Pomiary Automatyka Robotyka, ISSN 1427-9126, R. 24, Nr 1/2020, 67–74, DOI: 10.14313/PAR_235/67

Identyfikacja zagrożeń w macierzowym modelu stanu pracy i bezpieczeństwa urządzeń IoT

Władysław Iwaniec
Państwowa Wyższa Szkoła Zawodowa w Tarnowie, Wydział Politechniczny, Katedra Automatyki i Robotyki, ul. Mickiewicza 8, 33-100 Tarnów

Streszczenie: W artykule przedstawiono wybrane zagadnienia bezpieczeństwa urządzeń Internetu Rzeczy. Przedstawiono klasyfikację zagrożeń w środowisku współdziałających urządzeń IoT w modelu 5M + E. Jako podstawową przyjęto klasyfikację TOP-10 OWASP dla IoT i dostosowano ją do potrzeb analizy przy pomocy diagramu Ishikawy. Powiązano zagrożenia z grupami przyczyn i zastosowano diagram Ishikawy do oceny jakościowej zagrożeń. Zaproponowano macierzowy model bezpieczeństwa układu urządzeń pracujących zgodnie z zasadą IFTTT. Przyjęto typowy, trójstanowy model oceny stanu bezpieczeństwa każdego z urządzeń i wykazano przydatność modelu macierzowego do oceny stanu pracy i bezpieczeństwa systemu. Wskazano na możliwości podziału zadań w modelu macierzowym na obliczenia we mgle i w chmurze.

Słowa kluczowe: Internet Rzeczy, zagrożenia sieciowe, bezpieczeństwo, model macierzowy, diagram Ishikawy

1. Wprowadzenie

Ewolucja IoT w okresie 20 lat od wprowadzenia tego pojęcia przez Kevina Ashtona przyczyniła się w istotny sposób do powstania Przemysłu 4.0. Dążąc do intensywnego rozwoju oferowanych produktów producenci często marginalizowali problemy cybernetycznego bezpieczeństwa tych urządzeń. Szereg incydentów takich, jak Stuxnet czy wykorzystanie kamer do ataków DDoS obnażyły słabości systemu bezpieczeństwa IoT i uwypukliły konieczność intensyfikacji prac nad bezpieczeństwem tych urządzeń.

Prognozy Gartnera [1] już w 2014 r. wskazały, że w 2020 r. liczebność urządzeń IoT osiągnie 25 miliardów, (z tego ponad 13 mld będzie w grupie tzw. urządzeń konsumenckich), a zatem problem ich bezpieczeństwa jest wyzwaniem o podstawowym znaczeniu. Prace, które pojawiły się w ostatnich kilku latach wskazują na konieczność poszukiwania nowych metod, gdyż konwencjonalne podejście oparte głównie na ochronie punktu końcowego oraz tworzenie zapór na brzegu sieci nie jest adekwatne do oceny i neutralizacji aktualnie występujących zagrożeń.

W artykule [2] został dokonany obszerny przegląd stosowanych metod bezpieczeństwa Internetu Rzeczy. W pracy [3] zwrócono uwagę na specyfikę zagrożeń i rozwiązań z zakresu bezpieczeństwa w środowisku robotów przemysłowych, w pracy [4] wskazano na złożoność ochrony urządzeń w środowisku konsumenckim, zwłaszcza ze względu na interakcje urządzeń poza siecią TCP/IP, w pracy [16] przedstawiono syntetycznie istotne grupy ataków.

