UNIVERSITÉ DE NANTES

IETR
INSTITUT D'ÉLECTRONIQUE ET DE TÉLÉCOMMUNICATIONS DE RENNES

Recommandation letter for Bogdan Gorelkin

07/12/2020

Dr Maria Méndez Real
Associate Professor
Ecole Polytechnique Universitaire de l'Université de Nantes
IETR lab UMR CNRS 6164
3 rue C. Pauc, 44300, Nantes
maria.mendez@univ-nantes.fr
02-40-68-30-21

To whom it may concern,

I know Bogdan Gorelkin from Université de Nantes where he obtained his International Master degree in Wireless Embedded Technologies (WET) in 2020.
I supervised Mr Gorelkin 5-month research internship on embedded security. His topic was about the implementation of a RSA cryptosystem on an STM32 board. His internship wan on the frame of a bigger project involving a PhD student who will use Mr Gorelkin implementation for capturing and maliciously exploiting embedded sensors leakages.
This topic was new for Bogdan so he needed to acquire different knowledge on security but also on embedded system programming.
He successfully implemented an RSA cryptosystem and studied techniques to support *bigger* RSA key lengths (above 32 bits).
In his work, Mr Gorelkin was able to trigger the RSA encryption/decryption from his laptop, to send or generate the secret keys on the STM board, ton encrypt on the board and to send back to the laptop the encryption/decryption result. He learned about security concepts, RSA encryption algorithms and C programming. He successfully integrated our research group and regularly exchanged with a PhD student. During his internship Mr Gorelkin was a serious student, respectful and was motivated to learn. I thus recommend Mr Gorelkin for internships on embedded systems and I will be pleased to further discuss about him and his work.

Sincerely,
Dr Maria Méndez Real