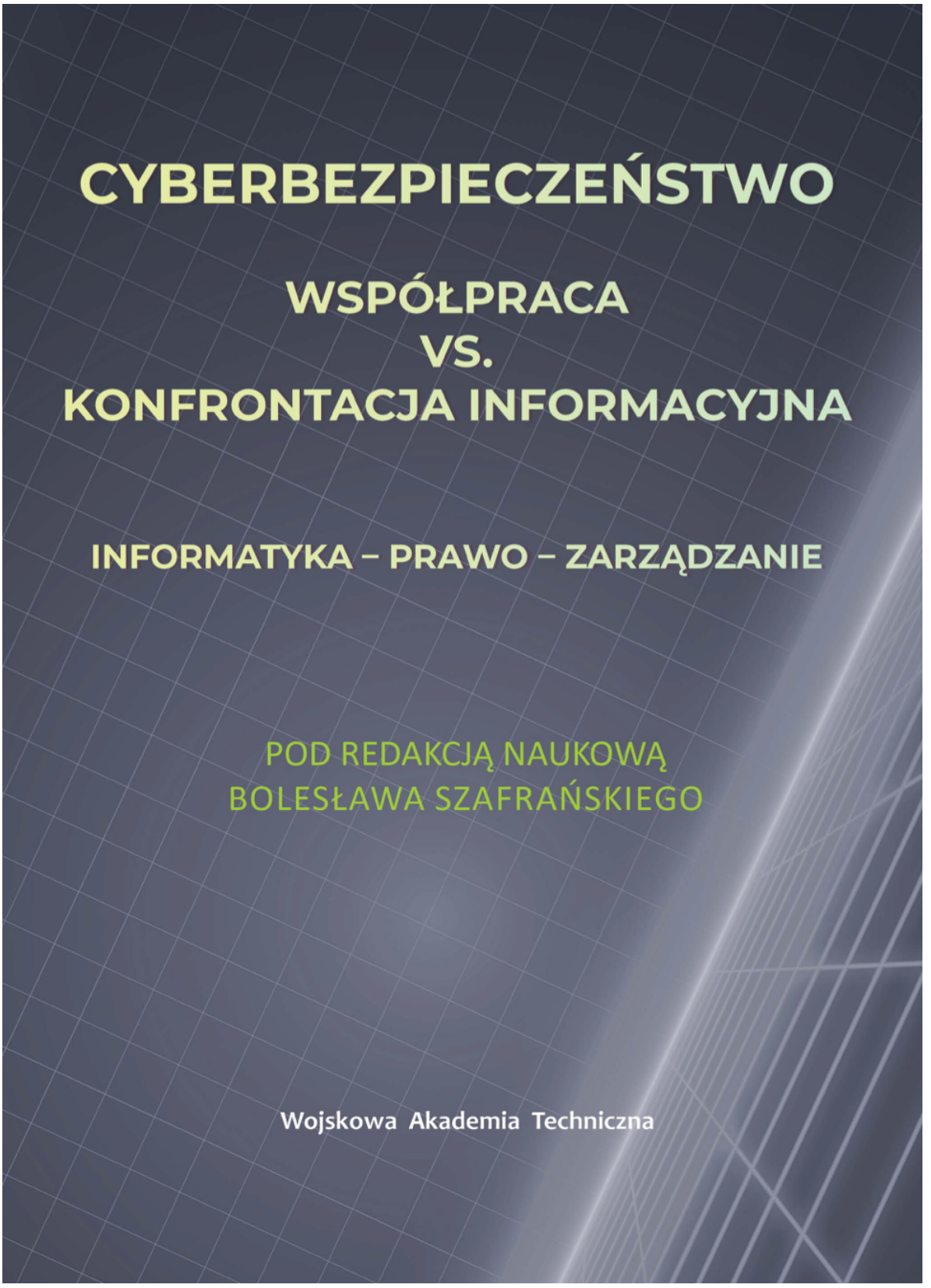
Okładka książki



Rozdział XVIII

Atak na czas, opóźnienie i synchronizację IT/OT: Skuteczna cyberbroń przyszłości

Tomasz Widomski
ELPROMA Elektronika Sp. z o.o.
05-152 Czosnów, ul. Duńska 2a

1. Wstęp

Współczesna informatyka wymaga synchronizacji względem jednego, wiarygodnego wzorca czasu. Zapotrzebowanie na synchronizację w IT, a szczególnie na tę o wysokich precyzjach, stale rośnie. Czas używany jest do celów informacyjnych, automatyzacji, zapewnia chronologię, jest ważnym katalizatorem nowych zaawansowanych technologii. Koordynuje pracę komputerów, robotów, systemów operacyjnych, aplikacji, a nawet całych serwerowni współtworzących rozproszone środowisko IT połączone siecią TCP/IP.

Celowo wywołana desynchronizacja dostarcza stronie atakującej narzędzie dezinformacji, destabilizuje zautomatyzowane komputerowo procesy, wywołuje chaos (zaburza chronologię), blokuje koordynację (katalizator) rozproszonej architektury IT. Skutkiem jest obniżenie wydajności pracy systemów, brak dostępu do wybranych usług, awarie, a nawet blackout. W przypadku infrastruktury krytycznej coraz bardziej zależne od siebie wewnętrzne podsystemy mogą przy awarii jednego z nich wywołać efekt lawinowy. Nic więc dziwnego, że czas i synchronizacja stały się elementem współczesnej wojny hybrydowej. W użyciu hakerów blackhat desynchronizacja stanowi bardzo skuteczne, trudne w rozpoznaniu, a więc również do obrony, narzędzie powodowania destabilizacji IT w dużej skali, a w przemyśle OT (ang. *Operational Technology*), w tym przede wszystkim w sieciach infrastrukturalnych, odizolowanych od Internetu ze względu na cyberbezpieczeństwo.

W rozdziale opisano zagadnienie synchronizacji złożonych systemów IT i OT, na których oparte są infrastruktury krytyczne określone w dyrektywie unijnej NIS2[1]. Autor zachęca do zapoznania się z pozycjami literatury [1], [2], będącymi wstępem, a w dużej mierze rozwinięciem poruszanej tematyki.

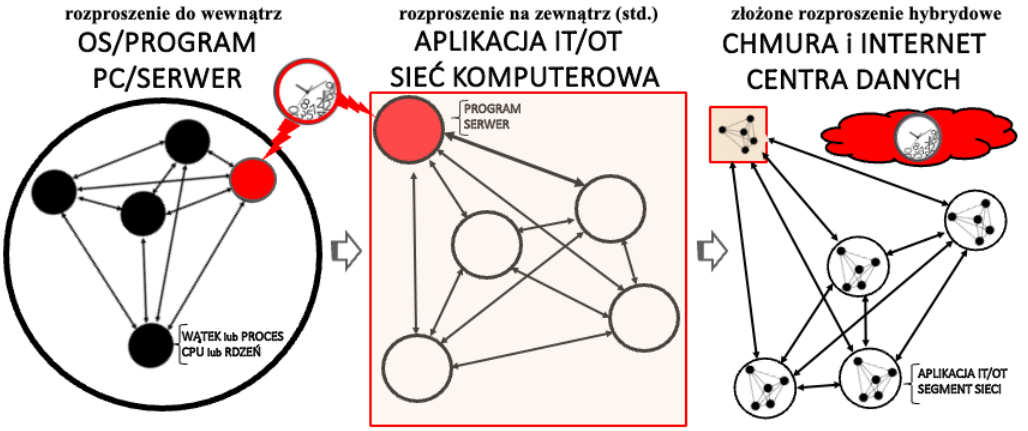
2. Rola synchronizacji w złożonych systemach rozproszonych

Zanim świat połączył Internet, zgodny czas w informatyce nie był aż tak istotny. Synchronizację procesów w pojedynczym komputerze zapewniały semafory i ich pochodne. Chroniły one dostęp do współdzielonych zasobów sprzętu i oprogramowania oraz do danych.

[1] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

Wadą operacji wyłącznego dostępu był efekt uboczny błędów popełnianych przez programistów, polegający na zawieszeniu systemu, a często również na utracie cennych danych. Sytuacja zmieniła się wraz z rozwojem sieci. Osiągając granice maksymalnej prędkości pracy procesorów (CPU), świat przyjął jedyny pozostały mu kierunek zwiększania wydajności w informatyce – zrównoleglanie i rozpraszanie przetwarzania informacji. Trend ten trwa nadal i osiągnął dziś bardzo niebezpieczny poziom tworzenia zbyt silnych wzajemnych powiązań całych systemów informatycznych, pracujących wcześniej niezależnie. Ryzyko poważnych awarii narasta, ponieważ rośnie złożoność systemów oraz ich rozproszenie na coraz większe odległości. Tworzone są nowe nadrzędne duże struktury, tzw. systemy systemów. Taka złożoność wymusza zmiany podejścia w zarządzaniu systemami IT i OT określane terminami *obserwowalność* (ang. *observability*), *koordynacja czasowa* TCC (ang. *Time Coordinated Computing*). Powstają nowe odmiany sieci, tzw. *sieci niskich latencji* (ang. *Low Latency Networking*) oraz idealnie optymalny Ethernet TSN (ang. *Time Sensitive Networking*).

