Performance Enhancement: An Advanced Nearly Indestructible Video Surveillance System

Stephan Sutor
KiwiSecurity Software GmbH
1050 Vienna, Austria

***Abstract*— This paper presents a novel architecture for high performance, scalable video surveillance systems. The goal of this architecture concept is the creation of an advanced, virtually indestructible video surveillance system with the highest possible performance level, even under worst-case circumstances. The security management process used to build up such a system is introduced and analyzed, with the focus on how to achieve the highest possible security performance level. The presented system was subject to several test methods and phase levels to evaluate system performance. From the end user's point of view, all the achieved results verified the high performance and nearly indestructible characteristics of the system.**

***Keywords*— Video Surveillance; Performance; Availability; Reliability; Security Management Process; Physical Security; System Architecture; Quality of Service.**

I. INTRODUCTION

During the last few years, the world was confronted with several security tragedies, bank robberies and art crimes. Accordingly, the advance in research and development of security systems, especially video surveillance systems, has reached a remarkable progress worldwide. However, this progress has in turn urged organized crime and underground organizations to develop corresponding advanced technologies. Recently masked robbers brandishing handguns succeeded to steal four 19th century masterpieces by van Gogh & Monet from a Zurich museum in broad daylight [1]. This incident demonstrates the lack of security management processes for many systems.

II. Available State-of-the-Art Video Surveillance Systems

Video surveillance (hereafter VS) products currently available on the market can be segmented into four categories:

- Household surveillance products
- Commercial small scale products
- Commercial large scale systems
- High Performance Surveillance Systems/Solutions (HPSS)

The HPSS category is providing different levels of availability, reliability, integrity and performance measures in a scalable configuration.

This paper presents a new architecture of video surveillance systems, with extremely high level of robustness and performance; subsequently the configuration and technological aspects are presented. Accordingly a new category is presented: “Advanced Nearly Indestructible Video Surveillance System: NIVSS”

III. NIVSS Security Management Process

In order to design and develop a large-scale VS system, which should measure up to the NIVSS standard, security has to be part of the planning stage. ISO 27001 [2] provides a general blueprint for such a security management process. This section gives a first idea of how this process needs to be customized to be specifically valid for NIVSS systems. The topics to fill this blueprint with can be taken from ISO 17799 [3], which is considered the best practice collection of activities for security management. Fig.1 shows the selected topics from ISO 17799, which will be relevant for achieving an NIVSS standard in the future.

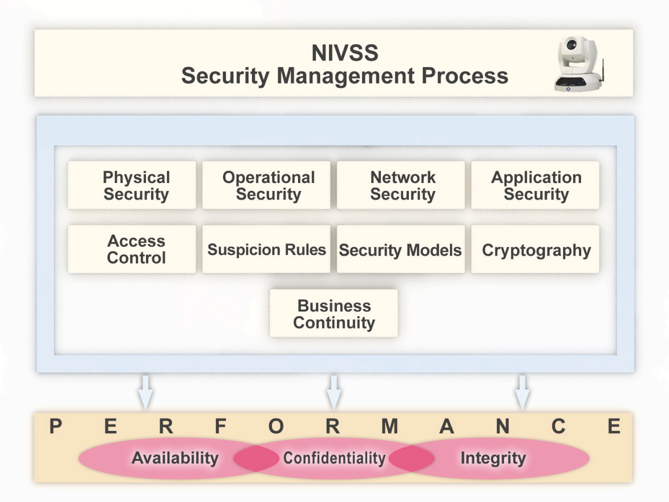

Figure 1: Security Management Process Components, relevant for the NIVSS

According to a recent study [4] the building blocks of the VS security management process are the following:

Access Control takes care of all situations, where assets need to be accessed and can possibly be manipulated (modified or deleted). Here identification methods and technologies for authentication and authorization have to be evaluated for aptness; policies for the implementation have to be developed. The scope ranges from user management aspects for the users accessing the database to the privileges under which an application process can access the operating system's kernel processes.

Modern advanced security models deal with the formalized description of how information flows within a system in a secure way. This includes the states in which a secure system should be. In this respect the selected security model will also have a distinct influence on access control [5].

Physical security in general is concerned with any kind of physical influence on the system. For the proposed architecture this will be a major concern, as it will be physically distributed and the locations of the cameras mainly a given fact. So the planning of measures against natural disasters as well as intentional assault will be a challenge. Access control of the data center on a physical level, of the server farms hosting the applications and of the transmission network is also a topic warranting utmost attention.

