ZWROT W PODEJŚCIU PRODUCENTÓW DO SYSTEMÓW KONTROLI DOSTĘPU

CZYŻBY REWOLUCJA NA RYNKU SKD?

Andrzej TOMCZAK

Przecieraliśmy oczy ze zdumienia, czytając sprawozdanie z seminarium dotyczącego kontroli dostępu, przeprowadzonego przez przedstawicieli producentów SKD. Był to swoisty „coming out”[1] wytwórców urządzeń KD, którzy z rozbrajającą szczerością przyznali, że przez wiele lat wmawiali klientom, że ich systemy świetnie zabezpieczają, nawet szczególnie zagrożone obiekty, a tak naprawdę „wykorzystywane przez nich technologie zatrzymały się na etapie ‘wczesnodziecięcym’. Przyznali też, że kodowanie nie było rozwijane – niektórzy do dziś wykorzystują jednokierunkową, niekodowaną transmisję Wieganda i niekodowane karty”. Tak szczerego, aż do bólu, wyznania nikt się nie spodziewał. Co mogło ich do tego nakłonić? Być może niedaleka perspektywa wejścia w życie *Ogólnego rozporządzenie o ochronie danych* (GDPR)[2], gdy po 22 maja 2018 r. w UE surowo karane będzie naruszanie zasad ochrony danych, w tym także zaniedbanie odpowiedniego ich zabezpieczania. A być może to, że potrafią już zaoferować coś w zamian. Czy szykuje się rewolucja w systemach kontroli dostępu? Chyba jednak tak.

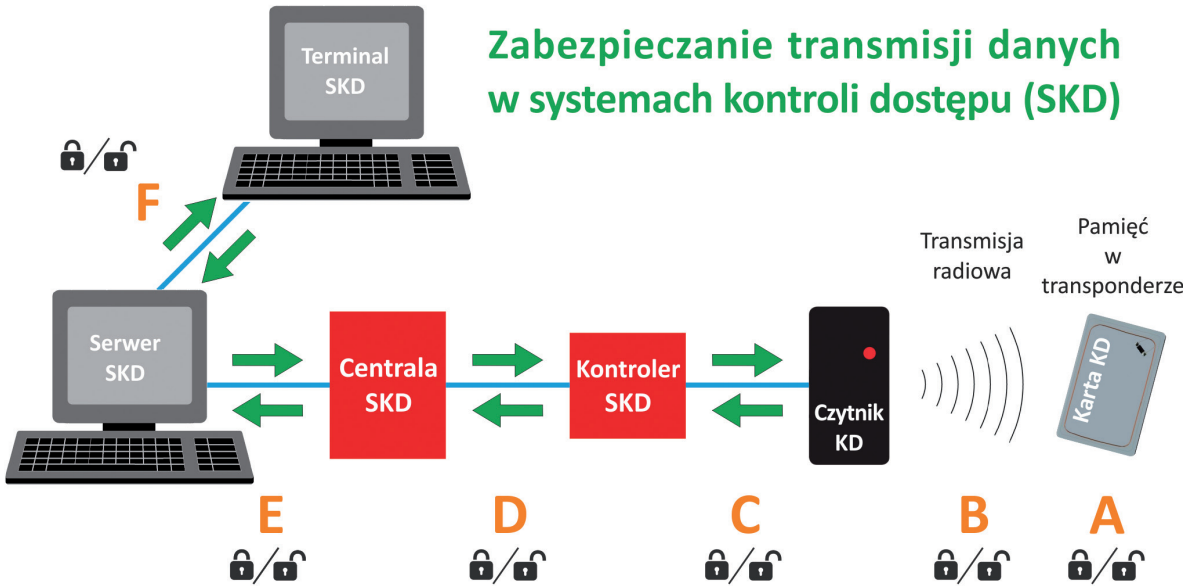
Czytelnicy zapewne nie bardzo się przejęli zwierzeniami producentów SKD, ale być może po przeczytaniu tego tekstu „staną im włosy na głowie”. Może po raz pierwszy dowiedzą się o tzw. kartach, delikatnie mówiąc, „lekkich obyczajów”[3] i innych „ciekawych sprawach”, dotyczących bezpieczeństwa ich systemów. Aby uspokoić tych, którzy mają „swoje za uszami”, przyrzekamy nie pisać z nazwy o przykładach negatywnych. Nie zdradzimy również nic poza faktami ujawnionymi przez producentów, ze względu na bezpieczeństwo zainstalowanych SKD. Postaramy się jednak wyjaśnić czytelnikom, do czego tak naprawdę przyznali się producenci. Proponujemy inwestorom, którzy w niedalekiej przyszłości będą planowali zakup systemu SKD lub wymianę aktualnie wykorzystywanego na nowy, uważne przeczytanie tych uwag.