Identyfikowanie wektorów zagrożeń jest prowadzone przez wielu praktyków i badaczy, a także organizacje, w tym OWASP (ang. *Open Web Application Security Project*) [5], jednakże w zaproponowanej przez OWASP liście 10 najistotniejszych zagrożeń [6] nie ujęto problemów wynikających z interakcji środowiskowych między urządzeniami. Interesująca metodyka analizy takich interakcji, pozwalająca na ocenę tej grupy zagrożeń, z uwzględnieniem problemu skalowalności, została przedstawiona w pracy [4]. Do identyfikacji jakościowej zagrożeń można wykorzystać metody znane z zarządzania, np. diagramy Ishikawy (metodykę 5M + E: Man, Material, Machine, Method, Management + Environment) [7–9] i – poszerzając interpretację wektora E o interakcje między urządzeniami – połączyć w analizie listę TOP-10 organizacji OWASP i szeroko rozumiane zagrożenia środowiskowe.

Celem niniejszej pracy była analiza możliwości zastosowania opisu zagrożeń i interakcji środowiskowej między urządzeniami IoT z wykorzystaniem modelu macierzowego reprezentującego ocenę stanu bezpieczeństwa i stanu pracy każdego z urządzeń wchodzących w skład systemu IoT.

Autor korespondujący:
Władysław Iwaniec, wiw@pwsztar.edu.pl

Artykuł recenzowany
nadesłany 18.11.2019 r., przyjęty do druku 12.02.2020 r.

2. Zastosowanie diagramu Ishikawy do identyfikacji stanu bezpieczeństwa urządzeń przed zagrożeniami wg klasyfikacji TOP-10 OWASP dla IoT

Jedną z podstawowych metod stosowanych obecnie do szacowania ryzyka związanego z informacją jest analiza jakościowa oparta na ocenie ryzyka wywołania incydentu przez ocenę zagrożenia na jednym z trzech poziomów – niskim, umiarkowanym lub wysokim. Dla urządzeń IoT można przyjąć, że poziomy te

odpowiadają trzem stanom bezpieczeństwa – prawidłowemu, niepewnemu i błędnemu. Dla każdego urządzenia można utworzyć diagram Ishikawy i – przypisując do każdej z gałęzi klasyfikację zagrożenia – na jednym z trzech poziomów ocenić jego stan bezpieczeństwa.

2.1. Klasyfikacja zagrożeń wg OWASP

OWASP, analizując wektory zagrożeń dla Internetu Rzeczy, opublikowała w 2018 r. klasyfikację 10 najistotniejszych zagrożeń bezpieczeństwa w tym sektorze. Klasyfikacja ta obejmuje następujące zagrożenia:

1. Korzystanie z haseł słabych, podatnych na atak siłowy, haseł publicznie dostępnych lub też niezmiennych (ang. *Weak, Guessable, or Hardcoded Passwords*).
2. Niezabezpieczone lub zbędne usługi sieciowe, podatne na zagrożenia wynikające z naruszenia poufności, integralności, dostępności lub nieuprawnionego uwierzytelnienia (ang. *Insecure Network Services*).
3. Niezabezpieczone (zwykle mobilne) punkty dostępu w systemie, niewłaściwe przetwarzanie danych w chmurze, niezabezpieczone API, wskutek niewłaściwego zabezpieczenia uwierzytelniania, autoryzacji, szyfrowania i filtrowania/walidacji danych (ang. *Insecure Ecosystem Interfaces*).
4. Brak możliwości bezpiecznej aktualizacji oprogramowania urządzenia, w szczególności sprawdzania poprawności zainstalowanego oprogramowania, szyfrowania aktualizacji w procesie ich przesyłania, brak powiadomień o aktualizacjach i zapewnienia możliwości powrotu do ostatniej prawidłowo działającej wersji oprogramowania (ang. *Lack of Secure Update Mechanism*).
5. Korzystanie z przestarzałych lub niezabezpieczonych komponentów oprogramowania, jak również ze sprzętu z nieautoryzowanego łańcucha dostaw (ang. *Use of Insecure or Outdated Components*).
6. Brak wystarczającej ochrony prywatności danych osobowych (ang. *Insufficient Privacy Protection*).
7. Brak szyfrowania i autoryzacji dostępu w każdym z trzech stanów danych – zwłaszcza podczas przesyłu i przechowywania danych (ang. *Insecure Data Transfer and Storage*).
8. Brak wsparcia dla bezpieczeństwa urządzeń na każdym etapie cyklu życia, w szczególności zarządzania aktualizacjami (ang. *Lack of Device Management*).
9. Stosowanie urządzeń i oprogramowania dostarczanego z ustawieniami domyślnymi bez wystarczających zabezpieczeń lub brak możliwości rekonfiguracji ustawień fabrycznych (ang. *Insecure Default Settings*).
10. Brak możliwości utwardzania sprzętowego (ang. *Lack of Physical Hardening*).

