

## Study programme: Information and IT security

### Proposed topics of Master's thesis

2018.10.07

Topic	Description, requirements
	* More details will be provided upon request. Contact supervisor or consultant.
<b>Lecturer Vitalijus Gurčinas</b> <a href="mailto:vitalijus.gurcinas@vgtu.lt">vitalijus.gurcinas@vgtu.lt</a>	
Short text corpus for stylometric analysis (unsupervised learning).	More details will be provided upon request. Contact supervisor or consultant.
Adaptive writeprint for stylometric research.	
Automated textual evidence collection.	
Writeprint-based plagiarism detection.	
Research of authorship anonymization tools (text feature modification, anti-stylometric methods).	
Methodology of authorship attribution accuracy evaluation according to author personality and context information.	
Virtualized infrastructure for ethical hacking.	
Deployable virtualized penetration-testing framework.	
<b>Prof. dr. Dalius Mažeika</b> <a href="mailto:dalius.mazeike@vgtu.lt">dalius.mazeike@vgtu.lt</a>	* More details will be provided upon request. Contact supervisor or consultant
Defending a cyber system with early warning mechanism	Due to the increasing reliance on networks, defending a cyber system is of vital importance. Mechanism of early warning for defending a cyber system that has become a key component of constructing network defense in practice. We should study the reliability of a system under attack from single or multiple sources. In particular, we will discuss the effect of an early warning mechanism on the system reliability. The optimal strategy for defending a cyber system with early warning components in the worst attack scenario must be proposed. The theoretical results must be validated by simulation.
Biological Approach to System Information Security	Biological systems employ an inherently multi-agent approach for protection from external biological assault. If properly modeled and expanded to computer networking systems, new systems for information security can be designed and adopted. These approaches would be efficient and effective at not only preventing systems failure and damage from known forms of attack, they would be able to detect and limit the damage from an unknown form of attack.
Intrusion detection using machine learning methods	An Intrusion Detection System (IDS) is a software that monitors a single or a network of computers for malicious activities (attacks) that

	<p>are aimed at stealing or censoring information or corrupting network protocols. Most techniques used in today's IDS are not able to deal with the dynamic and complex nature of cyber attacks on computer networks. Hence, efficient adaptive methods like various techniques of machine learning can result in higher detection rates, lower false alarm rates and reasonable computation and communication costs. Student must study several such schemes and compare their performance. Also be DOS attack must be simulated and IDS reliability must be tested.</p>
Detection of compromised software in the network computers	<p>Compromised computers are a significant problem for governmental agencies and corporations. The methods of detection such computers must be analyzed, compared and practical simulation and validation on methods efficiency must be performed.</p>
<b>Assoc. prof. Justinas Janulevičius</b> <a href="mailto:justinas.janulevicius@vgtu.lt">justinas.janulevicius@vgtu.lt</a>	<p>* More details will be provided upon request. Contact supervisor or consultant</p>
Business Process Management System Based on Smart Contracts	<p>Process-oriented management of business provides benefits of structured and traceable activities, responsibilities and workflows. What is more, business process management (BPM) provides various forms of formalizing such processes. Since formalization brings a structured framework for the description of such processes, there evolves an opportunity to automate them.</p> <p>Industrial automation, promoted as Industry 4.0, involves automation of never previously connected devices, thus bringing the concept of Internet of Things to rise. This not only helps to ensure adequate quality control in the production, but also serves as management automation and statistical data collection, enabling the highest maturity CMM processes (Level 5) that have an ability of self-learning and self-improvement.</p> <p>The only major open issues restraining from implementing these beneficial concepts into real-life systems until now have been the management of third-party contractual agreements and high implementation costs. However, since the introduction of blockchain and the following concept of smart contracts – the issue of contractual agreements and tampering with data seem to have found a solution. Introducing smart contracts into the business process management allows for the client to monitor the activities of the service provider in detail. Moreover, the client can be sure that the production data ledger is in its' original form due to the use of blockchain.</p> <p>The research aims at proposing a business process managing (e.g. executing, controlling, monitoring) system architecture based on smart contracts. The architecture shall provide integrity and traceability of execution of any process. The research results are to be deployed in the development of business process management system intended for commercial use. Such architecture also allows iterative processes management between two or more parties.</p> <p><a href="https://www.ibm.com/developerworks/library/mw-1705-auberger-bluemix/1705-auberger.html">https://www.ibm.com/developerworks/library/mw-1705-auberger-bluemix/1705-auberger.html</a></p>
User Interface Design Influence on Information Security	<p>Specific aspects of user-machine interaction lead to certain behavioral patterns that may encourage and/or allow various vulnerabilities. The research aims at defining the main categories of these features and analyze their influence on the overall security of the systems.</p>
Analysis of Social and Economic Factors in the Governance and	<p>Legislative aspects play an important role when it comes to the organizational management, especially in the form of constraints [cite].</p>