Zacznijmy od początku, wyjaśniając etapy, gdzie spodziewać się można potencjalnych zagrożeń dla systemów SKD, związanych z transmisją danych. Na rys. 1 zaznaczono literami od A do F miejsca występowania poważnych zagrożeń dla bezpieczeństwa SKD, a tym samym dla chronionego obiektu. Kłódki oznaczają zabezpieczenie lub brak zabezpieczenia, zaś strzałkami zaznaczono kierunek transmisji.

[1] Coming out, od ang. *to come out of the closet* – „wyjście z szafy”, oznaczające samodzielne, oficjalne przyznanie się do oszukiwania otoczenia, najczęściej dotyczy samodzielnego ujawnienia ukrywanej do tej pory odmiennej orientacji seksualnej czy tożsamości płciowej.

[2] GDPR (ang. *General Data Protection Regulation*) – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, które wejdzie w życie 22 maja 2018 r.

[3] W slangu *call cards* (od ang. *call girls*) – karty, które nikomu nie odmawiają dostępu do siebie.



© *Andrzej Tomczak*

Rys. 1. Miejsca występowania poważnych zagrożeń transmisji danych w systemach kontroli dostępu

Bardzo wiele systemów, nawet instalowanych współcześnie, nie zostało wyposażonych w jakiekolwiek zabezpieczenia kart i transmisji. Stąd m.in. biorą się, tak ulubione przez inwestorów, niskie ceny. Najniższa cena wydaje się najgorszym doradcą przy wybieraniu systemów kontroli dostępu. Czyli bardzo często firmy oferują niską ceną, fundując klientom „otwarte kłódki" przy literach od A do F – oczywiście nie chwaląc się tym wcale. A skąd klient ma wiedzieć, jaka jest prawda? Spróbujemy uchylić rąbka tajemnicy.

Bardzo wiele systemów, nawet instalowanych współcześnie, nie zostało wyposażonych w jakiekolwiek zabezpieczenia kart i transmisji. Stąd m.in. biorą się, tak ulubione przez inwestorów, niskie ceny. Najniższa cena wydaje się najgorszym doradcą przy wybieraniu systemów kontroli dostępu.

O CO CHODZI Z OTWARTYMI KARTAMI?

Wyjaśnimy to w dużym uproszczeniu. Karta bezpieczna to taka, która współpracuje tylko z zadeklarowanymi przez użytkownika czytnikami. Trudno jest coś takiego uzyskać bez wprowadzenia jakichkolwiek zabezpieczeń karty. A niestety większość kart pracujących na częstotliwościach 125 kHz takich zabezpieczeń nie miała. Czym ta przypadłość się objawia? Wystarczy umieścić taką kartę w zasięgu anteny dowolnego czytnika, generującego sygnał zbliżony do 125 kHz i… karta grzecznie odpowiada całą zawartością swojej pamięci. Dlatego tak działające karty nazwano, delikatnie mówiąc, kartami „lekkich obyczajów". Wystarczy zbliżyć się z ukrytą anteną do osoby posiadającej taką kartę i bez problemu odczytać jej numer oraz zrobić duplikat. Znanym redakcji wyjątkiem są karty systemu Granta, obecnego na polskim rynku już od lat 90., sprzedawanego przez firmy Cotag, Bewator, Siemens i Vanderbilt. Otóż karta taka odpowiada tylko na sygnał radiowy systemu, do którego jest przypisana. Wspominamy system Granta technologicznie wyprzedzał konkurencję o dekady i choć aktualnie są na rynku dostępne systemy bardziej wyrafinowane, to w dalszym ciągu w kwestii bezpieczeństwa bije na głowę bardzo wielu aktualnych konkurentów. I dlatego jest jeszcze wykorzystywany w wielu obiektach i nawet dość często rozbudowywany. Oczywiście epoka technologii kart pracujących w zakresie fal długich powoli mija, ale co najmniej niefrasobliwością można nazwać zastępowanie dość bezpiecznego systemu Granta nowym, ale niekoniecznie bardziej bezpiecznym systemem.