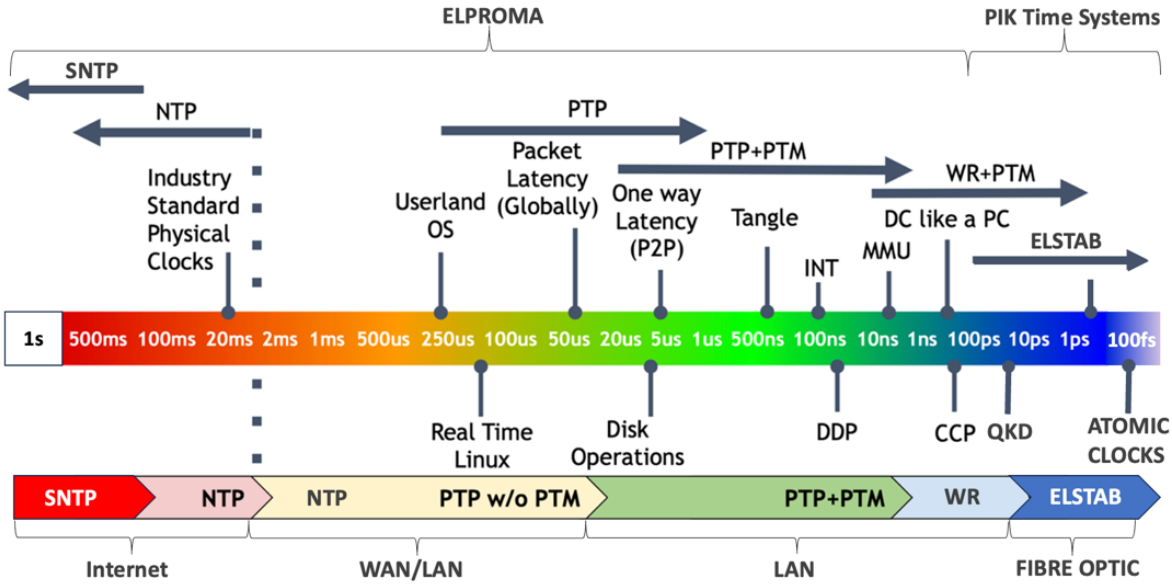
Observability to zdolność definiowania stanu wewnętrznego nawet bardzo złożonych systemów teleinformatycznych na podstawie ich zewnętrznych danych. Można powiedzieć, że system jest obserwowalny, kiedy zbieranie pochodzących z niego danych daje możliwość badania, jak ten system działa, jakie występują w nim problemy oraz jak wpływają one na pracę całego systemu. Oznacza to konieczność umiejscowienia pracy systemów we wspólnej domenie czasu. Następnie z użyciem metodyki *DevOps* można w nich wpływać na zarządzanie systemem, tworzyć dynamicznie obejścia zapobiegające awariom. Całość można wykonywać bez modyfikacji kodu programów i bez zmian na poziomie firmwaru urządzeń. Zapewnia to skuteczne narzędzie obsługi najbardziej złożonych, na różnych poziomach abstrakcji sprzętu (HW) i oprogramowania (SW), rozproszonych systemów IT i OT. Jest to możliwe wyłącznie pod warunkiem zapewnienia im zgodnego wzorca czasu (rysunek 1).



Rys. 1. Rodzaje rozpraszania do wewnątrz i na zewnątrz oraz ich ewolucja złożoności HW i SW. HARDWARE (HW): procesor/rdzeń => serwer/sieć => infrastruktura IT/OT => centra danych; SOFTWARE (SW): wątek/proces => program/os => aplikacja IT/system OT => chmura/Internet

3. Synchronizacja systemów operacyjnych Windows i Linux

Wszystkie komputery i urządzenia przemysłowe dołączane do sieci komputerowej TCP/IP wyposażone są w zegar. Nie mówimy tu jednak o zegarach sprzętowych ani o wyświetlaczach informacyjnych czasu, ponieważ nie stanowią one poważnego zagrożenia dla IT/OT i mogą co najwyżej dezinformować. Poruszamy bardzo ważną, niszową problematykę utrzymania wspólnej domeny czasu w skali UTC[2] oprogramowania, które pracuje w złożonej strukturze rozproszonej komputerów o zróżnicowanej architekturze sprzętu. Najmniejszym, a zarazem najważniejszym wspólnym elementem całej struktury synchronizacji jest system operacyjny (OS), a w przypadku urządzeń (HW) jest to firmware oparty na OS, np. Linux.

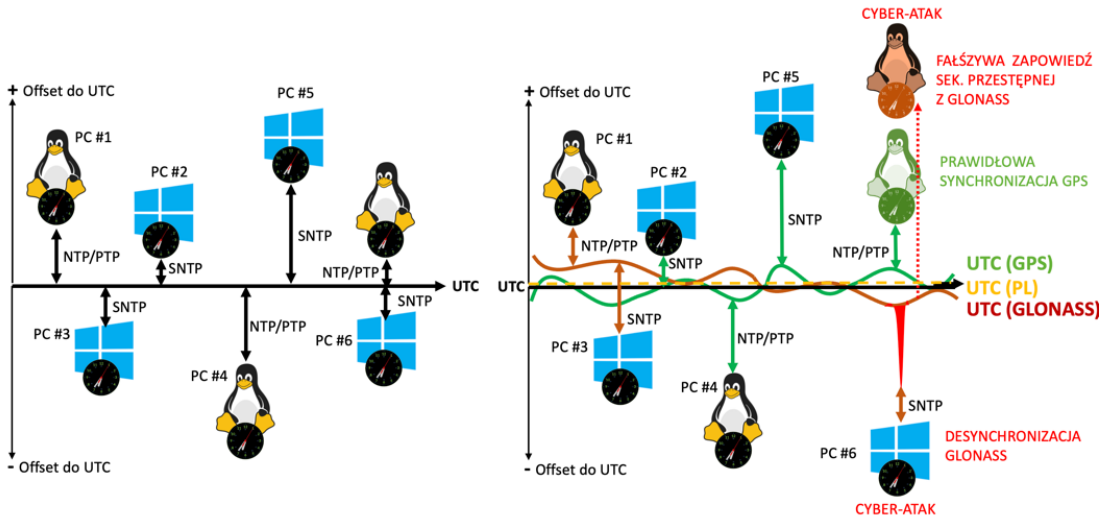


Rys. 2. Porównanie dokładności synchronizacji: NTP, PTP, PTP+PTM i White Rabbit (WR)
Źródło: Ahmad Byagowi (Facebook), zaktualizowane przez firmę ELPROMA

Każdy system operacyjny, *Windows*, *Unix*, *Linux* oraz ich pochodne posiada wbudowany zegar programowy na poziomie swojego jądra (ang. *kernel*). Wymaga on synchronizacji do zewnętrznego źródła UTC. Wzorcowy czas dostarczany jest lokalnie interfejsem szeregowym lub siecią TCP/IP z wykorzystaniem protokołów NTP[3] (*Network Time Protocol*) i PTP[4] (*Precision Time Protocol – IEEE 1588*). Protokoły różnią się oferowaną dokładnością synchronizacji (rysunek 2). Dokładność synchronizacji może osiągać dziś pojedyncze nanosekundy, ale wymaga to specjalnej wersji kart sieciowych z tzw. znakowaniem sprzętowym PTM korygującym wewnętrzne opóźnienie pakietów ze znacznikami czasu. Dostarczony czas może być przeliczany na lokalny czas strefowy, ale odbywa to się zawsze w wyższej warstwie OS poza jądrem *kernel* lub wręcz na poziomie aplikacji.

[2] https://en.wikipedia.org/wiki/Coordinated_Universal_Time.
[3] https://en.wikipedia.org/wiki/Network_Time_Protocol.
[4] https://en.wikipedia.org/wiki/Precision_Time_Protocol.

