Andrzej KOCHAN, Emilia KOPER

Cyberbezpieczeństwo systemów kierowania i sterowania ruchem kolejowym

Streszczenie

Systemy sterowania i kierowania ruchem kolejowym realizują funkcje związane z bezpieczeństwem ruchu kolejowego. Od ich niezakłóconego działania zależy bezpieczeństwo pasażerów i przewożonych ładunków. W dążeniu do stosowania najnowszych osiągnięć techniki coraz więcej funkcji realizowane jest z wykorzystaniem technik informatycznych. Jednocześnie dąży się do centralizacji systemów sterowania celem ograniczenia personelu niezbędnego dla obsługi urządzeń sterowania. Te dwa trendy rodzą nowe zagrożenie w postaci cyberataków na infrastrukturę kolejową. W artykule przedstawiono rodzaje źródeł takich ataków. Zaprezentowano przykładowy schemat cyberataku. Omówiono mechanizm bramy jednokierunkowej transmisji danych jako propozycję dodatkowego zabezpieczenia dla systemów krytycznych z punktu widzenia zabezpieczenia ruchu kolejowego. Przestawiono koncepcję zastosowania tego rozwiązania w architekturze krajowego scentralizowanego systemu kierowania i sterowania ruchem kolejowym.

WSTĘP

Systemy sterowania i kierowania ruchem kolejowym realizują funkcje związane z bezpieczeństwem ruchu kolejowego [3]. Tak jak inne obszary systemu kolei funkcje te realizowane są przy wykorzystaniu różnych technologii poczynając od urządzeń mechanicznych na technice komputerowej kończąc. Systemy komputerowe stosowane są na sieci PKP a obecnie sieci PKP PLK od lat 80-tych ubiegłego wieku [6]. Na przestrzeni tego okresu sposób wykorzystania komputerów się zmienił. Początki zastosowań w systemach sterowania ruchem kolejowym były związane ze wspomaganiem techniki przekaźnikowej. Ten kierunek utrzymywany jest dalej w postaci rozwiązań hybrydowych. Jednak obecnie mówiąc o technice komputerowej automatyk kolejowy ma na myśli przede wszystkim takie rozwiązania jak nastawnice komputerowe, sterowniki obiektowe, komputerowe pulpity nastawcze. Zjawisko, które w tej chwili jest najbardziej aktualne to łączenie tych rozwiązań w rozległe, skomplikowane struktury z wykorzystaniem sieci komputerowych. Trzeba przyznać, że systemy na kolei przechodzą tą metamorfozę z pewnym opóźnieniem w stosunku do systemów przemysłowych innych dziedzin gospodarki. Nie należy tej sytuacji jednak wiązać z brakiem chęci unowocześniania techniki. Przyczyn takiego stanu rzeczy jest wiele, między innymi odpowiedzialność za bezpieczeństwo, ale ich omówienie jest poza zakresem tego artykułu.

W dalszych punktach poruszone zostaną zagadnienia profili cyberprzestępców, zaprezentowany zostanie schemat typowego ataku na sieć komputerową przykładowej organizacji, którą może być zarządca infrastruktury kolejowej oraz rozwiązanie techniczne w znacznym stopniu zwiększające bezpieczeństwo krytycznych segmentów sieci np. systemów sterowania ruchem kolejowym.

1. CYBERPRZESTĘPCY

Wiele miejsca w dostępnych publikacjach poświęca się rozwiązaniom technicznym, które mają zabezpieczać przed cyberatakami. Wiadomo też, że stopień zabezpieczeń należy odpowiednio dobierać w zależności od znaczenia i wartości chronionych zasobów. Rzadko jednak identyfikuje się potencjalnych atakujących chronione zasoby. Kolejne akapity pokazują profile potencjalnych cyberprzestępców. Można tu wyróżnić:

- pracowników wewnętrznych,
- przestępczość zorganizowaną,
- operatorów systemów sterowania,
- włamywaczy komputerowych działających dla idei,
- agencje wywiadowcze
- podmioty wojskowe.

Pracownicy wewnętrzni – osoby, które mają dostęp do sieci komputerowej organizacji oraz pewien stopień zaufania. Ich uprawnienia nie są zbyt szerokie, mają dostęp do wybranych zasobów sieci. Osoby takie bywają dobrze usytuowane w strukturze organizacji, aby pozyskiwać w sposób nieuprawniony dostępy do innych części sieci stosując techniki inżynierii społecznej. Celem takich osób są informacje dotyczące kontraktów, wewnętrznych zasad funkcjonowania, harmonogramów, itp. Wiedza tych osób na temat cyberbezpieczeństwa nie jest zbyt głęboka podobnie jak wiedza na temat systemu sterowania. Ich bezpośrednie działanie nie będzie przynosić zagrożenia bezpieczeństwa czy tez szkód materialnych.

Przestępczość zorganizowana – jest odpowiedzialna za większość spamu, złośliwego oprogramowania dostarczanego różnymi sposobami do sieci komputerowej organizacji. Organizacje przestępcze płacą profesjonalnym programistom za tworzenie takich środków ataku, aby ich rozwiązania cały czas wyprzedzały rozwiązania zwalczające złośliwe oprogramowanie takie jak programy antywirusowe czy ściany ogniowe (ang. firewall)[14]. Przestępczość zorganizowana posiada finanse oraz zdolności do rozprzestrzeniania swoich środków ataku. Jej celem jest zarażenie jak największej liczby komputerów. Z zarażonych komputerów pozyskiwane są dane, które mogą przynieść korzyść przestępcom. Szkodliwość złośliwego oprogramowania tego typu nie ma dużego wpływu na systemy sterowania. Jednak zdarzały się przypadki, gdzie takie ataki powodowały wyłączenie się systemu sterowania. Negatywne skutki tych ataków najczęściej sprowadzają się do kosztownego procesu oczyszczenia zakażonych komputerów ze złośliwego oprogramowania. Wyjątkiem są ataki oprogramowaniem typu ransomeware. Oprogramowanie takie może unieruchamiać komputery poprzez szyfrowanie plików. Pliki najczęściej mogą być w całości odzyskane po zapłaceniu okupu.

