CHALMERS

Information Security in Crisis Management Systems

Master's Thesis in Networks and Distributed Systems

UMMUL KHAIR ISRAT ARA

Chalmers University of Technology
University of Gothenburg
Department of Computer Science & Engineering
Gothenburg, Sweden, March 2014

Evaluation of Document and Search Query Processing Frameworks
Ummul Khair Israt Ara

Examiner: Fang Chen

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden, March 2014

Abstract

Information security is an important part of almost any kind of Information System. Crisis Management Systems (CMS) are a type of Information System that deals with information which needs to be secure. Natural disasters, IT outages or terrorist attacks, no matter what kind of crisis, the Crisis Management Information Security System (CMISS) shouldn't be compromised.

There are many challenges regarding exchange of qualified information and interoperability between various Expert Systems and the CMS. It is important to have strong security in terms of technology, skills, security requirements, sensitivity of information and trust-worthiness [1]. Depending on the type of crisis situation, different sets of security components should be triggered, since the security requirements vary between situations. For example, a terrorist attack has different security requirements in the system compared to a natural disaster or a medical emergency.

In this paper, the importance of Information Security in CMS will be discussed. Methods for secure exchange of qualified information are analyzed and a secure and dynamic CMISS design is introduced.

Contents

1

Introduction

1.1 Background

Crisis is a word with six letters whereas describes vast area. A crisis or disaster is a natural or man-made disruptive event. It's a dynamic word and can match with different situations to confer full statement. Depending on the perspective or research study, the word 'Crisis' gives totally different perceptions. If considering natural disasters then earthquakes, tsunamis, hurricanes, volcanic disruptions, etc are included whereas nuclear attacks, terror attacks, bomb blasts or threats, chemical carrier or oil depot explosions relates to man-made disasters.

A crisis can be big or small, but if we can know the situation before it happens, then we can take action to save human lives and properties. But if disasters happen unexpectedly then Crisis Management System can help by giving information, or make information available to everyone, so everyone can know the present situation and help in any possible way. The information in the system can help dcision makers to take decisions.

1.2 Introduction

Crisis Management Systems (CMS) are Information Systems, connected with many different Expert Systems (ES). This Information System not only consists of hardware, software and interfaces, but also people as cyber world dynamics [1]. Examples of some ES are Police, Medical Team, Rescue Team, Energy, Water, Fire brigade and Geo-information, etc. Information Systems are used in many different areas such as finance, health, fire service, energy, defense, health and police. Geographical Information Systems (GIS) are one of the more important types of information systems in crisis management.

These ES might have different roles when acting in the community , but they need to share information between each other in order to achieve a common goal and to increase

the awareness of local and global authorities/decision makers. Different ES are mostly classified in different security levels depending on the information they process, and can vary in terms of security requirements, security levels and access rights. Establishing the information security is a challenge in CMS as data exchange is required between the different security levels [1].

In this study, secure information exchange between different security levels is discussed and a Crisis Management Information Security System (CMISS) is detailed, where data is shared and access restricted. Different heterogeneous ES are connected to the CMS, each system has its own security policy, but all systems share their data with the CMS, so they have to work together which is where interoperability and sharing comes in. CMISS will manage who can access which information. Decision makers will get processed and trustworthy data through a Decision Support System, based on which decision is to be taken and Command and Control will be triggered. For secure information exchange, firstly the necessary information is to be filtered, classified and finally transformed to a common format.

1.3 Examples of previous crises

1.3.1 Chemical Spill turned River Rhine Red

The leak at the factory called Sandoz in 1986 was Europe's worst environmental disaster for a decade.

Near Basel in Switzerland a catastrophic fire at a chemicals factory sent tons of toxic into the nearby river Rhine and turned it red. November 1st 1986, early in the morning, a fire broke out in a storage building of Sandoz factory that was used for mercury, pesticides and other highly poisonous agricultural chemicals.

Local residents were woken by sirens sounded by local authorities to alert them to the disaster. The surroundings region on the border between Germany and France were told to stay indoor including the people in the city of Basel. Foul smell of rotten eggs and burning rubber has been reported by witnesses, including one of the firemen fighting the blaze with fourteen other people who were treated in hospital after inhaling the fumes.

It has been thought that the chemicals were washed into the water used by fire fighters to tackle the fire. About 30 tons of pesticides were discharged into the river, western Europe's most important waterway. Before flowing into the North sea the river flows through four countries, Switzerland, Germany, France and Holland. Within 10 days the pollution reached the North sea. Half a million fish were killed and some species were wiped out entirely.

http://www.crismart.org/

1.3.2 Kista blackout in Sweden

March 11 2001 became a day that the people at Kista in Stockholm in Sweden will always remember. Power supply went down for the whole municipality early in the morning and continued for the next two days. This power failure caused great consequences

and dramatic problems for the residents of Kista. It caused severe effects on daily life, business and in public administration of the over 100 000 inhabitants of the northwestern suburbs with eight districts in Stockholm.

