In this chapter an introduction to gametheory will be given with the formulas that will be used troughout this paper. We start with the basics of gametheory. People that have a background in gametheory can skip this chapter.

1 Virusses

Many network security threats today are spread over the Internet. The most common include:

Viruses, worms, and Trojan horses Spyware and adware Zero-day attacks, also called zero-hour attacks Hacker attacks Denial of service attacks Data interception and theft Identity theft

Computer virus through mail. Though virus spreading through email is an old technique, it is still effective and is widely used by current viruses and worms. Sending viruses through email has some advantages that are attractive to virus writers: Sending viruses through email does not require any security holes in computer operating systems or software. Almost everyone who uses computers uses email service. A large number of users have little knowledge of email viruses and trust most email they receive, especially email from their friends [28][29]. Email are private properties like post office letters. Thus correspondent laws or policies are required to permit checking email content for detecting viruses before end users receive email [18].

Send a email with malicious attachment. Only again infected if attachment again opened. Thus this is the action of attacking every neighbour node + also can attack again the node where the virus was coming from. There are also email viruses were the malicious program is hidden in the txt and the attachment does not need to be opened.

1.1 What are my topics

- Security, Costs, Cybersecurity
- Viruses, kinds
- Gametheory
- Flip-it
- Flip-it multiple resources
-

1.2 Malware

Relevant researches:

-

2 Conclusion

The final section of the chapter gives an overview of the important results of this chapter. This implies that the introductory chapter and the concluding chapter don't need a conclusion.