Operatorzy systemów sterowania – są to osoby, które mają dostęp do systemów sterowania i jednocześnie odpowiednio wyższy poziom zaufania zatrudniającej ich organizacji. Charakterem odpowiadają oczywiście opisanym wcześniej użytkownikom wewnętrznym. Jednak posiadają większa wiedzę na temat cyberbezpieczeń-

stwa i znają system sterowania. Takie osoby mogą podejmować próby modyfikacji konfiguracji systemu sterowania. Najczęstszą motywacją takiego działania jest chęć odwetu za realne lub urojone krzywdy.

Włamywacze komputerowi działający dla idei (ang. hacktivists) – osoby takie przeważnie mają znaczną wiedzę na temat cyberbezpieczeństwa a czasami są specjalistami o najwyższych kwalifikacjach. Charakteryzuje ich fakt, iż większość czasu poświęcają na próby włamania do komputerów innych użytkowników lub sieci. Takie osoby przeważnie są amatorami w związku z czym ich działania w większości przypadków nie powodują strat. Są to osoby, które nie posługują się zaawansowanymi technikami włamań (małe środki finansowe, samodzielna działalność). Jednak należy pamiętać, że skrzętnie będą wykorzystywać wszelkie otwarte furtki w systemie zabezpieczeń. Pomimo ich niewielkiego profesjonalizmu nie należy lekceważyć pochodzącego od nich zagrożenia. Przykładem może być atak przeprowadzony na Ukrainie gdzie 200 000 osób zostało pozbawionych prądu, podczas którego użyto typowych technik dla tej grupy ataków.

Agencje wywiadowcze – dysponują różnymi podmiotami finansowanymi przez władze poszczególnych krajów. Ich działanie jest zorganizowane w sposób profesjonalny i mają zapewnione znaczne finansowanie. Stosują techniki ukierunkowanej zdalnej kontroli i dostępu jak również złośliwe oprogramowanie o dużym poziomie zaawansowania technicznego i niewielkich rozmiarów. Pionierem cyberszpiegostwa były Chiny jednak obecnie te techniki stosuje większość krajów. Celem działań tych jednostek jest kradzież różnego rodzaju informacji od danych osobowych poczynając na dokumentacji technicznej kończąc. W grę wchodzi również dyskretna manipulacja opinią społeczną czy też parametrami technicznymi. Niektóre z agencji takie techniki stosowały również na potrzeby akcji sabotażowych jednak obecnie takie działania są zaliczane do elementów działań wojennych wymierzonych w inne kraje.

Podmioty wojskowe – stosują wszystkie wymienione wcześniej techniki. Dysponują wysoko specjalizowaną, nieznaną publicznie i techniczną oraz praktycznie nieograniczonymi środkami finansowymi. Celem działań takich jednostek są wszelkie elementy składające się na prowadzenie działań wojennych w szczególności charakterystycznych dla „zimnej wojny". Wojsko posiada wystarczające środki w celu pozyskania pracowników podmiotów przemysłowych dla zdobycia wiedzy w zakresie sposobu dostępu oraz wiedzy o sposobie działania systemów sterowania infrastrukturą. Powiązanie systemów sterowania z sieciami informatycznymi zarządców infrastruktury i pośrednio z Internetem daje możliwość zdalnego oddziaływania na obiekty sterowane w dowolnym zakresie, ograniczonym tylko przez techniczne możliwości struktur sieciowych. Nie należy jednak ograniczać tych możliwości do rozwiązań udokumentowanych.

2. SCHEMAT CYBERATAKU

Nie należy sądzić, że inwencję cyberprzestępców można zamknąć w schematy, ale na podstawie zebranych doświadczeń można próbować tworzyć pewne modele. Dalej opisany został jeden z typowych schematów zaawansowanego ataku [2].

Cyberprzestępcy przeszukują portale społecznościowe w celu zdobycia danych personalnych, pod które się podszywają i wysyłając maile do pracowników organizacji, która jest celem, próbując wymusić kliknięcia w zarażone fragmenty widomości w celu aktywowania pobrania i zainstalowania złośliwego oprogramowania.

Oprogramowanie antywirusowe nie rozpoznaje złośliwego oprogramowania, ponieważ jego sygnatury nie są rozpowszechniane dzięki wykorzystywaniu tylko w celowych ukierunkowanych działaniach. Powszechnie używane oprogramowanie antywirusowe zapewnia obronę przed złośliwym oprogramowaniem, które już kiedyś było wykorzystane i to w takiej skali, że mogło być zidentyfikowane i wskazane do natychmiastowego zablokowania ze względu na znaczne prawdopodobieństwo wystąpienia. W zaawansowanych atakach złośliwe oprogramowanie rozsyłane jest w ograniczonej liczbie kopii, ponieważ cel jest określony. Istnieje nieduże prawdopodobieństwo, że dotrze ono do producentów oprogramowania antywirusowego.