It was an extreme case for the firefighters in Stockholm because the power supply failure was caused by a fire in a 110kV power cable which was placed 330 meter inside a cable tunnel. In this crisis situation the fire department in Stockholm was a major actor and were responsible for handling the situation. It took 48 hours for them to control the whole situation to a normal state. Through local radio news the fire department in Stockholm got to know the news, even though they had telephone in the department but because of the power failure the telephones became inactive. The fire was 30-40 meters below ground level with limited visibility and 35 firefighters were engaged to extinguish the fire in these hard conditions.

Heating, fresh water supply, sewage pumping had stopped functioning during this crisis situation. All kind of electronics appliances such as Radio, TV, internet, cooking ceased to function, elevators stopped and people got stuck. All of these problems caused a huge panic and inhabitants suffered. Public safety was threaten on that time as traffic in the crisis area went out of order and a panic situation took place.

Kista blackout was a situation which showed the vulnerability of the technical infrastructure. On this crisis situation Brika energy was responsible to update the public but their performance couldn't reach a satisfactory level as a result the public trust on the crisis management activities was declined. Thus it is clear from the Kista blackout that communication between different actors on the right time is really important to handle the crisis situation faster.

1.4 Purpose

The purpose of this thesis is to design a system to assist in Crisis Management which will provide information security. The needs of a crisis management organization will be analyzed and the unique demands of various crisis situations will be researched. From these requirements we will design and propose a Crisis Management System ...

1.5 Study outcome

The outcome of this study is the proposal of a Crisis Management Information Security System which meets both the security demands of an organization with confidential information that must be shared between actors, and the flexibility demands of a rapidly evolving crisis situation.

2

Literature

2.1 Crisis Types

The term 'crisis' can be hard to define, and no general definition is accepted by everyone. Therefore, when trying to define and categorize crises, this can vary between organizations. Following the definition by Shaluf, Ahmadun and Said [2], crisis types can be divided into four groups.

Community Crisis types include an crisis which occurs due to natural disaster, industrial crisis, or non-industrial crisis that occurs due to political or no-conflict crisis.

Non-community Crisis, which do not impact the community itself, are mainly transportation accidents.

Conflict Crisis include crisis which occur due to any inter-humanitarian conflict or struggle. From the point-of-view of the community, these can be External crisis, such as e.g. war, threat or terrorism, or Internal crisis, such as e.g. dictatorships, religious conflicts or riots.

Non-conflict Crisis can include any kind of Economic crisis, or Social crisis which may include e.g. sabotage/product tampering, corruption, threats and other problems.

2.2 Crisis Stages

Fink S. suggests that a crisis can be divided into four separate stages[3]:

- prodromal crisis stage,
- acute crisis stage,
- chronic crisis stage,
- crisis resolution stage.

Generally, an organization may or may not detect the possibility that a crisis will appear. If it does detect the crisis ahead of time, the organization enters the *prodromal crisis stage*. During this stage, action should be taken to prevent the crisis and reduce its impact, however it is not uncommon that an organization does not act even though it knows about the impending crisis. During the *acute crisis stage*, the community or organization is subject to harm from the crisis; the level of harm inflicted depends on how well prepared the organization is. During the *chronic crisis stage*, the organization attempts to recover from the crisis. At this stage there may still be lingering effects from the crisis. In the *crisis resolution stage*, the organization resumes full operability.

2.3 Efficient Crisis Management

Paraskevas conducted research on a case-by-case basis to analyze the effectiveness of Crisis Management Protocols (CMP) [4]. It was found that a protocol which describes specific actions to take does not allow actors the freedom to tackle a rapidly evolving situation with varying needs. What is recommended for a crisis handling organization is a system which can provide robustness and resilience to crisis situations. Such a system should not attempt to define actions and behaviors for specific actors. It should provide structure for operations and information flow, define actor interaction rules and allow flexibility for agents to reorganize. It should also be flexible enough to change depending on the specific needs of the unique crisis situation.

2.4 Security

In Information Security there are many sources of vulnerability which must be secured [1, 5], see Figure 2.1:

Physical security for the protection of physical property,

Transmission security protecting against unintended electromagnetic emissions,

Communication security to prevent data from being intercepted from the physical communication media,

Network security to protect the data transmitted on the network from digital interception attempts,

Access and authentication security to prevent unauthorized access to computers and network components.

2.5 Need-based resource requesting

A real-world example of a crisis management system which allow for requests based on the need of the requester can be seen in the California Standardized Emergency Management System (SEMS) [6].

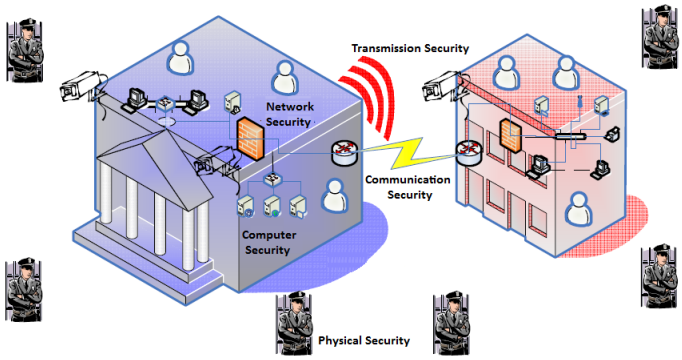

Figure 2.1: Information Security View [1]

The SEMS system description (reference!) states that:

> SEMS has been established to provide effective management of multi-agency and multijurisdictional emergencies in California.

