICT) Security, On-Line Risk Monitoring, Trust and Reputation Management, Trust and Reputation Service (TRS)

DOI: 10.4018/ijsse.2013100103
INTRODUCTION

Critical infrastructures (CIs) provide services that build the centre of our society and economy. For example, telecommunication infrastructures allow us to communicate with people and businesses at remote locations, transport and air traffic infrastructures allow us to travel to places far away for free-time or business activities. The electricity infrastructure enables a variety of services and applications that we take for granted. Furthermore, CIs depend on each other (dependency) or mutually depend on each other (interdependency). A good example is the electricity infrastructure that is a requirement for all other CIs, since almost everything relies on a constant supply of energy. A failure in one CI can cascade to other CIs and cause single or multiple service disruptions.

As operating complex systems like CIs can be problematic, CI providers put substantial effort into keeping CIs running while trying to reduce any kind of risk. For example, the risk of failure, the risk of intrusion or the risk of incorrect operation. Previous work on CI security modelling, which will be introduced in more detail in this paper, establishes a CI model based on risk that enables on-line risk monitoring of (inter)dependent CIs. In the CI security model, CIs are decomposed into services they offer and dependencies between those services (either internally or to services provided by another CI). The model can estimate CI service risk, in terms of a breach of Confidentiality, a breach of Integrity and degrading Availability (C,I,A), by observing base measurements (e.g. sensors) in the systems that are used to provide the service. This risk estimate can then be distributed to dependent services, which use it to update their own risk estimate.

A drawback of this approach is that a CI service has no means of evaluating the correctness of risk alerts received from a dependency, especially if this dependency is part of an external CI. Faulty or inaccurate risk alerts can have multiple reasons, for example faulty monitoring equipment or security attacks. To address this problem, in this work we propose to study, model and evaluate risk alerts received from a dependency, based on observations about that dependency in terms of quality-of-service and the behaviour of the dependent service. We introduce a trust and reputation service (TRS) that is able to built a trust relationship between two dependent CI services by comparing received risk alerts to measured quality-of-service and by observing the general behaviour of the exchanged risk alerts for compliance to pre-defined rules. We use the calculated trust measures to re-evaluate the risk received from dependent services and adjust the impact of the received risk alert in the service risk estimate, depending on weather received risk alerts are trusted or not.

We validate the applicability of our approach by simulating a use case scenario using information from a real-world infrastructure, namely the Grid’5000 (Bolze et al., 2006; Grid5000, 2012) platform. The Grid’5000 project maintains an academic computing grid with clusters distributed at several locations in France and Luxembourg to perform large-scale experiments that require substantial processing power and/or storage. The scenario describes a dependency between the computing grid and the telecommunication infrastructure used to interconnect each site of the infrastructure. The trust is evaluated based on a dataset of measurements gathered by monitoring tools.

The rest of the paper is organized as follows: In the next Section, related work is discussed followed by an introduction to CI security modelling and trust and reputation services. Section “Trust and CI Security Model” details how a trust relationship in CIs can be established using abstract risk information. Section “Trust Based Dependency Weighting” describes how trust can be used to re-evaluate risk alerts received from dependent services. Section “Case study: the Grid’5000 project” validates the approach using a realistic case study and finally, this work is concluded and an outlook on future work is given.
Impact of Fault-Prone Components on Effective Software Testing: An Industrial Survey
www.igi-global.com/article/impact-of-fault-prone-components-on-effective-software-testing/134433?camid=4v1a

Analysis of ANSI RBAC Support in EJB
www.igi-global.com/article/analysis-ansi-rbac-support-ejb/55268?camid=4v1a