# Ochrona dostępu z użyciem technologii opartych na elektronice

*Nasz niezwykle połączony ze sobą świat sprawił, że obiekty, które wcześniej nie miały wartości, stały się cenne. Dotyczy to nie tylko przedmiotów fizycznych, ale i różnego rodzaju tworów niematerialnych, takich jak dane i informacje. Rozwój technologii dał nowe narzędzia osobom, które chcą uzyskać niepowołany dostęp do wartościowych obiektów, ale też pozwala lepiej zabezpieczać cenne zasoby. W artykule opisujemy w jaki sposób można i warto korzystać z elektroniki, by zwalczyć różnego rodzaju zagrożenia bezpieczeństwa dostępu.*

Wiek XXI opiera zdecydowaną większość zabezpieczeń na technologiach informatycznych. Być może w przyszłości, wraz z pojawieniem się komputerów kwantowych, sytuacja ta się zmieni, ale obecnie to kryptografia jest podstawą wszelkiego rodzaju mechanizmów chroniących dostęp.

Oczywiście, by kryptografia faktycznie zabezpieczała przed niepowołanym dostępem, musi być odpowiednio zaawansowana i poprawnie zaimplementowana. A żeby była wygodna, musi szybko działać. To sprawia, że jedynym sensownym sposobem jej wykorzystania jest użycie elektroniki z adekwatnymi rozwiązaniami informatycznymi. I choć wielu osobom może wydawać się, że delikatna elektronika nigdy nie będzie tak bezpieczna, jak kawał żeliwnego zamka mechanicznego, w praktyce dobrze zrealizowane algorytmy stanowią znacznie silniejsze zabezpieczenia niż cokolwiek, co jesteśmy w stanie zrealizować mechaniczne.

## Bezpieczeństwo mechaniczne a elektroniczne

W ostatnim czasie na rynku pojawia się coraz więcej różnego rodzaju zamków czy nawet kłódek opartych na rozwiązaniach elektronicznych. Jak dotąd w Polsce nie cieszą się one dużym powodzeniem, szczególnie w porównaniu do popularności tego typu aplikacji w USA czy w dalekiej Azji. Nie tylko wierzymy w wyższość rozwiązań czysto mechanicznych nad elektronicznymi, ale też wątpimy w jakość wykonania zabezpieczeń elektromechanicznych. I o ile ta podejrzliwość jest bardzo uzasadniona, o tyle ślepa wiara w mechanikę jest zwyczajnie błędna.

Nie każdy zdaje sobie z tego sprawę, ale klasy bezpieczeństwa, jakie przyznaje się poszczególnym zamkom i zabezpieczeniom mechanicznym, odnoszą się bezpośrednio do czasu, jaki jest potrzeby na ich pokonanie. Im wyższa klasa bezpieczeństwa, tym więcej czasu i bardziej zaawansowane narzędzia (w tym elektryczne) są niezbędne do włamania się. Zależnie od przyjętego podziału bywa, że zamki są przewidziane na stawianie oporu przez kilka lub kilkanaście minut. W wielu przypadkach to wartości zupełnie wystarczające, by w praktyce uniemożliwić dostęp do cennych zasobów – wszak 10 minut hałaśliwych prób włamania może być z łatwością wykryte (choć to zależy od otoczenia). W tym kontekście czas potrzebny do złamania bardziej zaawansowanych szyfrów przy użyciu obecnie dostępnych narzędzi, przekraczający czas istnienia Wszechświata, sprawia, że w praktyce każde zabezpieczenie mechaniczne będzie wydawać się bezwartościowe. O ile nowoczesne narzędzia elektroniczne pozwalają coraz sprawniej łamać zabezpieczenia mechaniczne, o tyle zastosowanie odpowiednio mocnego szyfru będzie nie do pokonania jeszcze przez wiele lat.

Zatem jak to się dzieje, że pomimo tak zaawansowanych algorytmów, coraz częściej słyszy się o włamaniach do systemów, w których

**Tabela 1. Trzy klasy odporności mechanicznej zamka wg normy PN-EN 1303**

| Klasa | Odporność na wiercenie (w minutach) | Odporność na atak przecinakiem (liczba uderzeń) | Odporność na ukręcenie (liczba skręceń) | Odporność na wyrwanie z siłą 15 kN (w minutach) | Odporność na moment obrotowy (w Nm) |
|---|---|---|---|---|---|
| 0 | – | – | – | – | 1 |
| 1 | 3–5 | 30 | 20 | 3 | 20 |
| 2 | 5–10 | 40 | 30 | 5 | 30 |

bezpieczeństwo oparto na rozwiązaniach informatycznych lub elektronicznych? Praktycznie zawsze przyczyna leży w jednym z dwóch powodów: albo zabezpieczenia zostały błędnie zaimplementowane i nie dołożono odpowiednich starań, by je utrzymać, albo zawiodło coś innego – jak np. otaczająca elektronikę mechanika lub ludzie korzystający z tych zabezpieczeń.