SEMS is an emergency management system connected across several parties, which is designed to be flexible and adaptable to the various types of crises that can occur. The system allows the Emergency Operations Centers (EOC) of the connected regions to request resources, such as vehicles and personnel, from EOC in other regions or states. In this way the system allows mutual aid between the involved parties. The type of requests that an EOC is allowed to perform depends on the type of crisis and its severity, see Exhibit A-1 in [6].

3

Method

3.1 Purpose

The area of Crisis Management Systems is a relatively new field of research. Crisis Management Systems were identified as a type of system and an area of research where security has so far not been a primary concern. It is also a type of system with unique security requirements. The purpose of this thesis is to identify and analyze security requirements for this type of system and to suggest a complete system design which can handle these requirements.

3.2 Research Approach, Research Strategy

Information security is often a highly confidential part of a system, regardless of what kind of system it is, for any company or organization. While researching on this field we found it very hard to gain access to information on current CMS security systems, to measure present security levels and vulnerabilities. Therefore our work has been mostly focused on literature.

3.3 Data Collection

For data collection, past crises have been studied and their unique security needs have been considered. In addition we have also considered theoretical situations. When studying a crisis situations we have focused on the impact that the situation has on communication between different actors and the information need that decision makers and field agents may have in such a situation.

Attempts have also been made to study Crisis Management Systems used in productions and by corporations. However, since these are usually surrounded by strict security

and secrecy regulations, the study of existing systems has focused on those with publicly available information, such as OASIS[7] and SEMS[6].

4

System Design

4.1 System goals

The goals for the design of the Crisis Managements Information Security System (CMISS) have been:

- Ability for decision makers to temporarily raise or lower access rights for groups
- Rapid, automatic access elevation for certain groups in certain crises based on information need
- Security should meet requirements for handling highly confidential or sensitive data such as US government data
- System securely provides information from ES to DSS
- Scalable, robust, flexible, secure system

4.2 System Design

In CMISS, the main database is connected to several ES and Decision Support Systems (DSS). In addition, actors may connect to the system and request information. Access will be restricted on both the input and output sides according to the users role and access rights. Security will be provided on all sides and internally. The system design is shown in Figure 4.1:

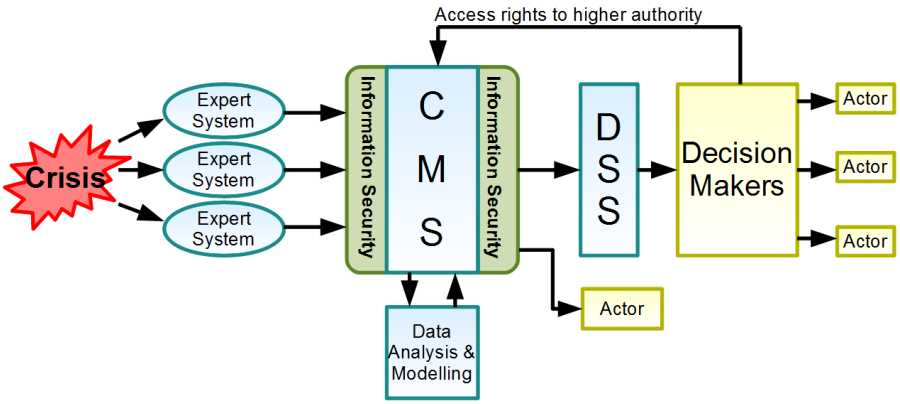

Figure 4.1: Proposed system design for CMISS

Each DSS is connected to human decision makers in a decision table, with a chief of every department, such as police, medical, fire brigade, etc. This department head will have direct access control over their part of the information system and any time if the system gets compromised or confidentiality of some data should change, then they have rights to change access rights to allow or deny access in real time. Theoretical examples of such situations are for example:

- During a disaster such as chemical spill, oil leak etc, the company decides to allow access to previously confidential data in order to help with containing and fighting the disaster, improve public relations, etc.
- Police decides to make available (previously restricted) location data of persons now considered dangerous so that other units may avoid the area.
- The security of the CMS is believed to have been breached and all data deemed sensitive (for example personnel location) is to be made inaccessible, but the system must still function normally with other non-sensitive data (for example fire, power and water grid, etc).

In this system, it is assumed that each system is secure enough to handle the level of security of its data. Each ES is connected to the CMS through secure tunnels. The data obtained from all ES will be stored and processed in an internal data analysis and modeling software.

Actors, or field agents, are able to connect to CMISS via any internet connected device capable of making a secure connection to the system, such as a VPN.

