BEZPIECZEŃSTWO TINYWATCH

Prywatny monitor, który nie wychodzi poza dom.

TinyWatch zamienia dwa telefony w monitor pokoju działający lokalnie przez Wi-Fi: bez chmury, bez konta i bez zewnętrznych serwerów przenoszących obraz z kamery. W tym dokumencie wyjaśniamy prostym językiem, co technicznie stoi za tą obietnicą.

Tylko lokalnie

Obraz i dźwięk przechodzą bezpośrednio między telefonami przez Twoje Wi-Fi albo hotspot osobisty. Nie trafiają na nasze serwery.

Szyfrowane w transmisji

Strumień audio-wideo używa obowiązkowego w WebRTC szyfrowania DTLS-SRTP, czyli standardu znanego z dużych aplikacji do rozmów wideo.

Parowanie kodem QR

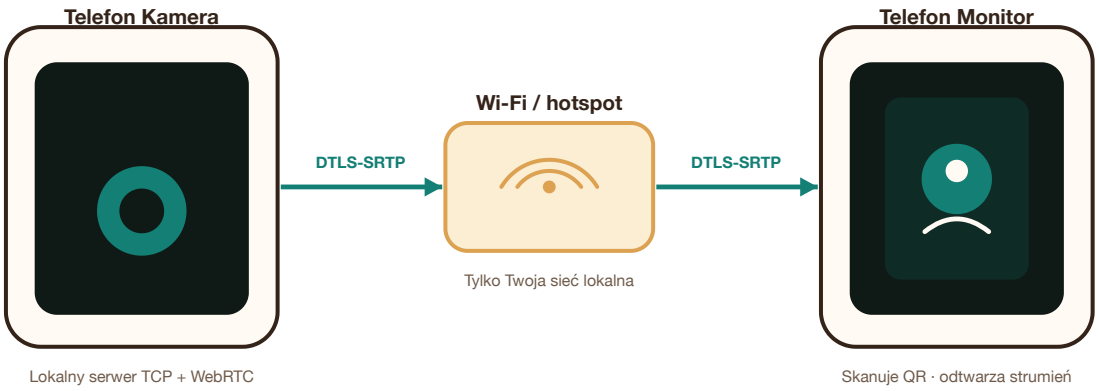
Każdy Telefon Kamera ma 48-bitowy sekret zapisany w kodzie QR. Monitor musi znać ten sekret, aby uruchomić strumień.

Dalej pokazujemy szczegóły: jak działa parowanie, jakie szyfrowanie chroni transmisję, jak ograniczamy ataki brute force i czego TinyWatch z założenia *nie* zabezpiecza.

01 · ARCHITEKTURA

Jak powstaje sesja TinyWatch

Każda sesja TinyWatch to bezpośrednia rozmowa dwóch telefonów w tej samej sieci lokalnej. Żaden element tej pętli nie działa na naszych serwerach.



Rysunek 1 · Sesja ma trzy realne strony: dwa telefony i sieć Wi-Fi między nimi. Nie ma czwartej strony.

Co dzieje się po kolei

- **Telefon Kamera** uruchamia mały lokalny serwer TCP (domyślnie na porcie 58212) i pokazuje kod QR z prywatnym adresem IP, portem oraz świeżym losowym sekretem parowania.
- **Telefon Monitor** skanuje kod QR, odczytuje sekret i prosi Telefon Kamera o ofertę WebRTC uwierzytelnioną tym sekretem.
- **Dalej pracuje WebRTC.** Obraz i dźwięk płyną peer-to-peer między telefonami w pakietach SRTP szyfrowanych przez DTLS, czyli tym samym transportem, z którego korzystają współczesne aplikacje do rozmów wideo.

CO PRZECHODZI PRZEZ NASZE SERWERY

Nic. Aplikacja TinyWatch nie przesyła obrazu, dźwięku ani lokalnych adresów IP telefonów do infrastruktury TinyWatch. Wszystko zostaje na dwóch telefonach i w sieci Wi-Fi albo hotspocie osobistym między nimi.

