Szczęśliwi czasu nie liczą

„Wy macie zegarki, a my mamy czas", tymi słowami tybylcy witali dawniej europejskich kolonizatorów w Afryce czy Azji, co często miało charakter zawoalowanej groźby (wasz czas minie, a nasz nie). Obecnie to przywitanie często słyszą europejscy „podróżnicy" cieszący się ze swego *dolce far niente*[1] niejako na potwierdzenie, że dobrze wybrali destynację.

Paweł Henig

absolwent Wydziału Elektroniki Politechniki Warszawskiej. Od połowy lat 90. budował dla centralnej administracji rządowej centra przetwarzania danych i sieci rozległe. Audytor wewnętrzny systemów zarządzania obejmujących normy: zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), zarządzania bezpieczeństwem i higieną pracy (OHSAS 18001), bezpieczeństwem produkcji wartościowej (CWA 14641 – Intergraf) oraz zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001. Certyfikowany audytor systemów IT (CISA), posiadacz certyfikatu ITIL Foundation. Rzeczoznawca PTI, ekspert PIIT. Dyrektor Operacyjny Trusted Information Consulting Sp. z o.o.

1 Z włoskiego, słodkie nieróbstwo – okres wakacji, odpoczynku od pracy.

Czas miał zawsze istotne znaczenie, chociaż nie do końca uświadomione. Cykle przyrody, takie jak pory dnia czy pory roku, zawsze nadawały rytm działalności człowieka, który – aby przeżyć – musiał zsynchronizować się z tym rytmem. Dało to podstawę dla kulturowego, cyklicznego oglądu czasu dobrze widocznego w okresie antyku. Judaizm, a następnie chrześcijaństwo wprowadziło czas linearny, gdzie świat od stworzenia dążył do pewnego celu, czyli sądu ostatecznego oraz finalnego zbawienia lub potępienia. Postrzeganie czasu ma w dużej mierze znaczenie kulturowe, istotnie związane z językiem pozwalającym na precyzyjne wyrażenie myśli na temat upływającego czasu oraz osadzenia go w chronologii zdarzeń.

Upływ czasu jest jedynym wspólnym elementem łączącym międzykulturowe postrzeganie czasu z jego fizyczną emanacją. Samo postrzeganie upływu czasu ewoluowało od pełnej płynności w starożytności (chociaż przy zachowaniu jego cykliczności), poprzez absolut czasu sformułowany przez Newtona aż po teorię względności Einsteina, czy jej rozwinięcie w teorii strun, gdzie występuje powiązanie czasu z przestrzenią oraz zjawiskami relatywistycznymi mającymi wpływ na upływ czasu.

Informatyka i czas

Podobnie jak w kulturze, postrzeganie czasu zmieniało się wraz z rozwojem technologii komputerowych. Można powiedzieć, że w pierwszym, początkowym okresie rozwoju techniki komputerowej dominowała klasyczna koncepcja trzech jedności: czasu, miejsca i akcji. Ówczesne komputery były monolityczne, przetwarzanie – scentralizowane, a ewentualna synchronizacja ze zjawiskami świata zewnętrznego odbywała się za pomocą wewnętrznego zegara nadającego rytm przetwarzania sekwencji kolejnych instrukcji. Szybko jednak inżynierowie dostrzegli konieczność synchronizacji zegarów komputerów połączonych w sieć, podobnie jak to miało miejsce ponad 130 lat wcześniej po otwarciu pierwszej linii kolejowej użytku publicznego w Wielkiej Brytanii (tzw. *railway time*)[2]. Technologia sieciowej synchronizacji czasu została przedstawiona pierwszy raz w trakcie *National Computer Conference*, która miała miejsce w czerwcu 1979 r. w Nowym Jorku. Pokazano wtedy usługę internetową działającą poprzez transatlantycką sieć satelitarną.

Technologia ta została później opisana w 1981 r. w *Internet Engineering Note* (IEN) 173, a następnie opracowana w postaci protokołu udokumentowanego jako RFC[3] 778 *„DCNET Internet Clock Service”*. Pojawiło się również rozszerzenie protokołu ICMP[4] poprzez RFC 781 *„A specification of the Internet Protocol (IP) timestamp option”*. Synchronizacja czasu była więc na tyle istotna, że znalazła się w pierwszym pakiecie standaryzacji protokołów Internetu. W 1985 r. powstała „zerowa wersja” stosowanego powszechnie protokołu NTP (ang. *Network Time Protocol*) jako RFC 958. Obecnie jest ona już nieaktualna, zastąpiona następnymi RFC, najczęściej rozszerzającymi specyfikację lub korygującymi nieścisłości, błędy lub podatności niezidentyfikowane na wcześniejszych etapach rozwoju standardu. Obecna wersja protokołu NTP jest oznaczana numerem 4 wraz z obszerną listą opcji, a ostatnia aktualizacja w postaci RFC 9109 została wydana w sierpniu 2021 r. i dotyczy między innymi bezpieczeństwa (łagodzenie tzw. ataków *Off-Path*).