Programowy zegar systemowy OS inicjuje swoją wartość początkową w chwili ładowania systemu operacyjnego. Pobiera go z podtrzymywanego bateryjnie zegara sprzętowego. Z chwilą gotowości OS do pracy czas odmierzany jest dalej wyłącznie programowo na poziomie jądra OS i proces ten wymaga stałej synchronizacji zewnętrznej do wzorca UTC. Do tego celu używa się sieciowego protokołu synchronizacji NTP, a ostatnio również bardziej dokładnego PTP IEEE 1588. Oba pracują w warstwach L2–L4 sieci Ethernet, używając pakietów UDP (TCP/IP). Oba mogą również działać jednocześnie w tej samej sieci, a nawet na tych samych komputerach, co wymaga dużego doświadczenia w konfigurowaniu. Synchronizacja sieci korporacyjnej odbywa się z użyciem serwerów czasu[5] NTP/PTP dostrajanych do wzorca UTC bezpośrednio z metrologii NMI, za pośrednictwem satelitów GNSS, do infrastruktur krytycznych, np. 5G, do grup serwerów publicznych POOL[6] i eCzasPL[7].



Rys. 3. Komputery PC różnią się offsetem czasu względem idealnego UTC (a), rzeczywisty offset czasu zależy od tego, do jakiej skali UTC(k) się synchronizują (b)
Źródło: własne

Skala czasu UTC nie jest jednolita. Współtworzy ją wiele laboratoriów na świecie. Skale UTC(k) poszczególnych państw różnią się nieznacznie na poziomie nanosekund. Skala UTC dla systemu satelitarnego GPS jest wojskową skalą laboratorium USNO w USA i będzie się różnić od skali rosyjskiego GLONASS. Obie różnią się od pozostałych systemów rodziny GNSS (Galileo, Beidou, IRNSS). Wszystkie będą się różnić od polskiej skali czasu urzędowego UTC(PL), jaką wytwarza Główny Urząd Miar RP. Ma to niewidoczny dla systemu dodatkowy wpływ na rozbieżności czasu między synchronizowanymi węzłami rozproszonej sieci, ale tylko tam, gdzie istotne są duże dokładności osiągane z pomocą PTP-PTM. Wpływa to pośrednio na jakość synchronizacji, a w konsekwencji na desynchronizację ograniczającą funkcjonalność rozwiązania realizowaną dopiero na poziomie aplikacji. Dlatego bardzo ważne jest, aby dbać o synchronizację tylko do jednego wzorca UTC. Na

[5] https://en.wikipedia.org/wiki/Time_server.
[6] https://www.ntppool.org/zone/pl (nierekomendowane do używania innego niż w zast. domowych).
[7] https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html (rekomendowane do użycia).

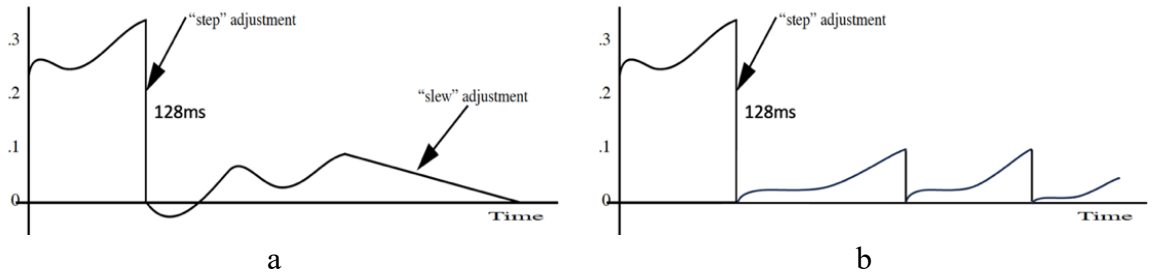
obszarze RP obowiązuje polska skala UTC(PL). Oficjalny polski czas definiuje ustawa o czasie urzędowym z dnia 10.12.2003 r. (Dz.U. Nr 16, poz. 144), a metody dystrybucji określa rozporządzenie (Dz.U. Nr 56 z 2004 r., poz. 548), wywołując skutki prawne w Polsce. O ile dystrybucja systemu Linux jest standardowo wyposażona w protokół NTP, to systemy operacyjne Windows mają jedynie wbudowaną uproszczoną jego wersję – SNTP. Oba rozwiązania różnią się trzema bardzo ważnymi dla cyberbezpieczeństwa cechami (tabela 1).

Tabela 1. Trzy ważne cechy różnicujące funkcjonalności protokołów NTP i SNTP

Różnice:	**NTP**	**SNTP**
1) **Płynne** dostrajanie czasu UTC na poziomie jądra *OS kernel*	TAK	NIE
2) **Wielośródłowość** – obsługa wielu wzorców UTC jednocześnie	TAK	NIE
3) **Uwierzytelnienie** kryptograficzne źródłowych serwerów UTC	TAK	NIE

W dużym uproszczeniu płynne strojenie zegara NTP w jądrze OS do zewnętrznego wzorca UTC realizowane jest na wzór einsteinowskiego relatywistycznego zjawiska dylatacji czasu. Efekt taki osiąga się w komputerze przez rozciąganie lub kurczenie wirtualnego czasu we wnętrzu *kernel*. Technicznie wykonuje się to przez okresową redefinicję parametru częstotliwości zegara. Wpływa ona płynnie na podstawowy interwał pomiaru upływu czasu w systemie operacyjnym.

Dla zilustrowania mechanizmu działania płynnej korekcji zegara niech upływ jednej sekundy reprezentowany będzie zliczaniem w pętli wartości od 0 do 999. Skracając zliczanie do wartości 899, zmniejszamy interwał wewnętrzny płynnie o 10% względem upływu czasu w świecie rzeczywistym. Analogicznie zwiększając wartość zliczania do 1099, czas odmierzany w komputerze będzie płynął wolniej o 10%. W ten sposób można płynnie manipulować strojeniem czasu jądra OS, unikając skoku zegara. Odbywa się to kosztem chwilowej rozbieżności (na czas prowadzenia korekcji) między wirtualnym upływem czasu w systemie operacyjnym a czasem rzeczywistym, jakiego doświadczamy w świecie fizycznym. W praktyce proces płynnego strojenia zegara i synchronizacji NTP jest znacznie bardziej złożony. Płynne strojenie jest często błędnie utożsamiane z jakością próbkowania DSP konwersji analogowo-cyfrowej, która z natury zawsze tworzy dyskretny obraz schodkowy. Płynne strojenie zegara programowego OS jest więc innym zagadnieniem.



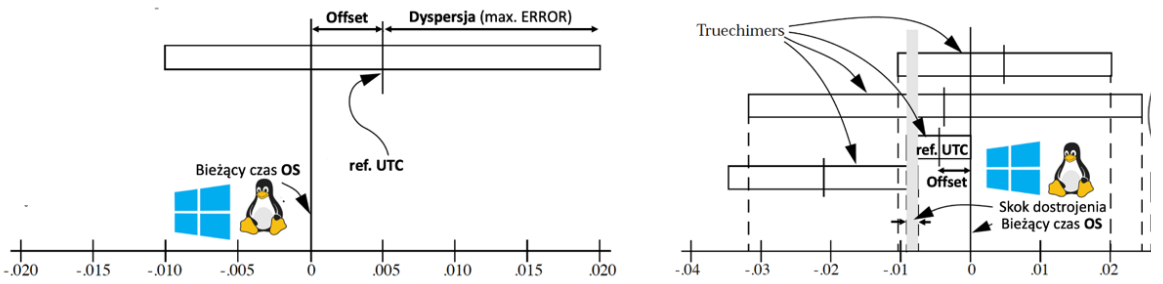
Rys. 4. Płynne dostrajanie zegara w NTP (a), skokowe dostrajanie zegara SNTP (b)
Źródło: własne

Skokowe dostrajanie SNTP czasu jądra Windows i Linux jest dla nas bardziej intuicyjne, ale w praktycznej realizacji niestety bardziej niebezpieczne dla stabilności rozwiązania. Technika ta przypomina zwykłe zapytanie do serwera o czas z natychmiastowym dostrojeniem własnego zegara do uzyskanej odpowiedzi. Wadą tej metody są wymuszone przestawienia czasu zegara na poziomie OS *kernel*, a w konsekwencji „luki" w czasie wirtualnym systemu operacyjnego tworzące ryzyko stabilności dla poziomu aplikacji. W przypadku skoordynowanego w domenie czasu przetwarzania rozproszonego TCC może to prowadzić do niedeterministycznego zachowania się całego rozwiązania. Dlatego skokowa korekcja SNTP powinna być używana wyłącznie w komputerach użytkowników końcowych i nie powinna być stosowana w serwerach ani na poziomie firmwaru urządzeń sieciowych, jak routery.

Dobrą wiadomością dla użytkowników systemów firmy Microsoft jest to, że można samodzielnie skompilować protokół NTP dla rodziny systemów operacyjnych Windows. Gotową do użycia binarną wersję protokołu NTP, tę z płynną regulacją dostrajania zegara OS i płynną korekcją *leap sekundy* UTC, udostępnia Główny Urząd Miar RP na stronach serwisu eCzasPL.