Zainstalowane złośliwe oprogramowanie w dogodnej sytuacji łączy się serwerami atakujących i przesyła dane z lokalnej sieci potrzebne do infiltracji systemu informatycznego organizacji będącej celem. Oprogramowanie takie posiada również funkcjonalności oprogramowania pozwalającego na zdalny dostęp do zainfekowanych maszyn, podobnego do narzędzi wykorzystywanych np. przez różne podmioty serwisujące systemy. Oprogramowanie zdalnego dostępu umożliwia przestępcom wydawanie zdalnych poleceń do zarażonych urządzeń, obserwowania efektów tych poleceń a nawet przejmowania obrazu z monitora oraz funkcjonalności klawiatury i myszy.

Operatorzy używają złośliwego oprogramowania do bardzo ostrożnego przeszukiwania otoczenia sieciowego, instalowania złośliwego oprogramowania na innych maszynach jak również pozyskiwania nazw i haseł kont użytkowników o większych uprawnieniach, przy pomocy których można uruchamiać wykonywalne pliki na wewnętrznych serwerach.

Po uzyskaniu danych kont administratorów cyberprzestępcy tworzą dla siebie konta o maksymalnych uprawnieniach oraz połączenia VPN (ang. Virtual Private Network)[] na zewnątrz i nie muszą już używać złośliwego oprogramowania, które usuwają dla zatarcia śladów. Przy mocy tak pozyskanych środków stopniowo zapoznają się ze strukturą sieci organizacji dążąc do zdobycia informacji o segmentach sieci sterowania.

Po rozpoznaniu struktury systemu sterowania i reguł jego wykorzystania cyberprzestępcy są gotowi do ingerencji w działanie systemu sterowania, w tym do oddziaływania na urządzenia np. odpowiedzialne za bezpieczeństwo ruchu kolejowego.

3. BRAMY JEDNOKIERUNKOWE TRANSMISJI DANYCH

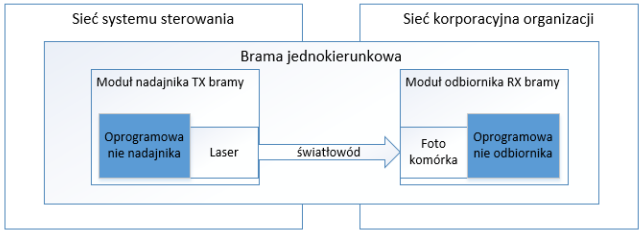
3.1. Struktura bramy jednokierunkowej

Jednokierunkowe bramy transmisji danych [5] (dalej nazywane jednokierunkowymi bramami) są rozwiązaniem, które może w znaczący sposób podnieść bezpieczeństwo krytycznych struktur infrastrukturalnych, do których należy zaliczyć systemy kierowania i sterowania ruchem kolejowym. Jest to rozwiązanie, które może być zamiennikiem dla ścian ogniowych, które w świetle przytoczonych wcześniej faktów mogą okazać się zabezpieczeniem niewystarczającym. Bramy jednokierunkowe to technologia, która łączy sieci o bardzo zróżnicowanych poziomach znaczenia dla bezpieczeństwa zasobów np. systemów sterowania ruchem kolejowym, najczęściej łącząc systemy krytyczne ze względu na bezpieczeństwo z sieciami komputerowymi organizacji (np. zarządcy infrastruktury), połączonymi z sieciami zewnętrznymi - w tym z siecią Internet. Dla potrzeb dalszych rozważań przyjmijmy rozróżnienie następujących segmentów sieci komputerowej: Internet, segment DMZ (ang. Demilitarized Zone), segment biurowy, segment sterowania.

Technologia jednokierunkowych bram jest kombinacją rozwiązań sprzętowych i oprogramowania. Sprzęt wchodzący w skład jednokierunkowej bramy składa się z dwóch modułów połączonych przez światłowód – modułu nadawczego i modułu odbiorczego. Moduł nadawczy składa się z nadajnika optycznego – lasera i nie jest wyposażony w żadne urządzenie odbiorcze. Moduł odbiorczy jest wyposażony w odbiornik optyczny – fotokomórkę i nie jest

wyposażony w żadne urządzenie nadawcze. Rozdzielenie sprzętowe nadawania i odbierania jest celowe i ma gwarantować jednokierunkowość przepływu danych. Najczęstszym zastosowaniem bram jednokierunkowych jest zapewnienie pewności przesyłania danych tylko na zewnątrz sieci systemu sterowania do ogólnej sieci organizacji. Żadne informacje nie są przesyłane z segmentu sieci biurowej do segmentu sieci sterowania i nie ma fizycznej możliwość do zrealizowania takiej transmisji. Jest to wystarczające zabezpieczenie, aby żaden atak nie mógł zostać przeprowadzony do sieci sterowania, ani żaden zdalny dostęp nie mógł być do niej zrealizowany. Nie jest możliwe również zdalne uruchomienie żadnego złośliwego oprogramowania, które wcześniej mogło być manualnie umieszczone w sieci systemu sterowania.

Schematyczna struktura bramy jednokierunkowej przedstawiony jest na rys. 1.



Rys. 1. *Struktura bramy jednokierunkowej (źródło: opracowanie własne)*

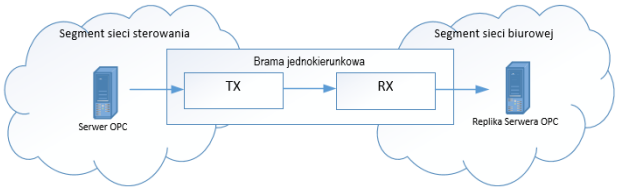
Brama jednokierunkowa składa się z:
- oprogramowania modułu nadawczego,
- sprzętowego nadajnika modułu nadawczego - lasera,
- sprzętowego odbiornika modułu odbiorczego - fotokomórki,
- oprogramowania modułu odbiorczego,
- światłowodu – fizycznego połączenia.

