PROFUNDERE SCIENTIAM

nr 15
styczeń 2020

BIULETYN CENTRUM STUDIÓW ZAAWANSOWANYCH POLITECHNIKI WARSZAWSKIEJ

Cyber(nie) bezpieczeństwo

Krzysztof Szczypiorski

Streszczenie

Celem artykułu jest przedstawienie trzech tez: kulturowej → cyberprzestrzeń jest zaawansowanym tworem techniczno-kulturowym – jest realizacją marzeń wielu twórców, wynalazców i inżynierów; technicznej → bezpieczeństwo i cyberprzestrzeń to nierozłączne elementy (stąd: cyberbezpieczeństwo) i paranoicznej → pełne bezpieczeństwo, jeśli jest osiągalne, nie jest stanem stałym (stąd: cyber(nie) bezpieczeństwo). Cyberprzestrzeń jest rozumiana jako zbiór technik cyfrowych służących do wymiany informacji, ale także jako nowego typu przestrzeń społeczna częściowo wirtualna, która może być bytem całkowicie odseparowanym od fizycznego. Geneza nazwy: w latach 1968-1970 duńska artystka Susanne Ussing we współpracy z duńskim architektem Karstenem Hoffem stworzyła serię kolaży pod tytułem „CYBERSPACE". Dekadę później termin pojawił się w literaturze (William Gibson). Tradycyjnie ludzie próbowali rozumieć świat przez relacje pomiędzy różnymi zjawiskami fizycznymi zachodzącymi w otoczeniu np. poprzez żywioły. Cyberprzestrzeń jest tworem sztucznym jednak posiada związki z otoczeniem fizycznym – można ją traktować jako kolejny żywioł. Jako cezurę powstania cyberprzestrzeni można podać rok 1968, w którym pojawił się *routing* w sieci ARPANET, a także pierwszy programowalny sterownik logiczny (PLC). Natomiast dla cyberbezpieczeństwa będzie to rok 1976 – opublikowanie algorytmu uzgadniania klucza przez Witfielda Diffiego oraz Martina Hellmana. Rozwój bezpieczeństwa jest skorelowany z działaniami wojennymi i zbrojeniem – branża wojskowa dokonywała historycznie największych inwestycji w tym obszarze. W dalszej części wykładu przedstawiono cyfryzację mowy oraz wybrane ataki (podsłuch, modyfikacja, podszycie się i wyparcie). Określono podstawowe związki pomiędzy podstawowymi usługami cyberbezpieczeństwa: poufnością, integralnością, uwierzytelnieniem i niezaprzeczalnością. Przedstawiono związki pomiędzy zagrożeniem, podatnością, zasobami i ryzykiem, a następnie zaprezentowano generycznie projektowanie zabezpieczeń jako iteracyjny proces zawierający analizę ryzyka, projekt polityki bezpieczeństwa i oszacowanie kosztów. W dalszej części przedstawiono zagadnienia rozpoznawania znanych ataków i anomalii tłumacząc złożoność tworzenia modeli zachowania w cyberprzestrzeni, które przeważnie nie odzwierciedlają wszystkich cech i ich dynamizmu. Zagadnienie fałszywych alarmów wpływa na rzetelność systemów wykrywających anomalie, w szczególności błędy drugiego rodzaju prowadzą do nierozpoznawania ataków.

1. Wstęp

W toku ewolucji ludzkość rozwinęła swoje możliwości poznawcze i przystosowawcze dążąc do ekspansji w

{CIĄG DALSZY NA S. 6}

W NUMERZE

między innymi:

KWANTECHIZM
czyli klatka na ludzi (fragm.)

Andrzej Dragan

Obrót czasoprzestrzeni

HISTORIA ŻYCIA NA ZIEMI to jakieś parę miliardów lat. Historia naszej cywilizacji to najwyżej kilkadziesiąt tysięcy lat. Oznacza to, że wkład, jaki wnosimy w historię życia na naszej planecie (będącej skądinąd pyłkiem na skraju jednej z dziesięciu miliardów galaktyk), jest mniej więcej taki, jak wkład rozdeptanej muchy umieszczonej na czubku Pałacu Kultury do jego wysokości.

Z punktu widzenia Ziemi, którą matematyk Hugo Steinhaus nazywał „kulą u nogi" gatunek ludzki jest więc najwyżej niesfornym epizodem. Podczas

{CIĄG DALSZY NA S. 19}

„Przez miliony lat, ludzkość żyła tak jak zwierzęta. Potem stało się coś, co uwolniło siłę naszej wyobraźni. Nauczyliśmy się rozmawiać, nauczyliśmy się słuchać. Rozmowa umożliwiła przekazywanie pomysłów, dzięki czemu nauczyliśmy się wspólnie budować to, co niemożliwe. Największe osiągnięcia ludzkości tworzone są w rozmowie, a jej największe niepowodzenia są skutkiem braku rozmowy. Nie musi tak być. Nasze największe marzenia mogą stać się rzeczywistością. Z techniką, którą dysponujemy, możliwości są nieograniczone. Wszystko, co musimy zrobić, to upewnić się, że wciąż rozmawiamy."

