CERT
Emergency Network

UNIVERSITEIT VAN AMSTERDAM

SURFnet

G.A. van Malenstein
R.P. Vloothuis

Supervisor: J. Meijer

Introduction

- Introduction to CERTs
- Key problem
- Main research question
- Research methods
- Organizational problems
- Technical solutions
- Deployment
- Conclusion
- Future work

CERTs

- Computer Emergency Response Team
- 1st CERT 1988 after worm attack
- No hierarchy between CERTs
- Communication structure
  - Pagers, mobile phones and mailing lists
- No Emergency Communication plan
- GOV-CERT, SURFnet-CERT, UvA-CERT
- Formal structure: SURFnet, UvA, OS3

Key problem

- CERTs communicate by Internet and by (mobile) telephones
- KPN introduces an All-IP network
- No communication possible in case of an emergency
- Example 1: SURFnet
- Example 2: CISCO

Main research question

- *Which ways of communication can be used for the CERTs for mutual communication when the regular communications networks (Internet, telephone) fail?*

Organizational problems

- No official communication structure in case of emergency
- No overall chart of CERTs
- Who has to communicate with whom?
- Point-to-point communication requires communication plan
- No priority given by CERTs

Technical solutions

- Requirements
  - Scalable
  - Flexible
  - Affordable
  - Physically separated from the Internet
  - Available

Technical solutions

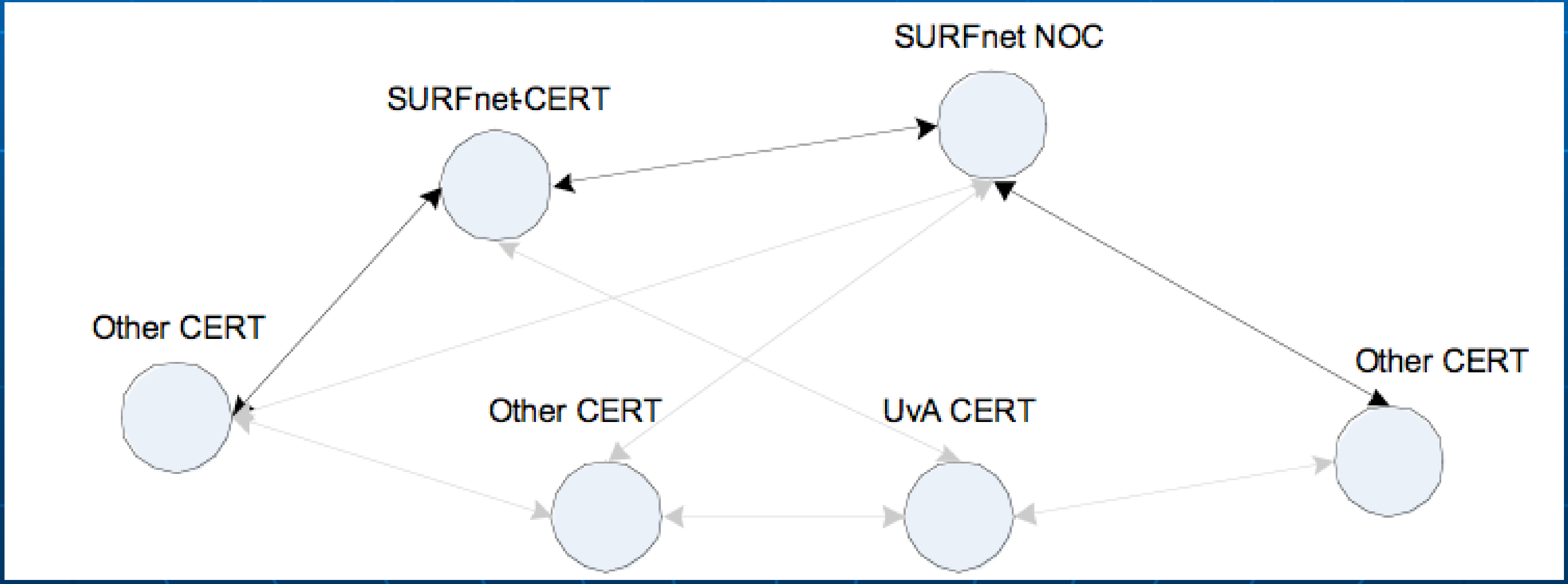
- TETRA
  - Mobile units and masts
  - C2000, MCCN
- KPN Emergency Network
  - PSTN -> All-IP
  - Not a mobile network
  - 6000 connections
- Radio
  - Amateurs, packet radio
- WiMAX
  - 4th Generation Mobile Services
- Satellite communications
  - Flexible, affordable

Overview

	Scalable	Flexible	Affordable	Separated network	Available
TETRA	+	0	--	+	+
KPN Emergency Network	--	-	0	-	0
Radio	-	+	++	++	+
WiMAX	+	0	-	-	-
Satellite	++	++	+	+	++

Solution direction

- 6 mobile satellites units:
  - € 9.000,00 total non-recurring costs
  - € 20,00 per CERT is charged
    - Total of € 1.440,00 per year
- In case the Emergency Network is used, the costs of calling by satellites phone are € 1,00 per minute



Deployment

- To deploy an Emergency Network, the following steps have to be taken:

1. Organize a meeting with at least 2 CERTs
2. Create agreements on how the network is set up
3. Describe these agreements in a communication plan
4. Connect all participating CERTs to the satellite network
5. Add all CERT names and numbers to the communication plan
6. Update and distribute the communication plan on a frequent basis
7. Get more CERTs interested to participate in the arisen Emergency Network; start again at step 1.

Conclusion

- *Which ways of communication can be used for the CERTs for mutual communication when the regular communications network (Internet) fails?*

- Satellite communication, best solution:
  - Completely separated network
  - Always worldwide available
- No communication structure between CERTs in case of (partial) failure of the Internet:
  - Communication plan needed.
    - All procedures and (mobile) satellites phone numbers of the participating CERTs
- No priority, CERTs have to take action now!

Future Work

- Communication plan
- Further research technical solutions
- Open dialog with radio amateurs
- Research security aspect

The End

- Any questions?