

Department	School of Computing
Supervisors	Prof. Leandros Maglaras, Prof. Bill Buchanan, Dr Naghmeh Moradpoor
Project Title	Novel E2E mechanisms for mobile devices
<p>PROJECT DESCRIPTION</p> <p>Using several messenger applications like Signal where data are not backed up or stored reduces the chance of messages being accessed, but the main problem of the data being created and consumed in cleartext on end devices remains. The bulk of the already available chat applications is primarily focused on the process of data transmission using an E2EE strategy (End-2-End Encryption method). An adversary can commit acts of technological violence by installing spyware within an application to accomplish a wide range of capabilities. These capabilities can include monitoring, changing, or accessing information or credentials that are saved on a person’s mobile device. When a mobile user accesses, edits, or otherwise manipulates data or credentials in any other way, one way to reduce the likelihood of a vulnerability of this kind arising is to use Multi-Factor Authentication techniques.</p> <p>This project aims on building on our previous E2E prototype mechanism in order to provide a holistic solution for securing mobile phones from eavesdropping attacks. The solution that will be developed should be able to be applied to any mobile phone operating system and be user friendly and robust against cybersecurity threats.</p> <p>Perspective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisors.</p> <p>Academic qualifications A first degree (at least a 2.1) ideally in Electrical/Electronic/Communications Engineering, Computer Science/Engineering, Mathematics with a good fundamental knowledge of Communication Principles, Digital Communications, Cryptography, Algorithms.</p> <p>English language requirement IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University’s policy are available online.</p> <p>Essential attributes:</p> <ul style="list-style-type: none"> • Experience of fundamental cryptography and cybersecurity • Competent in software development • Knowledge of communication principles, cryptography, algorithms • Good written and oral communication skills • Strong motivation, with evidence of independent research skills relevant to the project • Good time management <p>Desirable attributes: Team player, eager to learn new technologies, flexible and knowledge of R or Java.</p>	
Indicative Bibliography	Nithish Velagala, Leandros Maglaras, Nick Ayres, Sotiris Moschoyiannis, Leandros Tassioulas, "Enhancing Privacy of Online Chat Apps Utilising Secure Node End-To-End Encryption (SNE2EE)", 27th IEEE Symposium on Computers and Communications (ISCC 2022), 30 June - 3 July 2022, Rhodes, Greece, DOI: 10.1109/ISCC55528.2022.9912888

	<p>Leandros Maglaras, Nick Ayres, Sotiris Moschoyiannis, Leandros Tassiulas, "The end of Eavesdropping Attacks through the Use of Advanced End to End Encryption Mechanisms", IEEE International Conference on Computer Communications (INFOCOM 2022), 2-5 May 2022 // Virtual Conference</p> <p>Andrabi, S. J., Reiter, M. K., & Sturton, C. (2015). Usability of augmented reality for revealing secret messages to users but not their devices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 89-102).</p> <p>Dong, Y., Ling, Y., Wang, D., Liu, Y., Chen, X., Zheng, S., ... & Huang, W. (2022). Harnessing molecular isomerization in polymer gels for sequential logic encryption and anticounterfeiting. <i>Science Advances</i>, 8(44), eadd1980.</p>
Enquiries	For informal enquiries about this PhD project, please contact l.maglaras@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process