4.3 Need-based access rights

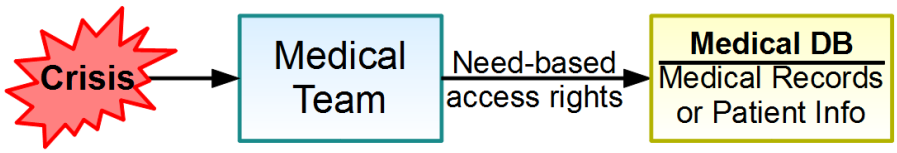

Figure 4.2: Need-based access rights

Crisis situations generate diverse requirements according to the scenario. Rules which normally apply, may not apply in a crisis situation. For example, if we consider a situation when an individual needs immediate medical treatment and a medical team requires instant access to confidential/restricted medical files, such as the patients medical history. Considering this situation, we introduce the concept of *System Flexibility* to open the access path to the required medical records based on the needs of the current crisis situation. We call this *Need-Based Access Rights*.

Need-based Access Rights intends to ease sharing of confidential information between actors and different ES, introducing flexibility into the process of receiving information.

In figure 4.2, a medical team needs access to information and medical records for a specific patient. With a system such as SEMS, the medical team is able to make a personal request to a different EOC. However, the response time in such a system cannot be guaranteed and during the time it takes for the third party to respond to the request, the patients situation may further decline.

Disaster type	**Information need**	Rescue team	Fire brigade	Police	Medical team	Gas	Water	Electri-city
Disease outbreak Chemical Spill	• Patient medical records • Geo-information	X			X		X	
Terror attack Explosion	• Criminal records • Terrorist identity • Patient medical records	X	X	X	X	X		
Bomb threat	• Suspect identity • Information on suspect • Bomb location		X	X	X	X		
Hurricane Tsunami	• Disaster area	X	X	X	X	X	X	X

Figure 4.3: Flexibility and Security

In a crisis situation, various groups of users may need elevated access rights in order to satisfy their unique information needs. To enable quick adjustment to the changing access needs of the various groups, CMISS is able to automatically elevate a groups' access rights when a crisis occurs.

Depending on the type of crisis situation, each group is mapped with a set of predefined access right elevations. When the crisis occurs the group is automatically given these elevated access rights for the duration of the crisis. See figure 4.3.

In addition to the elevated access rights, actors of each group should be able to request information as per usual.

4.3.1 Access Rights during Crisis Situations

In this section we will detail some crisis situations and the information flows that may be needed for all field agents to be able to handle the crisis in the best way possible. To enable these information flows, CMISS elevates access rights for information exchange between several ES and from ES to field agents.

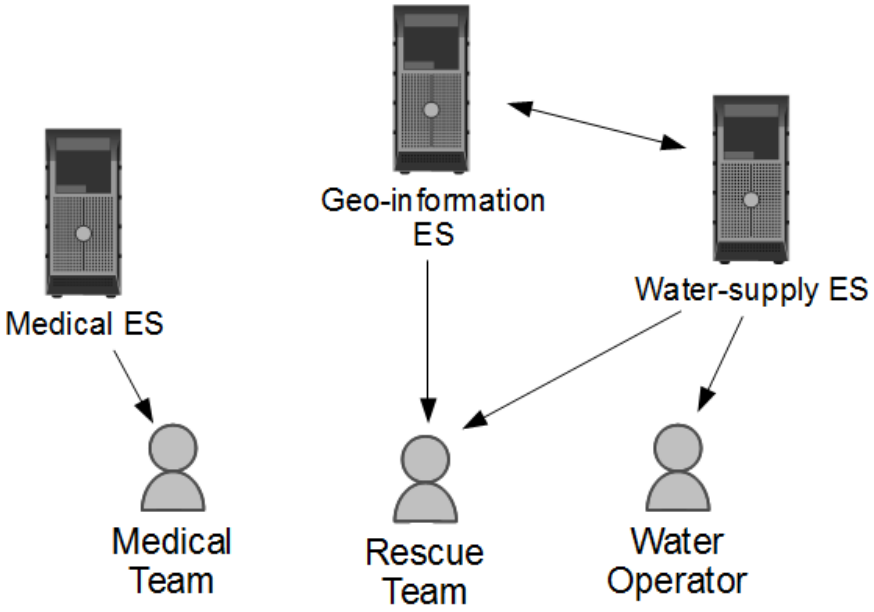

Figure 4.4: Access rights during a Chemical spill crisis

During a Chemical spill, see Figure 4.4, the spread and impact of the spill must be contained and affected people may need to be treated.

A Geo-information ES (GIS) is responsible for knowledge of the area and predicting how the chemical will spread through water. This information is relayed to a Water supply ES, which a water operator may analyze to decide when to recommend citizens in which areas to avoid using tap water or to shut off the water supply entirely. If water supply is shut off this information is relayed back to the GIS for use in further predictions.

The GIS information is also relayed to rescue teams so that they may know which areas have been or are likely to be affected.

Finally a Medical ES receives information about e.g. the type of chemicals spilled which is then relayed to medical teams.