Network security is concerned with the design of secure data transmission systems. This encompasses the development of a network architecture, which allows the separation of different types of networks (data, operations, security management, etc.), that provide secure areas (for the database) and demilitarized zones for data access of the various applications. It also deals with the lock down of the various network elements so that they do not provide any more functionality than absolutely necessary and only to those users (human or processes) who are allowed to access this functionality [6].

Cryptography deals with privacy aspects of transported or stored information. This is especially important as not only security critical data, but also personal data is sent via networks (possibly passing insecure channels). On the one hand the data must not be intercepted, on the other hand data must not be tampered with. Methods of how to achieve this and which cryptographic algorithms to choose are also a major concern of the VS security management process (e.g., if video surveillance is used across geographically distributed systems).

Application Security is dealing with the questions pertaining to the secure development installation and maintenance of application SW. Already in the planning phase detailed policies need to be worked out, which describe the way the applications have to be implemented.

Operation Security is concerned with all details, which concern the actual setup, execution and decommissioning of the system. The management process here needs to ensure that all processes are well described, operational security measures broken down to procedures, and operational descriptions for all parts of the system are present.

Business continuity is a topic, which is concerned with the high availability of the system. In the case of a surveillance system this is a number of policies for the implementation of software (e.g., backup & restore system), of redundant hardware (e.g., a complete offsite backup facility) and procedures to follow (e.g., definition of first response team and its actions) in case of disruptive events. Evidently business continuity will also play an important role in network security and application security, where secure and continuous operations of networks and applications are being planned.

IV. Threats against the NIVSS System

In order to define the NIVSS and its protection mechanisms, all types of threats against VS systems have to be investigated. These threats are divided into two main categories: The first category is the threat of content manipulation, i.e., forging or removing of data, or adding useless or misleading data. The second category is based on system disruption, which ranges from simple attacks like destruction of cameras and destroying cables to more sophisticated ones like network or software based attacks.

These two types of threats are discussed for each main building block of the NIVSS security management process as follows:

A. *Content manipulation*

Content manipulation is defined as tampering and manipulation of data in the system, ranging from cameras to the storage of the video streams. In this section the threat of content manipulation is discussed for each aspect of the security management process.

- As tampering with data is categorized as part of network security, content manipulation on a physical level is not possible.

- Social engineering, using interactions to obtain confidential information, is considered as the greatest operational security threat for a VS system.

- Network Security: An attack on data transferred between one of the cameras and the final stage of processing, including attacks on analog signals and digital TCP/IP streams. When the attacker gets in a position to observe and intercept data streaming, this is called man-in-the-middle attack. This would allow the forging of video data by playing pre-recorded video streams or by editing the actual video delivered by the camera.

- Application Security: The goal of application security is to gain control over the VS system processing the pre-processed information or the machine storing the data via standard attacks like Trojans, worms, buffer overflows or exploiting backdoors, which causes a denial of service [7].

B. *System disruption*

The four categories of threats in this case are:

- Physical Security: An attack against any hardware component of the VC system e.g., camera, processing unit, network element or power supply. This type is considered to be the most severe attack on the VC.

- Operational Security: During updates wrong configuration data could be introduced into the system and could cause disruption.

- Network Security: System disruption attacks on network security are most likely in the periphery and user interface blocks of the NIVSS.

- Application Security: In this attack hackers try to get control over machines to manipulate content in order to achieve a system disruption. Furthermore, the traditional method of flooding the network can be used to achieve DoS.

- The architecture of the current NIVSS system was designed to withstand any of the above-mentioned attacks.

V. NIVSS: SYSTEM ARCHITECTURE

To achieve maximum availability, optimal reliability and best performance, the NIVSS was designed according to the following boundary conditions [8]:

- Redundant components (e.g., hardware): There must not be any part of the network without another component that can take over its function automatically. That means that the whole system has no single point of failure.

- Redundant networks (including wired and wireless networks as well as network components such as switches and routers): Each part of the system has to be reached through an alternative route. Backup networks have to be in place to take over networks which are down or overloaded.

- Tampering protection (software mechanisms to prevent tampering of cameras, network components and server hardware)

- Scalability (both in terms of video analytics as well as network):
  The system has to be scalable up to 100.000 cameras and more, interconnecting multiple video surveillance sites.

The system is divided into four hierarchical zones:

- Periphery
- Data Processing Center
- Demilitarized Zone (DMZ) and
- User Interfaces

Each of the four zones is subject to high security conditions in addition to the overall security concept of the system.

