Abstract of invited Talk for 23nd Intern. Conference SAFECOMP 2004, Potsdam, September 2004, LNCS 3219, Springer-Verlag, Heidelberg 2004, 1-2.

Why Safety and Security should and will merge

Andreas Pfitzmann

Fakultät Informatik
TU Dresden
D-01062 Dresden
pfitza@inf.tu-dresden.de

In the past, IT-systems at most were either safety-critical (i.e. no catastrophic consequences for the environment of the IT-system) or security-critical (i.e. even determined attackers cannot gain unauthorized access to information within and/or withhold resources of the IT-system). In future, more and more IT-systems will be both, safety- and security-critical. The reason for this is that IT-systems are embedded in ever more influential parts of our living- and working environment and that these embedded IT-systems are networked – be it to enhance their functionality now (or just as an option for future use), be it to ease maintenance.

Of course the safety community might (and should) issue warnings against this attitude of system design, because it undermines the classical way to engineer and validate safety. Of course the security community should frankly admit that using the present IT-infrastructures incorporating all kinds of unmanaged design complexity, security is mainly unachievable. But my experience of 20+ years in the area of security and privacy suggests that our warnings will not be heard or at least downplayed with arguments like:

- "These tiny embedded systems can't cause serious catastrophes, so safety is not an issue." (But if you network many systems and their failures might therefore occur at the same cause, the consequences might be much more serious.)
- "Is security really an issue? Who should have both a possibility and a motivation to attack?" (But if networking gets ever more pervasive and conflicts in our real world are not going to disappear, the answer will soon be: quite a few. But when this manifests itself on a larger scale – remember the warnings against viruses and worms issued more than 15 years from now – fixing the problem within a reasonable time span will be impossible.)

Therefore, the safety and security communities should combine and integrate efforts to design and build the networked embedded systems as secure and safe as possible given the constraints of legacy systems to be used and functionality deemed necessary for the end-users.

So far so easy to argue and understand. But do we have a chance to successfully combine and integrate? I hope so:

- Fail-safe and confidentiality as an essential security property have many structural similarities as do providing at least a gracefully degraded service and availability as another essential security property.

- We have many mechanisms useful both for fault tolerance (security against unintentional “attacks”) and security, where discerning between unintentional and intentional is mainly interesting for legal consequences, since stupid errors made in a complex IT-systems tend to behave quite intelligent in other parts of the systems or w.r.t. its output.

This suggests that unifying our approaches is both necessary and promising.