Dla dobrego zrozumienia różnicy pomiędzy bramą jednokierunkową należy podkreślić następującą właściwość tej ostatniej. Żadna transmisja danych nie jest możliwa z sieci korporacyjnej do sieci sterowania. Pakiety sieciowe, które trafiają do nadajnika bramy nie są przesyłane do odbiornika. Przez łącze światłowodowe transmitowane są tylko dane stanowiące zawartość pakietów. W odbiorniku bramy tworzone są pakiety należące do segmentu sieci biurowej. Inaczej mówiąc żaden ruch sieciowy z sieci sterowania nie może być przekierowany do sieci korporacyjnej i dalej do Internetu. Niestety taka sytuacja może wystąpić w ruterze. Ponadto zaatakowany ruter może zostać przekonfigurowany zgodnie z intencjami cyberprzestępców. Takie działa są fizycznie niemożliwe w przypadku bramy jednokierunkowej.

3.2. Replikacja serwera i emulacja urządzenia

Funkcjonalność bramy jednokierunkowej, która została opisana powyżej może znaleźć zastosowanie przy tworzeniu obrazu bazy danych historycznych systemu sterowania po stronie sieci korporacyjnej oraz replikowaniu urządzeń pracujących po stronie systemu sterowania w segmencie sieci biurowej.

Tworzenie obrazu bazy danych historycznych może być zrealizowane w następujący sposób. Po stronie sieci sterowania elementem oprogramowania nadajnika bramy jednokierunkowej jest serwer OPC [12]. Ten moduł jest przystosowany do współpracy ze sterownikami tworzącymi sieć sterowania w celu pobierania od nich danych. Dane w ten sposób trafiają do bramy. Oprogramowanie realizujące nadania pobiera dane z serwera OPC (ang. OLE for proces control)[12] i przesyła je do odbiornika bramy i jego oprogramowania. Część tego oprogramowania stanowi klient OPC, który czyta te dane i zapisuje do bazy danych po stronie sieci korporacyjnej. Dane te są gromadzone przyrostowo i mogą być swobodnie wykorzystywane przez użytkowników sieci korporacyjnej. Taka separacja zabezpiecza segment krytyczny, segmenty sieci sterowania nawet w przypadku pomyślnego ataku na segment korporacyjny i zniszczenia znajdującej się tam bazy danych historycznych (rys.2).



Rys. 2. *Replikacja serwera z wykorzystaniem bramy jednokierunkowej (źródło: opracowanie własne)*

Emulacja urządzeń z segmentu sieci sterowania do segmentu sieci korporacyjnej przy pomocy bramy jednokierunkowej odbywa się w podobny sposób. Serwer OPC będący elementem nadajnika bramy jednokierunkowej komunikuje się z urządzeniami, które mają być replikowane pobierając informacje o stanach urządzeń. Dane te są odczytywane przez oprogramowanie nadajnika bramy jednokierunkowej i przesyłane do odbiornika bramy jednokierunkowej. Odbiornik bramy jednokierunkowej przesyła dane do klienta OPC będącego częścią modułu odbiornika bramy jednokierunkowej. Następnie klient OPC jest źródłem danych dla serwera OPC zainstalowanego w segmencie sieci korporacyjnej. Z tego serwera wszyscy zainteresowani (aplikacje, systemy, operatorzy) mogą czytać dane opisujące urządzenia tak jakby czytali je bezpośrednio. Takie rozwiązanie zabezpiecza segment sterowania. Nawet jeżeli segment korporacyjny zostanie zaatakowany lub zniszczony urządzenia realizujące sterowanie pozostaną bezpieczne.

3.3. Czasowe przełączenie kierunku

Czasami pojawia się konieczność przesłania danych z segmentu sieci korporacyjnej do segmentu sieci systemu sterowania np. w celu aktualizacji oprogramowania antywirusowego. W takiej sytuacji przedstawione rozwiązanie bramy jednokierunkowej jest niewystarczające. Potrzebna jest odmiana bramy jednokierunkowej rozbudowana o przełącznik kierunku (ang. flip). Brama jednokierunkowa z mechanizmem czasowej zmiany kierunku umożliwia okresowe utworzenie kanału transmisji od segmentu sieci korporacyjnej do segmentu sieci sterowania, pod warunkiem zamknięcia w tym czasie kanału w kierunku podstawowym. Taka konfiguracja uniemożliwia wykorzystanie kanału z kierunkiem do segmentu systemu sterowania dla ataku ze zdalnym dostępem ponieważ nie występuje jednoczesna komunikacja dwukierunkowa. Odwrócenie kierunku może następować tylko w określonym momencie i w ściśle określonym celu.

3.4. Stałe jednokierunkowe kanały

W niektórych przypadkach transmisja danych pomiędzy segmentami sieci musi być ciągła i dwukierunkowa. Dostęp do segmentu sieci sterowania musi być zapewniony w sposób ciągły np. w celu ciągłego uaktualniania nastaw. W takich sytuacjach należy zastosować dwie bramy jednokierunkowe, indywidualne dla kierunków transmisji. Dodatkowo bramy te umieszczane są w innych segmentach sieci lokalnych. To dalej daje nam pewne zabezpieczenie przed użyciem mechanizmu zdalnego dostępu, choć poziom bezpieczeństwa jest już obniżony. Składowe bramy jednokierunkowe tworzące takie rozwiązanie identyfikowane są z punku widzenia segmentu sieci sterowania. Brama dla transmisji z segmentu sieci

biurowej do segmentu sieci sterowania nazywana jest bramą danych przychodzących (ang. inbound gateway). Podobne rozwiązanie dla kierunku od segmentu sieci sterowania do segmentu sieci biurowej nazwane jest bramą danych wychodzących (ang. outbound gateway). Całe rozwiązanie nazywane jest zespołem dwóch bram jednokierunkowych rozdzielających kierunki transmisji.