Najnowsze systemy KD wykorzystują karty pracujące w paśmie przemysłowym na częstotliwości 13,56 MHz, dzięki czemu możliwe jest transmitowanie większej ilości danych niż korzystając z częstotliwości 125 kHz. Ale czy aby na pewno takie karty są bezpieczniejsze? I tak, i nie. Jeżeli karty 13,56 MHz, czyli większość aktualnie stosowanych kart, są wykonana zgodnie ze standardami ISO/IEC[4], to **obowiązkowo**

[4] Grupy normy dotyczących kart to: ISO/IEC 15693, ISO/IEC 14443A i ISO/IEC 14443B

muszą mieć jawny numer seryjny, nazywany UID[5] lub CSN[6]. Cóż to oznacza? Że dowolny czytnik, działający zgodnie ze standardami ISO/IEC, może ten numer odczytać. Numer seryjny powinien być unikalny, ale tak nie jest. Elementy elektroniczne kart są produkowane w kilku fabrykach, nie ma więc pewności, że numery seryjne się nie powtarzają. Do tego w niektórych typach kart UID (CSN) można zmienić za pomocą programatora. A informacje wracające z rynku są nieubłagane – zdarzyło się już nie raz, że w tym samym systemie zdublowały się karty. A jeżeli w niektórych typach kart można zaprogramować numer seryjny? Uważnemu czytelnikowi powinny w tym momencie „stanąć włosy na głowie". Karty, nawet najlepiej zabezpieczone, wykorzystane przez czytniki, rozpoznające jedynie UID (CSN), stają się kartami otwartymi, czyli kartami „lekkich obyczajów". Oczywiście produkowanie urządzeń czytających wyłącznie numer seryjny karty jest bardzo tanie, czyli ulubione przez inwestorów.

Karty, nawet najlepiej zabezpieczone, wykorzystane przez czytniki, rozpoznające jedynie numer seryjny UID (CSN) stają się niezabezpieczonymi kartami otwartymi.

A jak prawidłowo powinna działać zabezpieczona karta kontroli dostępu? Wzorcowo procedura wygląda tak: czytnik wysyła kod do odblokowania sektora karty, który chce odczytać, po weryfikacji kodu sektor zostaje otwarty, następuje wymiana informacji, a po skończeniu transmisji – ponowne zblokowanie czytanego sektora. I tak faktycznie działa część systemów, ale wykonanie tej procedury wymaga od producenta przeprowadzenia dodatkowych, dość skomplikowanych prac informatycznych. A to kosztuje. Bardzo wielu producentów unika utrudniania sobie życia i nie zabezpiecza sektorów w ogóle. Nie trzeba wysyłać kodów odblokowujących czytany sektor. Każdy może ten sektor odczytać, tym samym nawet teoretycznie najlepsza karta staje się niezabezpieczoną otwartą kartą, czyli kartą „lekkich obyczajów". Ale dzięki temu systemy stają się tańsze, a o to przecież inwestorom chodzi, nieprawdaż?

Tej przypadłości inwestor nie ma szans dostrzec, ale fachowcy, których jest, niestety, tylko kilku w naszym kraju, sprawdzą to bez problemu. I proszę uwierzyć, że na rynku jest całkiem niemało takich systemów, ale za to są tańsze w produkcji. Czyli ich producenci idą zgodnie z rynkowym trendem „najniższej ceny", czyli „po taniości".

