Protection against Cyber Attacks

Introducing Resilience for SCADA Networks

Antonios Gouglidis · David Hutchison

Abstract – The sovereignty of nations is highly dependent on the continuous and uninterrupted operation of critical infrastructures. Recent security incidents on SCADA networks show that threats in these environments are increasing in sophistication and number. To protect critical infrastructures against cyber attacks and to cope with their complexity, we advocate the application of a resilience strategy. This strategy provides the guidelines and processes to investigate and ensure the resilience of systems. In this abstract, we briefly refer to our definition of resilience, our research work on the verification of resilience policies, and our resilience architecture for protecting SCADA networks against cyber attacks.

1. Introduction

The protection of critical infrastructures (CIs) is of vital importance – more than ever before – given the severity and impact resulting from any kind of disruption to services hosted by CIs. Systems and networks in such environments generally appear to be ill-prepared for the adverse consequences of cyber attacks. Also, the increased interconnection between enterprise and SCADA networks appear to elevate the likelihood for additional attack vectors and paths. Depending on the incentives of threat actors, the attacks may be characterised by a variable level of sophistication and consequences. For effective protection of CIs, we embrace resilience management, eliciting information from various viewpoints of a system, viz. Organisational, Technical and Individual – the so-called OTI viewpoints [1].

1.1 Resilience Strategy

To ensure the resilience of systems, we apply a strategy called 'D^2R^2+DR' [2]. We define resilience as 'the ability of a network or system to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation' [2]. The steps in a two-loop process are: (inner loop) Defend against challenges to normal operation; Detect when an adverse event or condition has occurred; Remediate the effects of the adverse event or condition; Recover to original and normal operations; (and outer loop) Diagnose the fault that was the root cause; and Refine behaviour for the future based on past D^2R^2+DR cycles.

Antonios Gouglidis · David Hutchison
School of Computing and Communications, Lancaster University, LA1 4WA, United Kingdom
a.gouglidis@lancaster.ac.uk, d.hutchison@lancaster.ac.uk

1.2 Resilience Policies

Access control offers mechanisms to control and limit the actions or operations that are performed by a user on a set of resources in a system. Nevertheless, considering only restriction of access may not be enough in some environments, such as in CIs. The protection of systems in this type of environment requires a new line of enquiry. It is essential to ensure that appropriate access is always possible, even when users and resources are subjected to challenges of various sorts [3]. Resilience in access control is conceived as the ability of a system not to restrict, but rather to ensure access to resources. To fulfil this requirement, we have examined how attribute-based access control (ABAC) resilience policies can be specified in temporal logic and how these can be formally verified using automated model checking techniques.

1.3 Resilience Architecture for SCADA Networks

The increasing number of cyber attacks on CIs led us to the development of a method to monitor, detect and evaluate anomalous behaviour within critical infrastructures in accordance with our D^2R^2+DR strategy, embedded within a risk assessment process. The approach we have adopted considers the OTI viewpoints and supports the detection of anomalies using appropriate techniques at the different levels of an infrastructure. The architecture is evaluated in the context of a European utility network, and by using publicly available SCADA network datasets.

Acknowledgements

This work is sponsored by the European Union under Grant SEC-2013.2.5-4: Protection systems for utility networks - Capability Project, Project Number: 608090, HyRiM.

References

1. Gouglidis, A., Shirazi, S. N., Simpson, S., Smith P., & Hutchison, D. (2016). A multi-level approach to resilience of critical infrastructures and services. 23rd International Conference on Telecommunications (ICT) pp. 1-5.
2. Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 54(8), 1245-1265.
3. Gouglidis, A., Hu, V., Busby, J., & Hutchison D. (2017). Verification of Resilience Policies that Assist Attribute Based Access Control. 2nd Workshop on Attribute Based Access Control, Scottsdale, Arizona, USA.