Zaczynamy

Opowieść o zamkach, kartach i kamerach.

- Bezpieczeństwo fizyczne: skąd się wzięły zamki, karty i kamery i dlaczego serwerownia nie wystarczy zamknąć na klucz

Bezpieczeństwo fizyczne: skąd się wzięły zamki, karty i kamery i dlaczego serwerownia nie wystarczy zamknąć na klucz

Poziom: podstawy

Dotyczy: serwerownia i biuro Zielonej w Pamiątkowie, magazyn w Swarzędzu

Czas: ~15 min

Ta strona otwiera książkę o drzwiach, kartach, kamerach, alarmach i dyskach, które trzeba umieć zniszczyć. Opowiadamy w kilku datach, jak od klucza doszliśmy do karty, która dowodzi tożsamości szyfrem, i pokazujemy, jak jedno pytanie audytora zatrzymało IT w Zielonej. Na końcu stoi mapa książki.

Skróty użyte na tej stronie (9)

Skrót	Co znaczy
AES	Advanced Encryption Standard: powszechny szyfr blokowy, którym szyfrują dane karty DESFire i wiele innych systemów, w naszych przykładach z kluczem 128 bitów
CCTV	Closed-Circuit Television: telewizja przemysłowa, czyli kamery połączone z własnym rejestratorem, a nie z publiczną siecią telewizyjną
EAL5	Evaluation Assurance Level 5: piąty z siedmiu poziomów pewności w certyfikacji Common Criteria, wyższy niż EAL4
EV3	Evolution 3: trzecia generacja kart MIFARE DESFire z 2020 roku, z licznikiem czasu transakcji i certyfikatem EAL5+
IBM	International Business Machines: firma, w której laboratorium powstał model relacyjny i pierwszy działający silnik SQL

Skrót	Co znaczy
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
MIFARE	marka kart zbliżeniowych firmy NXP: Classic ze złamanym szyfrem Crypto-1 i DESFire z szyfrowaniem AES
RFID	Radio Frequency Identification: identyfikacja przez fale radiowe, bez konieczności widzenia znacznika
S3	Simple Storage Service: magazyn plików w chmurze AWS

Skąd się wzięło

> **Pojęcie: bezpieczeństwo fizyczne.** Wszystko, co chroni sprzęt i dane przed osobą, która stoi w tym samym pomieszczeniu: drzwi, zamki, karty, kamery, alarm, szafy zamykane na klucz i sposób pozbywania się starych dysków. Najlepsze szyfrowanie nic nie da, jeśli ktoś wyniesie serwer pod pachą.

Zamek jest starszy od pisma. Starożytni Egipcjanie zbudowali drewniany zamek kołkowy, w którym kołki wpadały w otwory zasuwy, a klucz podnosił je do góry [1]. Ten sam pomysł w metalu opatentował w 1848 roku Linus Yale senior, a jego syn w 1861 roku wprowadził mały płaski klucz, który nosimy do dziś [1]. Wcześniej, w 1818 roku, Jeremiah Chubb zbudował zamek, który zdradzał właścicielowi próbę otwarcia, po tym jak włamanie do stoczni w Portsmouth ośmieszyło wcześniejsze zamki [1].

Zamek kołkowy z Egiptu. Kołki wpadają w zasuwę i blokują ją, a klucz z odpowiednimi zębami podno

Zamek kołkowy z Egiptu. Kołki wpadają w zasuwę i blokują ją, a klucz z odpowiednimi zębami podnosi je dokładnie na wysokość, przy której zasuwa się przesuwa. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

Klucz ma jedną wadę, której nie naprawi żaden wynalazek mechaniczny: nie wie, kto go trzyma. Dlatego w drugiej połowie XX wieku zamek zaczęto łączyć z kartą. W 1969 roku inżynier IBM Forrest Parry przyklejał taśmę magnetyczną do plastikowych kart i podobno dopiero żelazko jego żony pozwoliło ją trwale przymocować [2]. Z paska magnetycznego wyrosły karty hotelowe i pierwsze systemy dostępu, ale pasek da się łatwo skopiować, bo jest tylko zapisem, a nie rozmową [2].

