Ciber(in)segurança da Infraestrutura de Transportes Públicos

Nelson Nobre Escravana

Engenheiro informático pelo IST com especialização em Gestão pelo ISEG. Tem efetuado no INOV INESC Inovação (Instituto de Novas Tecnologias) atividades associadas à criação e desenvolvimento de software para sistemas embebidos, de aplicações para operadores de telecomunicações móveis, consultadoria em segurança informática, análise de risco e auditorias de segurança com ênfase em testes de penetração. Atualmente coordena a área de Comunicações do INOV onde se inclui a área de investigação e desenvolvimento em cibersegurança.

João Lima

Aluno finalista de Engenharia Informática e Computadores do IST e investigador de segurança informática no INOV INESC Inovação.

Carlos Ribeiro

Licenciado em Engenharia Electrotécnica, mestre e doutor em Engenharia Informática e docente neste departamento do Instituto Superior Técnico. Tem duas obras publicadas sobre arquitetura de computadores e sistemas operativos. De 1995 a 1998 foi consultor de segurança do Gabinete Nacional de Segurança. Entre 2008 e 2011 foi vice-presidente do conselho diretivo do centro de informática do Instituto Superior Técnico. É, desde Janeiro de 2012, pró-reitor da universidade técnica de Lisboa para a área das tecnologias de informação.

Resumo

A insegurança informática tem estado principalmente associada a ataques a computadores pessoais, ao furto de cartões de crédito ou aos ataques de negação de serviço aos sítios de internet de organizações de alta visibilidade. No entanto com a recente proliferação de ataques informáticos de elevada complexidade e eficácia, tem crescido entre os operadores de transportes públicos a necessidade de aumentar a resiliência da sua infraestrutura informática contra este tipo de ataques.
Não obstante já existir um conjunto considerável de ferramentas construídas com o objetivo de prevenir e detetar ataques informáticos, estas não estão devidamente adaptadas às necessidades específicas de proteção de infraestruturas críticas. A nossa proposta consiste numa ferramenta de deteção de intrusões especialmente construída para ambientes com um elevado nível de automação e cujos processos podem ser facilmente descritos. O sistema desenvolvido pode ser uma forma especialmente eficaz de detetar ataques nas infraestruturas de transportes públicos e, por extensão, ser utilizada na proteção de infraestruturas críticas em geral.

Abstract
Cyber-(in)security in Public Transportation Infrastructure

Cyber-(in)security has been mainly associated with attacks to personal computers, credit card theft or denial-of-service attacks to high-visibility organization's websites. However, with the recent proliferation of cyber-attacks aimed at critical infrastructures, have been growing among public transport operators the need to increase the resilience of their technological infrastructure against this type of attacks.
Despite the significant amount of tools developed in order to prevent and detect cyber-attacks, these tools were not adequately adapted to the specific needs of critical infrastructure protection. Our proposal consists of an intrusion detection tool specifically developed to be used in environments with a considerable level of automation, whose processes may be easily described. These processes may be an especially effective way to detect attacks not only in public transport infrastructures but also in critical infrastructures in general, thus increasing their protection.