Securing the secure

Physical security has, to date, always revolved around prevention: detecting and reacting to unauthorised entry to buildings, spaces and possessions. Depending on the extent of the reward on offer, security systems become interesting targets for hackers and other criminals: a criminal who succeeds in gaining entry to a building or system can cause significant damage, or can gain access to vital company information.

Securing change

The design of a good security platform should always be the result of a thorough risk analysis, but should also include aspects like legal issues, for example the laws on data protection. Additionally, system designers have to match the conditions set, like ease of use, technical limitations, and budget. Issues like globalisation, new forms of working and technological developments have placed new and increasing demands on guaranteeing the security of the security platform itself.

Components and confidentiality

Physical security measures like fences, barriers, video cameras, intrusion detectors and electronic doors all form part of the design. These ensure the physical safety of the buildings or areas in question. The hardware often makes use of IP technology, brought together in an IP network, often with distributed controllers coupled to a central server / database infrastructure with a web-based management interface. Identification at the physical access points usually occurs using contactless cards. Thus, a security platform comprises a large number of components, linked via a network, where information and data is stored, where inter-component data communication occurs, and where a number of the components are directly exposed to external influences. This demonstrates that the security platform has become an integral part of a company's IT architecture and has to comply with the requirements set by the central IT architects for critical infrastructure. These requirements mainly focus on non-functional qualities like availability, reliability, integration, standardisation and security. Techniques like encryption are commonly used to secure IT systems. The key concepts of encryption are confidentiality and reliability, where reliability is often subdivided into authentication, integrity and nonrepudiation.

Analysing the threat

For each element of the security platform, an analysis has to be made of the extent to which it complies with requirements for data storage and data communication, as well as the extent to which it can resist external attacks which could compromise the system's confidentiality and reliability. System components with an interface to users (cards, readers, software), external systems (integrations, databases, the internet) or the outside world (computers, IP networks) are those that are especially scrutinized as part of this analysis.

The key to management

One of cryptography's key fundaments is the Kerckhoff principle: in a well-designed cryptosystem only the key needs to be secret; the algorithms used must not contain any hidden secrets. If we translate this to security systems, the secrecy of the cryptographic keys has to be guaranteed, and these keys have to be in the right hands. This is the field of key management, one of the most important aspects of cryptography. Key management focuses on the complete life-cycle of the cryptographic key and is constructed using a combination of an organisation's systems and procedures.

The weakest link

Based on the results of this risk analysis, the system designer has to determine which measures have to be taken to secure the system adequately for the complete chain: a system's security is only as good as its weakest link. A combination of asymmetric and symmetric cryptography is applied depending on the desired security level. Examples could include a PKI solution (public key infrastructure), RSA or Elliptic curve methods and, in those areas where comfort / speed is essential, symmetrical AES encryption. Important, privacy-sensitive data should be encrypted using SHA-3. Communication between components has to be encrypted using the TLS protocol with mutual authentication and a digital signature requirement. Exported data should be minimally secured with a cryptographic hash function and a digital signature.

Embedding legislative change

And as a final part of design, the security platform also has to comply with Europe's new data protection act (COM (2012) 11). In addition to a range of technical, legal and organisational requirements, from 2014, security systems will have to comply with the 'privacy by design' principle. This means that legal requirements are 'embedded' in the system; it will no longer be acceptable for legal requirements to be satisfied using a combination of procedures and directives. This is expected to have profound consequences for all security systems currently available on the market.

Secure in the future

Nedap Security Management helps clients design well-secured security platforms. In addition to the role of advisor, Nedap has invested significantly in building a knowledge-base in the field of cryptography, thereby ensuring that the AEOS security management platform is fully equipped to cope with the security requirements of the future.

Published in Security Journal, issue May 2013
Nedap Security Management
www.nedapsecurity.com