Thesis subjects Nedap Security Management

Contact: Albert Dercksen (albert.dercksen@nedap.com)

The business unit Security Management within the Nedap Company develops, supplies and supports integrated systems for access control, intrusion detection, video monitoring and alarm management. You can find the installed base of these systems in airports, the industry, the banking sector and governmental bodies.

Traditionally these systems were the responsibility of the (physical) security departments within the user organizations. Today, we find an increasing involvement of the IT departments in the physical security management. It is more and more expected and required that systems for physical security are developed with tools and methods meeting the 'best practices' as applied in the IT security domain.
This development presents interesting opportunities for suppliers of security management systems.

Nedap Security Management offers three different subjects on which a graduation thesis project can be created:

1. Key management: Handling keys in a secure, distributed environment.
   The management (and storage) of encryption / authentication keys in a security system is often a procedural matter. In case, in spite of the procedural measures, unauthorized access to master keys is obtained automated and testable key update procedures need to be in place. For this procedure one could use for instance SAM modules or a Java card.
   The objective of this task is to develop a design for key update procedures in a (physical) access control environment, based on available technologies.

2. The human factor in the development lifecycle of security systems.
   Modern software systems make use of reusable components in combination with near – and/or off shoring. It could be useful to develop an authorization and/or access control model to grant / receive access to the necessary sources for such projects.
   The objective of this task is to analyze which model (e.g. role based, MDAC, attribute based) possesses the best fit in a development environment as described. Aspects that are relevant are not limited to mandatory reviews, separation of concerns, principles of exclusion all aimed at providing higher levels of security conditions. Another element of the task would be conducting a risk assessment on the development process.

3. Attribute based access control in distributed access control systems.
   OASIS is about to release the XACML 3.0 standard. The ABAC model is generally accepted as the logic successor of RBAC, nevertheless hardly ever used for the development of physical access control systems. Nedap is interested to apply ABAC models in a distributed environment based on controllers and / or devices with limited resources.
   The objective of the task is to design an ABAC implementation approach suited for application in the development as described.

Nedap Security Management is looking forward to work together with the University of Nijmegen in adopting and adapting the ‘best practices’ from the IT security domain into the field of the management of physical security.