Prof. Stephen Hawking (1942-2018)

ziemskim ekosystemie. Jedną z ważniejszych umiejętności *homo sapiens* stała się rozwinięta komunikacja werbalna, która finalnie doprowadziła do umiejętności rozmowy i przekazywania za jej pomocą myśli oraz emocji. Rozmowa jest aktem, w którym strony komunikujące się zarówno mówią, jak i słuchają, niekiedy dzięki rozmowie zmieniają swoje myśli, a także emocje. Przez tysiące lat ludzie na różny sposób próbowali zrozumieć otaczający świat tworząc różne teorie na temat relacji pomiędzy zjawiskami głównie fizycznymi. Empedokles z Akragas wyróżnił cztery żywioły: ziemię, wodę, powietrze i ogień. W kulturze japońskiej pojawia się pustka oznaczająca też niebo, w kulturze chińskiej znika powietrze, a pojawia się drewno i metal. Z kolei w hinduizmie jako żywioł pojawia się dźwięk. Teorie żywiołów mają swoje odniesienie do przyrody, którą w dużym stopniu była eksplorowana przez ludzi poprzez obserwację, rzadziej przez przeprowadzenie doświadczenia. Żywioły mają charakter fizyczny, namacalny, są w dużym stopniu pozbawione kontroli, chociaż nie ulega wątpliwości, że ludzie posiadają potrzebę okiełznania ich.

Celem artykułu jest przedstawienie trzech tez:

1. kulturowej: cyberprzestrzeń jest zaawansowanym tworem techniczno-kulturowym – jest realizacją marzeń wielu twórców, wynalazców i inżynierów,
2. technicznej: bezpieczeństwo i cyberprzestrzeń to nierozłączne elementy (stąd: cyberbezpieczeństwo),
3. paranoicznej: pełne bezpieczeństwo, jeśli jest osiągalne, nie jest stanem stałym (stąd tytułowe: cyber(nie)bezpieczeństwo).

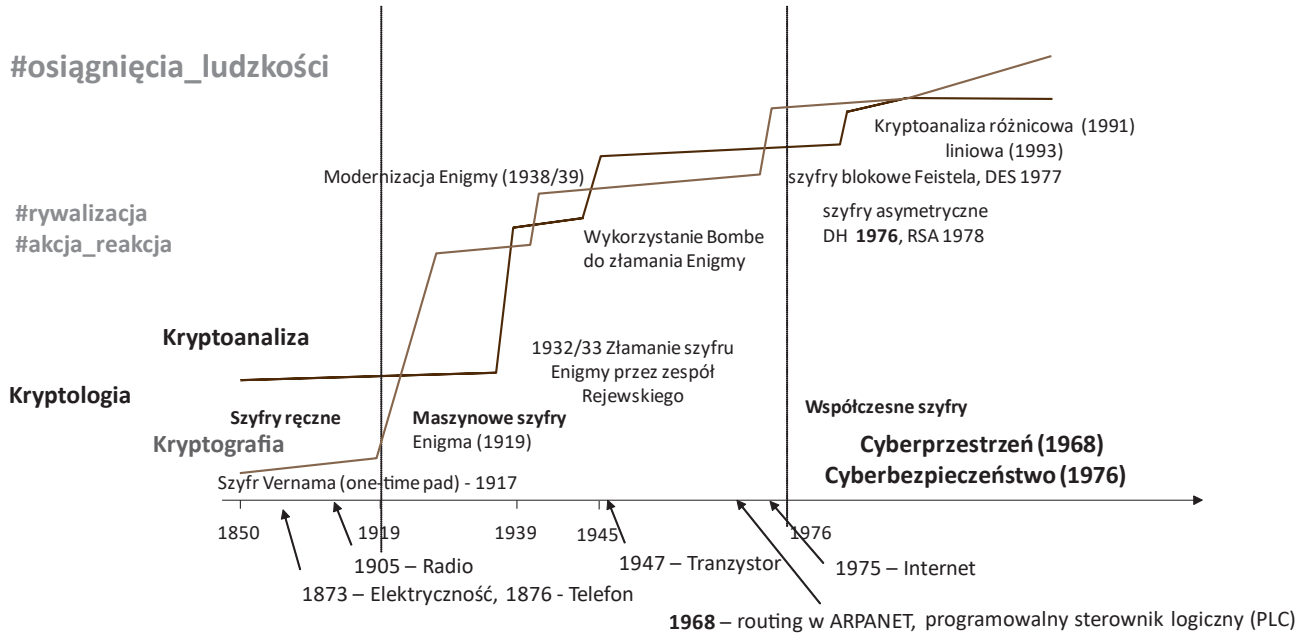
Artykuł ma charakter bardziej poglądowy, niż przeglądowy i składa się z pięciu rozdziałów, którego pierwszym jest niniejsze krótkie wprowadzenie. Drugi rozdział dotyczy genezy cyberprzestrzeni i jej bezpieczeństwa. Trzeci opisuje przebieg rozmowy w cyberprzestrzeni i związane z tym zagrożenia. Czwarty dotyczy zmienności i ryzyka wpływających na niebezpieczne związki, które stają się kluczowe przy projektowaniu systemów zabezpieczeń. Ostatni jest zwięzłym podsumowaniem niniejszej pracy.