Wielośródłowość (tabela 1, p. 2) jest kolejną bardzo ważną właściwością NTP, której nie ma SNTP. Nie jest tożsama z redundancją źródeł (serwerów) czasu UTC. O ile redundancja to zdolność do automatycznego rozpoznawania i zastępowania w procesie synchronizacji OS-*kernel* niedziałających źródłowych serwerów czasu NTP, o tyle wielośródłowość to mechanizm doboru wielkości korekcji lokalnego czasu zegara w jądrze OS. Wykorzystuje ona do tego statystyki błędów rozbieżności *offset* UTC chodu zegara OS-*kernel* porównywanego z wzorcem czasu wielu źródłowych serwerów czasu NTP jednocześnie (rysunek 5b). Wielośródłowość w protokole NTP oparto na algorytmie DTS algebry autorstwa K. Marzullo[8] opracowanym już w 1983 roku dla potrzeb armii USA. Niewiele osób zdaje sobie nawet dzisiaj sprawę, jak ważną rolę dla zapewnienia bezpieczeństwa synchronizacji pełni ten algorytm standardowo wbudowany w protokół NTP. Klasyfikuje źródłowe serwery czasu NTP na grupy Truechimers i Falsetickers, dopuszczając do synchronizacji wyłącznie te pierwsze. Pozwala to chronić się przed „zatrutymi" serwerami czasu, np. publicznej grupy serwerów POOL NTP (wątek poruszamy w kolejnych akapitach). Algorytm DTS pozwala podczas pracy NTP dynamicznie izolować z grupy te źródłowe serwery NTP, których czas jest manipulowany przez atakującego, np. przez naziemne zakłócanie sygnałów GPS (tzw. jamming i spoofing GNSS). W taki sposób można desynchronizować sieci odizolowane od Internetu, co jest najważniejszym przekazem tej publikacji. Gdy NTP używa jednego źródła czasu UTC, sytuacja jest dość prosta. Dla wartości offsetu większych niż 128 ms protokół NTP wykonuje jednorazowe dostrojenie skokowe i następnie przechodzi do płynnego strojenia (rysunek 5a). Używa w tym celu min. skoku strojenia, który zapewni zgodność zegara OS z ref. UTC podczas kolejnej kontroli. Gdy NTP używa wielu źródłowych serwerów czasu, procedura jest znacznie bardziej złożona. Algorytm Marzullo[10] klasyfikuje dostępne serwery czasu i wybiera z grupy Truechimers najlepszy źródłowy serwer NTP.

[8] https://en.wikipedia.org/wiki/Marzullo%27s_algorithm.

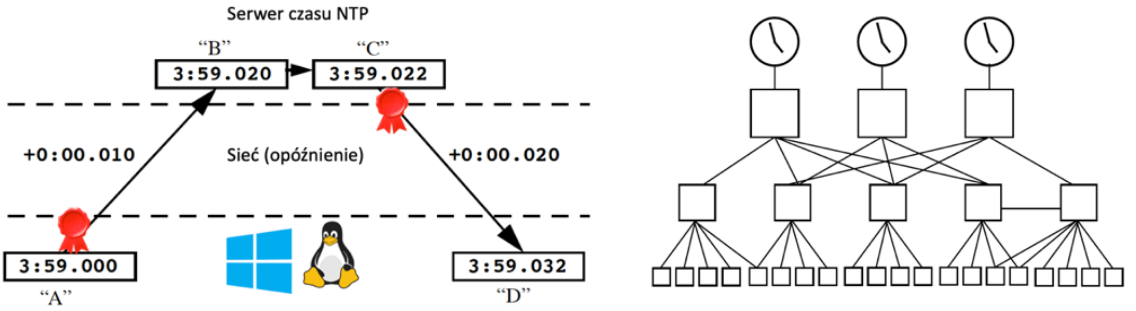


a b

Rys. 5. Synchronizacja do pojedynczego źródła (a) vs. wieloźródłowość (b)
Źródło: własne

Grupę tę tworzy największa liczba serwerów źródłowych NTP, o najmniejszym wspólnym obszarze prostokątów reprezentujących dyspersję – tzn. widziany przez zegar OS błąd serwera wzorcowego NTP (rysunek 5b). Wspólna część prostokątów wyznacza ostateczną najmniejszą wartość regulacji chodu lokalnego zegara OS dążącego płynnie do czasu wzorcowego serwera NTP z grupy Truechimers. Sewery czasu oznaczone jako Falsetickers uważa się za „zatrute" i nie biorą one udziału w procesie synchronizacji NTP. Opisany proces powtarzany jest cyklicznie, tworząc dynamikę zmian zawartości grup Truechimers/ Falsetickers, a to zapewnia prawidłowy proces synchronizacji.

Uwierzytelnienie kryptograficzne (tabela 1, p. 3) zapewnia wiarygodność używanych źródeł UTC, zapobiegając podmianie pakietów synchronizacyjnych na najniższym poziomie *round-trip*. Synchronizacja NTP tworzy wielopoziomową hierarchię STRATUM 0–15 (rysunek 6b). Pozwala to na synchronizację tysięcy klientów NTP jednocześnie.



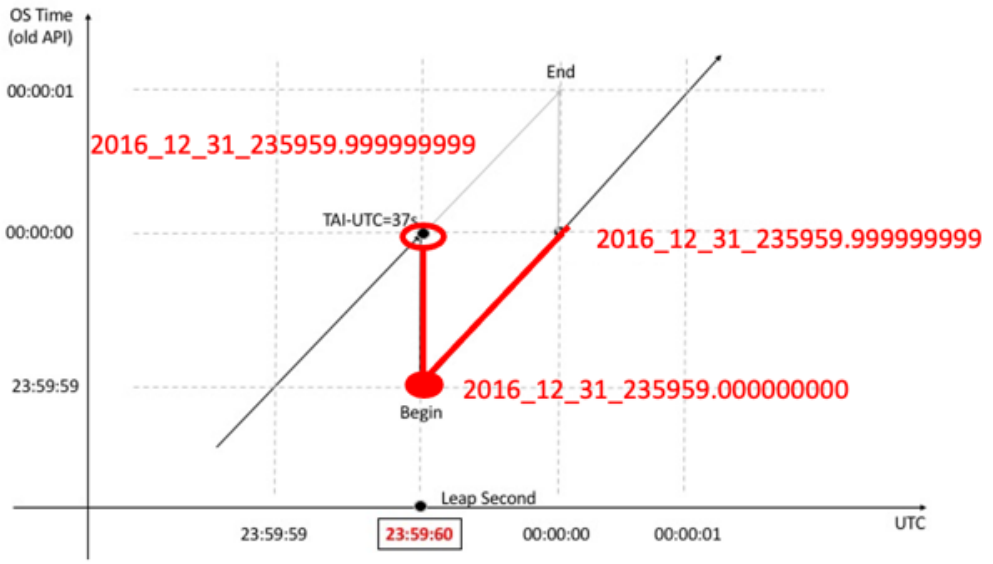
a b

Rys. 6. Round-trip uwierzytelnionych pakietów (a), drzewo STRATUM (b)
Źródło: własne

Trudniejszy w ocenie płynności strojenia czasu zegara jądra OS jest protokół precyzyjnej synchronizacji PTP IEEE1588. W standardowej implementacji Linux nie wspiera on sprzętowej korekcji opóźnień wewnętrznych kart sieciowych. Sprawia to, że zarówno dokładność, jak i sposób obsługi strojenia PTP są wtedy zbliżone do NTP. Sprzętowe wsparcie kompensacji opóźnień wewnętrznych w karcie LAN (tzw. *hardware time-stamping*) pozwala zwiększyć dokładność poniżej jednej nanosekundy. Ta jakościowa zmiana precyzji o kilka rzędów wielkości zaciera w PTP różnicę między płynnym

i skokowym strojeniem czasu zegara w jądrze OS, ale IEEE1588 kryje inną pułapkę. Bazuje ona na ciągłej skali czasu atomowego TAI, podczas gdy informatyka używa UTC. Obie skale różnią się dziś o 37 sek. przestępnych. Aby policzyć UTC, sterownik karty klienta PTP musi sam uwzględnić przesunięcie. Prosta operacja przeskalowania 37 sek. TAI-2-UTC wnosi trwały ślad synchronizacji na poziomie nanosekund podczas obsługi kolejnych nowych *leap sekund*. W finansowo-giełdowym sektorze zautomatyzowanych inwestycji HFT to dodatkowy wielomilionowy zysk lub strata. Dlatego musimy poświęcić uwagę tej jednej sekundzie UTC.