<p>Legislations of Information Technology</p>	<p>Based on legislations, certain processes may be encouraged, while others may not be allowed. Within the scope of European Union legislative framework, there are various types of legislations, however some, such as directives, may be adapted according to the regional needs, while others, such as regulations, are enforced Union-wide [cite].</p> <p>Certain factors cause the need for adaptation of these legislations. Most important of which are of social and economic nature [cite]. Recent developments in the Information Technology allows formalization of legislations, while ontological approach enables a non-linear analysis of the field.</p> <p>Information technology is one of the most dynamic fields that require governing and constrains. As new technologies appear very frequently, and the level of their disruptive power is high (e.g. cryptocurrencies), there is a need for a fast-response methodology to adapt centrally-issued legislations to local regional requirements and needs.</p> <p>This research aims at developing a methodology to extract and formalize the variables that depend on the social and economic factors in the field of Information Technology governance and to build a model, defining the influence of social and economic factors on these variables.</p>
<p>Cybersecurity Expert Calibration Based on the Cybersecurity Trend Forecasting</p>	<p>When considering a person “an expert”, it is assumed that the knowledge of the expert is unquestionable. However, when dealing with multiple experts, it is easy to notice that the opinions between them differ. Therefore, there is a need to define the level of sophistication of an expert. R. Cooke provides a method in “Experts in Uncertainty” for expert calibration, which, based on pre-defined facts, classified as “seed questions”, manages the weight of the experts, based on their knowledge of the domain. The research deals with the acquisition and application of this pre-defined information for expert weight assignment, which in this case is considered to be calibration.</p>
<p><b>Lecturer Paulius Narkevičius</b> <a href="mailto:paulius.narkevicius@vgtu.lt">paulius.narkevicius@vgtu.lt</a></p>	<p>* More details will be provided upon request. Contact supervisor or consultant</p>
<p>Research and design of 3D visualization based automated risk management system</p>	<p>Develop a prototype to improve the risk management process(es) using 3D visualization technologies.</p>
<p>Research and design of IT security process(es) using e-textile</p>	<p>Create a prototype to improve the IT security process(es) using e-textile.</p>
<p></p>	<p>Other IT safety topics related to visualization and risk research may be offered for consultation</p>
<p>Research and design for ensuring continuous work for IT security process(es) using e-textile</p>	<p>Create a prototype to ensure (partly ensure) power supply for e-textile based IT security process(es).</p>
<p></p>	<p>Other e-textile and IT security related topics can also be offered for consultation</p>
<p>Analysis of modern electronic security systems</p>	<p>Propose a way or method to improve the security of the modern electronic security system(s).</p>
<p>Research and design of modern electronic security system</p>	<p>Propose a method to improve the security of the modern electronic security system(s).</p> <p>Create a prototype, (pilot project) for demonstration of this method.</p>
<p></p>	<p>* More details will be provided upon request. Contact supervisor or consultant</p>

<b>Asocc. prof. Nikolaj Goranin</b> <a href="mailto:nikolaj.goranin@vgtu.lt">nikolaj.goranin@vgtu.lt</a>	
Optimization of rogue Wi-Fi access point detection methods in a 3D space (in a building)	
Analysis of attack tree optimization methods	
Development of the electronic voting protocol on the basis of blockchain technology	
Optimization of cyberattack methods with the help of genetic algorithms	
Development of a multicriteria method for selection of physical security and related (electric power supply, conditioning, etc.) controls for a datacenter	
Development of a neural network based method for „scientific spam“ detection	
Application of „Dead Hand“ principals in remote monitoring systems	
Investment into information security modeling on the organizational level	
Analysis of unmanned drones management protocols from the security perspective	
<b>Asocc. prof. Nikolaj Goranin</b> <a href="mailto:nikolaj.goranin@vgtu.lt">nikolaj.goranin@vgtu.lt</a> consultant <b>Dainius Čeponis</b> <a href="mailto:dainius.ceponis@vgtu.lt">dainius.ceponis@vgtu.lt</a>	* More details will be provided upon request. Contact supervisor or consultant
Analysis and processing of log files generated by the intrusion detection system.	The main task is to analyze OSSEC intrusion detection system generated log files and create the system capable of extracting malware changed specific files paths.
Heat map creation from malware generated system calls sequences.	The main task is to create a system that is capable of analyzing Windows OS system calls log files and create heat map for them. System calls sequences are generated by the malware and represents malicious.
Creation of a freely available malware cataloging system using the VirusTotal.com API.	The main task is to create a system capable of catalog freely available malware samples. Categorization is possible through malware hash values and public (or if more information is required - academic) API off VirusTotal.com database.