2. Geneza cyberprzestrzeni i jej bezpieczeństwa[1]

Cyberprzestrzeń pojawia się w historii ludzkości w drugiej połowie XX wieku. Jest wynikiem procesu tworzenia wynalazków i różnych teorii, z których wiele z nich ułatwiło komunikację. Zgodnie z [1] cyberprzestrzeń (ang. *cyberspace*) jest z jednej strony zbiorem technik cyfrowych służących do wymiany informacji, ale z drugiej nowego typu przestrzenią społeczną częściowo wirtualną, która może być bytem całkowicie odseparowanym od fizycznego. Z trzeciej jest środowiskiem, w którym następuje współczesna komunikacja za pomocą sieci teleinformatycznej. W psychologii ewolucyjnej zaproponowano nowe pojęcie *homo cyberus* [5] skojarzone z cybersocjalizacją. Pojęcie

[1] *Wykorzystano fragment opracowania autorskiego, które wchodzi w skład [1]*

↓ Rysunek 1. Cyberprzestrzeń: początki, w tle kryptologii nowożytnej



„CYBERSPACE" [3] (pisane wersalikami) pojawia się w cyklu kolaży tworzonych w latach 1968-1970 przez duńską artystkę Susanne Ussing we współpracy z duńskim architektem Karstenem Hoffem. Dekadę później termin pojawia się w literaturze – używa go twórca cyberpunku William Gibson [4]. O ile kolaże Ussing stanowią ekspresyjne wizje ludzi wtopionych w cybernetyczne formy, co raczej należy uznać za neutralne w odbiorze, o tyle cyberpunk, jako odmiana fantastyki naukowej, skupia się przede wszystkim na negatywnych stronach cyfryzacji świata i zetknięcia *homo sapiens* z maszynami. Tak małymi krokami objawia się nowy żywioł bez znamion cech fizycznych, w którym nie obowiązują prawa fizyki takie jak chociażby zasady dynamiki Newtona, w tym prawo ciążenia.

Bezpieczeństwo pojawia się w zasadzie od razu z cyberprzestrzenią jako jego immanentna część. Najpierw jest rozumiane dość naiwnie na poziomie fizycznym, jako odseparowanie sygnałów istotnych (np. tajnych) od pozostałych wręcz na poziomie duktów i okablowania (tzw. *air gap*). To oczywiście, już na pierwszy rzut oka, wydaje się niewystarczające i stąd do ochrony komunikacji zostaje zaprzątnięta kryptologia, w szczególności kryptografia. Zatem od strony technicznej powstanie cyberprzestrzeni i pojawienie się w niej (cyber)bezpieczeństwa można spróbować skorelować z rozwojem kryptologii nowożytnej (Rysunek 1). Z kolei sam rozwój kryptologii i w konsekwencji cyberbezpieczeństwa jest ściśle powiązany z prowadzonymi działaniami wojennymi. Kryptologia jest nauką, w której występują dwie siły: syntetyzująca, budująca (kryptografia) i analizująca, wręcz niszcząca (kryptoanaliza). W historii kryptologii te siły wzajemnie napędzają się i konkurują ze sobą – metody kryptograficzne muszą być odporne na znane ataki kryptoanalityczne. Powstaje swojego rodzaju wyścig zbrojeń, w którym algorytmy są ulepszane, a głównym miernikiem ich siły jest czas ich ochrony, wynikający w dużym stopniu z długości klucza. Na tę chwilę kresem tego wyścigu od strony kryptoanalizy jest wizja pojawienia się komputera kwantowego [6], a od strony kryptografii – algorytmy postkwantowe [7].