Karta hotelowa z paskiem magnetycznym. Pasek zawiera po prostu zapisany kod, więc każdy czytni

Karta hotelowa z paskiem magnetycznym. Pasek zawiera po prostu zapisany kod, więc każdy czytnik zapisu może go powtórzyć. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

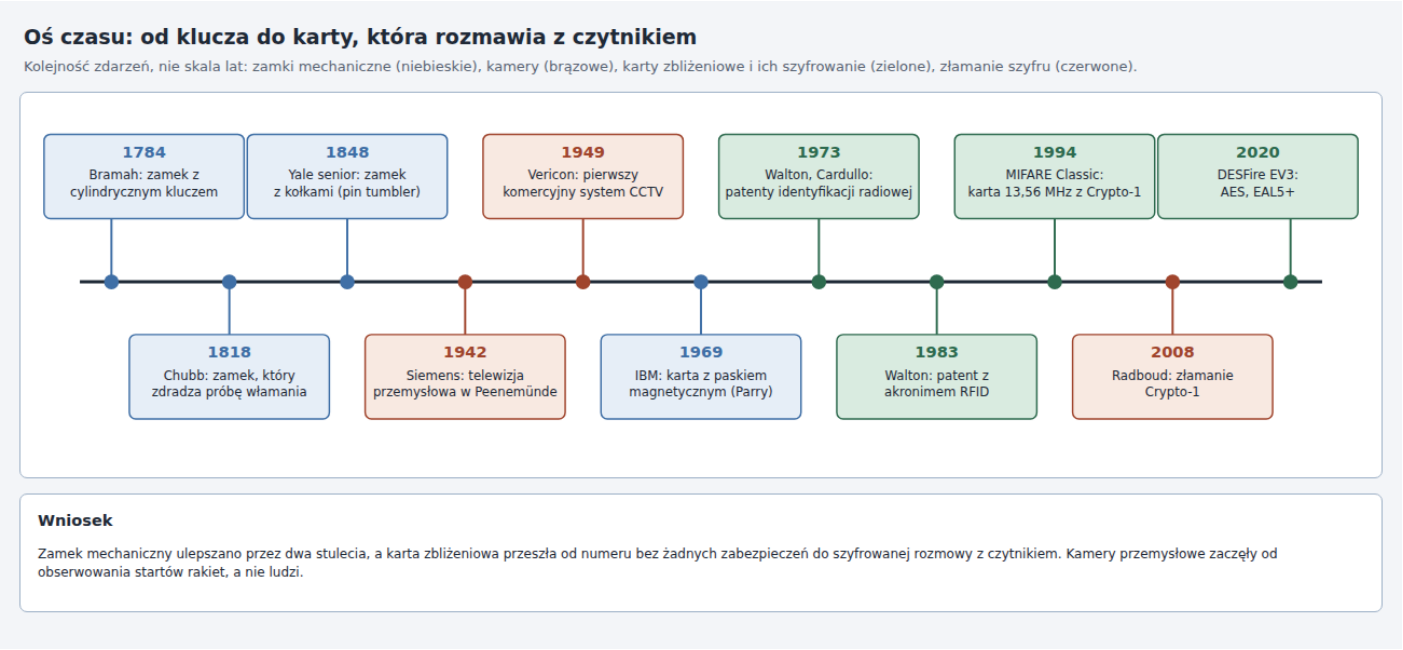
Karty zbliżeniowe zaczęły się od patentów. Mario Cardullo dostał 23 stycznia 1973 roku patent na pasywny transponder z pamięcią, który zasila się z sygnału czytnika [5][6]. Charles Walton opatentował 14 sierpnia 1973 roku system rozpoznawania przedmiotów przez sprzężenie indukcyjne [3], a 17 maja 1983 roku dostał patent na kartę wielkości karty kredytowej, który według Wikipedii jako pierwszy kojarzono ze skrótem RFID [4][5]. Obie daty są prawdziwe, ale dotyczą dwóch różnych patentów, więc zdanie, że Walton wynalazł RFID w 1973 roku, upraszcza historię.

Kamery przemysłowe mają inny rodowód: nie obserwowały ludzi, tylko rakiety. Według Wikipedii Siemens zainstalował w 1942 roku system telewizji przemysłowej na stanowisku badawczym VII w Peenemünde, żeby oglądać starty rakiet V-2 z bezpiecznego bunkra [7]. Za projekt często podaje się inżyniera Waltera Brucha, ale jego własny wpis wymienia jako pracodawcę firmę Telefunken i nie wiąże go z Siemensem, więc źródła się różnią [8]. Pierwszy komercyjny system CCTV w Stanach Zjednoczonych, Vericon, trafił na rynek w 1949 roku [7].