Protokół NTP ma swoje wady. Ma ograniczoną dokładność synchronizacji czasu i jest podatny na wiele form ataku, a szczególnie jego implementacje. Wyjątkowo duży wysyp podatności związanych z protokołem NTP odnotowano w 2019 r.[5], co między innymi przyczyniło się do wydania wspomnianego RFC 9109.

Alternatywnym, chociaż nadal niszowym, protokołem jest Precision Time Protocol (PTP)[6]. Jego zastosowanie wykracza poza Internet i pozwala na znacznie dokładniejszą synchronizację czasu. Pierwsza wersja protokołu PTP została opublikowana w 2002 r. jako IEEE 1588-2002. PTP w wersji 2, która nie jest kompatybilna z wersją 1 z 2002 r., została opublikowana jako IEEE 1588-2008 i znowelizowana jako IEE 1588-2019 przy zapewnieniu kompatybilności wstecznej.

2 Więcej na ten temat można przeczytać w artykule Jacka Grabowskiego „Czas na czas” zamieszczonym w Biuletynie PTI nr 1 z 2021 r.

3 RFC (ang. *Request for Comments* – dosłownie: prośba o komentarze) – zbiór technicznych oraz organizacyjnych dokumentów mających formę memorandum związanych z Internetem oraz sieciami komputerowymi. Każdy z nich ma przypisany unikatowy numer identyfikacyjny, zwykle używany przy wszelkich odniesieniach. Publikacją RFC zajmuje się Internet Engineering Task Force. 2021 r.

4 Powszechnie znanego z komendy „ping”.

5 Zapytanie https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ntp zwraca 151 podatności (dostęp 27 stycznia 2023 r.).

6 Protokół PTP jest jednym z elementów implementacji w projekcie opisanym w artykule Waldemara Sielskiego „Czas z gniazdka” zamieszczonym w Biuletynie PTI nr 1 z 2021 r.

Wzorce czasu

Istnieją również alternatywne w stosunku do sieci komputerowej mechanizmy synchronizacji czasu. W Polsce możemy odbierać sygnał DCF77 nadawany z Mainflingen, miejscowości położonej ok. 25 km od Frankfurtu nad Menem. Wzorcem czasu jest w tym przypadku atomowy zegar cezowy. Nadajnik o mocy 50 kW pracuje na falach długich o częstotliwości 77,5 kHz, pozwalając na odbiór sygnału w promieniu 2 tys. km. Praktyczna dokładność synchronizacji czasu wynosi mniej niż ±2 ms przy wykorzystaniu profesjonalnych odbiorników w optymalnych warunkach odbioru sygnału (najczęściej w nocy, z dala od sygnałów zakłócających, np. linii energetycznych czy pojazdów elektrycznych). Przy wykorzystaniu dodatkowej modulacji oraz korelacji sygnałów udało się uzyskać laboratoryjnie odchylenie od ±2 do 22 µs w laboratorium położonym poniżej 300 km od nadajnika. Wartość tę należy traktować jako graniczną, nieosiągalną na terenie Polski z uwagi na propagację fal radiowych. W sprzęcie konsumenckim, takim jak zegarki czy stacje pogodowe, uzyskuje się wartości na poziomie ±0,1 s. Są to wartości znacznie gorsze od uzyskiwanych w protokołach NTP (przy stałym opóźnieniu możliwe jest uzyskanie dziesiątych części milisekundy), nie wspominając o protokole PTP, gdzie możliwe jest uzyskanie dokładności na poziomie nanosekund, czyli aż o 6 rzędów wielkości bardziej precyzyjnie.

Obecnie tzw. serwery czasu korzystają z synchronizacji czasu z wykorzystaniem sygnałów GNSS (ang. *Global Navigation Satellite System*). Niewątpliwą przewagą tej synchronizacji jest wysoka dostępność tego sygnału[7] oraz na bieżąco monitorowana wysoka precyzja synchronizacji czasu wykorzystująca zegar atomowy. Teoretycznie ideał.