Koniec I wojny światowej to cezura końcowa epoki szyfrów ręcznych. Ponad wiek temu, w 1917 roku pojawia się algorytm Vernama, będący szyfrem idealnym, którego istotą jest wykonywanie dodawania modulo 2 wiadomości z losowym kluczem o długości tej samej co wiadomość (stąd określenie: szyfr z kluczem jednorazowym). Wejście w epokę szyfrów maszynowych, która trwa do połowy zimnej wojny, symbolizuje powstanie w Niemczech pierwszej wersji elektromechanicznej maszyny szyfrującej Enigma [8]. Marian Rejewski, Jerzy Różycki i Henryk Zygalski doprowadzają do złamania Enigmy, czego efektem jest modernizacja Enigmy (dodanie kolejnych rotorów) tuż przed wybuchem II wojny światowej. W trakcie wojny ulepszona Enigma zostaje złamana z wykorzystaniem Bombe [9] – elektromechanicznej maszyny stworzonej w Wielkiej Brytanii przez Alana Turinga na podstawie projektu i prototypu grupy Rejewskiego tzw. bomby kryptologicznej. W 1947 roku zostaje skonstruowany pierwszy tranzystor ostrzowy przez Johna Bardeena oraz Waltera Housera Brattaina. Staje się on punktem wyjścia do stworzenia współczesnych maszyn obliczeniowych, co następuje w ciągu kolejnej dekady. Pod koniec epoki szyfrów maszynowych w 1968 pojawia się *routing* (trasowanie) w sieci ARPANET [10], a także programowalny sterownik logiczny (*Programmable Logic Controller* – PLC) [11]. Rok 1968 możemy uznać za datę inicjacji cyberprzestrzeni. Sieć Internet w swojej pierwotnej formie debiutuje mniej więcej siedem lat później [12].

Cezura początkowa dla epoki współczesnych szyfrów następuje rok później po pojawieniu się Internetu – w 1976 zostaje opublikowany przez Witfielda Diffiego oraz Martina Hellmana [13] pierwszy algorytm wymiany klucza współdzielonego oparty na algorytmach asymetrycznych wykorzystujący złożoność obliczenia logarytmów dyskretnych. Zatem rok 1976 możemy uznać za symboliczną datę inicjacji cyberbezpieczeństwa. Rok później zostaje zaakceptowany jako standard federalny w USA [14] blokowy algorytm symetryczny DES (*Data Encryption Standard*), który staje się w 1981 roku standardem sektora prywatnego na kolejne dwie dekady. W 1978 roku Ron Rivest, Adi Shamir oraz Leonard Adleman publikują pracę [15] dotyczącą pierwszego kryptosystemu wykorzystującego klucz publiczny i problem złożoności faktoryzacji dużych liczb, nazwanego od liter ich nazwisk RSA.

Współczesnym motorem cyberbezpieczeństwa nadal pozostają działania zbrojne. W USA po okresie zimnej wojny, podczas której rozwinęła się Dolina Krzemowa [16], głównie przez ogromne inwestycje kapitałowe, zamachy z 11 września 2001 otworzyły etap walki z ogólnie pojętym terroryzmem. Z kolei drugi kraj przodujący na świecie w cyberbezpieczeństwie – Izrael, który po zakończeniu drugiej wojny światowej zaangażował się w długotrwały konflikt z Palestyną, przyjął podobny model jak USA podczas zimnej wojny – inwestycje w branżę zbrojeniową, która formalnie od dekady jest ściśle powiązana z cyberprzestrzenią. Przykładowo w USA Cyber Command [17] powstał w 2009 roku i uzupełnia działania sił zbrojnych USA dotychczas powiązanych z tradycyjnymi żywiołami (US Air Force – powietrze, US Army – ziemia, US Navy – woda) w cyberprzestrzeni.

Cyberprzestrzeń jest także obecna w przemyśle. Patrząc na wprowadzoną kilka lat temu klasyfikację [18]:

- Przemysł 1.0: wiek pary,
- Przemysł 2.0: wiek elektryczności,
- Przemysł 3.0: wiek komputerów,
- Przemysł 4.0: wiek zanikania bariery ludzie-maszyny,

cyberprzestrzeń pojawia się w tzw. wieku komputerów, gdzie masowa produkcja zostaje wsparta przez maszyny. Historycznie masowa produkcja powstała przez dodanie do przemysłu elektryczności, a z kolei sam przemysł przez wsparcie ręcznej produkcji maszynami parowymi. Wiek komputerów i sterowanie nimi za pomocą systemów SCADA (*Supervisory Control and Data Acquisition*) nie byłby możliwy, bez wspomnianego wcześniej, opracowania sterownika logicznego PLC (*Programmable Logic Controller*) w 1968 [11]. Za ojca tego wynalazku uznaje się Dicka Morley amerykańskiego inżyniera i wynalazcę. Urządzenie to pozwalało na fizyczne sterowanie maszyną i realizowanie konkretnego algorytmu niezbędnego do procesu produkcji. Natomiast przemysł 4.0 bazuje w dużym stopniu na dołączeniu systemów SCADA do Internetu (co technicznie nie jest problemem od dawna) i na wykorzystanie rozwiązań z obszaru przemysłowego Internetu rzeczy (*Industrial Internet of Things* – [19]). W tym przypadku pojawia się ogromna liczba danych wymagających zabezpieczenia.

Reasumując za datę powstania cyberprzestrzeni, zarówno w sensie kulturowym jak i technicznym, można przyjąć rok 1968. Cyberbezpieczeństwo pojawia się 8 lat później za sprawą

↑ Rysunek 2. a) Rozmowa[2]; b) Cyfryzacja mowy – pojawiają się dane[2]; c) Podsłuch[2]; d) Modyfikacja2; e) Podszycie[3]; f) Wyparcie się[2]

pierwszych algorytmów wykorzystujących kryptografię asymetryczną.

