

Rationale and impact of removing “SMI mediation” issues from P2600 PPs

Brian Smithson, Ricoh Americas Corp
6/16/08

Background

Since 2004, we have been trying to create a threat definition, objective, and requirements, to assure that a malicious user cannot access a customer’s network by establishing some kind of bridge from the fax modem to the network interface. We have also been trying to create a threat definition, objective, and requirements, to assure that malicious users could not use the HCD’s network services to attack other devices on a customer network.

Previous approaches

The fax-bridge threat requires the presence of both a fax modem and a network interface.

At one time, we used a security assurance requirement (ATE_FUN?), but at that time it was possible to fulfill an objective with an SAR. It is not possible to do that in CCv3.x, so we have looked for appropriate SFRs to establish the requirement.

To avoid the possibility of implying a requirement that all HCDs must have a network interface, we placed the threat, objective, and requirements in a separate “SMI” PP (within the family of PPs) that must applied when a network interface is present in a conforming product. We chose the SMI PP because the threat is against the network, not the fax.

To avoid the possibility of implying a requirement that all HCDs must have a fax modem, we expanded the threat definition to bridging to a network interface from *any* interface (including itself).

This expanded definition also made it possible to combine two policies, P.COMMS.NO_BRIDGE and P.COMMS.NO_PROXY, into a single policy (P.SMI.MEDIATION) that prevents bridging and also prevents threats like FTP bounce or open SMTP relays. The policy and its related objective state that shared-medium interface operations are mediated by the TSF.

Recent drafts used flow control SFRs FDP_IFF and FDP_IFC to fulfill this objective.

Current approach

We have discovered that FDP_IFF/IFC cannot be used for this purpose because even in the original case of fax-to-network bridging, an email notification about the receipt of a fax message constitutes an information flow from fax modem to network interface.

When we tried the PP+packages approach, we needed to put P.SMI.MEDIATION into the common PP but do so without implying a requirement for a shared-medium interface for all HCDs. This was

accomplished by expanding the policy to include all channels (channels == interfaces or hardcopy handlers).

The current approach uses FMT_SMF.1 to require a management function to permit or deny exchange of data between any interface and a network interface (it should also have used FMT_MOF.1). The wording is tricky because we do not want to require all HCDs to have administrator controls in cases where data exchange is simply not possible (as is typically the case for fax-to-network), we do not want to prohibit administrators from enabling bridging interfaces if that is their intention, and we do not want to prohibit legitimate network services from being used that might not involve the TSF (e.g., ping).

Rationale

Is fax-bridge a real threat or an urban legend?

Are there any HCD products that have the capability to establish a malicious data session from a fax modem to a network interface? Even if data connections to the fax modem are allowed (e.g., for field service), they are required to have access controls. If it is not a real vulnerability, then why should we codify the threat and require all HCDs to go through that kind of evaluation?

Limited value

There is some legitimate value to preventing misuse of network services, such as FTP bounce or SMTP relays, but such vulnerabilities should be identified by vulnerability assessment and not by evaluation of SFRs. Our current approach doesn't cover all forms of misuse; for example, cross-site scripting would not likely be addressed by management controls.

Forces an IT solution where an architecture/design solution exists

One problem that we have always faced is that the fax-bridge issue can be addressed by architecture (no data path from here to there), design (the fax modem chipset doesn't accept data connections), implementation (firmware disables data connections permanently), or an IT solution (the administrator can enable or disable data connections). A PP only deals with IT solutions.

No satisfactory solutions have been found

Not surprisingly, we have been unable to identify SFRs that address this kind of situation in a straightforward, understandable manner. Our previous approaches have been found to be unusable, and the current approach appears to be complex and will likely have unintended side effects.

Changes required to remove

Eliminate P.CHANNEL.MANAGEMENT and its objectives and requirements

If we agree to remove this issue from the P2600 PPs, it is very easy to accomplish in the PP+packages structure. We would remove P.CHANNEL.MANAGEMENT and O.CHANNELS.MANAGED from the common PP, and FMT_SMF.1 from the SMI package.

Remove or change compliance subclauses in IEEE Std. 2600

For consistency, we would need to amend the approved standard 2600 to remove compliance clauses 8.1.1.9, 8.1.1.10, 8.1.2.9, 8.1.2.10, 8.1.3.7, 8.1.3.8, 8.1.4.5, and 8.1.4.6. Alternatively, these clauses

could be retained if they are changed from “shall” to “should” (similarly to how we handled DoS attacks, as in clause 8.1.1.11).

Impact of removal

Data connections to the fax modem are still protected

If it is possible to establish a data connection to the fax modem, O.USER.AUTHORIZED establishes access controls so that only authorized users can successfully establish such a connection.

Common misuses of network services are still covered

During evaluation, vulnerability assessment should identify problems like FTP bounce or open SMTP relays.

STs can still specify and satisfy requirements about fax-bridging or other vulnerabilities

If we remove this issue from the P2600 PPs, vendors can choose to add requirements for assuring that there is no fax-bridge capability. They will face the same issues that we have faced in the PP, but they will benefit from being able to design their solution to suit a particular implementation.

STs may approach this issue in ways that are dubious (e.g., FDP_IFC/IFF) or undesirable in a PP (e.g., extended component definitions), and still get certified. However, I do not think that we should codify it in the P2600 PPs and burden all future ST evaluations with such an approach.