



University of Modena and Reggio Emilia
ICT Doctorate School



Security Issues in Emergency Networks

Alessandro Paganelli and

Maurizio Casoni

`alessandro.paganelli@unimore.it`

`maurizio.casoni@unimore.it`

IWCMC

Goal

The main goal of this presentation is to present a review of the main security properties that characterize an emergency network.

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

Emergency networks

- An *emergency response system* is a complex ICT system whose mission is to help and improve the coordination of the emergency response.
- An *emergency network* is the telecommunication infrastructure of an emergency response system.
 - It shares most of the requirements of a traditional computer network.
 - Some requirements, specific to emergency networks, are also present.

Functional requirements

From [1], the main functional requirements for emergency networks are:

- reliability, availability and survivability
- authentication and authorization
- information confidentiality
- scalability
- interoperability
- QoS support
- mobility support

The system architecture design means the “translation” of these requirements into a set of technologies and protocols.

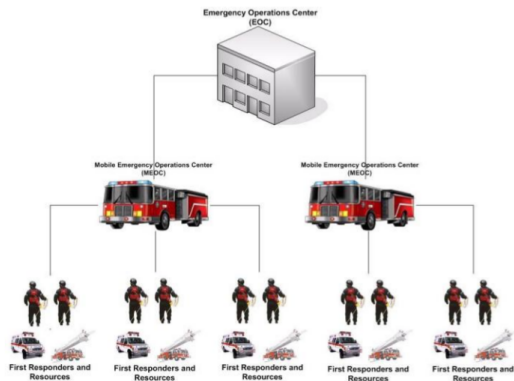
- Some of them are actually *security* requirements.

EU Large Scale Integration project

“A holistic approach towards the development of the first responder of the future” [2] is an European FP7 large scale integrated project that aims at the design of a complete emergency response system, by adopting the most promising ICT technologies currently available.

- To make a solid design, security needs to be considered since the very beginning.
- Our research activity about security is conducted within this project.

Reference Emergency Network Architecture



Three layers network:

- 1 Emergency Operation-control Center (EOC)
- 2 Mobile EOCs (MEOCs)
- 3 First Responders (FRs)

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties**
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

Generic security properties

The main security properties characterizing a computer network/system are:

- 1 Simple/mutual authentication
- 2 Data confidentiality
- 3 Data/origin authentication
- 4 Authorization and accountability
- 5 Data integrity
- 6 Non repudiation
- 7 Availability

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks**
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

The main goals of the following slides are:

- 1 Present a possible attacker scenario for emergency networks
- 2 Review the previous security properties from the emergency network point of view
- 3 Propose some possible solutions

Attack scenarios and security requirements

Possible attacker goals:

- 1 exploiting the crisis event for personal gain
 - e.g., access to healthcare data of the people involved
- 2 make the emergency response ineffective
 - e.g., terrorist attack

These attacks can be considered as *intrusion*, *data sniffing* and *denial of service*.

These examples suggest that confidentiality, availability, authentication and authorization represent the main security requirements for an emergency network.

Authentication

Authentication is one of the most important properties in emergency networks, because it has a significant effect on the design of the whole system.

Main requirements:

- Quick and simple
 - Tradeoff between security and usability (e.g., biometric, 2/3 factors)
- Viable in the case of network disconnection
 - In the worst case, two nodes should be capable to authenticate each other without using a third party.
- Interoperable

Our vision:

- Identity-based cryptography
 - Asymmetric crypto that uses public information (e.g., email address) as the public key
 - A centralized node (Private Key Generator) is needed to generate the private keys that can be used with the public ID. This node is needed only at the setup phase.
- “Web-of-trust”-like solutions
 - De-centralized solutions where each node digitally signs the public key of each other trusted node.
 - Two nodes that need to communicate have to find a “trust path” (by searching through the certificates they have) connecting them.

Data confidentiality

Implemented by means of cryptographic techniques.

The actual choice depends on:

- The transmission standard adopted
 - In fact, every standard provide its own crypto solution.
- The scope required for confidentiality (i.e., end-to-end or local)
- The presence of additional requirements (e.g., QoS)
 - QoS classification requires “cleartext” packets for inspection!

Data confidentiality

Our vision:

- Cryptography implemented at data-link layer with local scope for each network segment
- Implemented by means of IPsec for end-to-end scope
 - IPv6 Class and Flow fields can be used for QoS classification.

Availability

Can be enhanced by adopting redundant solutions, increasing the total number of alternatives available to serve each service request.

Our vision:

- As for computer systems: adopt replicas and caching
- As for the network: implement redundant links (i.e. more paths) and redundant technologies (which also increases interoperability)

Authorization and accounting

Authorization/access control and accounting can be usually found together with authentication (AAA servers).

In some cases they can be found separated from authentication (e.g., traffic filtering and logging).

Our vision:

- Network access:
 - Centralized access control and logging
 - Centralized traffic shaping and filtering
- Applications:
 - Server side access control
 - Client and server side logging

Data authentication, integrity, non repudiation

These features are implemented in almost every security protocol suite.

- At low layer, e.g., IEEE 802.11 and IEEE 802.16
- At high layer, e.g., IPsec and SSL/TLS

The actual choice depends on the technologies adopted for the implementation. Moreover, they have a limited effect on the network design.

Our vision:

- Local scope: both low-layer and high-layer solutions
- End-to-end scope: high-layer solutions (e.g., IPsec or SSL/TLS)

- 1 Introduction to Emergency Networks
- 2 Generic Security Properties
- 3 Security in Emergency Networks
 - Goal
 - Attacker scenario
 - Security properties
- 4 Conclusions

Conclusions

- In this paper we presented our security analysis for emergency networks.
- We found that authentication, confidentiality and availability affect the network design in a significant way.
- On the other hand, the remaining properties have only limited impact on the network design.

Thank you!

Questions?



Alessandro Paganelli

`alessandro.paganelli@unimore.it`

Special acknowledgment:

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° [242411].

References

-  [1] Statement of Requirements (SOR), Volume one and two, available online at: <http://www.safecomprogram.gov>
-  [2] G. Calarco, M. Casoni, A. Paganelli, D. Vassiliadis and M. Wodczak, “A Satellite based System for Managing Crisis Scenarios: the E-SPONDER Perspective”, 5th Advanced Satellite Multimedia Systems Conference and 11th Signal Processing for Space Communications Workshop, Cagliari, Sept. 13-15 2010.