現代の鉄道システムはサイバー攻撃に脆弱

January 19, 2016 10:00

by 『Security Affairs』

研究者チームが、現代の鉄道システムに実装されているサイバーセキュリティのレベルを調査したところ、数件の脆弱性を発見した。

研究者チームSCADA StrangeLoveのSergey Gordeychik氏、Alexander Timorin氏、Gleb Gritsai氏は、昨年末にドイツで開催された第32回カオスコミュニケーション会議（Chaos Communication Congress　以下CCC）で、現代の鉄道システムに関する調査結果を発表した。

鉄道は、発電所や水道施設、送配電網と並んで国の重要インフラである。研究者チームはCCCにて、鉄道システムに影響する多数のセキュリティ問題を発表し、鉄道システムにあるサイバー攻撃を受けやすいセキュリティホールの存在を警告した。

研究者チームのプレゼンでは特定の鉄道については言及されず、現代の鉄道システムが影響を受ける可能性のあるセキュリティ問題の概略に焦点が置かれた。特に詳しく述べられたのは、ヨーロッパで広く採用されている鉄道保護システム「SIBAS（Siemens Bahn Automatisierungs System）」についてだ。SIBASは、WinAC RTXコントローラー（訳注：制御ソフト）を含むシーメンス社のSIMATIC（訳注：中～大規模の制御向けコントローラー）を使用していた。これは、パソコンベースの自動化ソリューションをはじめ様々な目的向けに設計されている。WinAC RTXは、ハッカーが悪用する可能性のある複数のセキュリティ脆弱性の影響を受ける。

また研究者らは、競合進路設定を防止するために設計されたコンピューターベースの連動装置（CBI）も調査した。CBIのハッキングは物理的損傷を含めた深刻な問題につながる可能性があるという。

Sergey Gordeychik氏によると、攻撃者が鉄道システムの欠陥を悪用するためには深い知識が必要となるケースがあるものの、 これらの脆弱性を悪用するのは攻撃者にとって「本当に容易なこと」のようだ。

これらの問題の大部分が信号システムやロックのような鉄道ネットワークの自動化システムに影響する。研究者チームは現在の鉄道システムではテクノロジーの存在が大きいということを強