## Jakość wykonania

Bardzo dużym problemem we wszelkiego rodzaju zamkach wyposażonych w elektronikę jest zaskakująco niska staranność producentów, by wraz z odpowiednimi zabezpieczeniami algorytmicznymi zapewnić analogiczny poziom zabezpieczeń mechanicznych. W tym kontekście cenna jest podejrzliwość klientów, którzy zazwyczaj całkiem słusznie przewidują małą wytrzymałość zamków wyposażonych w obwody elektroniczne. Przy czym, co zabawne, niemal zawsze słabym ogniwem okazuje się mechanika.

Zamki elektroniczne nierzadko są oferowane jako gadżety technologiczne. Choć wykonane są z metalu, wytwarza się je na liniach produkujących elektronikę użytkową, a więc niezbyt przystosowanych do produkcji elementów wysoce trwałych. Bywa też, że kluczowe elementy blokujące mechanicznie dostęp są wyprodukowane z plastiku i nie potrzeba wcale dużej siły, by je zniszczyć. Producenci bardzo często notują wpadki, pozostawiając niespasowane otwory, niezabezpieczone szczeliny czy nawet niestarannie ukryte śrubki, umożliwiające prosty demontaż lub odbezpieczenie zamka. W końcu problemem pozostaje kwestia awaryjnego zasilania zamka w przypadku utraty prądu – czy to w wyniku wyczerpania się baterii, czy też z uwagi na zatrzymanie dostaw prądu. Na wypadek takich zdarzeń zdecydowana większość zamków jest wyposażana w otwór na klucz mechaniczny, który ma być używany tylko w sytuacjach awaryjnych. I o ile można zakładać, że skoro na co dzień klucz do takiego zamka nie jest w użyciu, a więc jest przechowywany w bardzo bezpiecznym miejscu i trudno go skraść czy podrobić, o tyle same zamki awaryjne są zazwyczaj tak niskiej jakości, że może je otworzyć nawet osoba o minimalnych umiejętnościach. Stąd tak ważne jest, by decydując się na zabezpieczenie elektroniczne, zwrócić uwagę na jego aspekty mechaniczne.

## Zabezpieczenia cyfrowe

Tak jak wspomniano powyżej, drugim ze słabych ogniw są zazwyczaj sami użytkownicy zabezpieczeń. Jeśli dostęp do danego systemu wymaga podania hasła, to bardziej prawdopodobne jest, że włamywacz wykradnie poświadczenia, niż że złamie zabezpieczenie elektroniczne w inny sposób. W dobie mediów społecznościowych zdobycie odpowiednich danych dostępowych staje się coraz łatwiejsze, gdyż często użytkownicy sami je ujawniają, czy to publicznie, czy też nieświadomie przekazując włamywaczom komplet danych potrzebnych do zalogowania. W tym zakresie coraz bardziej pomocna staje się nowoczesna elektronika.

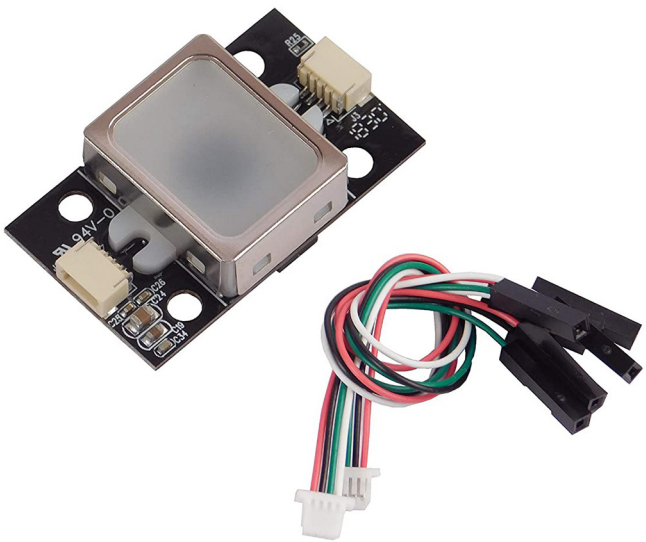
Uwierzytelnianie można bowiem podzielić na kilka etapów, które wymagają posiadania innych, oddzielnych informacji lub przedmiotów. Idealnie do tego celu nadają się urządzenia elektroniczne, które nie tylko potrafią zagwarantować bardzo wysoki poziom zabezpieczeń, ale też stały się niedrogie i działają na coraz bardziej innowacyjne sposoby.