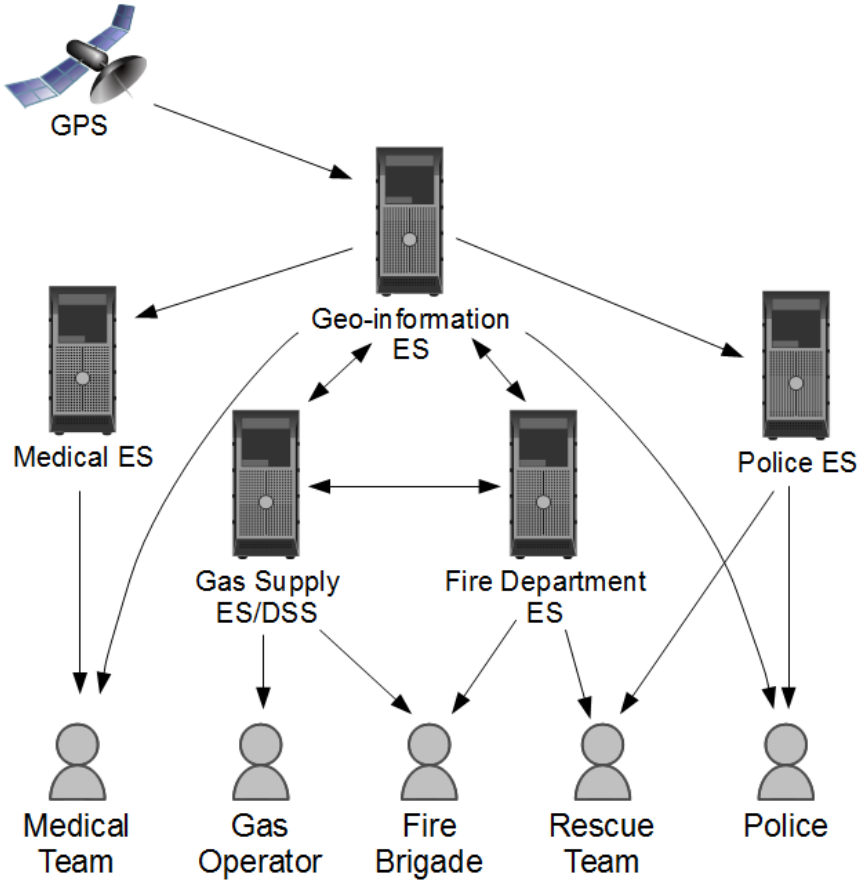

Figure 4.5: Information Flow during Explosion, Terror Attack or Natural Disaster

When an explosion, terror attack or natural disaster occurs, the damage needs to be contained, injured people must be treated and any fires must be handled.

A GPS system sends the locations of explosions, fires and other incidents to a GIS. The GIS then relays this information to other ES, see Figure 4.5. Fire brigades, police, rescue teams and medical teams act based on the information received from their respective ES. Additionally, as the rescue team needs to work in the field, they need to receive information from the GIS and the Police ES on field hazards such as ongoing panic, riots, fires and terror suspect locations.

The Fire department ES and the GIS relays information on explosions and fires to the Gas supply ES and DSS, which a gas operator may use to determine the risk of further fires or explosions cased by gas, and to take decision on whether to shut off gas supply to certain locations.

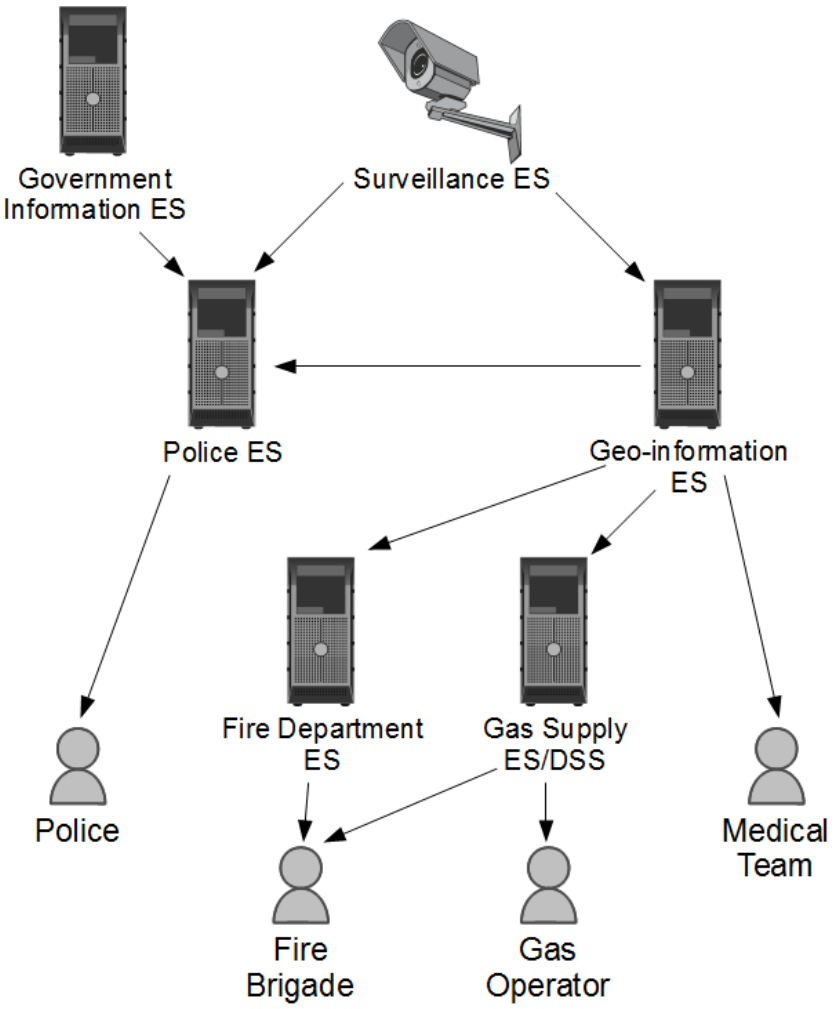

Figure 4.6: Information Flow during a Bomb threat crisis

During a bomb threat, see Figure 4.6, police are needed to handle the situation and prevent an explosion. Fire brigades, medical teams and rescue teams may also need to be on-site in case of an explosion. If there is a suspect, his location needs to be kept track of and relayed to all field agents.