3. Rozmowa w cyberprzestrzeni i związane z nią zagrożenia

Wróćmy do wątku rozmowy (Rysunek 2a[2]). Zanim mowa znajdzie się w cyberprzestrzeni musi zostać poddana cyfryzacji, czyli zmiany postaci analogowej na cyfrową (Rysunek 2b[2]). Cyfryzacja sygnału mowy składa się z dwóch procesów: próbkowania i kwantyzacji. Zgodnie z twierdzeniem Nyquista dot. próbkowania, częstotliwość próbkowania jest dwukrotnością próbkowanego kanału i przykładowo: 8 kHz – dla klasycznej telefonii stacjonarnej, 16 kHz albo 22,050 kHz – dla średniej jakości (radio UKF) oraz 44,1 kHz albo 48 kHz – dla jakości płyty kompaktowej (HiFi). Kwantyzacja jest procesem, w którym próbki są konwertowane na ustalone wartości liczbowe. Tak powstają dane – będące w omawianym przypadku przekształceniem mowy na postać binarną.

Dane rozpoczynają swoją podróż w cyberprzestrzeni: mogą być przesyłane (są danymi „w ruchu"), magazynowane lub przetwarzane. W każdym momencie swojej podróży mogą być podsłuchane (Rysunek 2c[2]), bądź zmodyfikowane (Rysunek 2d[2]). Istnieje możliwość podszycia się (Rysunek 2e[3]) pod wysyłającego dane (pod odbierającego też), a także wyparcie się faktu wysłania lub odebrania danych (Rysunek 2f[2]). Są to podstawowe zagrożenia, które dotyczą danych. Podsłuch jest działaniem pasywnym – nie wpływa na strukturę danych, pozostałe trzy zagrożenia wymagają aktywności i w zależności od źródła danych, mniej lub więcej zaangażowania. Najprościej operować na danych stworzonych od początku do końca w cyberprzestrzeni, a nie, tak w jak przykładzie rozmowy, biometrycznych – wtedy np. modyfikacja jest o wiele łatwiejsza do przeprowadzenia.

Dane jako takie, bez żadnego kontekstu, są wyłącznie binarnym zbiorem, są literami o nieuporządkowanej strukturze. Nabierają wartości dopiero, jeśli stanowią informacje [22], które można porównać już do słów. Możemy mówić zarówno o ochronie danych, jak i o ochronie informacji. Obecnie w czasach dostępności ogromnych przepustowości sieciowych i mocy obliczeniowej istnieje pokusa na to, żeby chronić wszystkie dane w zasadzie bezmyślnie. Wydzielenie informacji ważnych i dopasowanie do nich odpowiednich metod ochrony jest jak najbardziej pożądane i zasadne. Wynika to chociażby z tego, że „czas życia" poszczególnych

[2] *Wykorzystano zdjęcie z [20]*

[3] *Wykorzystano zdjęcie z [21]*

informacji, a więc potencjalna potrzeba ich ochrony jest różna np. położenie samolotów wielozadaniowych General Dynamics F-16 Fighting Falcon nad Polską to poziom kilkudziesięciu minut, a tożsamość szpiegów to minimum pół wieku.

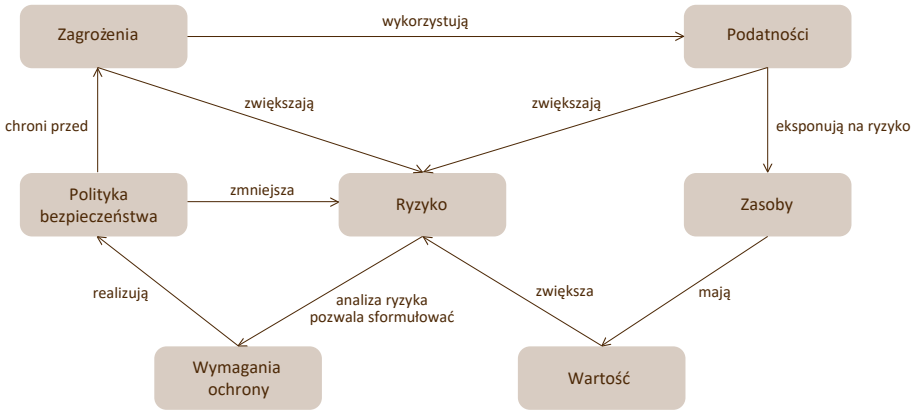
Na podstawie informacji jesteśmy w stanie budować wiedzę, która w kontekście cyberprzestrzeni jest magazynowaniem istotnych informacji, poszukiwaniem relacji i wyciąganiem wniosków. Wiedzę możemy porównać do zdań albo wręcz do myśli. Na końcu łańcucha przetwarzania danych możemy umieścić mądrość, jako umiejętność podejmowania właściwych (cokolwiek to znaczy!) decyzji na podstawie zdobytej wiedzy.

