Measuring Progress in Cyber-Security: An Open Architecture for Security Measurement Consolidation

Andrew Hutchison, T-Systems South Africa
Roland Rieke, Fraunhofer Institute for Secure Information Technology

Workshop on Cyber Security and Global Affairs, 2012

It is sometimes said that “what you cannot measure, you cannot manage”. Cyber Security is an area of great global focus, yet it is both hard to manage and – arguably – even harder to measure. But the two concepts go together: if some sort of measurement approach could be implemented, it should at least be possible to assess whether progress (or regress?) is being made in the difficult area of Cyber Security. In this paper, we present some ideas on global measurement of cyber security, but propose an approach whereby such activity can be started in a “bottom up” fashion so that at least at enterprise or organisational level some steps towards “measured” security can be applied. In the future this could possibly be extended to a national or international scale.

In spite of the fact that technical security solutions are deployed, there are numerous instances of processes or transactions being compromised. Without a holistic view from business process to logical and technical security realisation, there is high potential for gaps or mismatches to occur. Fueling this situation is the fact that life-cycle approaches to security are not easily applied – or measured. In this paper we argue for a *meta-model* approach to drive security from purpose to practicality, through an *analysis and refinement* approach, and also for a *security measurement* approach in support of local, enterprise, regional, national and even international consolidation of security health information. To achieve a meta-model approach for security, we present a Security Information Meta Model consisting of: (a) high level goal setting, (b) security requirements, (c) measurement requirements, and (d) objects of measurement.

Through applying this model, high level goals for security can be established and defined. Importantly measurement objectives are also developed and stated at this point. The ISO27004 standard outlines what these objectives could be, but we believe that they are hard to incorporate unless done as (and when) we are proposing. By proceeding in this way, security is designed in a manner which can be tested against. Necessarily, activities of *analysis and refinement* are required to move from security requirements to measurement requirements. In particular objects of measurement also need to be identified.

If the security semantics can be defined in this way, an interesting “control” model can be applied to systems based on a so-called **on/if/do/why** approach. What is meant by this?

On the occurrence of a specific event, then **if** a particular condition occurs the system will **do** an action and assess **why** in terms of security pertinence. As an example of an on/if/do/why approach, a core information system which is integrated in a Security Information and Event Management (SIEM) environment could be constructed along these lines. By providing an *event correlation engine* as one component, event conditions can be identified to provide the **on** element. Similarly *application and/or network state* (and possibly predicted state) can be interrogated to provide the **if** element. Depending on how the condition evaluates, the **do** element of *decision support* and/or *policy decision making* can be applied. A *security information modeller* can assist in the **why** determination.

Through such an approach a system can be measured and, arguably, better managed. By starting to apply this approach on a micro-scale, it can ultimately be scaled and expanded to allow for similar construction for enterprise, national or even international systems. In this way different facilities can be integrated to provide a “measured” security view. To achieve the measurement objective, the concept is to define measures very explicitly for a system – and to be able to measure the security effectiveness against such measures. By aggregating systems composite measurement can be performed. An area under consideration is whether measurement attributes could be incorporated into an SIEM platform like MASSIF[1] (a large-scale integrating project co-funded by the European Commission), to enable ongoing assessment of security effectiveness – helping practitioners to “manage”, based on a rich set of “measurements” if these can be built into the system.

[1] http://www.massif-project.eu