Surveillance systems are used to locate the identity of the suspect and his location. This information is relayed to the Police ES and the GIS. The GIS relays the information to the medical team, the Fire Department ES and the Gas supply ES. A gas operator may decide to preemptively shut off gas to the location to minimize potential damage. Fire brigades act based on information from both of these ES.

Information on the suspect may need to be relayed to police field agents, such as criminal history. Data on the suspect may be fetched from Government information systems to the Police ES which the police can then access.

4.3.2 Access Rights and Security

Granting of access rights to various components in CMISS can be achieved through:

- Physical Security
- Role based access control
- Need based access control
- Higher security on sensitive data
- On demand, minimal channel will be used to exchange data
- In event of a system breach, restriction over sensitive data

4.3.3 Method of Access Rights Elevation during a crisis

In this section we will present a suggestion for how to implement the Access Rights Elevation during a crisis situation, using the access control system in Linux by adding groups to a user.

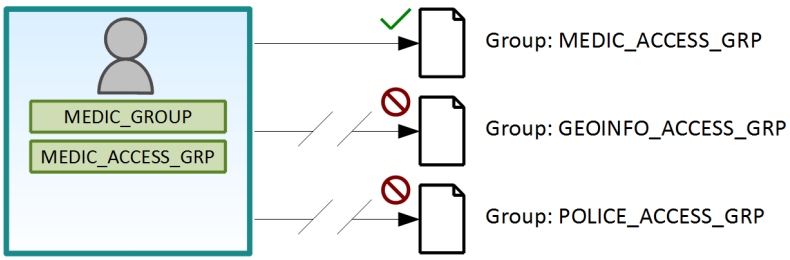

Figure 4.7: User access groups pre-crisis

Figure 4.7 shows a user during a normal situation. The user in this case is part of a medical team which is indicated by the user belonging to MEDIC_GROUP user group. In addition, he has the *access group* MEDIC_ACCESS_GRP which allows him to access any file which has this group as its owning group. In this example, every file in CMISS belongs to an access group depending on which type of user should be able to access the file, as seen in the picture where the two files that the user cannot access belong to the GEOINFO_ACCESS_GRP and POLICE_ACCESS_GRP respectively.

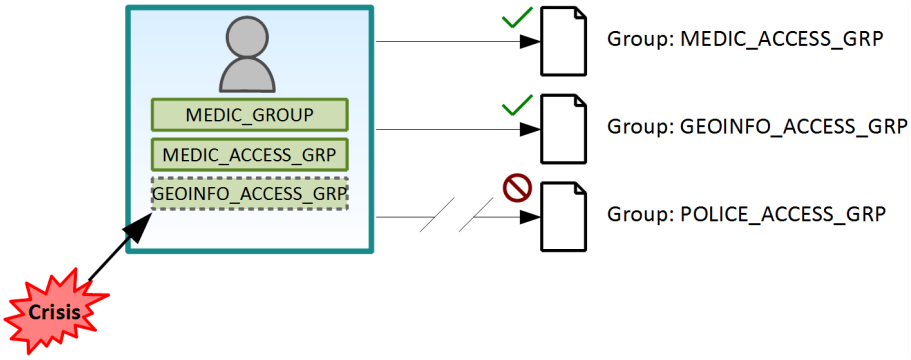

Figure 4.8: Access Rights Elevation during a crisis

When a crisis occurs, the user may need elevated access rights depending on the type of crisis as described in section 4.3. Let us assume an explosion has occurred and the medical user needs access to location data from the Geo-information ES. In this case CMISS adds the GEOINFO_ACCESS_GRP to the user, see figure 4.8. After the change has occurred, this will allow the user to access any file which has this group as its owning group, in effect giving the user access to the requested documents.

Finally, after the crisis situation is no longer in effect, the elevated access rights are to be removed.

4.4 Personnel Accountability

Accountability is an important requirement for CMISS. In order to ensure accountability, details on all parties connected to the system, such as their usage of CMISS, usage of data retrieved from CMISS and further information such as their location and movements, will be collected and stored for future reference. This will ensure that all connected parties and all communication with and use of the system can be accounted for at any time.

The collected data will be stored in log files, which will in turn be submitted to CMISS forlog management.

Examples of data which will need to be collected are:

- Names, personal details and access levels of each connected party
- Start and end times and other details for each connection
- GPS coordinates of connected parties
- Details of each transaction with the system
- Details on the usage of requested data, wherever technically possible

4.5 Information Security Principles

In Information Security, many different principles must be considered to ensure security of the information in a system[8]. The most important principles are Confidentiality, Integrity and Availability. These and the other required components are listed in Figure 4.9.