02 · PAROWANIE

Kto może się połączyć

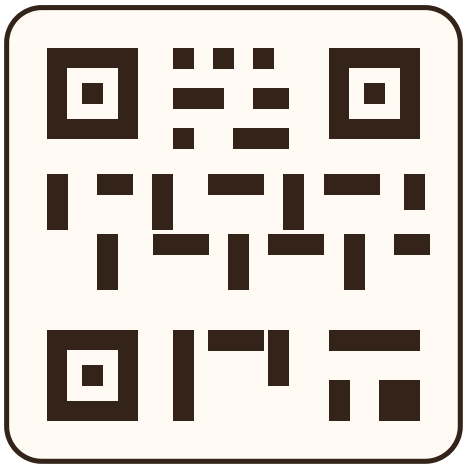
Osoba w Twojej sieci lokalnej może prawdopodobnie *zobaczyć*, że TinyWatch działa. Strumień może jednak uruchomić tylko ten, kto zna sekret parowania.

Sekret w kodzie QR

Za każdym razem, gdy startuje Tryb Kamery, aplikacja tworzy świeży losowy sekret przy użyciu kryptograficznego generatora liczb losowych systemu operacyjnego, czyli tego samego rodzaju źródła, z którego nowoczesne aplikacje korzystają przy tworzeniu haseł. Sekret ma **48 bitów** i jest zapisany w kodzie QR jako krótki ciąg bezpieczny do użycia w adresie URL.

Kod QR zawiera też lokalny adres IP kamery i port. Te wartości nie mają znaczenia poza Twoją siecią domową.

48	90	50
bitów entropii w sekrecie	dni ważności sekretu	błędnych prób na minutę przed blokadą



Rysunek 2 · QR niesie lokalny adres IP kamery, port i 48-bitowy sekret parowania: nic więcej.

Dlaczego 48 bitów wystarcza

48-bitowy sekret ma około **2,8 × 10¹⁴** możliwych wartości, czyli mniej więcej 281 bilionów. Nawet hipotetyczny atakujący w Twojej sieci Wi-Fi, zgadujący tak szybko, jak kamera potrafi odpowiadać (jedna próba co kilka milisekund), potrzebowałby średnio dziesiątek tysięcy lat ciągłego zgadywania, zanim trafiłby właściwą wartość. Limit prób opisany niżej wydłuża ten czas o kolejne rzędy wielkości.

BRUTE FORCE W KONKRETNYCH LICZBACH

Przy limicie 50 błędnych prób na minutę atakujący, który nigdy się nie poddaje, potrzebowałby średnio około

5,4 MILIONA LAT

, żeby znaleźć sekret. Pierwsi ludzie pojawili się około 300 tysięcy lat temu, więc taki atak musiałby zacząć się mniej więcej osiemnaście razy wcześniej niż nasz gatunek.

Rotacja

Sekret automatycznie wygasa po **90 dniach** od wygenerowania. Jeśli zrzut ekranu z kodem QR trafi kiedyś tam, gdzie nie powinien, na przykład do kopii czatu, galerii zrzutów ekranu albo wiadomości do supportu, po tym czasie przestanie działać nawet bez Twojej reakcji. Możesz też unieważnić go wcześniej, restartując Tryb Kamery.

03 · TRANSMISJA

Jakie szyfrowanie chroni strumień

Gdy oba telefony uzgodnią sekret parowania, właściwy obraz i dźwięk przejmuje WebRTC, czyli technologia peer-to-peer używana przez duże usługi rozmów wideo w przeglądarce.

Sygnalizacja

Krótka wymiana parametrów połączenia odbywa się przez zwykły socket TCP w Twojej sieci LAN. Każde żądanie jest uwierzytelniane 48-bitowym sekretem, a kamera odrzuca każdą wiadomość, która nie przejdzie tego sprawdzenia.