Pewnym mankamentem tej klasyfikacji jest znikome uwzględnienie wektorów oddziaływań środowiskowych i brak analizy wzajemnych oddziaływań między urządzeniami.

2.2. Jakościowa analiza powiązania zagrożeń z przyczynami w modelu 5M + E

Przedstawione (tab. 1) zaklasyfikowanie jakościowe każdego z wymienionych zagrożeń do grupy przyczyn zostało przeprowadzone z uwzględnieniem klasycznego modelu 5M + E, przy czym:

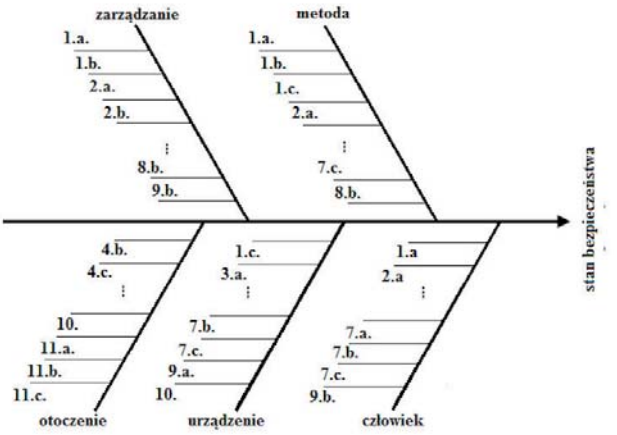
- **Człowiek** oznacza personel instalujący urządzenie oraz użytkownika,
- **Metoda** jest rozumiana bardziej jako procedury stosowane podczas eksploatacji urządzeń, niż jako stosowane w trakcie produkcji urządzeń technologie czy normy,
- **Zarządzanie** rozumiane jest głównie jako konserwacja (pielęgnacja) urządzenia (występująca zwykle jako kolejna przyczyna w podejściu 8M) a nie struktura organizacyjna, czy też kierownictwo lub organizacja pracy producenta,
- **Otoczenie** oznacza dostawców urządzeń.

Tabela zawiera klasyfikację uszczegółowionych zagrożeń z listy TOP-10, podzielonych ze względu na ich związek z grupą przyczyn. Po takim uszczegółowieniu podziału w miejsce 10 zagrożeń ujętych na liście OWASP można wyróżnić 23 zagrożenia, z których ponad 80% jest związanych z zarządzaniem, około 60% z personelem instalującym urządzenia lub użytkownikiem, a także sposobem eksploatacji urządzeń, około 48% z właściwościami urządzeń zależnymi od producentów, a 35% od otoczenia. Nie ma przesłanek do wiązania jakiegokolwiek zagrożenia wskazanego w klasyfikacji OWASP z materiałami.

Jak wspomniano, pewną słabością wykazu zagrożeń w klasyfikacji OWASP i identyfikacji jakościowej podatności urządzeń na potencjalne ataki tylko zgodnie z listą OWASP TOP-10 jest brak uwzględnienia zagrożeń środowiskowych, wynikających z oddziaływania na urządzenia innych urządzeń oraz parametrów środowiska, analizowanych w szczególności w pracy [3].

