



Subliminal Security Aspects

Perceiving technical security from another angle

Jürgen Pabel, CISSP

Building on the key points from “Security discrepancies”¹, it's not uncommon practice in today's IT industry, that security software products² are only scrutinized after everything else. Looking at the distribution of published security vulnerabilities over time, one quickly realizes, that vulnerabilities for security products have emerged only recently on a broad basis. Has this class of software outdone all other software in terms of robustness? No, it's only been recently, that security products are being analyzed for vulnerabilities on a broad scale. Recently published advisories show that security products are themselves vulnerable to all the same attacks known from other products. Albeit this is only a single indicator, it displays an apparently predominant but unconscious expectation: manufacturers of security products understand technical security and are therefore capable of producing secure products.

With the insight, that security software products are just as likely to contain security relevant flaws, it should be obvious, that it is an absolute necessity to investigate all planned and already deployed security products. The analysis should not be limited to technical implementation aspects, but also include technical design aspects: an antivirus mail scanner, that integrates into the mail server as a back-end component is conceptually a much more suitable approach, than to have the mail server component of the antivirus product interface with the network directly, and pass all accepted messages to the real mail server process for delivery. However, technical evaluations should start earlier: is the proposed concept optimal? That is, should one favor an alternative solution to those proposed: a bridging firewall eliminates many of the potential attack vectors of normal firewalls³. Another example would be the use VPN solution that limits the amplitude in case of exploitation: OpenVPN provides its VPN functionality as a regular server process, while IPsec is implemented as part of the operating system's core; a successful exploitation of an IPsec implementation will likely yield virtually unrestricted access to the VPN server, while an successful attack

-
- 1 Security discrepancies – Is security a functional idiom in today's world?
http://labs.akkaya.de/pub/ACLabs/Publications/SecurityDiscrepancies_en.pdf
 - 2 “Security products “: firewalls, antivirus scanners, VPN software and the like
 - 3 For attacks aiming to compromise the firewalling system itself



on OpenVPN merely yields restricted user privileges⁴.

The impacts of those underlying differences are often left unconsidered, yielding configurations that fail from a security standpoint: a single breach, that leads to the compromise of the entire environment.

⁴ Of course, it still represents a major security incident – it only limits the circumference of the intrusion for the time