Media

Właściwy strumień jest przesyłany w **pakietach SRTP w ramach sesji DTLS**. WebRTC wymaga takiego szyfrowania: nie ma trybu nieszyfrowanego. Oba telefony tworzą świeże klucze DTLS dla każdej sesji, więc nagrania jednej sesji nie da się użyć do odtworzenia innej.

AES-GCM szyfr | **DTLS 1.2+** uzgadnianie | **ICE** łączność | **Nowe klucze** co sesję, forward secrecy

Rysunek 3 · Strumień mediów jest szyfrowany na Telefonie Kamera i odszyfrowywany dopiero na Telefonie Monitor. Po drodze widać tylko zaszyfrowane dane.

DLACZEGO NIE DODAJEMY DRUGIEJ WARSTWY

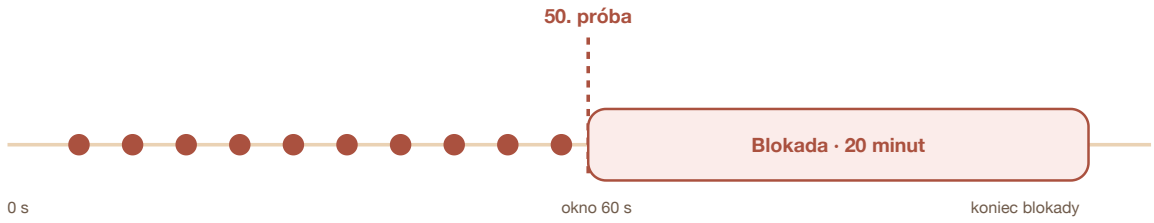
DTLS-SRTP to model bezpieczeństwa dla wideo na żywo, na którym opierają się Apple, Google, Microsoft i Mozilla. Dodanie własnej warstwy szyfrowania na wierzchu raczej zwiększyłoby ryzyko błędu, niż realnie podniosło bezpieczeństwo.

Co zatrzymuje obcą osobę w tej samej sieci Wi-Fi

Istnieją sieci Wi-Fi w kawiarniach. Istnieją wspólne sieci w budynkach. Sekret parowania nadal chroni sesję w nieprzyjaznej sieci LAN, ale dokładamy kilka zabezpieczeń na wypadek, gdyby ktoś mimo wszystko próbował odpytywać kamerę.

Limit prób dla każdego adresu źródłowego

Kamera zlicza nieudane próby uwierzytelnienia z każdego źródłowego adresu IP w ruchomym oknie 60 sekund. Po **50** błędnych próbach w tym oknie dany adres jest blokowany na **20 minut**, niezależnie od kolejnych zgadywań.



Rysunek 4 · Jeden adres może wykonać maksymalnie 50 prób w dowolnej ruchomej minucie. Bot robiący jedną próbę na sekundę dobija do limitu w niecałą minutę.

Limity rozmiaru żądań

- Bufor żądania TCP jest ograniczony do **1 MB**. Połączenie, które wysyła bajty bardzo powoli, nie może utrzymywać kamery w oczekiwaniu bez końca.
- Treść żądania POST jest ograniczona do **512 KB**. Oferta WebRTC rzadko ma więcej niż 30 KB, więc ten limit jest hojny, ale nadal wyklucza atak typu „wyślij Content-Length: 999999999”.
- Błędne nagłówki HTTP albo nienumeryczne wartości Content-Length są odrzucane odpowiedzią 400, a socket jest zamykany.

Co faktycznie musi zrobić atakujący w tej samej sieci LAN

Nawet przy idealnym wyczuciu czasu i pełnym wykorzystaniu 60-sekundowego okna w każdej minucie atakujący musi trafić los na loterii 48-bitowego sekretu. Limit prób spowalnia go miliony razy, a entropia samego sekretu spowalnia go biliony razy.

05 · PRYWATNOŚĆ

Czego nigdy nie widzimy, nie zapisujemy i nie sprzedajemy

TinyWatch jest w 2026 roku nietypową aplikacją: naprawdę nie ma konta, analityki przypisanej do Ciebie ani serwera, na który trafiałby strumień. Opisana wyżej architektura wynika też z naszego podejścia do prywatności.

