Research Plan

Enabling Privacy in Video Surveilled Areas

by
Torsten Spindler
Chair for CAAD
D-ARCH, ETHZ

Thesis Committee:

Prof. Dr. Ludger Hovestadt
Chair for CAAD
Department Architecture
Swiss Federal Institte of Technology Zurich

Prof. Dr. Andreas Steffen
Chair for Internet Technology and Applications
Information Technology
University of Applied Sciences Rapperswil

Abstract

Within the blue-c-ii project conventional video cameras and next generation 3D video cameras will be used to record video streams of people in a building. When automatic cameras stream all movements in buildings privacy becomes a delicate issue. Within this project a framework will be built that uses cryptography to improve privacy in such environments. The framework is built modular and in a flexible manner so it can be adopted easily. For example for use in an IP network based building automation system. The framework will be accessible by users with easy to use hand held devices. An easy to use interface that enables visitors to use and control these devices has to be created. An important part of this is the security aspect. Currently most building monitoring systems transmit their signals to a very restricted set of locations, where access to view these is limited. Within blue-c-ii it is planned to let visitors of a building use videos taken by 2d and 3d cameras. This makes almost everything happening in the building visible to the public. Clearly this is in conflict with privacy of people inside the building. To resolve this issue a system that allows each person to control access and protect their recorded images is envisioned. Everyone inside the building can limit access to the information provided by blue-c-ii system to others. An authentication and authorization system has to be developed, that provides necessary means to enable and disable the streaming video services to others. A key point is also how to modify these video streams close to real time so only those persons that gave permissions are displayed unscrambled. From an architectural point of view it is examined how the use of limiting the possibilities of monitoring creates a middle way between the concept of private and public rooms. Overall the projects goal is to enable people to control video information of them.

1 Video Controlled Spaces

Over the last decade almost all public spaces and commercial buildings have installed video cameras. Access to recordings of these cameras is usually strictly limited by security staff members and alike. In the near future projects as blue-c-ii will enable anybody to use tracking systems to locate a colleague or friend. Nevertheless it is important that everyone in a building equipped with this surveillance equipment is able to control who may

or must not see his movements. Clearly some people will have access to all information available, as security staff does nowadays.

2 Building Automation

Many existing buildings use some kind of hard wired automation system. Contemporary and next level building automation is about installing and controlling various electronical or mechanical devices within a building without adding extra cables or other error prone ways to extend a buildings intrinsic capabilities. One way to achieve this is to use an existing networking technology as Ethernet cabling with the well known and understood TCP/IP protocol stack. Based on this generic information transportation backbone devices can communicate with each other in a building. Control and configuration of these is researched, especially the aspect of scalability. As of summer 2003 and more devices are equipped with the capability to use IP based protocols for control and information transportation. In the home entertainment field several closed systems compete with each other. Yet the power of internet and it's accompanying protocols lies within their openness. Anyone interested and with sufficient technical knowledge can use the protocols definitions and implement their own flavor. Taken this principle into building devices means that based on open communication standards devices can be simply plugged into an existing network and are almost immediately usable. However within this context it is especially important that the value of each device can be further risen by means of collaboration with the rest of installed devices. While it is certainly nice to have several cameras or microphones setup in a room that all use the same transport mechanism, a large step forward is done when these can meaningful interact with each other. For this to happen a middleware service platform is envisioned, that is used by these devices to announce their services and also receive service information provided by other devices. Is it foreseen that abstraction layers can be used to provide higher and higher access to this information, using secondary sources to enrich this.

3 Enabling Privacy

Every person should be able to control the information about her that is recorded by the intrinsic or extrinsic capabilities of a buildings monitoring systems. With this goal in mind a person, thereafter called user, has the ability to

```
1) grant/restrict access to this information to another user
2) grant/restrict access to several other users
3) grant/restrict access to all others
```

Further it will be necessary to restrict/grant access based on locations. If there are rooms that have limited access, should a user that has no access to them view a video stream of these rooms? Clearly not so mechanisms to control this access control to video streams has to be based on the persons surveilled and location. Notwithstanding is the fact that supervisors like technicians and guards will have to have the ability to view all streams of interest to them.

4 Current Technology

The real time manipulation of videos to protect privacy of surveilled persons has attracted several companies and researchers focus. Most noteworthy are the attempts to create and use annotated videos. Added to the pure graphical information is meta information which consists of an interpretation of the scene recorded. For example the MPEG-7 standard is used heavily in research and industry for this purpose. Recently started US based company Eptascape focuses on this approach and is looking for partners to make good use of their annotated video technology. One important showcase for them is a privacy enhanced camera system. At EPF Lausanne projects exist that follow a similar approach, but are meant to cooperate with existing legacy camera systems. A spin-off company named Emitall Surveillance in Montreux is looking for a partners to realize products with this emerging technology. Another aspect are access control systems that are already integrated in buildings as well as in computer OS's. The former have taken a step from simple key based control to more advanced technologies during the last half century. In multiuser OS's different access control technologies have been developed to limit access to information associated with users. Many modern

OS use ACL (Access Control Lists) to control this. Unfortunately these can be quite hard to use as the consequences of alteration of ACLs are not always straight forward. Within buildings access to monitoring systems is controlled by giving access to rooms containing surveillance systems. Clearly both approaches are not sufficient. First ACLs are too hard to use, second to demand of users to visit certain surveillance rooms is quite impractical. Another approach that deals with access to multimedia streams are DRM systems. With watermarks and other techniques use and access to those streams is hoped to be achieved in combination with special hardware as it can be found in a trusted computing environment.

