IFIP WG10.4 65th Meeting: Session 1 Summary

Let's recall the 3 objectives of the workshop:
1. Current practices in security assessment,
2. Challenges that accompany these assessment needs, and
3. Metrics and methods that respond to these challenges.

The first of the two papers was on the security challenges of critical infrastructure, specifically, of the Acea company in Italy which provides water and energy. The presentation by Andrea Guarino, who is the head of cyber security for the Acea Group, pointed out that, in addition to the usual security problems faced by Information & Computing Technology (ICT), his company runs a very large, what most people call a cyber-physical system. It has millions of non-ICT devices such as meters, valves, pipelines, etc. which happen to have embedded electronics. And, these devices are geographically dispersed, making it that much more difficult to secure them in the field.

So, how does Acea perform security assessment of this very large and complex cyber-physical entity?

Acea takes a risk management approach (as opposed to fixing every weakness and vulnerability) that holistically examines a full spectrum of threats, including accidental faults, malicious attacks, supply chain risks, as well as fraud which appears to be a major concern. Risks are prioritized and top 10 risks are targeted for remediation/mitigation. Risks are re-evaluated every year.

The presentation did not address the other two goals of the workshop.

The second presentation, by Zbigniew Kalbarczyk of UIUC, had two parts.

The first part was focused on assessment tools and described 3 tools. ADVISE is a design-time security assessment tool that provides a relative goodness measure of alternative designs.

CyberSAGE, being developed in cooperation with researchers in Singapore, uses workflow as a basis for security analysis. Its inputs include a system description, an attacker model, empirical evidence, and security goals. CyberSAGE then outputs a quantitative assessment and supporting rationale.

The second part focused on metrics. Zbigniew described a SPOT framework that creates a user suspiciousness metric that help sys admins/managers focus on a few individuals who might pose a potential insider threat.

Lastly, a question was posed to Zbigniew by the session moderator: Would SPOT have flagged Snowden? His answer was "no."

There was continued discussion on a metric to characterize an attack surface area. The session moderator suggested that the following metric may be useful:

Attack Surface Area = a*V1 + b*V2 + c*V3…

where Vn is the number of vulnerabilities of criticality n, and a, b, c, … are weighting coefficients (higher weights for more critical vulnerabilities).

It was suggested by Laurie Williams that the number of I/O ports is a better measure (ingress and egress paths for the attacker).

A combination of the two may capture both characteristics of the attack surface area.