W kontekście wspomnianych zagrożeń (podsłuch, modyfikacja, podszycie się, wyparcie się) wprowadza się podstawowe usługi cyberbezpieczeństwa [23]: poufność, integralność, uwierzytelnienie i niezaprzeczalność. Uzupełnia się ten zestaw o usługę kontroli dostępu, dzięki której można sterować prawami korzystania z zasobów.

Usługi ochrony informacji są budowane za pomocą różnych mechanizmów, jednym z nich jest szyfrowanie leżące w obszarze kryptografii. Jak wspomniałem w poprzednim rozdziale głównym miernikiem siły algorytmów kryptograficznych jest czas ich ochrony, wynikający w dużym stopniu z długości klucza. Przy klasycznym modelu rozwoju technik obliczeniowych można dokonać predykcji szansy na złamanie chronionych informacji (także bazując na prawie Moore'a) i w ten sposób oferować ochronę na ustalony okres. Pojawiają się dwie ważne kwestie: pierwsza to umiejętne zarządzanie kluczami, w skład którego wchodzi ich generacja, dystrybucja, przechowywanie, a także zniszczenie po czasie użycia. Drugie to odporność danego algorytmu na znane ataki kryptoanalityczne, a także konstrukcja odporna na tzw. tylne furtki, czyli sposoby szybszego przeliczenia pewnych własności z wykorzystaniem słabych cech algorytmu [24].

4. Niebezpieczne związki: projektowanie systemów zabezpieczeń

Zagrożenia są pierwotną przyczyną działań w obszarze cyberbezpieczeństwa. Zagrożenia (Rysunek 3) wykorzystują podatności, które pojawiają się na etapie projektowania, wdrażania, bądź konfigurowania systemów teleinformatycznych. Podatności (podobnie jak zagrożenia) zwiększają ryzyko, które jest wskaźnikiem stanu lub zdarzenia, które może prowadzić do strat. Podatności eksponują na ryzyko zasoby, które mają wartość (nie tylko ekonomiczną). Im większa wartość tym potencjalnie większe ryzyko. Polityka bezpieczeństwa definiuje zabezpieczenia na poziomie organizacyjnym oraz technicznym i dzięki temu zmniejsza ryzyko i chroni przed zagrożeniami. Z kolei wymagania ochrony realizują politykę bezpieczeństwa, a dzięki kluczowej przy projektowaniu zabezpieczeń analizie ryzyka [25], dają się sformułować. Warto zauważyć, że polityka bezpieczeństwa wprowadza nowe zasoby wraz z nowymi, właściwymi dla nich, podatnościami.

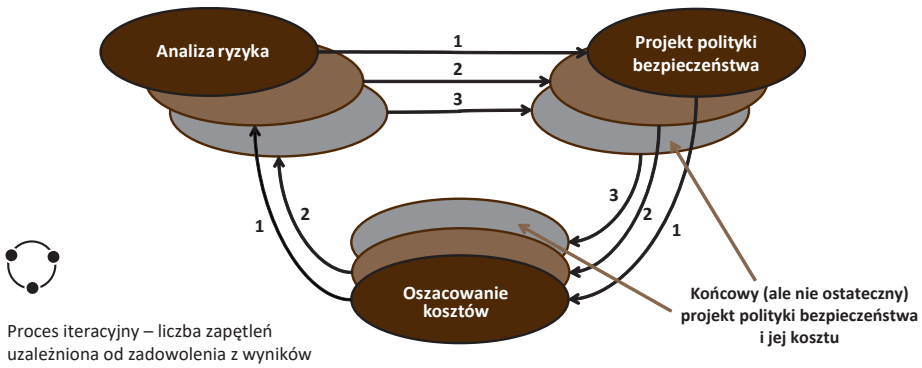


* Polityka bezpieczeństwa określa zabezpieczenia, które też stają się zasobami (z podatnościami!)

↑ Rysunek 3. Niebezpieczne związki

Analiza ryzyka, polegająca na przewidzeniu negatywnych skutków działań oraz zjawisk i odpowiednim obniżeniu potencjalnych strat wynikających z takich sytuacji jest procesem (Rysunek 4), który, jak wspomniano wcześniej, skutkuje projektem polityki bezpieczeństwa. Tak przedstawiony projekt podlega oszacowaniu kosztów. Jest to proces iteracyjny – przyjęcie akceptowalnego poziomu ryzyka przy akceptowalnych kosztach daje punkt wyjścia do przyjęcia polityki bezpieczeństwa i jednocześnie ciągły – w trakcie eksploatacji systemów zabezpieczeń powinien przebiegać okresowo.