3.5. Kontrola danych aplikacyjnych

Właściwości bramy jednokierunkowej mogą być wzbogacone poprzez kontrolę danych aplikacyjnych (KDA). Podobne rozwiązanie występuje w klasycznych ruterach, ale tam kontrola dotyczy pakietów telekomunikacyjnych. Kontrola danych aplikacyjnych polega na analizie zawartości przesyłanych ramek. Oprogramowanie bramy jednokierunkowej z funkcją KDA posiada wzorce dla przemysłowych transmisji danych. Przy replikacji serwerów funkcja KDA identyfikuje ramki protokołów i odczytuje dane. Dla odczytanych danych weryfikuje ich typ i wartości przypisując etykiety. Ten poziom kontroli uniemożliwia przesłanie do segmentu systemu sterowania danych nie związanych merytorycznie z procesami realizowanymi w tym segmencie.

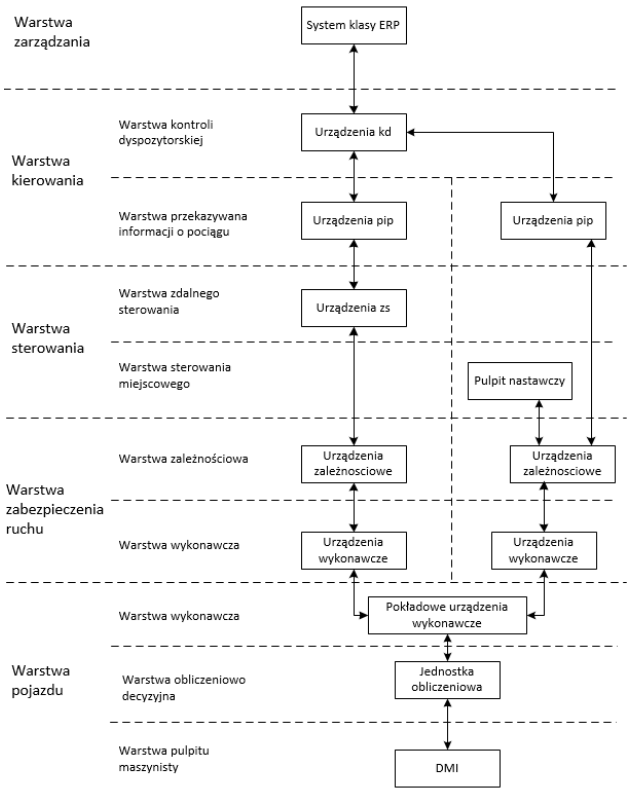
4. ZASTOSOWANIE BRAM JEDNOKIERUNKOWYCH W STRUKTURZE SYSTEMÓW KIEROWANIA I STEROWANIA RUCHEM KOLEJOWYM

4.1. Koncepcja krajowego scentralizowanego systemu kierowania i sterowania ruchem kolejowym

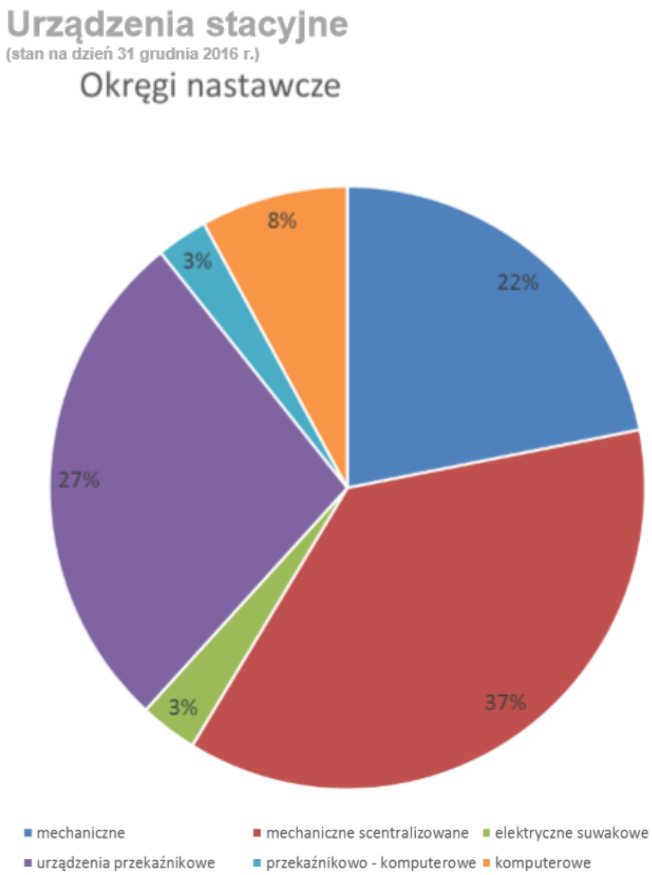
Struktura systemu kierowania i sterowania ruchem kolejowym ma charakter warstwowy [6][9](rys. 3), w którym możemy wyróżnić:

- warstwę zarządzania,
- warstwę kierowania,
- warstwę sterowania zdalnego,
- warstwę sterowania miejscowego,
- warstwę urządzeń zależnościowych i sterowników obiektowych,
- warstwę urządzeń przytorowych,
- warstwę pojazdu.