Periphery

As shown in Fig. 2, the periphery zone includes:

- Smart cameras:
  These cameras are analyzing the video image on their internal hardware and send results of this analysis to the data processing center. They track persons and vehicles, classify those and perform other tasks which are computationally intensive and which need to be done on the video images. This way the system stays scalable without sacrificing analysis quality. In addition to video analysis the smart cameras also encrypt and sign video streams to prevent unauthorized video streams from being injected.

- Cameras with image processing units:
  These are cameras (IP or analog), which are connected to an image-processing unit, which fulfills the same tasks as smart camera. With these units, existing cameras can be used in the system.

- Miscellaneous sensors:
  Various sensors (such as audio) help to identify events and tampering of cameras. Using multiple kinds of sensors, in addition to video, increases the security of the system considerably. If an intruder manages to tamper with a camera, injecting a video feed, simultaneous injection of audio material is more unlikely. Thus, if the system detects that sound does not correspond to video anymore, a tampering alarm can be triggered.

- Wired and wireless networks:
  Video and audio sensors are connected to the network with CAT 6 cables and wireless LAN, thus creating a redundant network. If one fails, the other one is still delivering data.

The NIVVS architecture is illustrated in Figure 2.

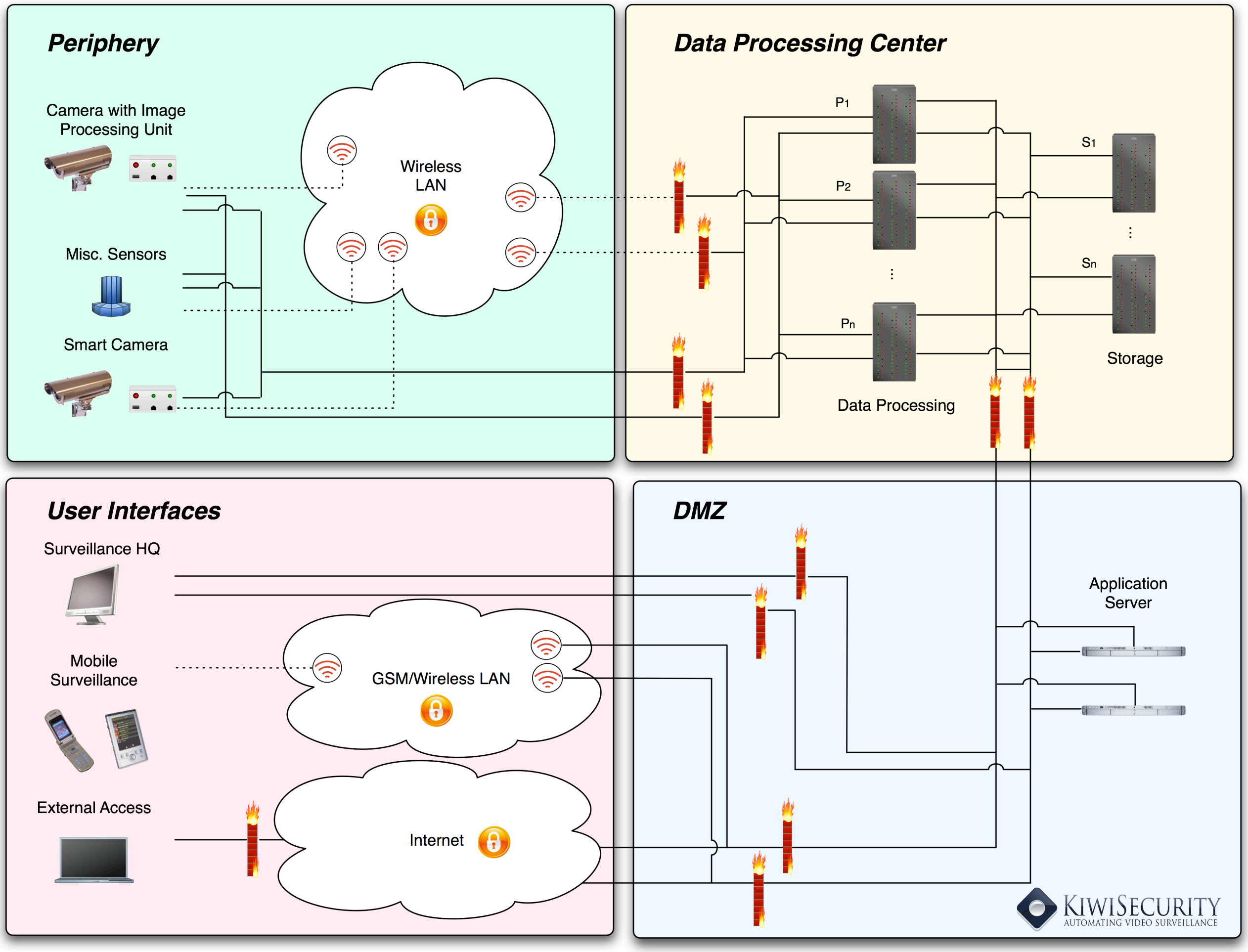

Figure 2: System architecture of the NIVSS system

Data processing center

Video information, including meta-information from image processing, is entering the "core zone" of the security system, the server network, through redundant firewalls with state full advanced package inspection and special intrusion detection systems. Just encrypted and correctly signed packages are allowed to pass. Both processing and the storage on the respective server hardware happen in parallel in consistency-checked self-healing clusters.