[5] UID – ang. *Unique Identifier Number*

[6] CSN – ang. *Card Serial Number*

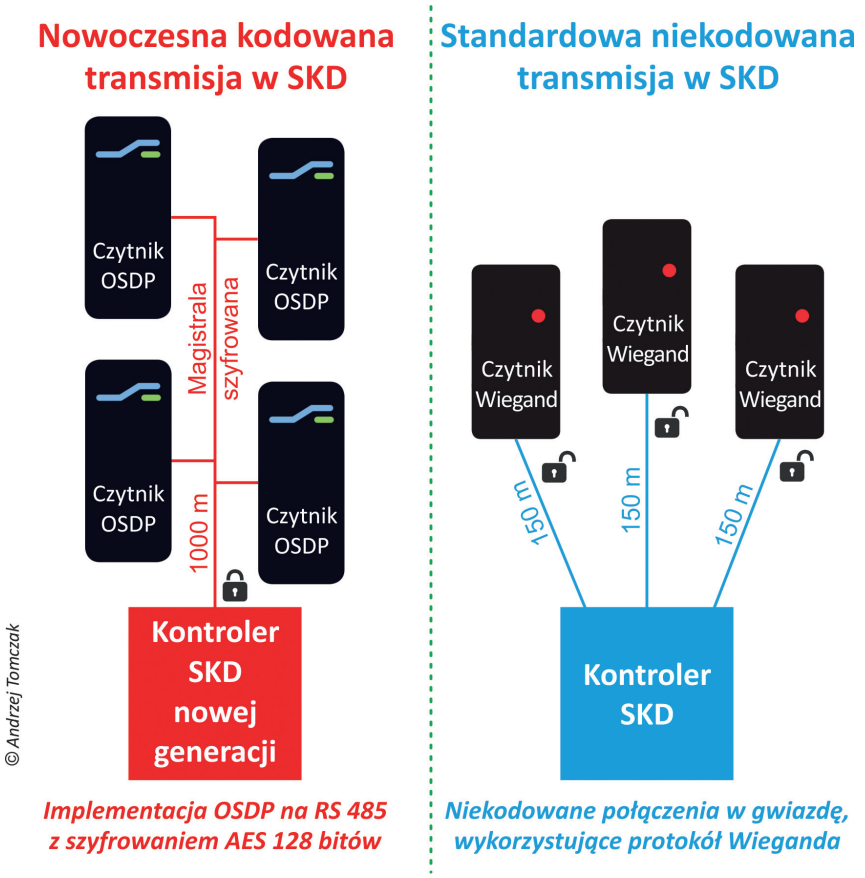
Nawet najlepsze karty, w których producent nie wykorzystuje dostępnych zabezpieczeń, stają się niezabezpieczonymi kartami otwartymi, tak jak otwarte stają się komputery czy smartfony, w których nie stosujemy procedury uwierzytelnienia użytkownika, np. hasłem.

KOMUNIKACJA POMIĘDZY CZYTNIKIEM A KONTROLEREM (CENTRALĄ, EKSPANDEREM ITP.)

Nie będziemy czytelników męczyli tematem bezpieczeństwa transmisji radiowej. Przejdziemy od razu do komunikacji, oznaczonej na rys. 1 literą C. Cóż oznacza stwierdzenie, że „niektórzy do dziś wykorzystują jednokierunkową, niekodowaną transmisję Wieganda"? Zastanówmy się nad słowem „jednokierunkowa", czyli wykorzystująca drogę transmisji tylko w jedną stronę. Wynika z tego, że powinna na rys. 1 pozostać przy literze C tylko jedna strzałka – w stronę od czytnika do kontrolera SKD. Jakie są tego konsekwencje? Na pewno na karcie nie można wpisywać do sektorów informacji znajdujących się w systemie, ponieważ nie można wysłać żadnej informacji z SKD do czytnika. W prostych systemach KD nie jest to problemem. Skupmy się więc na protokole Wieganda. Jest to protokół niezabezpieczony i dobrze opisany, coś jak dość powszechnie znany alfabet Morse'a. Dlaczego ten protokół przez wiele lat zdominował rynek? Odpowiedź jest dość oczywista. Potrzebny był prosty, uniwersalny, łatwy do implementacji, a dzięki temu tani sposób komunikacji pomiędzy czytnikiem a kontrolerem. Bowiem tajemnicą poliszynela jest to, iż producentów technologii czytania jest na świecie tylko kilku, zaś producentów systemów tysiące. Wspólny, dobrze opisany interfejs rozwiązuje ten problem. Tylko czy aby na pewno jest to bezpieczne? To tak, jakbyśmy w biurach super kodowali wszystkie informacje, czyli przenosząc to na SKD, np. stosowali bezpieczne karty i komunikację z czytnikami, a następnie komunikowali się ze światem zewnętrznym, stosując ogólnie znany alfabet Morse'a. I znów posłużmy się dobrym przykładem systemu Granta. W podstawowej konfiguracji nie wykorzystywano w nim interfejsu Wieganda, tylko firmową transmisję, szyfrowaną od kontrolera aż do karty 64-bitowym kodem. Malkontenci powiedzą, że teraz hitem jest AES[7] 128 bitów. Ale, ale... Przecież większość pozostałych systemów pomiędzy kontrolerem a czytnikiem w ogóle nie ma kodowania. Czyli może z lekka leciwa Granta nie jest jeszcze taka zła?