Stanowisko badawcze VII w Peenemünde na zdjęciu z 26 czerwca 1943 roku. Z takiego miejsca ludz

Stanowisko badawcze VII w Peenemünde na zdjęciu z 26 czerwca 1943 roku. Z takiego miejsca ludzie oglądali start rakiety przez kamerę, a nie przez okno. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

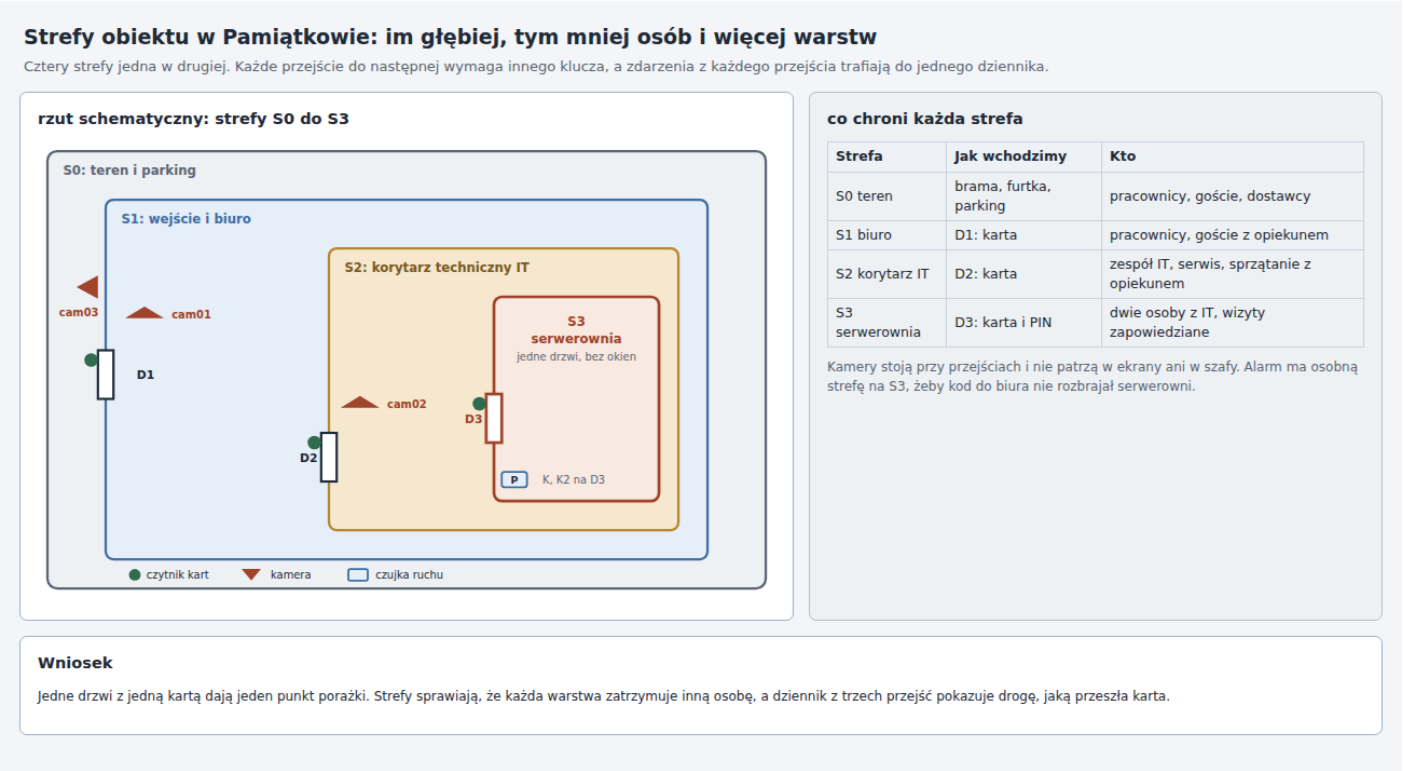
W 1994 roku pojawiła się karta MIFARE Classic na 13,56 MHz z własnym szyfrem Crypto-1 [9]. W marcu 2008 roku zespół z Radboud University w Nijmegen pokazał, że da się ten szyfr odtworzyć i odzyskać klucze bez drogiego sprzętu, a sprzedano już wtedy około miliarda takich kart [10]. Dziś rodzina DESFire z szyfrem AES i certyfikatem EAL5+ w wersji EV3 z 2020 roku jest rozsądnym następcą [9].



Rysunek 1. Oś czasu: od zamka Bramaha z 1784 roku przez karty z paskiem i patenty Waltona i Cardullo, po złamanie szyfru Crypto-1 w 2008 roku i kartę DESFire EV3 z 2020 roku. Warto zauważyć, że kamery przemysłowe i karty rozwijały się równolegle, ale z różnych powodów. (kliknięcie otwiera pełny rozmiar)

Jak to działa w jednym obrazku

Bezpieczeństwo fizyczne składa się z warstw, a nie z jednych drzwi. Każda strefa obiektu ma własny sposób wejścia, a im głębiej, tym mniej osób ma prawo przejść. Zdarzenia ze wszystkich przejść zbiera jeden dziennik.