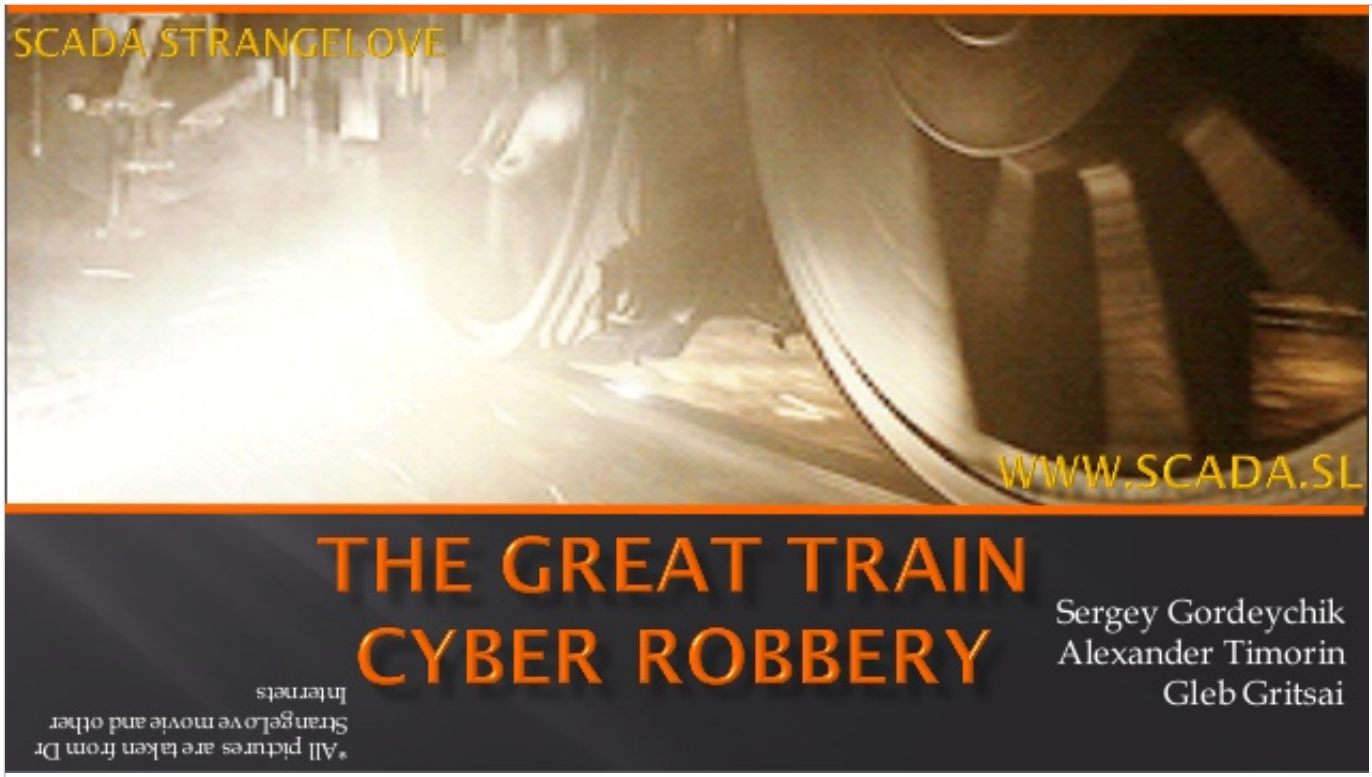
調した。

彼らが検査した鉄道システムは、多数の脆弱性の影響を受ける。これには権限確認による保護がないこと、不十分なメンテナンス、オペレーティングシステムやソフトウェアコンポーネントがアップデートされていないこと、そしてもちろんハードコードされたパスワードも含まれている。接続型システムやエンターテインメントデバイス等の新たなソリューションの存在により、現在の鉄道システムの攻撃可能な場所は拡大している。

「我々はオペレーターと共に3年間取り組んできた。初めのうちはとても懐疑的な態度であったが、今では彼らもその脅威について理解している」と Gordeychik氏はSecurityWeekへのメールの中で語った。「例えばエンジニアリング用の機器とユーザーシステムなど、同一のチャネルで多数のデバイスが動いている」

幸いにも、電車や他の交通システムに対する重大なサイバー攻撃が実施されたというニュースは出ていない。だが、「攻撃者は恐らくこれらのシステムをハッキングするだろう」とGleb Gritsai（Twitterアカウント@repdet）は言う。「しかし攻撃者らは、理解するためのセキュリティ調査を実施する機会がないのだ」。これがまさに研究者チームが取り組んでいることだ。

他の違法行為の方が利益を得られることから、サイバー犯罪者にはこのようなシステムをハッキングする金銭的な動機がない。しかし国家が支援するハッカーはこの機会を悪用し始める可能性がある。鉄道システムのサイバーセキュリティはどんな政府にとっても最重要事項となるに違いない。専門家らが見つけた脆弱性をハッカーが悪用するというリスクは現実なのだ。



1 of 110

CCCで発表するSergey Gordeychik氏、Alexander Timorin氏、Gleb Gritsai氏

翻訳：編集部

原文：Modern railroad systems vulnerable to cyber attacks

※本記事は『Security Affairs』の許諾のもと日本向けに翻訳・編集したものです

『Security Affairs』

イタリアのセキュリティ専門家、Pierluigi Paganini氏が主宰するセキュリティ・ニュースサイト。

http://securityaffairs.co/wordpress/
Twitter @securityaffairs
Security Affairs on Facebook
Security Affairs on Google+
Security Affairs on Pinterest