## Wieloskładnikowa autentykacja

Klasycznym sposobem na realizację takiego zabezpieczenia jest token elektroniczny, odpowiednio skonfigurowane, małe urządzenie, wyposażone w zegar czasu rzeczywistego z kalendarzem oraz w trwałe zasilanie bateryjne. Dzięki wysokiej precyzji działania jest w stanie generować klucze zgodnie z określonym z góry schematem, wynikającym z algorytmu. Klucz taki – najczęściej kilkucyfrowy – może następnie posłużyć do weryfikacji dostępu. Jeśli użytkownik jest w stanie podać kod przepisany z tokena i zgadza się on z aktualnym kodem, wygenerowanym na urządzeniu autentykującym, to dostęp zostaje przyznany. Tokeny (a właściwie generatory tokenów) tego typu są w użytku już od wielu lat i nie kosztują wiele, a największe ryzyko, jakie wiąże się z ich użytkowaniem, sprowadza się do możliwości ich kradzieży.

Obecnie chyba najbardziej popularną metodą autentykacji wieloskładnikowej, bo tak określa się właśnie zabezpieczenie polegające na użyciu więcej niż jednego poświadczenia, jest użycie telefonii komórkowej, a konkretnie wiadomości tekstowych SMS z przesłanym kodem, który przepisuje się na podobnej zasadzie jak tokeny. Ma ona tę przewagę, że nie ma możliwości wykradnięcia unikalnego identyfikatora, na podstawie którego generowane są nowe tokeny – mogą one być tworzone losowo. Niestety, opierają się na użyciu telefonu i sieci komórkowej, w której poważnym problemem w ostatnich dwóch latach stały się kradzieże kart SIM. Nie dosłowne, tylko wykonywane poprzez fałszywe zgłoszenie utraty i konieczności wymiany karty, przy wykorzystaniu skradzionych dokumentów. Złodziej jest wtedy w stanie otrzymywać kody potwierdzające, ale musi


**Fotografia 1. Sprzętowy generator tokenów uwierzytelniających**



**Fotografia 2. Moduł prostego czytnika linii papilarnych**

również dysponować jakimś innym poświadczeniem, które pozwoli mu na pełny dostęp do systemu.

## Zabezpieczenia biometryczne

Dlatego z czasem na wartości będą zyskiwać zabezpieczenia oparte na mechanizmach biometrycznych – również realizowanych z wykorzystaniem elektroniki.

Czytniki linii papilarnych są już komponentami powszechnie dostępnymi i łatwo je zaimplementować. Nie wymagają skomplikowanego oprogramowania – często dostarczane są w postaci gotowych modułów, które pozwalają na zaprogramowanie kilku wzorców odcisków palców. Różnią się między sobą precyzją i szybkością działania. To bardzo istotne cechy, które decydują o tym, czy czujnik faktycznie stanowi zabezpieczenie oraz czy jego użytkowanie jest wygodne. Trzeba bowiem pamiętać, że implementując zbyt niewygodne w korzystaniu metody zabezpieczeń, należy się spodziewać, że ich użytkownicy będą starali się obchodzić zastosowane mechanizmy, co w konsekwencji sprawi, że będą one nieskuteczne.

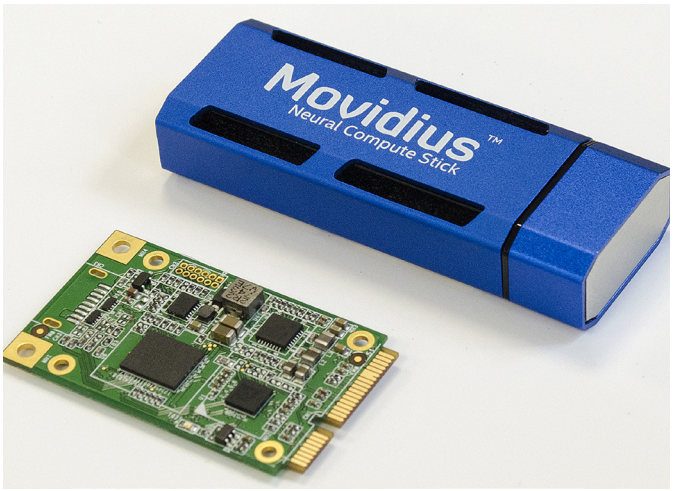
Dobierając czytniki linii papilarnych, zdecydowanie warto poprosić wcześniej o próbki od różnych producentów i zweryfikować, czy składane przez nich deklaracje niezawodnego działania mają pokrycie w rzeczywistości. Ponadto trzeba pamiętać o tym, że czujniki tego typu mogą być narażone na uszkodzenia – ich podatność też wypada przetestować, szczególnie jeśli mają zabezpieczać obiekty zewnętrzne.