Demilitarized Zone (DMZ)

The collected and processed information is provided to the security guards through application servers. These servers are positioned in an internal Demilitarized Zone (DMZ) just beside each other because there is no need for them to be clustered. To protect the inner and core server nodes, solely reading rights on selected data are granted for these application servers. The network outside the DMZ is a virtual network with no machines connected directly to it; even though it should be physically built of multiple firewalls for security and reliability reasons. The only function of this network is to be the endpoint of the secured tunnel connections from the client applications and application networks.

User Interface

Relevant information from the NIVSS is presented to the user on various interfaces, including terminals, PCs and mobile devices (such as PDAs), which are used by security guards on patrol to get live alarms instantaneously to react to security breaches. In addition to the interfaces for the end user, operation and maintenance personnel have the right to define suspicion rules and conditions to be detected by the system.

Redundancy in the system

At the camera level power and the network connections have to be redundant. To guarantee this with analog cameras is anything but trivial. To reach this in digital systems based on computer network protocols is more simple. For power redundancy, power over Ethernet (PoE) can be used aside local power and buffer batteries. Parallel networks can be based on different media from copper wires over different optical to radio communication. Especially for a camera the cooperation of radio networks and wired connections, that can be attacked only in completely different ways, is essential. Wireless communication is another advantage of digital systems. There, protection against tapping is a must on any network leaving a single secure room: Here, multi-tier encryption (application and network level) and signing provide protection must be implemented. The same applies to any communication channel [9-10] connecting nodes that are not servers in the same secure server room and physical redundant networks within this room.

Firewalls

The use of firewalls and separate networks for such a system is essential. However, firewalls should not be the only protection in the communication for clients. Furthermore, a security system must not only ever be connected to highly insecure networks like the internet or 'normal' corporate networks, but also an application server in an internal DMZ is required. This server has the most limited reading rights and connection rights in the primary server network. The processing servers and the DBMS servers have to be clustered as a consistency checked self-healing system. A well designed, maintained backup system is necessary, as well as an indestructible power supply including UPS, emergency power, over voltage and short circuit protection.

VI. Vandalism, Sabotage and Natural Catastrophic Scenarios

A system level failure is defined as the status of having a single non observed point or no alarm upon detecting a suspected object/person/behavior. Following scenarios of attack, destruction or vandalism against the system are discussed taking into account the system structure.

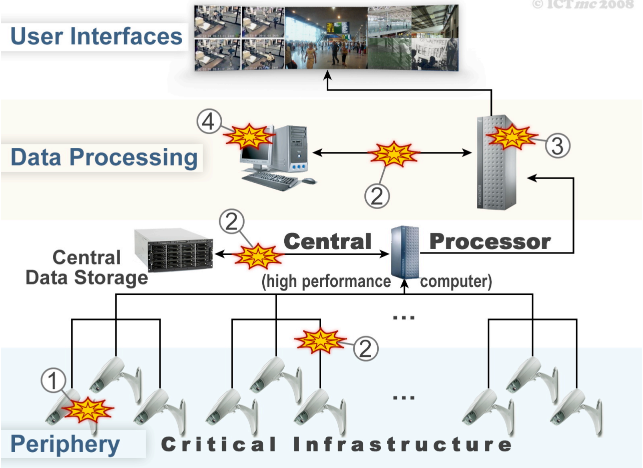

Figure 3: Attacks on a Single Site NIVSS

The periphery zone involves all the equipment outside the secured processing center. This includes cameras, image processing units attached directly to cameras and all networking connections and devices. Fig. 3 shows the infrastructure of a single site surveillance system, where all cameras and equipments are in the same VS centre, e.g., the main railway station, with the VS operation center directly connected to the central security authority or police station. Similarly, Fig. 4 illustrates attack attempts on a multiple site VS system, e.g., a large-scale airport, with several terminals and scattered infrastructure. Each of them is equipped with a local VS system, which is interconnected to the central VS operation & control room.