Confidentiality	Integrity	Availability
Log Management	Authentication and Authorization	Reliability
Non Repudiation	Access Control	Safety

Figure 4.9: Information Security Principles

The components in Figure 4.9 are briefly explained in the following sections, along with our chosen solution for each component.

4.5.1 Confidentiality

The protection and disclosure of information in electronic media from unauthorized people and processes, through methods such as encryption, even if data is captured by unintended parties. In CMISS, confidentiality can be achieved through [1,15,16]:

- Access restriction:
  - Physical access restrictions (badge to enter the control rooms for example)
  - Log-in credentials
  - Role based (definition of) user access rights and privileges for access to the CMISS
  - Firewall
- Encryption / Cryptography:
  - Message encryption
  - Protected communication channels (VPN, encrypted communication channels, key wrapping)
  - Key distribution
- Signature:
  - Digital signature

4.5.2 Integrity

The method that assures that received data is the same data which has been sent from sender, implying data has not been modified during transmission. In CMISS integrity can be achieved through

- Check sum. Hash function using SHA-256 algorithm is proposed.
- Insertion of validity parameter, such as time stamps, source identification, validity duration
- Use of Validated or Trusted Channels. Protected communication channels using end-to-end encryption and key wrapping.

4.5.3 Availability

Ensures and enables the authorized access to required information, by users at all times as necessary. The system have to be protected by security solutions through proper parameters. In CMISS, availability can be achieved through [7, 9]:

- Hardware security such as double power supply, RAID arrays .
- Replication of information systems or duplication of databases.
- Regular data backups on a remote site.
- Procedures for backups and restoration.
- Protection against viruses by using anti-virus and anti-spyware software.
- Virtualization technology can be used to host processes. Using migration of virtual machines, services can be relocated to other physical hosts if one stops working. Examples of such software is VMWare.

But still there is a big challenge for availability that comes through malicious behaviors such as Denial of Service (DoS) and Distributed DoS attacks. A DDoS protection system is discussed by Park [10].

4.5.4 Log Management

The storage of all incidents in a network is mandatory for future analysis. In CMISS, log management can be achieved by system management tools such as a Security Event Manager (SEM) which not only provides intrusion detection, anomaly detection and better correlation but also provides a deep level of event analysis[11, 12].

4.5.5 Authentication and authorization

Ensures that users have access to resources on the network through proper validation and right management. In CMISS, One Time Password (OTP), Digital signature and Valid Certificate can be used to achieve authentication and authorization.

4.5.6 Reliability

Ensures the balance of expected outcomes and actual results of the network services. In CMISS high reliability is a major factor and system design will ensure that.

4.5.7 Non Repudiation

For communication between sender and receiver, necessary steps must be taken to withhold non repudiation. In CMISS, this is achieved by using digital signatures.

4.5.8 Access Control

Granting of access rights to various components in network systems. In CMISS, this will be achieved through

- Physical Security
- Role based access control
- Digital signature, time limited valid certificate and x.509 certificates are proposed to handle the identities of user and nodes. MAC and IP filtering is also proposed.

4.5.9 Safety

For the system its must to have physical and technical safety protection. In CMISS this will be achieved by:

- Physical security of the system
- Backups
- Virtualization technology can be used to ensure up-time of vital processes (see 4.5.3)

4.6 Key Management

Key selection and management is one of the key issues in CMISS. Keys were chosen here by considering attack vectors of varying complexity, from brute force attacks to quantum computers. For Symmetric key generation AES-256 is proposed, for asymmetric key generation Elliptic Curve Cryptography (ECC) with SHA 384 bit keys are proposed. Key wrapping is proposed in communication channels. These key definition meet the requirements to handle data of all levels of confidentiality[13, 14].

Information should have priority level according to their type such as how sensitive information is along with time period, see Figure 4.1. Priority levels are 1=High, 2=Medium or Moderate, 3=Low.

Information Type	Description	Confidentiality	Integrity	Availability
Sensitive and durable data	Long-time duration	1	1	1
Sensitive short-term data	Useful during a current event	1 or 2	1	1
Non-sensitive data	Publicly available information	3	3	1 or 2 or 3

Table 4.1: Flexibility and Security

4.7 Use cases

The use of CMISS across a crisis event can be seen in terms of the four crisis stages, see 2.2.

4.7.1 Prodromal Crisis Stage

The use of CMISS in this stage largely depends on the ability of the connected ES to determine when a crisis is about to occur. When an ES detects indications that a crisis may occur, this information will be processed and sent to the DSS. The Decision Makers will then determine if the organization should enter the Prodromal Crisis Stage.

During this stage, a crisis has yet to occur, so the Need-based Access Rights system (see 4.3) may not have been activated. The decision makers may activate the system if the crisis is certain or unavoidable, in the case of for example an earthquake, hurricane or flood.

There may also be specific needs for specific crisis situations. In the case of for example a bomb threat, access to information about the suspect might be elevated to certain roles which may need the information to make a quick decision. For example, access to criminal and medical history to determine the probable actions of the suspect can be distributed to certain actors or roles, whereas the system security ensures other actors cannot access the data.