Warstwy zostały wymienione zgodnie z realizowanymi funkcjami w kolejności od funkcji bardziej ogólnych, organizacyjnych do funkcji zabezpieczenia ruchu kolejowego. W tej kolejności również narasta wrażliwość poszczególnych systemów składowych na zakłócenia spowodowane potencjalnym atakiem cybernetycznym. Choć udział w realizacji poszczególnych rozwiązań technologii informatycznych jest zróżnicowany (8% komputerowych urządzeń zależnościowych w roku 2017)[10] to istotnym jest fakt realizacji, w tej technologii inwestycji na najważniejszych liniach kolejowych w Polsce.



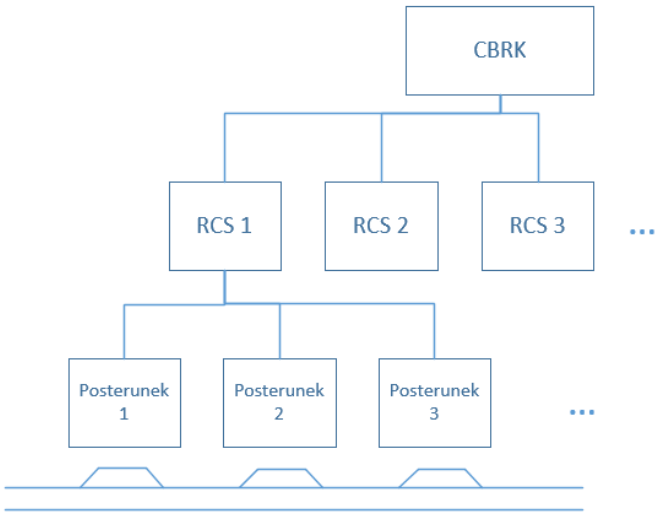
Rys. 3. *Model warstwowy sytemu kierowania i sterowania ruchem kolejowym*



Rys. 4. *Udział poszczególnych technologii wykonania stacyjnych urządzeń sterowania w Polsce [10]*

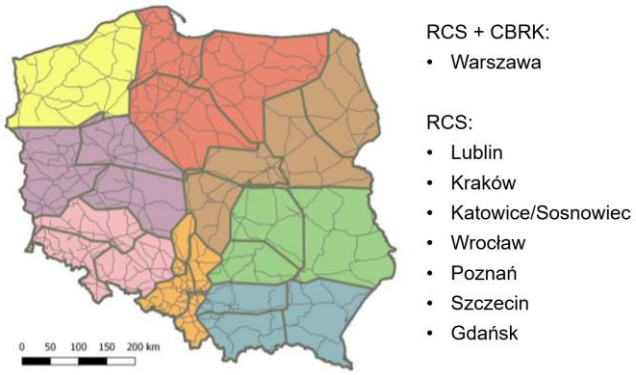
Rozważając stosowane architektury podsystemów kierowania i sterowania ruchem kolejowym wspomniany model warstwowy

należy nałożyć na propozycję scentralizowanego systemu kierowania i sterowania ruchem kolejowym o zasięgu krajowym.



Rys. 5. *Koncepcja struktury scentralizowanego systemu kierowania i sterowania ruchem kolejowym o zasięgu krajowym (źródło: opracowanie własne).*

Koncepcja taka została opracowana w ramach projektu „Opracowanie dokumentacji przedprojektowej dla projektu „Utworzenie centrum bezpieczeństwa ruchu kolejowego", w ramach zadania: „prace przygotowawcze dla wybranych projektów perspektywy 2014-2020"" realizowanej w latach 2015-2016 dla PKP PLK S.A.. Proponowana architektura scentralizowanego systemu przedstawiona jest na rysunku 5. W koncepcji zakładano zbudowanie ośmiu centrów sterowania (RCS) pokrywających swym zasięgiem całą Polskę (rys.6) organizacyjnie nadzorowanych przez Centrum Bezpieczeństwa Ruchu Kolejowego (CBRK).



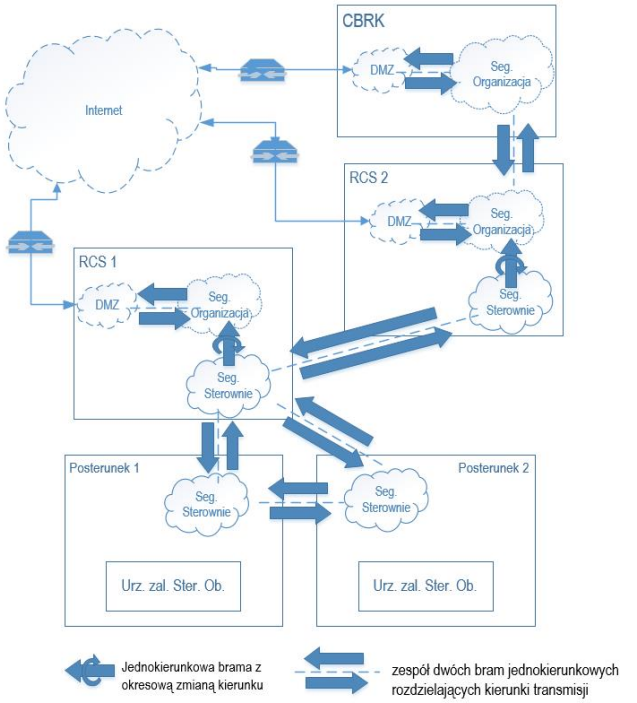
Rys. 6*. Zasięg obszarów sterowania RCSów w koncepcji scentralizowanego systemu kierowania i sterowania ruchem kolejowym o zasięgu krajowym. [4]*

Brama jednokierunkowa w różnych wariantach implementacji jest stosowana zwykle dla oddzielenia warstw definiowanych w modelach warstwowych [5]. W warstwowym modelu architektury systemu kierowania i sterowania ruchem kolejowym może być zastosowana na następujących granicach segmentów sieci:

– CBRK DMZ – Internet,
– CBRK Organizacja – CBRK DMZ,
– RCS DMZ – Internet,
– RCS Organizacja – RCS DMZ,
– RCS Organizacja – CBRK Organizacja,
– RCS Sterowanie – RCS Organizacja,
– RCS Sterowanie – RCS Sterowanie,
– Posterunek Sterowanie – RCS Sterowanie,
– Posterunek Sterowanie – Posterunek Sterowanie,
– Posterunek Sterowanie – Posterunek Urządzenia zależnościowe i sterowniki obiektowe,

Wskazane granice oddzielają od siebie różne segmenty sieci:

– CBRK DMZ – segment sieci korporacyjnej dostępny dla całego otoczenia CBRK zabezpieczony w sposób standardowy dla systemów IT, zawiera kopie serwerów baz danych segmentu CBRK Organizacja w zakresie danych udostępnianych poza siecią PKP PLK,
– CBRK Organizacja – segment sieci korporacyjnej dostępny dla pracowników nie związanych bezpośrednio z funkcjami odpowiedzialnymi za zabezpieczenie ruchu kolejowego,
– RCS DMZ – segment sieci korporacyjnej dostępny dla otoczenia RCS zabezpieczony w sposób standardowy dla systemów IT,
– RCS Organizacja – segment sieci korporacyjnej dostępny dla pracowników nie związanych bezpośrednio z funkcjami odpowiedzialnymi za zabezpieczenie ruchu kolejowego,
– RCS Sterowanie - segment sieci sterowania dostępny dla dyżurnych ruchu, pracowników realizujących funkcje sterowania ruchem (operatorów systemu sterowania) z odpowiedzialnością za zachowaniem bezpieczeństwa ruchu kolejowego,
– Posterunek Sterowanie - segment sieci sterowania dostępny dla dyżurnych ruchu, pracowników realizujących funkcje sterowania ruchem (operatorów systemu sterowania) z odpowiedzialnością za zachowaniem bezpieczeństwa,
– Posterunek Urządzenia zależnościowe i sterowniki obiektowe - segment sieci sterowania, nie jest dostępny dla pracowników realizujących funkcje sterowania ruchem, segment jest dostępny tylko dla serwisu na miejscu (monterzy, serwis producenta).



Rys. 7. *Koncepcja zastosowania bram jednokierunkowych dla struktury scentralizowanego systemu kierowania i sterowania ruchem kolejowym o zasięgu krajowym (źródło: opracowanie własne).*

Na granicy CBRK DMZ – Internet należy zastosować klasyczny firewall, ponieważ zasoby znajdujące się w tym segmencie nie mogą w żaden sposób oddziaływać na bezpieczeństwo ruchu kole-

jowego, natomiast CBRK musi mieć łączność z innymi podmiotami przy wykorzystaniu Internetu.

Na granicy CBRK DMZ – CBRK Organizacja należy zastosować zespół dwóch bram jednokierunkowych rozdzielających kierunki transmisji. Transmisja w kierunku wyjściowym ma umożliwić replikację serwera bazy danych z informacjami generowanymi operacyjnie przez CBRK i podrzędną mu strukturę systemu. Transmisja w kierunku wejściowym ma zapewnić niezbędny przepływ informacji z otoczenia organizacji CBRK.

Rozwiązania dla granicy RCS DMZ - CBRK DMZ oraz RCS DMZ -Internet są takie same jak dla granicy Internet – CBRK DMZ ze względu na podobne zależności pomiędzy segmentami.

Rozwiązania dla granicy RCS DMZ – RCS Organizacja należy zastosować zespół dwóch bram jednokierunkowych rozdzielających kierunki transmisji. Transmisja w kierunku wyjściowym ma umożliwić replikację serwera bazy danych z informacjami generowanymi operacyjnie przez RCS i podrzędną mu strukturę systemu. Transmisja w kierunku wejściowym ma zapewnić niezbędny przepływ informacji z otoczenia organizacji PKP PLK.

Na granicy RCS Organizacja – CBRK Organizacja należy stosować zespół dwóch bram jednokierunkowych rozdzielających kierunki transmisji. Obydwa segmenty muszą ze sobą współpracować na bieżąco. Pomiędzy nimi nie występuje żadna podrzędność z punktu widzenia cyberbezpieczeństwa. Oba typy segmentów muszą bronić się przed atakami z zewnątrz i jednocześnie mogą się stać źródłem ataku np. przez pracowników wewnętrznych

Na granicy RCS Sterowanie - RCS Organizacja należy stosować bramę jednokierunkową z mechanizmem czasowej zmiany kierunku. Główny kierunek transmisji zwrócony jest do segmentu RCS Organizacja dzięki czemu w tym segmencie mogą być replikowane bazy danych serwera OPC zbierającego dane z procesu sterowania. Czasowa zmiana kierunku jest wykorzystywana przez personel serwisu IT dla uaktualniania oprogramowania systemowego segmentu sterowania.

Na granicy RCS Sterowanie – RCS Sterowanie należy zaimplementować dwie bramy jednokierunkowe separujące transmisje danych w przeciwnych kierunkach. Segmenty te współpracują ze sobą przesyłając informacje o ściśle określonej treści związanej z realizowanymi funkcjami [9][11]. W tym przypadku dodatkowym zabezpieczeniem może być kontrola danych aplikacyjnych.

Rozwiązania na granicy Posterunek Sterowanie – RCS Sterowanie, Posterunek Sterowanie – Posterunek Sterowanie oraz Posterunek Sterowanie – Posterunek Urządzenia zależnościowe i sterowniki obiektowe powinny być takie same jak na granicy RCS Sterowanie – RCS Sterowanie ze względu na podobny charakter współpracy. Co prawda na granicy Posterunek Sterowanie – Posterunek Urządzenia zależnościowe i sterowniki obiektowe zmienia się rodzaj danych, które są ukierunkowane na polecenia nastawcze i meldunki o stanie urządzeń jednak charakter zabezpieczeń pozostaje taki sam.