Wspólnym wyzwaniem NTP i PTP jest obsługa sekund przestępnych[9] UTC OS-*kernel*. Kolejna 38 dodatnia *leap sekunda* stworzy precedens związany z koniecznością cofnięcia czasu o 1 s. Wprowadza tym samym ryzyko replikacji prac porządkowych (ang. *utilization*), jakie system prowadzi OS w jądrze. Może to zawiesić Windows BSoD[10] i Linux KP[11], w tym firmware urządzeń opartych na Linuxie.



Rys. 7. Obsługa dodatniej *leap second UTC*
Źródło: własne

Z kolei pierwsza w historii UTC ujemna *leap second* pozostawiłaby jednosekundową lukę w UTC. Tworzy to z kolei ryzyko pominięcia ważnych prac porządkowych w *OS kernel*. Obecnie systemy OS stosują zaproponowaną w 2015 roku technikę Google Smear[12].

[9] https://en.wikipedia.org/wiki/Leap_second.
[10] https://en.wikipedia.org/wiki/Blue_screen_of_death.
[11] https://en.wikipedia.org/wiki/Kernel_panic.
[12] Google Smear Leap Second, https://developers.google.com/time/smear.

4. Atak na czas, opóźnienie i synchronizację IT/OT

Według Wiesława Paluszyńskiego[13] z PTI desynchronizacja stanowi poważne zagrożenie infrastruktur krytycznych NIS2[14]. Działa ona podobnie do wpływu arytmii serca na zdrowie człowieka. Może skutecznie zaburzyć stabilność pracy energetyki, łączności 5G, transportu (kolej, lotnictwo), IT administracji państwowej, produkcji przemysłowej, służb i wojska. Rozsynchronizowanie sprzężonych siecią TCP/IP serwerów opartych na Windowsie, Linuxie (również urządzeń, których firmware oparto na ww. systemach) prowadzi do nieprawidłowości obliczeń *delay* odizolowanych od Internetu sieci infrastrukturalnych. W przypadku rozproszonej automatyki przemysłowej może to prowadzić do akceptacji zdezaktualizowanych danych i odrzucenia tych prawidłowych. W konsekwencji sterowane coraz częściej predykcją sztucznej inteligencji AI systemy przemysłowe mogą podjąć błędną decyzję, co doprowadzi je do awarii. Definiuje to nowy rodzaj zagrożeń istotny w czasach trwającej transformacji cyfrowej *Industry 4.0*, którym towarzyszy niezauważona postępująca złożoność wewnętrzna systemów oraz powstające zbyt duże współzależności całych systemów informatycznych (rysunek 1), które mogą w efekcie domina doprowadzić do awarii wywołujących kryzys. Dlatego desynchronizację uważa się za cyberbroń. Określono też dwa rodzaje nowych cyberataków: **Time Synchronization Attack** (atak na czas) i **Time Delay Attack** (atak na opóźnienie). Głównymi instrumentami realizacji ataków są:

- **jamming i spoofing GNSS** – zakłócenia sygnałów satelitarnych, np. GPS;
- **zatrucie POOL.NTP** publicznej sieci anonimowych serwerów NTP.

Antidotum na powyższe zagrożenia to odpowiednio:

- **naziemne używanie skali UTC(PL)** z Głównego Urzędu Miar RP (GUM);
- **używanie eCzasPL** – kontrolowanej przez GUM RP alternatywy dla POOL.

Podkreślmy jednocześnie, że nie należy całkowicie wykluczyć z synchronizacji technik satelitarnych GNSS, a jedynie świadomie nadać priorytet synchronizacji do polskiej skali czasu urzędowego UTC(PL) za pośrednictwem systemu eCzasPL[15]. Tam, gdzie brakuje sieci TCP/IP, należy nadal używać GNSS stanowiący zapasowe źródło czasu, ale wyłącznie ograniczyć się do konstelacji GPS i Galileo. Nie należy używać rosyjskiego wojskowego systemu Glonass ani chińskiego Beidou. Bardzo ważne jest ustanowienie procedur postępowania awaryjnego w przypadku całkowitego braku sygnałów GNSS i jednoczesnej przerwy łączności NTP/PTP z systemem eCzasPL Głównego Urzędu Miar RP. W takim przypadku trzeba również brać pod uwagę mobilne urządzenia do przenoszenia czasu z podtrzymaniem UTC.

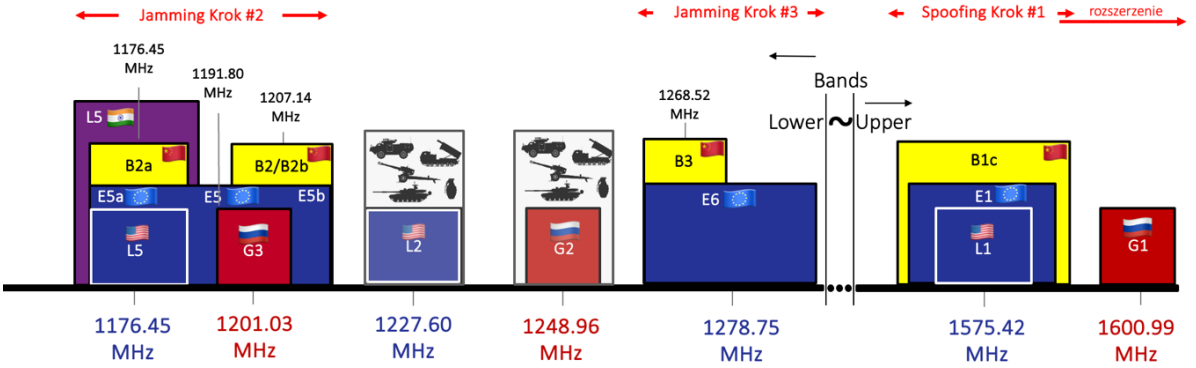
[13] Wywiad z prezesem PTI Wiesławem Paluszyńskim dla eCzasPL, https://youtu.be/smRxpEoyEDw.

[14] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en.

[15] https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.

5. Jamming i spoofing GPS/GNSS

Być może okaże się w niedalekiej przyszłości, że obecne zakłócanie sygnału GPS nad Polską ma na celu przyzwyczajenie nas, abyśmy nie reagowali, również wtedy, gdy nadejdzie prawdziwy atak, który odsłoni swoje pełne możliwości operacyjne destabilizacji IT/OT. Taki scenariusz ataku spoofingowego GPS wspierany blokowaniem innych konstelacji symuluje się już dziś na stołach laboratoryjnych[16]. Nie obronią się przed nim nawet wyposażone w ochronę antyjammingową i spoofingową najnowszej generacji odbiorniki GNSS. Mogą one być nadal manipulowane, jeżeli dobrze dobierze się sekwencje ataku (rysunek 8).



Rys. 8. Kolejne fazy ataku radiowego na IT/OT fałszujące GPS L1 i zakłócające pozostałe GNSS
Źródło: własne na podstawie symulacji laboratoryjnej ataku

6. Zagrożenia *backdoor* w chipach odbiorników GNSS

Jedną z bardzo prawdopodobnych przyczyn powstania amerykańskiej prezydenckiej dyrektywy bezpieczeństwa EO13905[17] był fakt identyfikacji w USA dużej liczby odbiorników GNSS, które zamiast GPS pozostawały pod kontrolą rosyjskiego GLONASS i chińskiego BEIDOU. Działo się tak mimo programowego wyłączania wsparcia obu wrogich konstelacji.

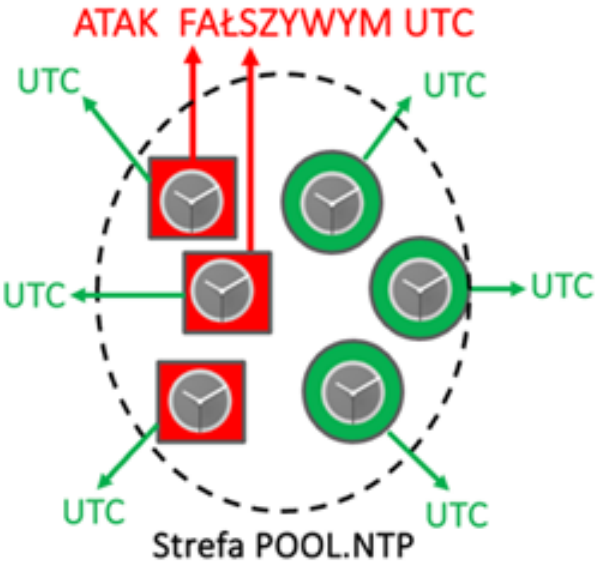
Skala problemu okazała się na tyle duża, że ówczesna administracja prezydenta D. Trumpa przygotowała rozporządzenie rekomendujące uniezależnienie się infrastruktur krytycznych USA od własnego systemu wojskowego GPS i korzystanie w to miejsce z naziemnych systemów dystrybucji wzorca czasu UTC z NIST. Rysunek 3b ilustruje sytuację wpływania na odbiornik GPS z poziomu GLONASS. Jeżeli Windows synchronizowany jest do UTC (GLONASS), to rosyjski system ma kontrolę i może dowolnie wpływać na zmianę jego czasu. Z kolei jeżeli Linux korzysta prawidłowo z GPS, to nieodizolowanie GLONASS może wywołać fałszywą sztuczną *leap second* odbiornika, doprowadzając do desynchronizacji. Skok czasu może być duży, bo w praktyce odbiorniki GNSS nie radzą sobie z obsługą tej jednej sekundy przestępnej UTC.