Zagrożenia te, jak np. wartości parametrów fizycznych środowiska czy wzajemnych zależności stanów pracy urządzeń mogą być analizowane w grupie przyczyn E, przy czym wówczas konieczne jest dodanie do klasyfikacji przedstawionej w tabeli 1 uzupełniających zagrożeń „otoczenia" 11.a. – rozumianego jako zagrożenia wynikające z błędów lub zaniedbań dostawców urządzeń, 11.b. – zagrożeń wskutek niekontrolowanego wpływu parametrów środowiska fizycznego i 11.c. – zagrożeń będących skutkiem wzajemnego oddziaływania urządzeń.

Graficzna prezentacja przeprowadzonej analizy zagrożeń za pomocą diagramu Kaoru Ishikawy jest przedstawiona na rysunku 1.



Rys. 1. Diagram Ishikawy oceny stanu bezpieczeństwa IoT w modelu 5M + E
Fig. 1. Ishikawa IoT safety assessment diagram in the 5M + E model

Tworzenie diagramu Ishikawy do jakościowej oceny stanu bezpieczeństwa urządzenia lub systemu może być również z powodzeniem stosowane przy przyjęciu innych klasyfikacji zagrożeń, np. zaproponowanych w pracy [10].

3. Macierzowy model oceny stanu pracy i bezpieczeństwa urządzeń

W pracy [4] wskazano, iż oprócz konwencjonalnych ataków, wśród których można w szczególności wymienić ataki DDoS, ataki związane z wykorzystaniem urządzeń IoT, wyciekiem danych i przejęciem kontroli danych nad inteligentnymi licznikami energii elektrycznej czy też przejęciem kontroli nad kamerami dozorującymi zachowanie małych dzieci, możliwe są także skuteczne ataki korzystające z urządzeń pracujących zgodnie z zasadą *IF-This-Then-That* (IFTTT). Przykładowo wskazano, że przejęcie kontroli nad inteligentną wtyczką (np. Belkin Wemo) umożliwia włączenie ogrzewania w pokoju, co skutkuje wzrostem temperatury wywołującym otwarcie okien i fizyczne naruszenie bezpieczeństwa.

Tabela 1. Powiązanie zagrożeń OWASP TOP-10 IoT z grupami przyczyn
Table 1. Association of OWASP TOP-10 IoT threats with cause groups

Zagrożenie	Grupa przyczyn					
	Człowiek	Metoda	Urządzenie	Materiał	Zarządzanie	Otoczenie
1.a. Słabe hasła	×	×			×	
1.b. Hasła publicznie dostępne		×			×	
1.c. Hasła niezmienne (sprzętowe)		×	×			
2.a. Niezabezpieczone usługi sieciowe	×	×			×	
2.b. Zbędne usługi sieciowe		×			×	
3.a. Niezabezpieczone punkty dostępu	×		×		×	
3.b. Niewłaściwe przetwarzanie danych w chmurze	×	×			×	
3.c. Niewłaściwy dobór API	×	×			×	
4.a. Brak szyfrowania aktualizacji w drodze	×	×	×		×	
4.b. Brak weryfikacji poprawności zainstalowanego oprogramowania	×				×	×
4.c. Brak powiadomień o aktualizacjach		×			×	×
5.b. Korzystanie z nieautoryzowanego sprzętu	×		×			
6. Brak wystarczającej ochrony prywatności	×	×	×		×	×
7.a. Brak szyfrowania i autoryzacji dostępu do danych „w drodze”	×	×	×		×	×
7.b. Brak szyfrowania i autoryzacji dostępu do danych „w spoczynku”	×	×	×		×	
7.c. Brak szyfrowania i autoryzacji dostępu do przetwarzanych danych	×	×	×		×	
8.a. Brak wsparcia dla zarządzania aktualizacjami					×	×
8.b. Brak wsparcia dla bezpieczeństwa urządzeń w cyklu życia urządzenia		×			×	×
9.a. Brak możliwości rekonfiguracji ustawień fabrycznych			×			×
9.b. Stosowanie urządzeń i oprogramowania z ustawieniami domyślnymi	×				×	
10. Brak możliwości utwardzania sprzętowego			×			×

