Key points from Security Workshop Day 1

Drafting Committee

Me Sebek, Mr Kang, Mr Robart, Mr Minard, Mr Stevens, Mr Golodna.

General Objectives

Our challenge is to establish effective collaboration and cooperation within the security standards community.

We need to address both old threats and the new/emerging threats.

Big question: How can we build on the cooperation and good will of this workshop and the collective experience of our respective SDOs to address these problems in the future?

Re-use of standards

The bigger challenge is the integration of the existing security protocols with existing and emerging applications.

Interconnecting existing protocols to IP changes a great deal from a security standpoint. If we re-use existing we may discover a whole new world of threats.

To what extent can existing protocols can be reused as opposed to developing new protocols –Traditionally there has been a tendency to reinvent rather than re-use (not just in standards) What compromises have to be made to reuse a security standard? How is the issue evaluated? Who decides?

Some security requirements are applicable to all networks, some depend on what you want to do on the network.

How can we learn from each other? How can we avoid making mistakes that have been made previously?
(SG16 seems to have some useful experience here. The mandate of SG16 is MM not security but, as a developer of application standards, SG16 has not only recognized the need for security to be built-in, but has gone ahead and developed security standards to protect their apps. We know security expertise is scarce. How did SG16 find the expertise to develop their own security standards? To what extent did they draw on expertise and standards from elsewhere?)

Collaboration

We've seen references to liaisons. How well do they work? What determines which liaisons work well? To what extent are formal stds bodies (ISO & ITU) building on work being done by consortia and IETF

Addressing the gaps and dealing with technology developments

We need to consider how to address the gaps. Is there any established process for addressing the gaps in security standards? Are we just waiting for someone to propose a new work item? Are the NWIs truly responding to market priorities for security standards? (Note: in the past, much effort has sometimes been spent on some standards that have failed when subjected to the test of the market place.)

We have seen some major security implications in the above technology outlines. Given the rate of change of technology, if we are to avoid wasted effort, will need to consider what we should standardize and what we should avoid standardizing. In some cases technology just bypasses the standardization process. Do we need some process that allows for recognition of interim standards where technology may change in short term?

For a topic like RFID, where the security implications are very broad, how do we begin to identify which SDOs should be involved? How will the work be carved up? Who is in the best position to respond to need for the various security standards?)

Robustness of security standards

Diverging views here:

Ease of deployment is more important than the robustness of the security solution (Layer 3 vs Layer 4 – ability to deply solutions outside OS Kernal).
Pressure to get products to market may result in problems in implementation aside from inherent problems in the standards. Some standards have gone forward even though some people believed that there were inherent flaws at the time they were developed.
We need to be discriminating about where we focus the network security efforts.objective standards for quality.Priorities for security standards

How do we address issue of priorities for standards?

Could we share priorities among the groups represented here? Do groups have similar priorities?

If not, how much does it matter?

Does the urgency of the requirement impact not influence the acceptable rigorousness of the standard? (see above).

ISO and ITU have fast track processes but fast track requires that the specification presented be reasonably stable and have a good measure of agreement within the submitting community. In identifying candidates for security standardization should we perhaps be encouraging the consortia processes in some cases rather than launching some NWIs directly into the formal standards processes?

Addressing the invisible stakeholders

Are we adequately considering requirements of the "forgotton" stakeholders (Consumers, Research orgs, educational orgs, NGOs, regulators, administrations)?
Note: some of these stakeholders may not be able to articulate their requirements in technical terms.

Should we leave it to market forces or is their some way of representing those stakeholders who are not directly involved in standards processes?

Information sharing/Reducing duplication of effort

Comment from floor: "I didn't realize there was so much security standards work going on."

Clearly, if people don't know what standards exist, what standards are under development, who is involved or what work is planned, there is a much greater risk of duplication of effort.

Our Security Standards Roadmap could help overcome this problem if it is shared widely.