[16] Symulacja ataku na infrastrukturę IT z użyciem spoofingu GPS: https://youtu.be/BR6YIweVjeY.
[17] US Federal Register, https://www.govinfo.gov/app/details/DCPD-202000071.

7. Zatrucie POOL.NTP publicznej sieci anonimowych serwerów

Z puli anonimowych publicznych serwerów POOL.NTP[18] korzysta standardowo każda dystrybucja Linux oraz oparty na niej sprzęt: serwery, routery sieciowe i urządzenia IoT. Używając POOL, nie wiemy, do czego się synchronizujemy. System losowo przydziela nam na poziomie DNS serwery NTP, które każdy może wstawić do POOL i zdalnie kontrolować.

Atak przez „zatrucie" dowolnego kraju polega na fizycznym zainstalowaniu na jego terytorium dużej liczby kontrolowanych przez atakującego serwerów NTP i zgłoszenie ich do POOL. Serwerami takimi można wybiórczo manipulować na poziomie adresacji IP.



Rys. 9. Czerwone serwery są zatrute, zielone nie. Prawdopodobieństwo użycia zatrutych to 50%
Źródło: własne

Można tak celowo wysyłać błędny wzorcowy czas do wyselekcjonowanych IP użytkowników (np. instytucji rządowych, administracji publicznej, telemetrii przemysłowej itp.) i jednocześnie utrzymywać prawidłowy czas innym użytkownikom, w tym monitorującym jakość usługi serwerom w USA. Antidotum trucizny polega na prewencyjnej instalacji 2–4 razy większej (od istniejącej populacji) grupy „zdrowych" serwerów czasu NTP synchronizowanych do wiarygodnego wzorca UTC. Tylko w ostatnim kwartale roku 2024 Rosja zwiększyła tak liczbę swoich serwerów o 200%. Wcześniej w 2012 roku Niemcy i Francja zwiększyły liczbę swoich serwerów o 100%. Było to podczas tzw. kryzysu EURO. Kryzys finansowy w 2008 roku pozostawił w statystyce POOL NTP wyraźny ślad 100% wzrostu liczby serwerów POOL NTP w USA i UK. W Polce mamy Uchwałę #2 RdC MC KPRM z dnia 3.02.2022 r. rekomendującą wzrost liczby krajowych serwerów NTP strefy *pl.pool.ntp.org* do min. 400 serwerów[19]. Wpływ zatrucia POOL.NTP minimalizuje używanie NTP (w miejsce SNTP), ale niewielu administratorów o tym wie. Dlatego bezpieczeństwu szkodzi fakt, że Microsoft Windows używa std. SNTP.

[18] https://www.ntppool.org/zone/europe.
[19] https://www.gov.pl/attachment/a748fde4-8912-4412-b8b2-0718e4e27e0b.

8. Błędy przepełnień wynikające z numerycznej reprezentacji

Skuteczność ataków z użyciem zakłócania GNSS i sieciowego spoofingu nie byłaby tak istotna, gdyby nie słabość techniki wynikająca z numerycznej reprezentacji czasu w IT.

Rys. 10. GPS overflow
Źródło: GUM RP

Przejawia się to skłonnością do efektywnego powstawania przepełnień numerycznych (rysunek 10). Wyzerowanie formatu, zmiana choćby 1 bitu informacji o czasie potrafi skutkować skokiem nawet o dwadzieścia lat. Problem znany jako WNRO[20] można wywoływać również sztucznie w odbiornikach GNSS kodowanym atakiem jammingowym GPS, wpisując wartość 0 do depeszy nawigacyjnej. Innym przykładem problemów może być skutek błędu telemetrii GPS znany jako SVN23[21].

9. Wpływ desynchronizacji na awarie IT i OT

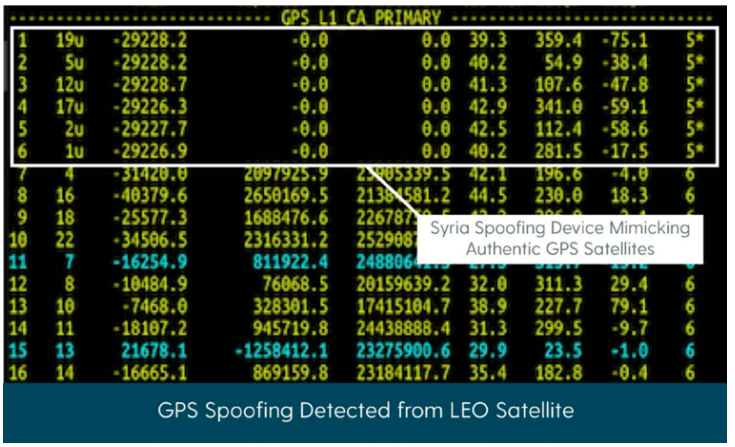
Popularny dziś Microsoft Active Directory (AD) wymaga dokładności 5 minut, aby Kerberos[22] poprawnie uwierzytelnił dostęp do wewnętrznych zasobów zarządzanych kontrolerem domeny (DC). Prawidłowy czas elementów AD zapobiega atakom typu *replay*, a Microsoft wykorzystuje to do rozwiązywania konfliktów replikacji w środowisku sieci Windows. Administratorzy IT nie doceniają bardzo szerokiego zakresu czasowego, jaki daje desynchronizacja, zarówno ta z użyciem sieciowego protokołu NTP, jak i satelitarnego spoofingu GPS. Tym samym desynchronizacja AD większa od 5 minut powoduje odmowę zalogowania. Z kolei transport kolejowy, który należy do ważnych dla bezpieczeństwa państwa infrastruktur krytycznych, wymaga już nieco większych subsekundowych dokładności. Tu problemem jest złożoność systemu i jego duże terytorialne rozproszenie, które wystawia kolej na ekspozycję desynchronizacji.

[20] https://en.wikipedia.org/wiki/GPS_week_number_rollover.
[21] https://www.itnews.com.au/news/satellite-failure-caused-global-gps-timing-anomaly-414237.
[22] https://aaltodoc.aalto.fi/server/api/core/bitstreams/4a888111-c704-44ab-83c8-50a23e8cee26/content.

Rys. 11. Mobilny programowalny spoofer i jammer GPS
Źródło: własne

Strona atakująca ma duże możliwości manipulacji czasem z użyciem spoofingu radiowego. Taki atak można zorganizować lokalnie z użyciem mobilnych grup dywersyjnych dysponujących przenośnymi urządzeniami zakłócania GNSS (rysunek 12). Mobilny atak jest szczególnie trudny do wykrycia przez systemy monitorowania zakłóceń GNSS, gdy pracują one z dala od bezpośredniego miejsca ataku, np. Lokalnego Centrum Sterowania (LCS). Efektywny czas potrzebny na desynchronizację odbiornika GNSS wspierającego pracę systemów zarządzania ruchem na kolei zależy od producenta i może trwać od kilkunastu minut do wielu godzin. W przypadku wysokiej klasy drogich odbiorników GNSS atakujący może być zmuszony do jednoczesnego użycia spoofingu i jammingu, następujących w odpowiednich sekwencjach po sobie. Podczas gdy odpowiednio wzmocniony sygnał radiowy ze spoofera, np. HackRF-One, atakuje kod na konkretnej częstotliwości, np. GPS L1, drugi jammer w tym samym czasie blokuje pozostałe systemy Galileo, Glonass, Beidou, IRNSS, w tym również te w pozostałym zakresie częstotliwości cywilnych L5 (rysunek 8). Uniemożliwia to udzielenie wsparcia atakowanej fałszowaniem wiązce GPS L1 kod C/A. Niektóre profesjonalne zakłócacze mogą wspierać jamming kodowany GPS L1. Wpisuje on najczęściej wartość samych zer w odpowiednie pola depeszy nawigacyjnej (rysunek 13). Może to wywołać desynchronizację odbiornika GNSS nawet o 19.7 lat (rysunek 10), jeżeli odbiornik nie jest odporny na problem GPS WNRO[22]. Stosowanie wielu metod zakłócania odbiornika jednocześnie zwiększa szanse awarii przez zwiększenie ryzyka wywołania błędów przepełnień numerycznych, a tym samym może skutecznie zdestabilizować serwer NTP/PTP kolei.