System teleinformatyczny możemy obserwować poprzez składowe obiekty i relacje między nimi [26]. W każdym obiekcie możemy obserwować cechy, które mogą mieć charakter stały, ale część z nich może podlegać zmianie. Zmiana jest związana z przejściem cechy w inną. Obserwacja cechy jest ważna, wtedy tylko, kiedy można z informacją o zmianie tej cechy coś zrobić. Nie każda obserwacja zatem jest wartościowa z praktycznego punktu widzenia. W obiekcie można wyróżnić wiele cech do obserwacji, jednak w wielu przypadkach nie posiadamy pełnej wiedzy o wszystkich cechach. Jednocześnie pewne cechy mogą niespodziewanie pojawiać się, a inne z kolei znikać. Z drugiej strony część z cech nie jest istotna dla obserwacji zmiany bądź co gorsza obserwator nie ma świadomości ich istotności. Po wyróżnieniu konkretnej cechy, obserwacji podlega zmiana własności cechy w porównaniu do różnych miar, często



Proces iteracyjny – liczba zapętleń uzależniona od zadowolenia z wyników końcowych (w tym stopnia zabezpieczeń oraz kosztów) – później następuje **eksploatacja**, która jest częścią tego procesu

↑ Rysunek 4. Projektowanie systemów bezpieczeństwa

wyliczanych na podstawie poprzednich okresów obserwacji. W przypadku sieci teleinformatycznych obiektem jest przeważnie protokół telekomunikacyjny. Dla każdego protokołu budowany jest osobny model wyróżniający istotne cechy np. połączeniowość, mechanizmy retransmisji, obsługę opóźnionych lub uszkodzonych jednostek danych. Badając każdy z tych aspektów, analizie podlegają parametry sieciowe skojarzone z daną cechą przy mechanizmach retransmisji (liczniki czasu typu *timeout*, wielkość okna retransmisji, stopa błędów). Dopatrzenie się różnicy w profilu protokołu jest oznaką zmiany i z dużym prawdopodobieństwem oznacza atak sieciowy. Budowanie wiedzy na podstawie informacji, które są jednoznacznymi wskazaniami na atak, ułatwia tworzenie odpowiednich sygnatur, natomiast zjawiska, które są w jakimś stopniu nierozpoznane mają status anomalii. W eksploatacji systemów bezpieczeństwa zagadnienie fałszywych alarmów wpływa na rzetelność systemów wykrywających anomalie, w szczególności błędy drugiego rodzaju (*false positives*) prowadzą do nierozpoznawania ataków. Błędy pierwszego rodzaju (*false nagatives*) konsumują zasoby, ale nie są krytyczne dla bezpieczeństwa systemów (coś co nie jest atakiem w rzeczywistości, jest traktowane jako atak).

5. Podsumowanie

Cyberprzestrzeń jest zaawansowanym wytworem ludzkiej wyobraźni nie tylko w sensie technicznym, ale także w społeczno-kulturowym. Dzięki technice stworzona całkowicie w umyśle człowieka wizja stała się rzeczywistością – jest to przykład spełnienia marzeń.

Cyberprzestrzeń przenika się ze światem fizycznym, chociaż może być całkowicie wirtualna. W swojej naturze jest nierozłączna z bezpieczeństwem, które jest zmienne i nigdy nie jest pełne stąd tytułowe „cyber(nie) bezpieczeństwo".

Ludzie (w tym autor początkowego cytatu) od dawna marzyli o eksploracji kosmosu, a być może także o przeniesieniu życia na obcą planetę. Tymczasem mamy cyberprzestrzeń, być może będziemy w stanie replikować się w niej i dzięki temu staniemy się nieśmiertelni i w pełni szczęśliwi. Motyw ten jest znany z fantastyki naukowej (np. z filmu „Lucy" w reżyserii i wg scenariusza Luca Bessona [27]) i być może wymaga ponownej rewizji.

LITERATURA

[1] J. Woźniak, A. Bęben, J. Mongay Batalla, M. Natkaniec, Z. Piotrowski, K. Szczypiorski, K.Wesołowski – *Tendencje w rozwoju polskiej i światowej telekomunikacji i teleinformatyki* (w przygotowaniu), 2020

[2] https://en.wikipedia.org/wiki/Cyberspace (data pobrania: 21.10.2019)

[3] https://kunstkritikk.com/the-reinvention-of-cyberspace/ (data pobrania: 21.10.2019)

[4] https://en.wikipedia.org/wiki/William_Gibson (data pobrania: 21.10.2019)

[5] Pleshakov V.A. - *Human cyber socialization: from Homo Sapiens'a to Homo Cyberus'a*: monograph. M.: Publishing house of the Moscow State Pedagogical University "Prometey", 2012.221

[6] Frank Arute, Kunal Arya, Ryan Babbush, et al. – *Dave Bacon Quantum supremacy using a programmable superconducting processor*. Nature. Volume 574, pages 505–510 (23 October 2019)

