VISPER: The VIrtual Security PERimeter for digital, physical, and organizational security

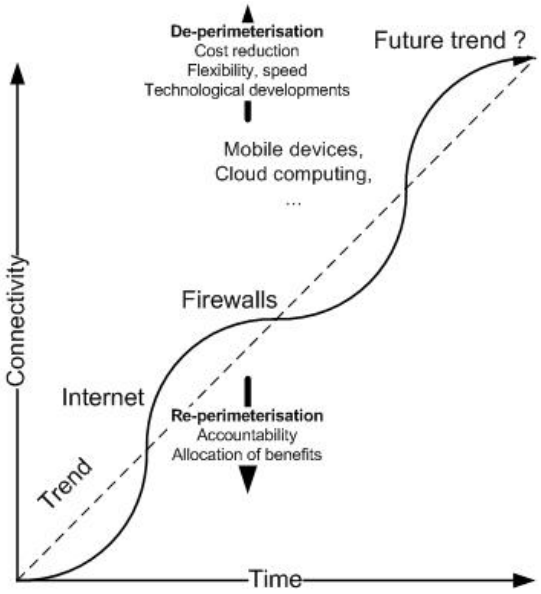
Name: Dimkov Trajce **Duration:** 2007-2011
Advisors: Wolter Pieters,
Pieter Hartel

Description of research

De-perimeterisation is the disappearing of traditional boundaries between IT systems. Both organizational and personal data is more vulnerable if connections and interdependencies increase, unless security requirements are explicit and alternative protection mechanisms are put in place. Such requirements and mechanisms may include physical, digital and social aspects.

In VISPER, we develop methodological and experimental tool support for the specification and analysis of security policies that are integrated across the social, digital and physical domain, as well as security mechanisms that link these domains.

The security perimeter, which once was simply defined as the fence around the premises of an organization, is becoming increasingly flexible and adaptable to the environment and the circumstances. We call this process re-perimeterisation (ReP). The effects of ReP are felt in the digital domain (where data moves from organization to organization through networks), the social domain (where one individual may play a variety of roles in cooperating organizations) and the physical domain (where appliances such as mobile phones and laptops move around).



ReP brings about new security risks because of the difficulty of keeping the domains aligned. For example, stealing a laptop (social domain) with a motion sensor triggers an alarm (physical domain), which then selects a security policy that blocks access to all sensitive data (digital domain). By making the security perimeter explicit in business processes, security policies and security mechanisms, we intend to foster alignment of the three domains.

Sponsor

The VISPER project is a joint project of the Distributed and Embedded Security and the Information Systems research groups of the University of Twente. VISPER is supported by AtosOrigin, the Dutch Tax and Customs Authority, Fox-IT, GetronicsPinkRoccade and BiZZdesign. The project is funded by the Sentinels program.

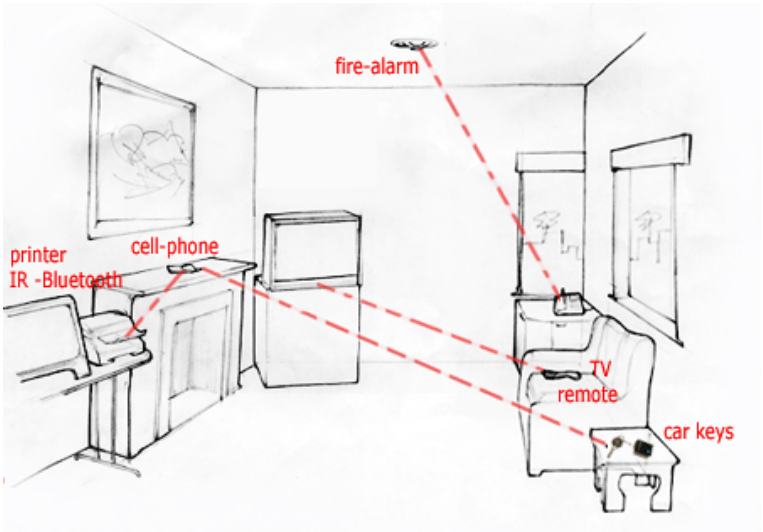
Strategic Research Orientation:

ISTRICE - Integrated Security and Privacy in a Networked World

The Future of Information Society – The Key-free Society

In near future, every household appliance will be accessible over Internet. The accessibility will enable scenarios such as instantly checking from the supermarket what is in the fridge at home, or turning the heater at home just before leaving work. In the next stage, these appliances will start talking to each other, leading to scenarios where the hater turns off when the electricity tariff is high, or the fridge automatically orders new cheese from the supermarket when there is little cheese left.

Parallel with this progress, the household security will also become digital and integrated, replacing door locks with digital locks and connecting them together with cameras over Internet. A person will never need to care where he left the keys again, since the locks will be based on a PIN number or biometrics such as fingerprint, iris(eye) or voice recognition.



The increased connectivity and accessibility of the devices will make them complex to configure and maintain, since the normal user does not have the sufficient skills to know how to do it properly with every single device. Thus, a number of new outsourcing companies will emerge, with responsibility to remotely configure and secure household devices.

The few families that decide to manage their household security without external help will face risks, such as the kid from the neighboring house playing with the heating temperature, or locking/unlocking the doors of the house. The families that outsource their household appliances to a third party will fall under another threat. Now, a thief does not need to break a door or steal a key. All he needs to do is to break into the organization that outsources the security for the neighborhood, and instantly get full access to all houses in the area.

There will be turbulence in society after the first burglaries where the thieves freely open and rob whole neighborhoods by using a single master key, which will lead to strengthening the legal liabilities to the outsourcing companies. In the future, the companies will not sell products, but trust. An average customer will give his household to the outsourcing company it trusts the most, the company with least reported breaches.

After the outsourcing companies reach a maturity level and the technology becomes more resilient, the security of households will be restored. The houses will start recognizing their owners without keys, let them enter the house and allow to operate with the household appliances. The visitors will have restricted rights, such as free access to part of the rooms and usage only to the entertainments system, but not the kitchen appliances. The key-free society will have smaller burden of keys, and bigger control over appliances and facilities.