W wyniku doświadczeń z konfliktu z Pakistanem (maj –czerwiec 1999 r.), Indie zdecydowały się na budowę własnego, niezależnego systemu nawigacji satelitarnej. System GLONASS jest pod kontrolą Rosji, obecnie jawnie wrogiego państwa, które konsekwentnie realizuje swą politykę, wykorzystując globalizację, nieszczelność kontroli eksportu oraz „neutralność" w szczególności Szwajcarii do prowadzenia „własnych biznesów". Przykładem może być NVS Technologies AG, zarejestrowana w Szwajcarii (zarząd: Vasily Engelsberg), która produkuje wielosystemowe odbiorniki GNSS, które niezależnie od ustawień są kontrolowane przez GLONASS. Innym, chociaż mniej jawnie kontrolowanym przez Rosję dostawcą jest U-blox AG, który ma jedno z biur technicznych w St. Petersburgu[8] w Rosji, a jego odbiorniki GNSS są najczęściej identyfikowane w dronach i rakietach wykorzystanych do ataków w wojnie w Ukrainie[9].

> *Musimy jednak pamiętać, że wszystkie systemy GNSS mają rodowód militarny i pozostają pod kontrolą rządu państwa właściciela systemu, który ma pełną kontrolę nad informacjami przesyłanymi przez satelity GNSS.*

Sygnał GNSS jest dość słaby, a tym samym stosunkowo prosty do zakłócenia. Profesjonalne systemy zakłócające działają w strefach istotnych z punktu widzenia wojskowego, np. najbliżej w Kaliningradzie i okalającym go torze wodnym, co jest dobrze widoczne w systemach nawigacyjnych cywilnych samolotów[10]. Popularność GNSS stworzyła również rynek „zagłuszaczy", czyli urządzeń nazywanych z języka angielskiego *jammer*. Są one teoretycznie nielegalne, ale łatwo dostępne. Najtańsze można kupić za niecałe 100 zł, a bardziej zaawansowane za kilka tysięcy złotych. Ich zasięg oraz funkcjonalność[11] nie są porównywalne ze sprzętem wojskowym, ale wystarczające do uniemożliwienia poprawnego odbioru sygnału GNSS w promieniu kilkudziesięciu metrów.

Czas i kryptografia

Czy faktycznie czas ma tak istotne znaczenie? Dlaczego jego synchronizacja jest tak ważna? Przecież większość z nas nie buduje dronów bojowych. Czas jest zjawiskiem

7 Systemy GPS, GALILEO, GLONASS i BEIDOU pokrywają całą kulę ziemską, natomiast Indyjski IRNSS ma obecnie zasięg regionalny, obejmujący Indie i terytoria sąsiadujące w promieniu ok 1,5 tys. km.

8 Informacja o pobiciu rekordu Guinnessa przez rój dronów wyposażonych w układy NEO-M8P RTK wykonane przez U-blox nad St. Petersburgiem 3 września 2020 roku https://www.spatialsource.com.au/record-for-largest-drone-swarm-broken-twice-in-september/

9 O łańcuchu dostaw realizowanych przez europejskie firmy i pozwalających na budowę przez Rosję dronów bojowych, w tym dotyczących technologii GNSS, można przeczytać tutaj https://storymaps.arcgis.com/stories/b9b6bca72ee54b0a9c5f683708248b32

10 Zebrane dane można obejrzeć na stronach https://gpsjam.org/?lat=55.02363&lon=20.33058&z=7.6&date=2023-01-29

11 Oprócz zakłócania możliwości odbioru sygnału poprzez wysyłanie silnych sygnałów na częstotliwości pracy odbiornika, rozwiązania klasy profesjonalnej (wojskowej) mają możliwość manipulowania danymi poprzez spoofing (wysyłanie fałszywych danych) czy meaconing (sztuczne opóźnianie prawdziwych danych).

trudnym do uchwycenia, dlatego nie każdy zdaje sobie sprawę, jak często jest wykorzystywany. Hasło Kerberos jest znane prawdopodobnie ograniczonej liczbie osób, natomiast bardziej znana jest jego implementacja wykonana przez firmę Microsoft, popularnie nazywana „logowaniem do domeny".

Nie wnikając w szczegóły, uwierzytelnianie w tym protokole polega na przesyłaniu tzw. ticketów. Tickety zawierają materiał kryptograficzny (klucze), dlatego mają określony czas życia (znacznik czasu – ang. *timestamp*), aby uniemożliwić złamanie kluczy lub ich kolejne wykorzystanie (atak typu *REPLY*). Z tego powodu kontroler domeny jest domyślnie serwerem czasu, gdyż rozsynchronizowanie zegarów[12] domeny oraz klienta uwierzytelniającego się w protokole Kerberos uniemożliwi uwierzytelnienie się, czyli mówiąc prostym językiem: nie będzie można się zalogować, jak również nie będzie można zmienić hasła. W efekcie system nie będzie dostępny.