Czytniki linii papilarnych oczywiście też da się oszukać, przy czym różnice w zastosowanych technologiach, precyzji działania i jakości wykonania silnie wpływają na łatwość złamania takiego zabezpieczenia.

W ostatnich czasach popularyzuje się wykorzystanie mechanizmów rozpoznawania twarzy. Jest ono coraz łatwiejsze do zaimplementowania dzięki rozwojowi technik sztucznej inteligencji. Proces przetwarzania obrazów może być przeprowadzany w chmurze, jeśli pozwala na to infrastruktura. I właśnie w ten sposób najczęściej się to realizuje, choćby dlatego że i dane osób uprawnionych do odbezpieczenia systemu często przechowywane są na zdalnych serwerach. Nowoczesne technologie pozwalają już na szybkie rozpoznawanie wielu twarzy jednocześnie na miejscu, bez potrzeby korzystania z centrów danych. Z całą pewnością tego typu aplikacje będą się szybko rozwijały w najbliższych latach.

Niestety, klasyczne rozpoznawanie twarzy nie nadaje się obecnie do zapewnienia wysokiego stopnia bezpieczeństwa. Zdecydowanie lepiej sprawdza się jako mechanizm rozróżniania użytkowników, by zwiększyć wygodę korzystania z systemów. Typowe systemy oparte na analizie obrazu z kamery da się z łatwością oszukać za pomocą wydrukowanej, a czasem nawet pokazanej na wyświetlaczu fotografii. Dlatego w ostatnim czasie pojawiły się nieco bardziej rozbudowane

**Fotografia 3. Rozpoznawanie twarzy wymaga zaawansowanej analizy obrazów**




**Fotografia 4. Intel Movidius – sprzętowe moduły sztucznej inteligencji o mocy obliczeniowej wystarczającej do błyskawicznego rozpoznawania nawet wielu twarzy jednocześnie, bez korzystania z chmury obliczeniowej**

metody, które polegają na zastosowaniu dodatkowego czujnika, mierzącego głębię rejestrowanego obrazu. Mowa o sensorach ToF (*Time of Flight*), które mierzą czas potrzebny na odbicie światła od badanego obiektu. Nie są to jednak zwykłe czujniki do mierzenia odległości. Tak jak sensory CMOS różnią się od czujników natężenia światła, tak sensory ToF różnią się od laserowych mierników odległości. Cechują się rozdzielczością, która mówi o tym, z jaką precyzją są w stanie wykreować obraz opisujący kształt obiektu. Zastosowanie czujnika ToF wraz z sensorem obrazu i bardziej rozbudowanym algorytmem rozpoznawania twarzy umożliwia implementację zabezpieczenia, które aktualnie uważa się za bezpieczne. Do jego oszukania konieczne byłoby sięgnięcie po trójwymiarowy, kolorowy model twarzy.

Pozostałe dwie technologie biometryczne, rozpoznawanie siatkówki i rozpoznawanie głosu, nie są aktualnie powszechnie stosowane. Pierwsze z tych zabezpieczeń uważa się za bardzo zaawansowane i jest implementowane tylko w nietypowych sytuacjach. Drugie natomiast jest zbyt łatwo złamać poprzez użycie zarejestrowanego wcześniej nagrania głosu osoby upoważnionej do dostępu. Niemniej systemy rozpoznawania głosu jest dosyć łatwo zaimplementować i nie wymagają stosowania zaawansowanych komponentów elektronicznych.