[7] Daniel J. Bernstein, Tanja Lange – *Post-quantum cryptography*. Nature, Volume 549, pages 188-194 (14 September 2017)

[8] https://en.wikipedia.org/wiki/Enigma_machine (data pobrania: 21.10.2019)

[9] https://www.cryptomuseum.com/crypto/bombe/ (data pobrania: 21.10.2019)

[10] https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (data pobrania: 21.10.2019)

[11] https://library.automationdirect.com/history-of-the-plc/ (data pobrania: 21.10.2019)

[12] https://tools.ietf.org/html/rfc675 (data pobrania: 21.10.2019)

[13] W. Diffie, M. Hellman – *New directions in cryptography*, IEEE Transactions on Information Theory, Volume 22 Issue 6, Nov. 1976, pp. 644-654

[14] Federal Information Processing Standard (FIPS) 46: Data Encryption Standard (DES), January 1977, https://csrc.nist.gov/publications/detail/fips/46/archive/1977-01-31 (data pobrania: 21.10.2019)

[15] R. L. Rivest, A. Shamir, L. Adleman – *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Volume 21 Issue 2, Feb. 1978, pp. 120-126

[16] https://en.wikipedia.org/wiki/Silicon_Valley (data pobrania: 21.10.2019)

[17] https://www.arcyber.army.mil (data pobrania: 21.10.2019)

[18] https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html (data pobrania: 21.10.2019)

[19] H. Boyes, B. Hallaq, J. Cunningham, T. Watson – *The industrial internet of things (IIoT): An analysis framework*, Computers in Industry, Volume 10 1, 2018, pp. 1-12

[20] https://glavcom.ua/scotch/showbiz/kultovaya-trilogiya-matrica-oficialno-poluchit-perezapusk-483980/g358176.html (data pobrania: 21.10.2019)

[21] https://www.cinemablend.com/new/Matrix-Fan-Theory-Puts-Agent-Smith-One-It-Kind-Works-121077.html (data pobrania: 21.10.2019)

[22] B. Stefanowicz – *Informacja. Wiedza. Mądrość. Sześćdziesiąty* szósty tom Biblioteki Wiadomości Statystycznych, Główny Urząd Statystyczny, 2013

[23] ISO 7498-2:1989 – Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

[24] N. Perlroth, J. Larson, S. Shane – *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*. 05.09.2013, New York Times – https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html (data pobrania: 21.10.2019)

[25] ISO 31000:2018 – Risk management – Principles and guidelines

[26] J. Bieniasz, M. Stępkowska, A. Janicki, K.Szczypiorski – *Mobile Agents for Detecting Network Attacks Using Timing Covert Channels*, Journal of Universal Computer Science, Volume 25 Issue 9, Sep. 2019, pp. 1109-1130

[27] Lucy (2014), https://www.imdb.com/title/tt2872732/ (data pobrania: 21.10.2019)

Artykuł na podstawie wykładu inauguracyjnego roku akademickiego 2019/2020 na Wydziale Elektroniki i Technik Informacyjnych PW wygłoszonego 1 października 2019 w Dużej Auli w Gmachu Głównym PW.

{**Krzysztof Szczypiorski** - jest profesorem Politechniki Warszawskiej na Wydziale Elektroniki i Technik Informacyjnych. Jest założycielem Zakładu Cyberbezpieczeństwa na macierzystym Wydziale, którego jest kierownikiem od 2015 roku. Ukończył studia na Politechnice Warszawskiej w 1997 roku, a w kolejnych latach uzyskał stopień doktora i doktora habilitowanego w dziedzinie telekomunikacji ze specjalizacją w zakresie bezpieczeństwa informacji. Ukończył również podyplomowe studia na SWPS w Warszawie oraz Hass School of Business na Uniwersytecie Kalifornia w USA. Jest współzałożycielem i kierownikiem nowego kierunku studiów na Wydziale Elektroniki i Technik Informacyjnych - Cyberbezpieczeństwo. Wizytował m.in. takie uczelnie jak: George Mason University, Fairfax, Virginia, USA (2014), Luxembourg Institute of Science & Technology, Belval Innovation Campus, Esch-sur-Alzette, Luksemburg (2015), University of California, Berkeley, USA (2013) i ponad 50 innych miejsc na krótkoterminowe pobyty naukowe. Od ponad 25 lat Krzysztof Szczypiorski jest niezależnym konsultantem w dziedzinie cyberbezpieczeństwa, telekomunikacji i informatyki dla wielu podmiotów, w tym: Cisco Systems, Hewlett-Packard, Ministerstwa Finansów (Polska), Biura Bezpieczeństwa Narodowego (Polska), Oracle, Orange, Parlamentu Rzeczypospolitej Polskiej, Polskiej Grupy Energetycznej, PwC, T-Mobile Polska. Jest autorem lub współautorem ponad 200 artykułów i ponad 70 zaproszonych rozmów, a także 3 zgłoszeń patentowych (jedno z nich jest przyznane).}