Producenci przyznali się do niekodowania transmisji do czytników prawdopodobnie dlatego, że opra-

[7] AES – ang. *Advanced Encryption Standard*



Rys. 2. Porównanie przykładowych implementacji szyfrowanego standardu OSDP i nieszyfrowanego interfejsu Wieganda

cowany został nowy standard kodowania pomiędzy czytnikami, pod nazwą OSDP[8], wykorzystujący szyfrowanie AES 128 bitów i uwierzytelnianie MAC[9]. Przykłady porównania implementacji systemów z interfejsem Wieganda i OSDP pokazano na rys. 2.

ZABEZPIECZANIE KOMUNIKACJI WEWNĄTRZ SYSTEMU KONTROLI DOSTĘPU

Mowa będzie o transmisji, oznaczonej na rys. 1 literą D. W tym miejscu warto przypomnieć sobie inne seminarium, wygłoszone na IFSEC 2017 – *Jak technika cyfrowa przesuwa systemy zabezpieczeń na „ciemną stronę”*. Autor wskazał tam, że systemy wykorzystujące komunikację zamkniętą, nieopartą na sieci komputerowej, gdzie wszystkie urządzenia pochodzą zwykle od jednego producenta, są z reguły dużo lepiej zabezpieczone niż systemy, które wewnątrz wykorzystują komunikację za pośrednictwem sieci Ethernet. Dlaczego? Wyjaśnienie okazuje się proste. „Systemy zamknięte, niesieciowe, mają bezpieczeństwo zagwarantowane przez producenta, zaś w systemach sieciowych bezpieczeństwo w dużej mierze zależy od umiejętności wykonujących i zarządzających tymi systemami. Piętą Achillesa branży zabezpieczeń jest niski poziom edukacji w zakresie tworzenia bezpiecznych sieci komputerowych i zarządzania nimi. Oferujący rozwiązania sieciowe w branży security pomijają milczeniem konieczność tworzenia aktywnych punktów dystrybucyjnych, które powinny być zabezpieczane i zasilane tak, jak inne elementy systemów zabezpieczeń. Trudno o takie zabezpieczenia i gwarancję zasilania, wymaganą dla systemów security, przy wykorzystaniu istniejącej infrastruktury”[10]. Należy pamiętać, że wówczas dla sprawnego i bezpiecznego działania SKD należy zagwarantować bezpieczeństwo fizyczne aktywnych punktów dystrybucyjnych i rezerwowe zasilanie, na wypadek zaniku napięcia sieci energetycznej. A to są dodatkowe koszty, tak nielubiane przez inwestorów. Czyli tego typu zabezpieczenia są najczęściej pomijane, żeby utrzymać się w ulubionym przez inwestorów trendzie „najniższej ceny”.

A czy sama komunikacja sieciowa jest bezpieczna? To już zależy od producenta systemu. Oczywiście zawsze taniej będzie nie zabezpieczać tej komunikacji niż ją zabezpieczyć. I znowu te przebrzydłe koszty!

Nie będziemy już dłużej zanudzać czytelników informacjami, jakie zagrożenia niosą za sobą wybory systemów kontroli dostępu oparte na najniższych kosztach. Raczej nie zmienimy rynkowego negatywnego nastawienia do stosowania dobrych, czytaj: droższych, rozwiązań prewencyjnych. Mamy jednak obowiązek uprzedzić rynek, że od przyszłego roku niefrasobliwość związana z brakiem odpowiedniego zabezpieczenia danych, co niewątpliwie wiąże się również z zabezpieczeniem danych w systemach kontroli dostępu, przestanie być bezkarna.

[8] OSDP (ang. *Open Supervised Device Protocol*) – szyfrowany protokół transmisji dla urządzeń peryferyjnych. Por. https://www.securityindustry.org/SiteAssets/SIAStore/Standards/OSDP_V2%201_5_2014.pdf

[9] MAC (ang. *Message Authentication Code*) – kod uwierzytelniania wiadomości

[10] *Jak technika cyfrowa przesuwa systemy zabezpieczeń na „ciemną stronę”*. Seminaria i panele dyskusyjne na IFSEC 2017, SEC&AS, nr 4/2017.

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym