

# “Seamless IP/Internet Security and Information Assurance – Utopia?”

Author: Lennart Damm

Affiliation: Siemens AG (Munich) <sup>1</sup>

## Abstract

High performance intra-domain security solutions for Mobile IP/Internet Networks (MIIN) are multi-level, multi-faceted, complex constructions, so far shown to be minimally, if at all, simulation prone. Moreover, inter-domain network security has been even harder to master. After addressing security performance issues in general, potential security performance enhancements based on simulations is analyzed in this paper.

MIIN security is separated into intra-security and inter-security. For each of these domain types, starting with the intra-domain, a Security Risk Management approach is analyzed, where generic technical infrastructure solutions, policy solutions, process solutions, and network and network element administrative and monitoring aspects are addressed. To this can be added, although not covered in this paper, custom based security aspects unique to a certain operator’s network implementation. Finally a possible performance enhancing security simulation procedure is analyzed.

The security analysis is mainly intended for mobile wireless networks that are IP/Internet based, such as GPRS/EDGE, UMTS (WCDMA/TD-SCDMA), cdmaOne/cdma2000, and WLAN. But the methodology can be applied to fixed networks as well, addressing the emerging merging of wireline and wireless network solutions, also in the security area.

There is no one-for-all-solution, but an initial step in approaching the difficult problem of security and how to predict its performance can be taken. Here “supernational” organizations, such as the European Union, have a responsibility to take the lead by providing well-balanced and comprehensive international wireless telecommunication networking security guidelines, specifically addressing open IP/Internet based networks.

## Background

IP and, specifically, Internet security is an increasingly hot topic. Not only for mobile network operators and service and application providers, but also for end-users (quite naturally) and infrastructure and mobile terminal manufacturers.

Putting the end-users in focus, there is a need for improved, secure applications offered via the Internet. But technology alone will never provide high-security solutions. A paradigm shift towards secure processes (!) for the total product lifecycle is a must. These products include security products which are aimed at enhancing network and network element security in one respect or the other. But even more important is building in security in all software and hardware in a network. So we are talking “non-security products” here. If this is done right, there will be a very limited need for security enhancing additional products.

By “non-security” products are here meant such products as operating systems and servers.

---

<sup>1</sup> Current affiliation: Independent Security Researcher and Consultant based in Sweden, with email address LennartDamm@OnePuttSolutions.com and web site www.OnePuttSolutions.com.

This paper is intended to make people start to think in terms of “trust” and “awareness” when they hear the word “security” mentioned. It is also meant to promote the initiation of simulation activities in the area of IP/Internet Security.

Problem definition

Internet security is shaky. You hear it every day of the week. New threats and risks emerge constantly. And viruses probable are not the main concern. The actual loss of important, or even confidential, information happens mostly as a result of unintelligent handling of information and information devices.

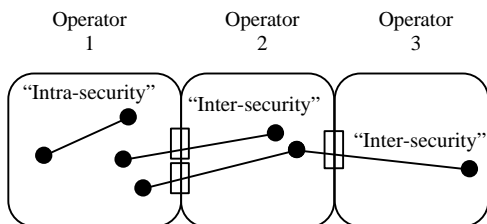


Figure. “Intra-security” and “inter-security” in and between IP based networks. Roaming means “inter-security” is applied.

The way forward

To reach the ultimate security goals a number of aspects must be addressed, some of which are very general and some of which are more case-to-case. For example, there is no inter-security without first having intra-security. Thus each operator must see to its own territory, this being a pre-requisite.

Among the approached taught within the security community, perhaps Security Risk Management is the most promising. This means looking at the role of people all through the life-cycle of a, or rather any, networked product.

What is to be simulated is each process in a product’s life-cycle, first the original process with its eventual security flaws, and then the process with an additional security process incorporated. The original (generic) process is defined within the security community, involving established security companies. But also with participation from the telecoms world where the application knowledge resides.

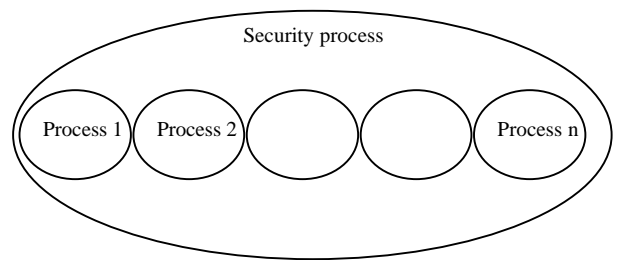


Figure. Product life-cycle processes and an overlaid security process.

Everyone talks about it, but little is done to promote it on a daily basis. There is no security without wide-spread security awareness, on all levels in every organization.

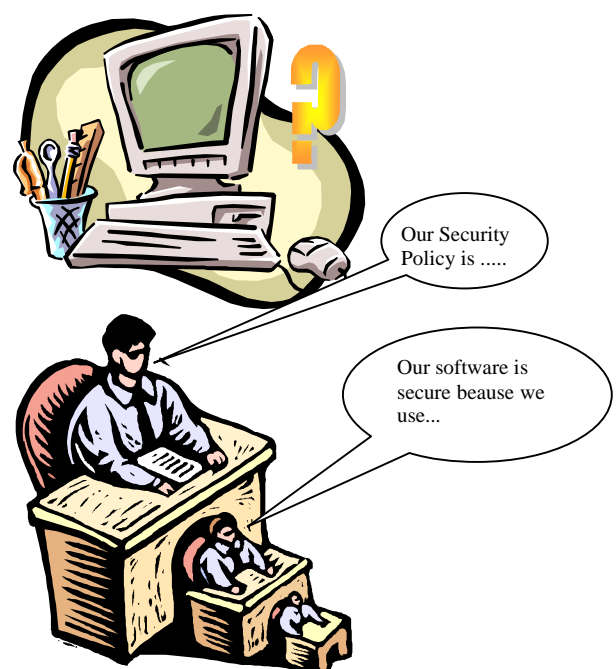


Figure. Security technology, including security simulations, is worth nothing – without company-wide security awareness and timely security processes.

security is relative, has a cost attached to it, and must be weighed against what we want to spend on it. The rest of the risk must be covered by an insurance policy, even for abstractions like lost company image.

### Can security be simulated?

To the author's knowledge no reported simulation results, with the purpose of security performance enhancement, exist in the area of IP/Internet security. And if there were, they probably would not be worth implementing in a real system. When asked if security can be simulated, the obvious choice for a first answer is "no". However, taking the great complexity of IP/Internet security into account, it should be possible to establish a simulation environment around a "minimum requirement security" solution, which by the way does not have to be based on strictly defined standards. This minimum level of security will evolve over time, perhaps in the same manner as the continuous update of virus protection. The latter we have learnt to live with, the former would indeed be a revolution for the notion of "security" and "trust".

We suggest that "known threats and risks" be simulated together with the solutions at hand, these being rather good or less perfect. This process can then be refined as new threats emerge. The results are published on a (well-known) web site for introduction in all systems just as security alerts are published today.

Every single individual in the telecoms "networking business" must gain a basic understanding of the importance of secure processes (most important) and security processes (as needed to enhance partly secure or non-secure processes).

### Conclusion

Full network security – utopia! Seamless network security – utopia! Rather good security – possible, but with some continuous effort! We need to accept that