Abstracts

1. *What are abstracts and why do we write them?*

2.
Abstracts are very common in academic writing, and they have a fairly standard form. Which essential parts should an abstract consist of?

3. *Watch the following abstract of Grant Barclay and analyse its structure and characteristics:*
http://www.inholland.nl/INHOLLANDCOM/Studying+at+INHOLLAND/Events/Diverse2008/Papers+abstracts+and+posters/Papers+abstracts+and+posters.htm

4. *Read the abstracts below and identify their parts.*

(a)
(1) The present study was conducted to determine the prevalence of *Listeria monocytogenes* in smoked fish in Sokoto, Nigeria. **(2)** A total of 115 different species of smoked fish from the various retail outlets and market places within the metropolis were analysed for the presence of *L. monocytogenes* using ISO culture method. **(3)** Out of the 115 samples analysed, 29 (25%) were positive for *L. monocytogenes*. **(4)** Other Listeria species isolated in this study are *L. grayi* 13 (11%), *L. innocua* 10 (9%) and *L. ivanovi* 15 (13%). **(5)** The remaining 48 (42%) of the sample were negative for Listeria species. **(6)** The study shows that *L. monocytogenes* and other *Listeria* species are common contaminant of smoked fish, and this may pose serious public health implications. (Salihu et al., 2008)

(b)
(1) Personalized Web applications automatically adapted for different clients and user preferences gain more importance. **(2)** Still there are barely technologies to compensate the additional effort of creating, maintaining and publishing such Web content. **(3)** To address this problem, this paper introduces a declarative, component-based approach for adaptive, dynamic Web documents on the basis of XML-technology. **(4)** Adaptive Web components on different abstraction levels are defined in order to support effective Web page authorising and generation. **(5)** Hierarchical document components playing a specific semantic role are also defined. **(6)** The hyperlink view for defining typed links is spanned over all component layers. **(7)** Beside the reuse of both implementation artefacts and higher level concepts, the model also allows to define /sic./ adaptive behaviour of components in a fine-granular way. **(8)** As a further benefit the support for ubiquitous collaboration via component annotations is introduced. **(9)** Finally, the stepwise pipeline-based process of document generation is introduced and performance issues are sketched.

(Adapted from: Štěpánek, L., deHaaf, J., Hradilová, A.(2011): p.172; (Fiala et al. 2003:58) UVT seminar, 1.11.2011)

5. *Read the abstracts above again and identify words or groups of words in each sentence that determine the sentence function.*

6. *Fill in the table with appropriate abstract characteristics.*

Abstracts are usually written in tightly worded sentences which	
prefer ► …… (verb tenses) ► …… (verb voice) ► …… (verb person) ► ……... (number of words) ► …… .(length of sentences) ► …… ► ……	**avoid:** ► …… ► …… ► …… ► …… ► …… ► …… ► ……
in short: Abstracts eliminate redundancy.	

(Adapted from: Graetz (1985) in Swales, J.M. (1990): Genre Analysis: English in Academic and Research Settings.)

7. *Read the following abstracts and analyse their quality focusing on the clarity of the message expressed by verbs.*

7.1. Using of Time Characteristics in Data Flow for Traffic Classification

This paper describes a protocol detection using statistic information about a flow extended by packet sizes and time characteristics, which consist of packet inter-arrival times. The most common way of network traffic classification is a deep packet inspection (DPI). Our approach deals with the DPI disadvantage in power consumption using aggregated IPFIX data instead of looking into packet content. According to our previous experiments, we have found that applications have their own behavioral pattern, which can be used for the applications detection. With a respect to current state of development, we mainly present the idea, the results which we have achieved so far and of our future work.

7.2. Aspect-based Attack Detection in Large-scale

In this paper, a novel behavioral method for detection of attacks on a network is presented. The main idea is to decompose a traffic into smaller subsets that are analyzed separately using various mechanisms. After analyses are performed, results are correlated and attacks are detected. Both the decomposition and chosen analytical mechanisms make this method highly parallelizable. The correlation mechanism allows to take into account results of detection methods beside the aspect-based detection.

7.3. Security Monitoring of Building Automation and Control Networks

This paper presents an approach to monitor network traffic in a building automation and control networks to detect security incidents. We focus especially on Building Automation and Control Network (BACnet) protocol used as the standard for communication in such networks. In the paper we propose a framework covering network data observation, mappings enabling transfer of the BACnet communication specific information via IP Flow Information eXport (IPFIX) protocol and data collection with the IPFIX collector.
Flow monitoring became a useful technology for detection of security incidents in a large IP networks. It allows to analyse flow of the data passing through the network instead of inspecting context of each packet. However control and automation networks often basically differ from common IP networks, they face similar issues and security threats. We are basing on this similarity and applying flow approach for network security monitoring of the automation and control networks.

7.4. A Flow-level Taxonomy and Prevalence of Brute Force Attacks

Online brute force and dictionary attacks against network services and web applications are ubiquitous. We present their taxonomy from the perspective of network flows. This contributes to clear evaluation of detection methods and provides better understanding of the brute force attacks within the research community. Next, we utilize the formal definitions of attacks in a long-term analysis of SSH traffic from 10 gigabit university network. The results shows that flow-based intrusion detection may profit from traffic observation of the whole network, particularly it can allow more accurate detection of the majority of brute-force attacks in high-speed networks.

7.5. Embedded Malware – An Analysis of the Chuck Norris Botnet

This paper describes a new botnet that we have discovered at the beginning of December 2009. Our NetFlowbased network monitoring system reported an increasing amount of Telnet scanning probes. Tracing back to a source we have identified world wide infected DSL modems and home routers. Nowadays, various vendors use Linux in this kind of devices. A further investigation has shown that most of deployed SoHo (small office/home office) devices use default passwords or an unpatched vulnerable firmware. Some devices allow a remote access via Telnet, SSH or a web interface. Linux malware exploiting weak passwords allows fast propagation and a virtually unlimited potential for malicious activities. In comparison to a traditional desktop oriented malware, end users have almost no chance to discover a bot infection. We call the botnet after Chuck Norris because an early version included the string *[R]anger Killato : in nome di Chuck Norris* !

7.6. NetFlow Based Network Protection

Protecting network perimeter against adversaries both from inside and outside is a crucial task for nowadays network administrators. Inspecting all network traffic by traditional deep packet inspection is very resource intensive task in high speed networks and scalable solutions are needed. In our work, we describe network protection system based on NetFlow data. It uses hardware accelerated monitoring center (HAMOC) for inspecting network traffic, generating NetFlow data and also for active filtration/blocking of malicious traffic. Active network protection use case against brute force dictionary attacks is presented and also other network protection use cases are discussed. Main contribution of this work are: (i) scalable solution suitable for current high-speed networks (10 Gbps and more), (ii) use of hadrware accelerated HAMOC platform performing both monitoring and traffic filtering, (iii) light-weight alternative using software tools instead of hardware platform suitable for protection of networks with lower amount of traffic.