## Co wybrać?

Aktualnie najlepszą praktyką inżynierską wydaje się użycie więcej niż jednego zabezpieczenia. Mowa nie tylko o autentykacji dwuskładnikowej, ale wręcz trzyskładnikowej. Świetnym przykładem


**Rysunek 1. Producenci półprzewodników tworzą kompleksowe platformy zabezpieczeń, ułatwiających tworzenie w pełni bezpiecznych rozwiązań elektronicznych**

**Fotografia 5. Czujnik Time of Flight**


**Fotografia 6. Logowanie do systemu z użyciem hasła, kodu graficznego i biometryki**

tego typu mechanizmu jest wykorzystanie do logowania hasła, które musi pamiętać użytkownik oraz tokena (czy to generowanego jednorazowo, czy w oparciu na kluczu), ale z jednoczesnym zabezpieczeniem biometrycznym. Niektóre z komercyjnie dostępnych systemów logowania bazują na założeniu, że użytkownicy posiadają smartfony z aparatami z dwóch stron urządzenia. Procedura logowania do systemu elektronicznego wymaga wtedy nie tylko podania hasła i ewentualnie tokenu, ale też jednoczesnego zeskanowania kodu graficznego (z użyciem obiektywu z tyłu smartfona) zaprezentowanego na ekranie i zeskanowaniu twarzy użytkownika (z użyciem aparatu i ew. czujnika ToF z przodu smartfona). To jedno z najbardziej zaawansowanych rozwiązań, które ponadto uniemożliwia skopiowanie tokena i przekazanie go osobom trzecim.

To właśnie takie i inne połączenia kilku technik uwierzytelniania, oparte na elektronice, będą stanowiły najbardziej przyszłościowe i zalecane rozwiązania w najbliższych latach.

## Zabezpieczenia zabezpieczeń

Wszystkie opisane powyżej techniki to sposoby na zabezpieczenie dostępu do obiektów lub systemów, ale w elektronice jest jeszcze jeden obszar, który można zabezpieczać – mowa o samych mechanizmach ochronnych. Wynika to z faktu, że przy odpowiedniej manipulacji podzespołami lub systemami da się oszukać system tak, by uzyskać niepowołany dostęp do chronionych obiektów. Co więcej, wartość samą w sobie mogą mieć zaimplementowane algorytmy, które też często należy chronić.

Zabezpieczenia elektroniczne można pokonać na jeden lub nawet dwa dodatkowe sposoby. Pierwszy polega na rozmontowaniu elektroniki i takim doprowadzeniu do niej sygnałów, by pozwoliła na dostęp do chronionych elementów. Drugi ze sposobów dostępny jest tylko, jeśli zabezpieczenie opiera się na wykorzystaniu ruchu sieciowego. Odpowiednie manipulowanie przesyłanymi pakietami pozwala zasymulować zgodę na dostęp do zasobów.

Znacznie ciekawsze z punktu widzenia elektroników jest ochronienie się przed pierwszym z opisanych problemów. Producenci układów scalonych opracowują specjalne mechanizmy, których celem jest wykrywanie niepożądanej manipulacji przy obwodach. Typowo stosowane metody opierają się na detekcji przerw, obniżenia lub utraty napięcia na określonych wyprowadzeniach układu. Jeśli takie zjawisko miało miejsce, to jest możliwe, że ktoś spróbował dostać się do układu i odpinał jego połączenia. W takiej sytuacji scalak może przejść w tryb autodestrukcji – o ile nie tak wybuchowy jak na filmach, to po prostu polegający na wyczyszczeniu zapisanej pamięci, a więc całkowitym ukryciu przechowywanych danych i trwałym uniemożliwieniu dostępu do chronionych zasobów. Jeśli obwód nie ma wbudowanych aż tak zaawansowanych mechanizmów wykrywania prób włamania, czasem wystarczy prosta detekcja otwarcia obudowy urządzenia. Da się ją zrealizować nawet przy wyłączonym urządzeniu, pozostawiając pewien ładunek zgromadzony w kondensatorze, który wykorzystywany jest do wyzerowania pamięci układu w momencie, gdy przełącznik krańcowy wykrywający obecność obudowy zostanie zwolniony.

Natomiast przed zagrożeniami sieciowymi warto zabezpieczać się, stosując odpowiednie mechanizmy programowe, takie jak sieci VPN i szyfrowanie. Ponieważ wszystko to co opiera się na zaawansowanych algorytmach kryptograficznych, niemal zawsze polega na dosyć skomplikowanym kodzie oprogramowania, zdecydowanie warto jest pilnować, by podłączony do sieci sprzęt elektroniczny miał możliwość aktualizacji firmware'u. Dobrze jest też zapewnić wygodne metody pobierania i instalacji aktualizacji, dzięki którym użytkownicy końcowi będą mogli zadbać o bezpieczeństwo swoich systemów przez cały, długi czas życia produktu. Warto też poszukać takich dostawców półprzewodników, którzy w swe układy wprowadzają sprzętowe mechanizmy szyfrowania, znacznie przyspieszające pracę z certyfikatami i kryptografią.

**Marcin Karbowniczek, EP**