No dobrze, ktoś powie, ale ja nie korzystam z domeny Microsoft – to znaczy, że jestem bezpieczny i nic nie muszę robić z czasem. Mam hasło i jak je wpiszę, to się zaloguję. Nikt wtedy nie sprawdza żadnego czasu. Niestety, wszyscy już (mam nadzieję) jesteśmy na tyle świadomi, że samo hasło to za mało. Standardem powoli staje się uwierzytelnianie wieloskładnikowe (MFA – *Multi-Factor Authentication*). Rozwiązań jest wiele, np. *Google Authenticator* czy *Microsoft Authenticator*. Nie potrzeba nic kupować (bo podobno każdy ma smartfon), aplikacja jest „za darmo". Mechanizm wykorzystywany przez te platformy to TOTP (*Time-based One-time Password Algorithm*; opisany w RFC 6238) jako rozszerzenie HOTP (*HMAC-based One-time Password Algorithm*; opisany w RFC 4226). Wygenerowane hasła jednorazowe (z wykorzystaniem aktualnego czasu jako jednego z czynników) są ważne zazwyczaj 30 sekund. W przypadku rozsynchronizowania zegarów klienta i serwera zalogowanie się takim hasłem jednorazowym nie będzie możliwe. Zatem znów z powodu braku synchronizacji czasu możemy stracić dostęp do naszych zasobów.

Ktoś może powiedzieć, że nigdzie się nie loguje i wszystko trzyma na jednym komputerze, a czas mu jest potrzebny jedynie orientacyjnie. Niestety, tu też nie mam dobrych wiadomości. Wszystkie obecnie użytkowane powszechnie systemy operacyjne są wielozadaniowe, niezależnie, czy jest to rodzina Windows, czy rodzina systemów operacyjnych wywodząca się z systemu UNIX (BSD – rodzina systemów Apple czy odmiany systemu Linux niezależnie od wersji, w tym Android). Oznacza to, że jądro tych systemów zarządza zasobami i wątkami. Jednym z elementów wykorzystywanych przez jądro jest czas, którym znakowane są zarządzane obiekty. Wszystko dzieje się zazwyczaj asynchronicznie, a dzięki tym znacznikom czasu jądro systemu może zapanować nad tymi zasobami, w tym ich chronologią. Zmiana czasu może wywołać zjawiska, w których jądro systemu utraci kontrolę nad chronologią tych zjawisk (np. wątek potomny ma wcześniejszy znacznik czasu niż wątek, który go utworzył). Obsługa takiego „błędu" może doprowadzić do kontrolowanej awarii znanej jako *kernel panic* lub *blue screen of death*. Skutkiem będzie najczęściej czasowa niedostępność systemu i/lub utrata niektórych danych.

> *Wszystkie metody kryptograficzne odwołują się do czasu w sposób mniej lub bardziej jawny, gdyż każdy klucz można złamać, wymaga to jedynie czasu. Czas jest zatem komponentem chroniącym ten klucz.*

Potrzeby synchronizacji czasu najczęściej nie trzeba tłumaczyć osobom odpowiedzialnym za rozbudowane systemy przetwarzania danych. Niestety, najczęściej problem synchronizacji czasu jest traktowany po macoszemu, gdyż nie jest tak widoczny, jak np. problemy wydajnościowe. Sprawę komplikuje fakt, że wielu producentów dostarcza domyślne konfiguracje wskazujące różne źródła czasu, często z różnymi nieaktualnymi protokołami. Powoduje to, że rozwiązanie działa po pierwszym uruchomieniu, co skutecznie usypia czujność, lecz de facto nie działa poprawnie. Pamiętajmy, że „atak na czas" daje objawy, jakby wystąpił błąd w jakimś module lub protokole zupełnie niezwiązanym z czasem. Odwraca to uwagę od sedna problemu, gdyż szukamy jego przyczyn nie tam, gdzie trzeba. Niekontrolowana zmiana czasu powoduje, że dzienniki zdarzeń (ang. *log*) tracą swoją spójność[13], przez co stajemy się „ślepi i głusi". Dodatkowo wiele organizacji posiadających serwery czasu korzysta z odbiorników, które mają błędy interpretacji liczników czasu GNSS[14] lub są zmanipulowane tak, aby pozostawały pod kontrolą wrogiej Rosji poprzez GLONASS. W tym miejscu nie należy pytać „czy", lecz „kiedy" te podatności zostaną wykorzystane.

Faktycznie, szczęśliwi czasu nie liczą. Pytanie tylko, jak długo ich *dolce far niente* będzie mogło być opatrywane przymiotnikiem „słodkie".

12 Dla Active Directory ten czas liczony jest w pojedynczych minutach.

13 Zdarzenia są zapisywane asynchronicznie, przez co nie można powiązać kolejności wpisów z faktem ich wystąpienia. Podstawą jest wtedy jedynie znacznik czasu, który może zostać zmieniony w przypadku ataku na czas.

14 W przypadku GPS może to dawać skoki czasu o ponad 19 lat (GPS WNRO).