Aby przeciwdziałać takim potencjalnym zagrożeniom konieczne jest budowanie modeli oddziaływań zarówno w sieci, jak też w środowisku fizycznym. Należy podkreślić, że urządzenia IoT charakteryzują się ograniczonymi zasobami i heterogenicznością systemów operacyjnych, zatem dążenie do tworzenia oprogramowania antywirusowego dla tak szerokiej gamy urządzeń nie jest uzasadnione. Dla pewnej grupy urządzeń, np. smartTV pracujących na platformie systemu Android, takie oprogramowanie jest rozwijane, jednakże – jak wynika z analizy zagrożeń OWASP TOP-10 – założenie o powszechności instalowania i aktualizacji oprogramowania antywirusowego jest nieuprawnione.

Aktualizacja oprogramowania użytkowego w celu eliminacji luk także napotyka na szereg przeszkód, m.in. ze względu na konieczność ręcznego wykonywania tego procesu lub też brak aktualizacji oprogramowania przez producentów. W konsekwencji zadania ochrony punktu końcowego muszą być przenoszone na brzeg sieci, względnie do chmury lub mgły.

W koncepcji IoTSec przedstawionej w pracy [3] przewiduje się tworzenie dodatkowych elementów sieci, tzw. µmboxów (realizujących funkcje mikrobezpieczeństwa sieci), które działają jako bramki bezpieczeństwa dla każdego urządzenia IoT. Logicznie scentralizowany kontroler IoTSec monitoruje konteksty różnych urządzeń i środowiska operacyjnego i generuje widok globalny dla wymuszania zasad dla różnych urządzeń. Na podstawie tego widoku tworzone są zasady ochrony i konfigurowane są poszczególne µmboxy. Taka koncepcja ochrony jest dość ogólna i może korzystać z różnych modeli zarządzania IoT, np. modelu urządzeń bezpośrednio połączonych do punktu centralnego IoT i kontrolowanych przez smartfony.

Założenie o zapewnieniu na smartfonie zasobów wystarczających dla potrzeb bezpieczeństwa systemu jest jednakże założeniem bardzo optymistycznym; pod względem dostępności zasobów i skalowalności systemu realne jest podejście przetwarzania w chmurze, jednakże wiąże się ze zwiększeniem opóźnienia w podejmowaniu decyzji przez oprogramowanie odpowiedzialne

za stan bezpieczeństwa systemów i ich przesyłaniu do urządzeń końcowych.

W wielu pracach wskazano, że przeniesienie zadań scentralizowanego kontrolera IoTSec do warstwy mgły i jednoczesne rozproszenie realizacji tych zadań do kontrolerów monitorujących pracę urządzeń faktyczne i potencjalnie współdziałających ze sobą pozwoli na wykorzystanie zalet koncepcji mgły, przede wszystkim zmniejszenie opóźnień w ocenie bezpieczeństwa działających urządzeń.

3.1. Analiza przypadku szczególnego

Obszerną analizę zagadnień bezpieczeństwa przetwarzania we mgle zawiera przeglądowy artykuł [11]. W pracy [4] zwraca się uwagę, że w opisie interakcji między urządzeniami zachodzą pewne istotne ograniczenia bezpieczeństwa, wynikające m.in. z założenia, że reguły bezpieczeństwa mogą być określane niezależne dla każdego urządzenia, co może prowadzić do konfliktów reguł lub niejednoznaczności wyników (np. generowanie takiego samego sygnału alarmowego dla różnych zdarzeń), a także z trudności identyfikacji wszystkich możliwych interakcji.

Problem powiązania stanu bezpieczeństwa urządzeń IoT i ich interakcji może być rozwiązywany przez utworzenie modelu macierzowego stanów bezpieczeństwa i pracy urządzeń. Dla przykładu można rozważyć trzy urządzenia, z których dwa D_1 i D_2 mogą zostać włączone wtedy, gdy trzecie urządzenie D_3 przyjmuje określony stan, np. jest wyłączone.

