Modern railroad systems vulnerable to cyber attacks

January 2, 2016 By Pierluigi Paganini

A team of researchers has evaluated the level of cyber security implemented in modern railroad systems and discovered several vulnerabilities.

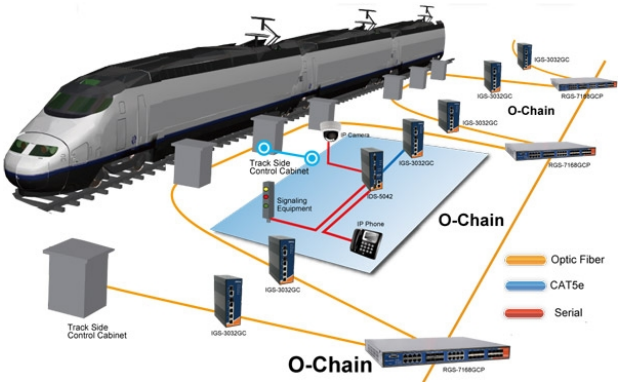
A team of experts composed of Sergey Gordeychik, Alexander Timorin and Gleb Gritsai of SCADA StrangeLove, recently disclosed their findings at the 32nd Chaos Communication Congress (32C3) in Germany.

the presence of security holes in the railroad systems that open them to cyber attacks, during the Chaos Communication Congress they disclosed a long list of security issued affecting railroad systems.

The experts did not mention specific trains when presented the results of their study, their presentation was focused on an overview of the security issues that potentially affect modern railroad systems.

In their presentation, the team of experts detailed SIBAS, a train protection system that is widely adopted in Europe. The SIBAS used the Siemens SIMATIC components, including the WinAC RTX controller, which is designed for different purposes, such as the PC-based automation solutions.
The WinAC RTX is affected by several security vulnerabilities that could be exploited by hackers.

The researchers also examined the computer-based interlocking (CBI), a signaling system designed to prevent the setting up of conflicting routes. The hacking of CBI would cause serious problems, including physical damage.



According to Sergey Gordeychik, for threat actors, “it’s absolutely easy,” to exploit these vulnerabilities, despite in some cases, the attackers would need a deep knowledge of railroad systems to exploit the flaws.

Most of the problems affects automated systems in railroad networks, such as signaling components and locks, the experts highlighted the huge presence of technology in modern railway systems.

The railway systems examined by the team are

affected by a large number of vulnerabilities, including the lack of authentication protections, poor maintenance, operating systems and software components not updated, and of course, hard-coded passwords.

The attack surface of modern railway systems is enlarging due to the presence of new solutions, including connected systems and entertainment devices.

"We worked with operators for 3 years and at the beginning there was a lot of skepticism, but now they understand the threats," Gordeychik said via email to SecurityWeek. "A lot of devices work on the same channel: like engineering equipment and user systems,"

Fortunately, there is no news of significant cyber attacks against trains and other transportation systems.

"People probably hack into them," repdet *said, "but they don't have an opportunity to conduct security research to understand," what exactly they're dealing with.*

While cyber criminals are not financially motivated in hacking such kind of systems, other illegal activities are more profitable for them, nation-state hackers could start exploring this opportunity.

Cyber security of railroad systems must be a priority for any government, the risk that hackers will exploit the vulnerabilities discovered by the experts is concrete.

Pierluigi Paganini

(Security Affairs – modern railroad systems, hacking)

Hacking | critical infrastructure | trains | nation-state actors | railroad systems

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the

field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
All BBC Websites went down after a major DDoS attack

NEXT ARTICLE
Hackers fully controlled a PlayStation 4 running a Linux distro

YOU MIGHT ALSO LIKE

Turkish hackers took over a Russian Govt Instagram account

January 3, 2016 By Pierluigi Paganini

@FFD8FFDB Twitter bot spies on

poorly configured cameras

January 3, 2016 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top