Four attack points or points of failure were identified. In attack-point 1 one of the cameras is destroyed or damaged. The system automatically detects such an event and causes an alert to be triggered and the task of the damaged camera is immediately covered either by the redundant camera or by one in the vicinity. In attack-point 2 the network connection is interrupted: The camera now uses full wireless transmission, and an alert describing the network failure is being sent.

In attack-point 3, the wireless network is jammed. However, the system can still rely on the cable connections and an alarm will be set off. If the attacker starts with the wired network, the system will switch into wireless mode and trigger an alarm immediately; hence the attacker will be stopped.

Attack-point 4 resembles an attack on one of the data processing servers or a storage server. Both these events will not affect the entire system, because each component is redundant, and the system will automatically distribute the load of the failed unit to the others. Measures of the required redundancy will be discussed in future work.

Even in case of disaster or natural catastrophes, where the whole surveillance site is under attack, an alert would be reported immediately to the authorities.

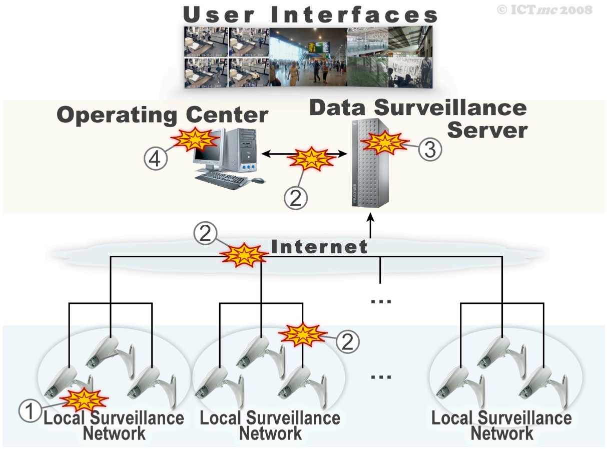

Figure 4: Attacks on a Multiple Site NIVSS Infrastructure.

VII. Conclusion

This paper presented a new security management process used to build a nearly indestructible, high-performance video surveillance system. Subsequently, a novel architecture for such a system was presented and analyzed. Accordingly, this video surveillance system was tested, validated and verified while running in real time at the highest possible performance level, even under worst-case circumstances, identifying different types of threats and corresponding counter-measures.

A patent application was filed for the NIVSS system architecture.

ACKNOWLEDGMENT

Discussions with Prof. O. Martikainen, Department of Information Processing Science at the University of Oulu, Finland, are highly acknowledged.

This work was further supported by the Austrian Research Promotion Agency "Österreichische Forschungsförderungs-gesellschaft" www.ffg.at and the Academic Business Incubator INiTS, www.inits.at. This work will be partially included in a Ph.D. thesis at the University of Oulu, Finland.

REFERENCES

[1] L. Moran, www.mainstreet.com, "Challenges, Dealing with being a Crime Victim, 12.02.2008

[2] "ISO/IEC FDIS 27001 "Information technology — Security techniques Information security management systems — Requirements" Final Draft 200

[3] ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management.

[4] K. Kraus, Security Management Process in Distributed, Large Scale High Performance Systems", Proceedings of the World Congress on Power and Energy Engineering, WCPEE'10, Alexandria, Egypt, October 3-7, 2010

[5] B. Howard, O. J. Paridaens and B. J. Gamm. "Information security: threats and protection mechanisms", Alcatel Telecommunications Review, pp. 117-121, 2001

[6] J. Gonzalez, V. Paxson, and N. Weaver, Shunting, "A Hardware/ Software Architecture for Flexible, High-Performance Network Intrusion Prevention", Proceedings of ACM CCS, October 2007

[7] J. Bellardo and S. Savage. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", Proceedings of the 12th conference on USENIX Security Symposium, pp 2-2, 2003

[8] F. Matusek, S. Sutor, F. Kruse, K. Kraus and R. Reda, "Large-Scale Video Surveillance Systems: New Performance Parameters and Metrics", The Third International Conference on Internet Monitoring and Protection, Bucharest June 29 - July 5, 2008

[9] R. Reda and N. Jordan, "Signpots for the Future of Mobile Communication" , e&I, elektronik und informationstechnik, heft 9.2006,published by Springer Wien New York, ISSN: 0932-383X EIEIEE 123(9) 361-408, a1-a44(2006)

[10] R. Reda and H. Volopich, Siemens AG Austria, (2003), e-Business Evolution, Market Trends, and Business Opportunities: Keynotes presented at the International Conference on e-Commerce, Hong Kong 2002