4.7.2 Acute Crisis Stage

During this stage CMISS will assist the organization in managing the ongoing crisis. This is accomplished through the connection between the various ES and the DSS which will assist the Decision Makers in the management of resources. Need-based Access Rights (see 4.3) will assist in providing actors with fast access to the data that they may need from CMISS and provide the organization with increased flexibility to handle the unique crisis situation.

4.7.3 Chronic Crisis Stage & Crisis Resolution Stage

During the Chronic Crisis Stage the crisis has passed and the organization is recovering from the damage caused. As there is no longer likely to be any emergencies, user groups will likely not retain their elevated access rights. CMISS can at this point be used to

access the information from the various ES. In the Crisis Resolution Stage the impact of CMISS has passed since the organization has fully recovered from the crisis.

5

Results

We have proposed the CMISS system design which aims to be robust, scalable and flexible. CMISS meets the security needs of a system in todays technological environment. Space has been left for further necessary additions to meet the changing security needs of the future.

The present system consists of different security levels and includes options for the adjustment of security levels. This is done by using elevation of information sharing and information flexibility according to needs, while leaving options for the decision makers to restrict information if any system breach or other threat is encountered.

Exchange of sensitive information between different components over a network is becoming a day-by-day challenge to keep it up to date on an advanced level. We have considered the importance of information security and system flexibility for the crisis management system.

6

Conclusion

Exchange of sensitive information between different components over a network is a crucial part of Information Systems and needs to be highly secure. In this study, we have defined the various components of Information Security, and proposed an implementation solution for a Crisis Management Information Security System (CMISS). The CMISS is designed to be secure enough to handle confidential information [10] and to be able to manage the changing needs on security and availability of a dynamic crisis situation.

We have proposed a system which aims to be secure and dynamic by ensuring access control, need-based access rights, flexibility, higher security on sensitive data, system will use minimal channels for information exchange based on situation and if system get breached, restrictions over accessing sensitive data will be in effect. For each security aspect, we have proposed precise implementation details and methods.

7

Future Work

As technology improves and changes at an ever increasing speed, in parallel security vulnerabilities are increasing linearly. For the time being, a few security areas that currently have some space for improvement. However, for some attack vectors, such as availability attacks like DDoS attacks, complicated set-ups are required to protect against these and are still not possible to completely secure against [7]. The system must also be thoroughly secured against common attacks such as SQL injection and cross site scripting.

In the future, currently unknown attacks will need to be considered and the system will need to be updated to protect against these vulnerabilities. Threats such as quantum computer based attacks must be considered as the technology becomes available. Adjusting for these needs should not prove difficult as the system is scalable and robust.

Bibliography

[1] Y. Vural, E. Ciftcibasi, M, and S. Inan, "Information security in maritime domain awareness," 2010.

[2] M. Shaluf, I, F. Ahmadun, and M. Said, A, "A review of disaster and crisis," *Disaster Prevention and Management*, vol. 12, no. 1, pp. 24–32, 2003.

[3] S. Fink, *Crisis Management – Planning for the Inevitable.* American Management Association (AMACOM), 1986.

[4] A. Paraskevas, "Crisis management or crisis response system? a complexity science approach to organizational crises," *Management Decisions*, vol. 44, no. 7, pp. 892–907, 2006.

[5] F. Tipton, H and M. Krause, *Information Security Management Handbook, Sixth Edition.* CRC Press, 2007.

[6] *SEMS Guidelines - Standardized Emergency Management System.* OES California Governors Office of Emergency Services, Sep 2008.

[7] M. Couturier, F. Gallet, J, and M. Sizun, J, Oct 2006.

[8] "Information security," Jan 2012. [Online]. Available: http://en.wikipedia.org/wiki/Information_security

[9] "(2006) information security for field workers in crisis situations," Dec 2008.

[10] K. Park, "Scalable protection against ddos and worm attack," 2004.

[11] "Security event manager," Jan 2012. [Online]. Available: http://en.wikipedia.org/wiki/Security_event_manager

[12] IBM, "Security event and log management service: Comprehensive, cost-effective approach to enhance network security and security data management," Dec 2007.

[13] E. Barker, "Suite b cryptography," March 2006.

[14] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management – part 1: General (revised)," March 2007.

[15] R. Hiltz, S, B. Van de Walle, and M. Turoff, "Information systems for emergency management," 2009.

[16] A. Arabo, M. Kennedy, Q. Shi, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Identity management in system-of-systems crisis management situation," 2011.

[17] J. Arber, D. Cooley, S. Hirsch, M. Mahan, and J. Osterritter, "Network security framework: Robustness strategy," 1999.

[18] B. Vani, A. L, A. Persia, and S. Sivagowry, "Inhibition of denial of service attack in wlan using the integrated central manager," *International Journal of Computer Applications; 29(8)*, vol. 29, no. 8, pp. 28–33, Sep 2011.

[19] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 2nd ed. Prentice Hall, Nov 2011.

[20] "Federal information procession standards publication (2009) digital signature standard (dss)," June 2009.