5 Goals

First a framework for the distributed environment had to be created. This was done in a prototypical fashion, focusing on evaluation rather than robustness and correctness. Next lessons learned from the prototype were used and integrated in a more mature framework. Lastly an interface running on a hand held device are implemented. Throughout the implementation Open Source software has been used wherever found to be useful. The resulting code is released under a free license as well. In parallel literature on the topics of video surveillance and surveillance within built architecture has been researched. Further available technologies are examined with the projects goal in mind.

6 Time Plan and Future Work

This dissertation is embedded within the blue-c-ii project. Work for blue-c-ii has commenced in January 2004. Before that the author gained experience within the field of digital video processing in the context of IP based building automation systems from the Building IP project, which was part of ETH World. Within blue-c-ii a close collaboration on the aspect of tracking has been undertaken with the Computer Vision Group. Parts of the work for this dissertation are already completed as part of the milestone goals within blue-c-ii.

In autumn 2004 the author decided to apply for a dissertation on this research plans topic. First Prof. Dr. Ludger Hovestadt agreed to supervise

the planned dissertation. Second a second examiner from the field of computer science with a focus on applied cryptography and security was found. Prof. Dr. Andreas Steffen agreed to supervise the computer science related part of this planned dissertation. Next the necessary steps for applying for an interdisciplinary dissertation were completed in Spring 2005. With that application an earlier version of this research plan was submitted and the application accepted. Now the research is in an advanced stage and the author wants to complete his dissertation within 2006. Time is a pressing matter for the author as his personal environment has changed and he plans to move to Montreal, Canada, no later than August 2006.

literature research	Winter 2003/2004 - Summer 2005
software evaluation	Winter 2003/2004 - Fall 2004
specification	Spring 2004
prototype	Spring 2004 - Fall 2004
refinement of spec	Winter 2004/2005
implementation	Spring 2005 - Fall 2005
experiments	Winter 2005/2006
dissertation	Winter 2005/2006 - Winter 2006

6.1 literature research

One aspect is to find information on how to design and implement scalable device organization software. Besides the embedded system field the area of operating systems covers important techniques in this field. Principles of organizing name spaces, organizing distributed information sources, providing fault tolerance are known and have to be evaluated on the specific task at hand. On the privacy issue cryptographic techniques will be collected and evaluated against properties as suitability in real time processing environments, known resistances against attacks. Another field is the manipulation of video streams in real time. Especially important will be ways to encode parts of a video stream. Further contemporary authentication and authorization methods will be looked upon.

6.2 software evaluation

With the Open Service Gateway initiative a framework capable of dealing with building device organization is already available. It will be evaluated

how these system scales for the planned task. Reference implementations of cryptographic techniques will be evaluated against video streaming and manipulation thereof. Further different available network technologies will be examined and compared to choose one suitable for the task to combine several hundred if not thousand of video streaming devices.

6.3 specification

Based on the findings of the literature research and software evaluation a specification of the overall system and it's capabilities and requirements will be created. This document will describe what mode of operations and what technologies the system will use. It includes software as well as hardware requirements. Further and beyond technological considerations the way users might view and use such a system are examined. This part will include demands to the user interface as well as administrative aspects.

6.4 prototype

As reference a room with video cameras and middleware for control and configuration will be created and tested as close to real application scenarios as possible. This prototype will be used as demonstration tool and is planned to be transportable. This work is hoped to be presented in conferences and probably in fairs as well, while being available within ETH buildings for the majority of time. It is considered to make this showcase available to members of CAAD and collaborating groups to detect any weaknesses, be they of technological or social kind. Also the systems ability to cooperate with other automated systems will be examined, like audio equipment as microphones and loudspeakers.

6.5 refinement of specification

Based on experiences with the prototype and additional requirements the specification will be modified. This step ensures that the risk of the projects failure is kept low. Also it can be expected that with development of new technologies in the areas of 3d video surveillance and cryptographic methods the system can be enhanced further. Special consideration will be placed upon the systems interface with the outside world, including the user level integration and the systems ability to be used in conjunction with others.

6.6 implementation

Based on the refined specification a reference software and hardware platform will be realized. Equipped with latest technology from the blue-c-ii project and contemporary cryptographic methods the system will hopefully be transportable so it can be put on show at various locations. When not traveling the system will be installed in rooms at the ETH and will be put to everyday use.

6.7 experiments

In a semi-permanent installation at ETH Hnggerberg within the rooms of the chair for Computer Aided Architectural Design the framework is setup. Feedback on the use or non-use of this installation will be gathered. The use of this technology within a pervasive gaming environment will be especially considered.

6.8 dissertation

In the written dissertation used technologies and the developed system will be explained and analyzed. Strengths and weaknesses of the overall system as well as the used technologies are examined. The social aspects of the use of this technology, that allows users to hide and show information of them will be of central interest as well. The written part will consist of detailed discussions of the used technologies, be they video hardware used, network equipment or cryptographics. Beyond technical matters it will be examined how users react and use this system. Is it easy enough to use, so one will hide from watchers? Is it clever to scramble users or is it better to allow access to all information by default? Can it be used to effectively allow private video conferencing between people at random places within a building? Clearly the non technical questions asked are numerous and very often as challenging.