- **Bez konta.** Nie wpisujesz adresu e-mail ani hasła. Nie mamy rekordu użytkownika, który moglibyśmy stracić przy wycieku danych.
- **Bez wideo w chmurze.** Obraz i dźwięk przechodzą przez Twoje Wi-Fi albo hotspot osobisty, nigdy przez naszą infrastrukturę. Nie moglibyśmy pokazać Ci nagrania z Twojej kamery, nawet gdybyśmy próbowali.
- **Bez wysyłania nazwy sieci Wi-Fi.** Na iOS pytamy o nazwę sieci tylko po to, żeby pokazać ją na ekranie przypomnienia i pomóc potwierdzić, że oba telefony są w tej samej sieci. Ta nazwa zostaje na urządzeniu.
- **Bez wycieku sekretu parowania.** Sekret nie opuszcza dwóch telefonów. Jest w kodzie QR na Telefonie Kamera i w pamięci Telefonu Monitor w trakcie aktywnej sesji. Nic innego go nie widzi.
- **Minimalna telemetria.** Używamy analityki produktowej tylko do zbiorczych liczników instalacji, uruchomień i awarii, nigdy do treści ani zachowania konkretnego użytkownika w sesji. Dokładna lista pól jest w polityce prywatności.

Uprawnienia iOS, po kolei

Aparat przechwycenie i strumieniowanie obrazu na żywo

Mikrofon przechwycenie i strumieniowanie dźwięku na żywo

Sieć lokalna odnalezienie sparowanego telefonu przez Wi-Fi

Informacje o Wi-Fi pokazanie nazwy sieci na ekranie przypomnienia

Lokalizacja podczas używania wymagana przez iOS do odczytu nazwy Wi-Fi

Prosimy o uprawnienia dopiero wtedy, gdy zaraz ma wystartować funkcja, która ich potrzebuje, a nie przy pierwszym uruchomieniu aplikacji. Jeśli odmówisz jednego z nich, aplikacja pokazuje dokładnie, którego brakuje i jak włączyć go ponownie.

06 · UCZCIWIE

Przed czym TinyWatch celowo nie chroni

Krótka, szczera lista. Wolimy pokazać ją od razu, niż pozwolić odkryć ją później.

UDOSTĘPNIENIE KOMUŚ KODU QR

Każda osoba, której dasz zrzut ekranu z kodem QR, ma taki sam dostęp do kamery jak Ty, dopóki 90-dniowy sekret jest ważny. Zrestartuj Tryb Kamery, aby unieważnić go od razu.

PRZEJĘCIE HASŁA DO WI-FI

TinyWatch zakłada, że osoba w Twojej sieci Wi-Fi jest już w zaufanej sieci. Jeśli hasło do domowego routera jest szeroko udostępniane, każde urządzenie z tym hasłem może przynajmniej *zobaczyć*, że kamera istnieje, nawet jeśli nie może pobrać strumienia.

PRZEJĘCIE SAMEGO TELEFONU

TinyWatch jest aplikacją, nie specjalnie utwardzonym urządzeniem. Ktoś z fizycznym dostępem do odblokowanego Telefonu Kamera może zrobić na nim wszystko, w tym obejrzeć podgląd na żywo w aplikacji.

UŻYCIE Z DUŻEJ ODLEGŁOŚCI ALBO SPOZA DOMU

TinyWatch z założenia działa tylko wtedy, gdy oba telefony są w tej samej sieci lokalnej. Nie obsługujemy oglądania kamery z innego miasta: nie ma serwera pośredniczącego, konfiguracji przekierowania portów ani trybu zdalnego dostępu. Właśnie dzięki temu możliwa jest taka prywatność.

Jeśli coś pójdzie nie tak

TinyWatch nie ma telemetrii, która pozwalałaby nam zdalnie zobaczyć Twoją kamerę albo sesje. Jeśli chcesz zgłosić problem, skorzystaj z adresów podanych w polityce prywatności i regulaminie: to jedyne kanały, przez które możemy pomóc.