W takim przypadku pozbawiony źródła czasu GNSS system IT/OT kolei szybko traci prawidłowe ustawienie godziny, które powiększa się, prowadząc nieuchronnie do awarii systemu zarządzania ruchem w regionie. Skuteczny wspomagający GNSS atak desynchronizacji można przeprowadzić również w przypadku, gdy telemetria kolei otrzymuje wsparcie za pośrednictwem sieci GSM z POOL.



Rys. 12. Wpisanie wartości zer w pole depeszy GPS L1. Zerując licznik tygodni, można wywołać skok o 19.7 lat
Źródło: Aerospace and Ocean Eng., Researchgate (2021)

Koleje powinny być całkowicie odizolowane od Internetu, ale zdarza się, że nieświadomi zagrożenia ze strony POOL administratorzy udostępniają synchronizację wewnętrznych komponentów za pomocą bezprzewodowych routerów GSM. Jest to szczególnie niebezpieczne na etapie trwającej transformacji cyfrowej kolei. Przygotowane odpowiednio wcześniej zatrute serwery w POOL umożliwiają atakującemu desynchronizację LCS. Proces zatrucia POOL trwa wiele tygodni, ale zatrute serwery mogą pozostawać w sieci niezauważone przez wiele lat. W niedalekiej przyszłości rozwój szybkich kolei zwiększy rygor precyzji synchronizacji, zmuszając do częstszego niż dzisiaj używania protokołu PTP.

Dokładność milisekund używana jest w kierowaniu ruchem lotniczym. Wizualizacja 3D ruchu polega na odczycie pozycji samolotów w wielu rozproszonych miejscach jednocześnie. Sensory pomiarowe znakują czasem depeszę informacyjną przesyłaną do centralnego systemu zarządzającego PAŻP, który znakuje je ponownie własnym czasem. Pakiety są filtrowane. Odrzucane są depesze informacyjne, których różnica czasu pomiędzy znacznikiem nadania z sensora a odbiorem w centralnym serwerze jest zbyt duża. Precyzja synchronizacji w ruchu lotniczym odgrywa ważną rolę, ponieważ prędkość cywilnych samolotów odrzutowych może dochodzić do 1000 km/h. Zaburzając prawidłowy czas któregokolwiek elementu rozproszonego systemu kierowania ruchem lotniczym, może dojść do nietypowego zjawiska, w którym depesza dotrze do serwera, zanim powstała i ją wysłano. Nic więc dziwnego, że systemy kierowania ruchem lotniczym są szczególnie wrażliwe na desynchronizację i szybko reagują zgłoszeniem awarii krytycznej. Podobne ryzyko ponosi energetyka smart grid.

W odróżnieniu od klasycznej jednokierunkowej dystrybucji „od elektrowni do odbiorcy" w smart grid[23] energia elektryczna jest przekazywana w obu kierunkach. Przełączaniem kierunku zarządza AI wbudowana w centralny system nadzoru WAMS[24]. Bieżąca ocena stanu energetycznego dużego regionu opiera się na wspomnianej we wstępie rozdziału technologii *Observability*. Kontroluje ona kilka KPI:

[23] https://en.wikipedia.org/wiki/Smart_grid.
[24] https://www.sciencedirect.com/topics/computer-science/wide-area-measurement-system#.

1) pomiar kąta fazowego (PMU[25]),
2) częstotliwość napięcia (Hz),
3) napięcie (kV),
4) stan synchronizacji infrastruktury.

Zgodnie z IEC C27.238 PMI w smart grid musi mieć zapewnioną mikrosekundową dokładność synchronizacji do UTC. Utrzymanie tak precyzyjnej 1 μs domeny czasu na dużym obszarze kraju jest trudne. Zapewnienie odporności na manipulacje czasem jest tu prawdziwym wyzwaniem. Aby temu sprostać, we wnętrzu smart grid utrzymywana jest synchronizacja na poziomie 100 nanosekund. Taką dokładność zapewniają wyłącznie specjalne czasowe odbiorniki GNSS oraz sieciowy protokół IEEE1588. Atak desynchronizacji na PMU smart grid opisano dokładnie w pozycjach literatury [3], [4].

Zmniejszając dokładność do poziomu nanosekund, dochodzimy do sektora giełdowo-finansowego zautomatyzowanych inwestycji HFT[26]. Wprawdzie dyrektywa UE MiFID II mówi o wymogu zapewnienia dokładności jedynie 100 μs, ale jest to wymagana wartość minimalna do spełnienia przez każdą giełdę papierów wartościowych. Chodzi o to, że tzw. kolokacja giełdowa komputerów HFT ma zapewnić sprawiedliwą szybkość dostępu do informacji i składania zleceń. Biura maklerskie HFT same doszukują się w precyzyjnym czasie elementu uzyskania przewagi nad rynkiem. Chodzi o tzw. arbitraż kupowania i sprzedawania. Jeśli akcje tej samej spółki A handlowane są jednocześnie na giełdach w Nowym Jorku i Londynie, a ich cena na obu rynkach różni się o kilka centów, algorytm HFT może kupić taniej w jednym miejscu i sprzedać drożej w drugim. Mechanizm jest w dosłownym znaczeniu „maszynką do robienia pieniędzy" pod warunkiem prawidłowej synchronizacji. Do tego celu używana jest centralna dystrybucja wzorca czasu precyzyjnym protokołem PTP w profilu HA (High Accuracy), który od roku 2019 wchodzi w skład standardu IEEE 1588.

Kwantowa dystrybucja klucza[27] (ang. QKD) jest przykładem technologii informatycznej wymagającej dokładności synchronizacji rzędu poniżej 100 ps. Tak precyzyjnej synchronizacji potrzebuje najnowsza implementacja starego algorytmu BB84[28] z 1984 roku. We współczesnej realizacji BB84 polaryzację pojedynczego fotonu zastąpiono kodowaniem w domenie czasu i częstotliwości (fazy). Wymaga to niezależnej transmisji zegara siecią optyczną lub dostarczenia zgodnego wzorca po obu stronach kanału kwantowego. Destabilizacja zegara dla QKD automatycznie blokuje (DoS) usługę kryptografii kwantowej.

Jak do tej pory Polska bardzo dobrze wypada na tle innych państw członkowskich UE i NATO. Nowy krajowy system dystrybucji czasu urzędowego eCzasPL[29,30] został oddany 10 grudnia 2023 r., a więc na dwa tygodnie przed pierwszymi zakłóceniami GPS nad Polską. Polskie serwery w GUM pozwalają również na kryptograficzne uwierzytelnienie protokołu NTP, co zapobiega manipulacji krajowym wzorcem UTC(PL) dostarczanym przemysłowi.

[25] https://en.wikipedia.org/wiki/Phasor_measurement_unit.
[26] https://en.wikipedia.org/wiki/High-frequency_trading.
[27] https://en.wikipedia.org/wiki/Quantum_key_distribution.
[28] https://en.wikipedia.org/wiki/BB84.
[29] https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.
[30] Oficjalny film eCzasPL, https://www.youtube.com/watch?v=rawcGu65OaE.

System eCzasPL ma też unikatową, autorską, mało znaną właściwość, która pozwala GUM kontrolować zdalnie UTC na odległych serwerach czasu NTP/PTP pracujących w przemyśle, również tych działających w wewnętrznych sieciach infrastrukturalnych odizolowanych od Internetu. Jest to wynik udziału polskich przedsiębiorstw jak ELPROMA w projektach takich jak DEMETRA[31] Horizon 2020, ale przede wszystkim nieograniczona chęć tworzenia w kraju rozwiązań, które inspirują wiodące światowe firmy sektora IT.

Rys. 13. Rodzina polskich serwerów czasu NTP/PTP firmy Elproma Elektronika Sp. z o.o. Urządzenia odporne są na zakłócenia jamming/spoofing GPS (GNSS) i posiadają kod NATO. Od góry: NTS-3000, NTS-4000, NTS-5000 OCXO, NTS-5000 Rubidium + OCXO
Źródło: ELPROMA (www.elpromaelectronics.com)

Autor dedykuje rozdział żonie Izabeli. Dziękuje ojcu Leszkowi Widomskiemu za uwagi.

LITERATURA

[1] Paluszyński W., „Rozdział XII. Niedocenione zagrożenie – źródło i dystrybucja czasu", [w:] B. Szafrański (red.), *Cyberbezpieczeństwo – redefinicja zagrożeń*, s. 177–214, Wojskowa Akademia Techniczna, Warszawa 2023.

[2] Widomski T., „Rozdział XV. Desynchronizacja IT/OT infrastruktury krytycznej – jak monitorować i zapobiegać", [w:] B. Szafrański (red.), *Cyberbezpieczeństwo vs. sztuczna inteligencja. Informatyka, prawo, zarządzanie*, s. 253–292, Wojskowa Akademia Techniczna, Warszawa 2024.