PODSUMOWANIE

Technika komputerowa już dawno wkroczyła do zastosowań w systemach kierowania i sterowania ruchem kolejowym. Obecnie należy zwrócić uwagę na fakt, iż coraz więcej funkcjonalności realizowanych jest przez oprogramowanie, natomiast stosowany sprzęt komputerowy jest coraz mniej specjalizowany. Dodatkowo widoczny jest proces łączenia różnych podsystemów przy pomocy standardowych sieci komputerowych (sieci typu Ethernet, protokoły IP). Te wszystkie czynniki tworzą środowisko podatne na ataki cyberprzestępców. W artykule przedstawiono profile potencjalnych zagrożeń wskazując na potrzeby wprowadzania dodatkowych rozwiązań w stosunku do tych stosowanych w sieciach teleinformatycznych ogólnego przeznaczenia. W odpowiedzi na tą potrzebę wskazano na rozwiązanie jednokierunkowych bram transmisji danych z różnymi modyfikacjami. Przedstawiono koncepcję zastosowania tego mechanizmu dla scentralizowanej architektury krajowego systemu kierowania i sterowania ruchem kolejowym. Problematyka cyberbezpieczeństwa w zastosowaniach przemysłowych jest już obecna od dłuższego czasu. W przypadku systemów kierowania i sterowania ruchem kolejowym dyskusja nabiera tempa i w najbliższej przyszłości będzie wymagała wprowadzania konkretnych rozwiązań do praktyki.

BIBLIOGRAFIA

1. Artes F. “The Targeted Persistant Attack (TPA) - When Thing That Goes Bump in the Night Really is the Bogeyman” NSS Labs, 2012,
2. Clark R. Hakim S. „Cyber –Phisical Security: Protecting Critical Infrastructure at the State and Local Level” Edycja 2017,
3. Dąbrowa-Bajon M. Podstawy sterowania ruchem kolejowym. Funkcje, wymagania zarys techniki. Oficyna Wydawnicza Politechniki Warszawaskiej 2002
4. Drobysz T. „Centralizacja sterowania i zarzadzania ruchem kolejowym na liniach PKP Polskie linie Kolejowe S.A – stan wdrożenia” Konferencja Naukowo-Techniczna „Innowacyjne technologie w sterowaniu ruchem kolejowym i łączności w kolejnictwie polskim”, Kielce 2016,
5. Ginter A. SCADA Security, What’s broken and how to fix it. Abterra Calgary 2016.
6. Grochowski K., Konopiński L. „Kierowanie i sterowanie ruchem kolejowym w inteligentnym systemie transportowym” Prace Naukowe Politechniki Warszawskiej – Seria Transport z. 61, Warszawa 2007, s. 55,
7. Grochowski K., Jakimowicz J., Latocha A., Sitek I.: System kierowania i sterowania ruchem typu WSKR. Technika Transportu Szynowego, 12/1999.
8. Kochan A. Model informacyjny systemu kierowania ruchem kolejowym, Komputerowe Systemy Wspomagania Nauki, Przemysłu i Transportu „TRANSCOMP 2006” , Zakopane 2006
9. Kochan. A. „System pokładowy w modelu warstwowym systemu kierowania i sterowania ruchem kolejowym” XIV Konferencja Naukowo Techniczna „Nowoczesne Technologie i Systemy Zarządzania w Transporcie Szynowym”, Zakopane 2015
10. Kuziemski M. - Ocena eksploatacyjna urządzeń sterowania ruchem kolejowym 2016 – Konferencji Naukowo-Technicznej. „Technologie w budowie, utrzymaniu, eksploatacji urządzeń sterowania ruchem kolejowym i łączności w kolejnictwie polskim” Cedzyna, 2017
11. Wilga M. Kochan. A “Uniwersalny elektroniczny pulpit nastawczy” Prace Naukowe Politechniki Warszawskiej. Transport 2016,
12. www https://opcfoundation.org, dostęp 2017-10-25,
13. www https://pl.wikipedia.org/wiki/Virtual_Private_Network, dostęp 2017-10-25,
14. www https://pl.wikipedia.org/wiki/Zapora_sieciowa, dostęp 2017-10-25,
15. www https://pl.wikipedia.org/wiki/Strefa zdemilitaryzowana_(informatyka), dostęp 2017-10-25,

Cybersecurity of the command control and signaling railway systems

Abstract

Railway traffic control and management systems perform functions related to railway traffic safety. Their uninterrupted availability guarantees the safety of the passengers and the loads carried. In pursuit of the latest technological advances, more and more functions are realized with the use of computer technology. At the same time, the centralization of control systems is aimed at limiting the personnel needed to operate the equipment. These two trends bring new threats in the form of cyber attacks on railway infrastructure. The article presents the sources of such attacks. An example of a cyberattack scheme is presented. The unidirectional data gateway mechanism was proposed as an additional security solution for critical systems from the point of view of rail traffic protection. The concept of using this solution in the architecture of the national centralized traffic control and control system has been discussed.

Autorzy:
dr inż. **Andrzej Kochan** – Politechnika Warszawska, Ośrodek Certyfikacji Transportu na Wydziale Transportu, ako@oct.wt.pw.edu.pl,
mgr inż. **Emilia Koper** – Politechnika Warszawska, Ośrodek Certyfikacji Transportu na Wydziale Transportu, eko@oct.wt.pw.edu.pl