Rysunek 2. Strefy obiektu w Pamiątkowie: S0 teren i parking, S1 wejście i biuro, S2 korytarz techniczny IT i S3 serwerownia. Warto zauważyć, że kamery stoją przy przejściach, a drzwi serwerowni wymagają karty i PIN-u. (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Wtorek, 10:00. Pan Wojtek, nasz zewnętrzny audytor, pyta uprzejmie, kto wchodził do serwerowni w zeszłym miesiącu i kto ma do niej klucz. Tomek otwiera szufladę przy recepcji i znajduje trzy klucze z napisem „serwerownia”, a w sejfie jeszcze dwa. Nikt nie wie, ilu jest wszystkich kluczy, a jeden z handlowców, który odszedł w marcu, nigdy swojego nie oddał.

Zielona ma serwerownię z jednymi drzwiami, biuro z kilkudziesięcioma osobami i magazyn, do którego codziennie wjeżdżają dostawcy. Przez lata drzwi zamykał klucz, bo był tani i wszyscy go rozumieli. Pytanie pana Wojtka pokazało jego jedyną wadę: klucz nie prowadzi dziennika. Ta książka pokazuje, jak od klucza dojść do systemu, który wie, kto, kiedy i którymi drzwiami wszedł, a także jak kamery, alarm i protokoły niszczenia dysków wypełniają luki, których sama karta nie zakryje.

Mapa tej książki

Książka ma trzy części: teorię kontroli dostępu, kamer, alarmu i niszczenia nośników, pytania, które zadajemy wykonawcom, oraz audyt z projektem do zbudowania samemu.

Strona	Na jakie pytanie odpowiada
Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień	Jaka karta jest bezpieczna, jak podpiąć kontroler do Active Directory i jak odbierać karty
Monitoring wizyjny: kamery IP, ONVIF, rejestrator i RODO	Jak ustawić kamery, sieć i okres przechowywania nagrań, żeby nie złamać prawa
Alarm i ochrona: centrala, czujki, strefy i połączenie z agencją	Co oznaczają stopnie 1 do 4 i co sprawdzić u wykonawcy przed podpisem
Niszczenie nośników: DIN 66399, kasowanie dysków i protokół	Jak pozbyć się starego dysku, żeby dane nie wyszły z firmy
Audyt fizyczny serwerowni i biura: lista kontrolna i własny czytnik kart	Co sprawdzamy w obchodzie i jak z numerem karty na ESP32 zrozumieć, dlaczego UID to nie hasło

Czujniki w serwerowni opisuje książka Warstwa fizyczna, a mapę czujników i drogę alarmu strona Serwerownia Zielonej: gdzie stoją czujniki i dokąd płyną alarmy. Kontaktrony na drzwiach i czujki ruchu wyjaśnia strona Kontaktrony i czujki ruchu: rodzaje, zasada działania i zastosowania.

Powiązane: Serwerownia Zielonej: gdzie stoją czujniki i dokąd płyną alarmy, Szafa 19 cali: jednostka U, wymiary, nośność i rozplanowanie szaf R1 do R6

Źródła:

1. Wikipedia, „Lock and key": en.wikipedia.org/wiki/Lock_and_key
2. Wikipedia, „Magnetic stripe card", historia i Forrest Parry: en.wikipedia.org/wiki/Magnetic_stripe_card
3. Patent US3752960A, Charles A. Walton, „Electronic identification & recognition system", zgłoszony 27 grudnia 1971, udzielony 14 sierpnia 1973: patents.google.com/patent/US3752960
4. Patent US4384288A, Charles A. Walton, „Portable radio frequency emitting identifier", zgłoszony 31 grudnia 1980, udzielony 17 maja 1983: patents.google.com/patent/US4384288
5. Wikipedia, „Radio-frequency identification", historia: en.wikipedia.org/wiki/Radio-frequency_identification
6. Patent US3713148A, Mario W. Cardullo i William L. Parks III, „Transponder apparatus and system", zgłoszony 21 maja 1970, udzielony 23 stycznia 1973: patents.google.com/patent/US3713148
7. Wikipedia, „Closed-circuit television": en.wikipedia.org/wiki/Closed-circuit_television

8. Wikipedia, „Walter Bruch": en.wikipedia.org/wiki/Walter_Bruch
9. Wikipedia, „MIFARE": en.wikipedia.org/wiki/MIFARE
10. Digital Security group, Radboud University Nijmegen, komunikat prasowy o słabości MIFARE Classic: sos.cs.ru.nl/applications/rfid/pressrelease.en.html