[3] Shereen E., „Security of Time Synchronization for PMU-based Power System State Estimation: Vulnerabilities and Countermeasures", Doctoral Thesis in Electrical Engineering, KTH Sweden Royal Institute of Technology, Stockholm 2021.

[31] https://doi.org/10.33012/2017.14982.

[4] Han M., Crossley P.A., „Vulnerability of IEEE 1588 under Time Synchronization Attacks", *2019 EEE Power & Energy Society General Meeting* (*PESGM*), 2019.
[5] Tavella P., Widomski T., „The Future of Coordinated Universal Time", *ITU-News Magazine*, No. 2, 2023.
[6] Widomski T., *Synchronization security at Smart Gird*, DG-Energy, 2017.
[7] Widomski T., Użycki J., Borgulski K. i inni, „Trusted Time Distribution with Auditing and Verification Facilities Project TSI#2", Conference Precise Time and Time Interval Meeting, ION/PTTI Monterey, California, 2016.
[8] Widomski T., *Analiza zjawiska desynchronizacji czasu jako nowej cyberbroni destabilizującej infrastruktury krytyczne państwa*, praca dyplomowa MBA Cyberbezpieczeństwo, WAT, 2024.
[9] Ustawa o czasie urzędowym z dnia 10.12.2003 r. (Dz.U. Nr 16, poz. 144), rozszerzone o rozporządzenie, Dz.U. Nr 56 z 2004 r., poz. 548.

O autorze

Tomasz Widomski, absolwent kierunku Informatyka na wydziale Elektroniki Politechniki Warszawskiej (PW). Ukończył studia podyplomowe w Szkole Głównej Handlowej (SGH) i MBA Cyberbezpieczeństwo na Wojskowej Akademii Technicznej (WAT). Twórca polskiej szkoły serwerów czasu NTP/PTP odpornych na manipulacje czasem, w tym na jamming i spoofing GPS. Urządzenia produkowane w kraju przez polską firmę Elproma, są używane przez infrastruktury krytyczne na całym świecie oraz przez armie europejskich państw członkowskich NATO. Konsultant Europejskiej Agencji Przemysłu Kosmicznego EUSPA i delegowany przez nią w 2018 do prac w DG-Energy i DG-Connect. Zarządzał polskim zespołem w międzynarodowych projektach Horizon 2020 DEMETRA (dot. budowy naziemnej dystrybucji czasu UTC satelitarnego systemu GALILEO), Polsko-Izraelskim projektem sub-nanosekundowej precyzyjnej synchronizacji Run-Rabbit, polską częścią projektu White Rabbit CERN oraz krajowym projektem systemu naziemnej dystrybucji czasu urzędowego UTC(PL) o nazwie eCzasPL w Głównym Urzędzie Miar. Krajowy delegat do ITU w Genewie przy ONZ (akredytacja Ministerstwa Cyfryzacji KPRM od 2021r). Autor polski**ej** kontrybucji do ITU. Ekspert ds. cyberbezpieczeństwa infrastruktur krytycznych w obszarze precyzyjnej synchronizacji.

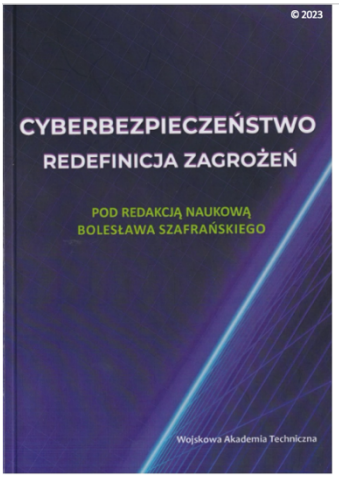
Recenzja

Rozdział XVIII pt. „Atak na czas, opóźnienie i synchronizację IT/OT: Skuteczna cyberbroń przyszłości" autorstwa Tomasza Widomskiego

W rozdziale przedstawiono szeroką, interdyscyplinarną analizę roli precyzyjnej synchronizacji czasu w infrastrukturze krytycznej i dowiedziono, że celowa desynchronizacja może stać się skutecznym narzędziem destabilizacji państwowych i przemysłowych systemów sterowania. Opracowanie łączy szczegółowy opis protokołów NTP, SNTP i PTP z praktycznym przeglądem technik zakłócania mechanizmów synchronizacji czasu w systemach rozproszonych. Tytuł wiernie oddaje zarówno techniczne, jak i strategiczne aspekty omawianego zagrożenia. Pod względem formalnym tekst posiada klarowny układ. Język jest rzeczowy i przystępny. W warstwie metodologicznej autor formułuje 11 wyraźną tezę, że manipulacja znacznikiem czasu staje się równorzędnym wektorem ataku wobec klasycznego malware. Merytorycznie rozdział prezentuje pogłębioną charakterystykę zagrożeń: wskazuje podatność systemów Windows na skokowe korekty SNTP, opisuje zależność błyskawicznych strategii giełdowych od nanosekundowej precyzji, omawia możliwe backdoory w chipach GNSS i konsekwencje różnic między skalami TAI a UTC, a jednocześnie proponuje konkretne środki zaradcze, takie jak priorytetowe korzystanie z polskiej skali UTC(PL), kryptograficzne uwierzytelnianie NTP, wdrożenie naziemnych serwerów czasu i procedur awaryjnych. Całościowo opracowanie wnosi wkład do dyskusji o nowej kategorii cyberbroni, łącząc fundamenty teoretyczne z bogatym materiałem ilustracyjnym i praktycznymi rekomendacjami.

Inne polecane pozycje

Literatura [1]



Literatura [2]

Okładka (tył książki)

Bolesław Szafrański – przewodniczący Komitetu Programowo-Organizacyjnego Forum Teleinformatyki

Z dorobku tej serii wydawniczej wynikają dwa istotne wnioski:
– należy systemowo rozwiązać problem gromadzenia, zarządzania i udostępniania zasobów danych na potrzeby trenowania algorytmów sztucznej inteligencji wykorzystywanych w systemie informacyjnym państwa (nie tylko w administracji publicznej);
– bez prawnego, finansowego, organizacyjnego, technicznego, poznawczego (naukowego) rozwiązania tego problemu nie da się zapewnić suwerenności polskich rozwiązań bazujących na sztucznej inteligencji.

Radosław Nielek – dyrektor NASK – Państwowego Instytutu Badawczego

Nie można być tak naprawdę bezpiecznym, nie rozumiejąc wykorzystywanych technologii i nie będąc ich współtwórcą. Mądrze rozumiana suwerenność technologiczna to jednak nie tyle konieczność tworzenia każdego rozwiązania samodzielnie, „od zera", co umiejętność bycia częścią globalnego łańcucha wartości. Im istotniejsze miejsce zajmiemy w tym łańcuchu, tym trudniej będzie nas z niego usunąć. Regulacje prawne, struktury organizacyjne czy nawet najnowsze technologie nie powstaną bez ludzi, którzy rozumieją otaczający świat i czekające nas wyzwania i są gotowi pracować nad ich rozwiązaniem.

Zbigniew Tarapata – dziekan Wydziału Cybernetyki Wojskowej Akademii Technicznej

W monografii specjaliści, również z Wydziału Cybernetyki, podjęli próbę analizy jednego z najważniejszych i najbardziej aktualnych dylematów współczesnego świata cyfrowego: w jaki sposób budować skuteczny system bezpieczeństwa informacyjnego, który z jednej strony opiera się na zasadzie ograniczonego zaufania, a z drugiej — wymaga efektywnej współpracy pomiędzy instytucjami, państwami, sektorami oraz środowiskami eksperckimi. Mam nadzieję, że publikacja ta stanie się istotnym głosem w toczącej się debacie naukowej i praktycznej oraz impulsem do dalszych poszukiwań optymalnych modeli współdziałania w erze cyfrowych zagrożeń.

Krzysztof Gawkowski – wicepremier, minister cyfryzacji

Nie pytajmy, czy cyberatak nastąpi. On już trwa – każdego dnia. Zapytajmy raczej, czy Polska jest na to gotowa. Czy my jesteśmy gotowi. Dziś nie wystarczy tylko korzystać z technologii. Musimy umieć ją dobrze wykorzystywać, aktywnie się bronić i świadomie uczestniczyć w cyfrowym świecie. Polska ma dwie drogi: może być celem albo przykładem. Wybieramy to drugie. I robimy wszystko, by ten wybór potwierdzić działaniem. Polska jako cyfrowa twierdza będzie silna tylko wtedy, gdy jej fundamentem będzie nauka, a zaprawą – wspólna odpowiedzialność.

WYDZIAŁ CYBERNETYKI WAT

e-FORUM TELEINFORMATYKI®

ISBN 978-83-7938-456-3