IFIP WG 10.4, January 2014, Sorrento

Workshop wrap-up, Session 3 summary

Tom Anderson

Introduction

Centuries ago most people believed that everything in the heavens revolved around the Earth, and that our planetary home was "**special**". But with thought, and science, and observation, and measurement and analysis, eventually Galileo Galilei's Siderio Nuncio told us the truth (if you look at Jupiter with any telescope or good binoculars you will see what Galileo observed at Padua, just a few hundred km from Sorrento).

Many decades ago, I was reprimanded for confusing reliability and safety (I had naively thought that reliability was a sufficiently generic term to encompass safety). They said that safety was a system property, a negative property, it was "**special**". At first I rebelled – everything is a system property, and what about de Morgan. But eventually I gave up, and repented and learnt to use *dependability* instead of reliability.

After a few years (but still long ago), I was again reprimanded – this time for confusing dependability and security (I had naively thought that defining dependability as fully generic would be enough). They said that security was a property of system plus environment, a negative property, it was "**special**". This time I gave up straight away, but did not repent, became apostate and sulked quietly (muttering "availability", in denial).

Terminology wars, while not entirely irrelevant, are not really the salient issue. Obviously security has differentiating properties but – admittedly long ago – there were many at that time who asserted that you could not assess, could not measure, could **not** predict operational security levels (because it was so special). It seems clear, albeit with hindsight, that what they meant was that it was so difficult it should, perhaps, be regarded as impossible.

Summary

What a pleasure, then, to listen to and learn about the current situation of so many approaches battering away at the still difficult task of providing a measurement capability for security.

Session 3 gave us two high quality, very different proposals, but both targeted on networked systems.

Richard Lippmann showed us an approach which – if you have the resources and the insight to follow it through – will give you a systematic and comprehensive way to create a capability for dynamically monitoring and assessing the level of operational security you can expect from your system network. The evaluation is on-going, derived from condition monitoring of system attributes. Of course, you have to define the attack modes you are addressing, for a structured set of capabilities; you need to establish the metrics in each case and formulate the

operational risk by estimating possible loss of assets. There is guidance on progress from checklists, to capturing "capability deficits", to modelling risk.

Steve Noel, in contrast, looked at the specifics of metricating the topologies of "attack graphs": the multi-step routes of exploitation of vulnerability in a network, by an attacker. The approach builds on the data obtained from existing vulnerability identification products, adding an analysis layer. Measurements (scores, specified as a range min to max) are normalised to intervals on 0 (best) to 10 (worst). Facets considered are aggregation of individual node risks, magnitude, containment boundaries and (of course) the graph of network topology. Scores can be combined and, if the results are to be presented to "the General", there is a dashboard of helpful graphics.

Something rather special happened during this talk – no, not the really slick animations: John Meyer almost had his question answered [I can reassure Steve that this is very high praise indeed from John].

And Roy Maxion had already suggested to me that we should remind the General that when he assesses a tank he doesn't say "just give me one number". And, in any case, Jay Lala reminded us all that the very last thing to expect from a 5-star General is blinkered stupidity – a spotlight on any sloppiness in your work is much more likely.

Conclusion

Almost every presentation we have heard at this workshop is open to challenge on limitations of applicability, accuracy of modelling, ignorance of parameters, discontinuous development of the attack profile, etc. Thus, it is indeed a bit like weather forecasting, and we should recognise that that is a very very favourable and encouraging comparison. Years ago, the weather forecasters had weak models, inadequate data, lack of capability, and didn't recognise or know the critical characteristics. Now they do a brilliant job (and don't believe those who criticise). We just need to follow in their footsteps.