Przykładem takiego układu może być wyodrębniony w układzie typowej automatyki domowej układ obejmujący sterowanie oświetleniem wybranych pomieszczeń (D_1), siłownikami otwierania okien (D_2) i instalację alarmową (D_3). Zakłada się, że układy sterowania oświetleniem wybranych pomieszczeń oraz otwierania okien mogą być włączone dopiero wtedy, gdy instalacja alarmowa zostaje wyłączona, czyli gdy w domu obecni są mieszkańcy. Oczywiście, można urządzenie D_3 zastąpić np. czujnikami ruchu, a wtedy zmienić warunek dopuszczalności włączania D_1 i D_2 stanem aktywności mieszkańców, przypisując mu stan pracy urządzenia „włączony". Założenie o podziale oświetlenia wybranych pomieszczeń wynika z konieczności zapewnienia możliwości sterowania włączaniem i wyłączaniem świateł przy włączonej instalacji alarmowej w celu symulacji obecności mieszkańców i uniemożliwienia potencjalnym włamywaczom ustalenia faktycznej obecności domowników.

Założenie o blokadzie systemu sterowania otwieraniem okien, zasygnalizowane już wyżej przy omawianiu pracy [4] uniemożliwia automatyczne otwarcie okien w opisanym tam przypadku wzrostu temperatury przy przechwyceniu przez intruza kontroli nad systemem ogrzewania, a blokada systemu sterowania oświetleniem dla wybranych pomieszczeń wyklucza straty finansowe wynikające z przejęcia przez intruza kontroli nad tym systemem, jeśli instalacja alarmowa jest włączona.

Typowo przyjmuje się, że stan bezpieczeństwa każdego z urządzeń może przyjmować trzy wartości:

p – prawidłowy,

n – niepewny,

u – błędny, nieprawidłowy (np. nieaktualizowany, mimo udostępnienia aktualizacji przez producenta).

Zbiór możliwych stanów bezpieczeństwa dla k urządzeń można oznaczyć przez

$$\mathbf{S}_k = \{p_1, n_1, u_1, p_2, n_2, u_2, ..., p_k, n_k, u_k\}.$$

Każde z urządzeń może przyjmować dwa stany pracy:

t_i – włączony,

f_i – wyłączony.

Przy takim założeniu zbiór stanów pracy dla k urządzeń można oznaczyć jako

$$\mathbf{W}_{2k} = \{t_1, f_1, t_2, f_2, ..., t_k, f_k\}.$$

Wtedy przestrzeń wszystkich możliwych stanów bezpieczeństwa i stanów pracy dla rozważanych w przykładzie trzech urządzeń można przedstawić jako iloczyn macierzy

$$\mathbf{Z} = \mathbf{S}_{3^3\times 3} \cdot \mathbf{W}_{3\times 2^3} = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_1 & p_2 & n_3 \\ p_1 & p_2 & u_3 \\ p_1 & n_2 & p_3 \\ \dots & \dots & \dots \\ u_1 & n_2 & n_3 \\ u_1 & n_2 & u_3 \\ u_1 & u_2 & p_3 \\ u_1 & u_2 & n_3 \\ u_1 & u_2 & u_3 \end{bmatrix} \cdot \begin{bmatrix} t_1 & t_1 & t_1 & \dots & f_1 & f_1 \\ t_2 & t_2 & f_2 & \dots & f_2 & f_2 \\ t_3 & f_3 & t_3 & \dots & t_3 & t_3 \end{bmatrix} \quad (1)$$

W podanym przykładzie uzyskuje się macierz $\mathbf{Z}$ o wymiarach $3^k \times 2^k$:

$$\begin{bmatrix} p_1 \cdot t_1 + p_2 \cdot t_2 + p_3 \cdot t_3 & p_1 \cdot t_1 + p_2 \cdot t_2 + p_3 \cdot f_3 & \dots & p_1 \cdot f_1 + p_2 \cdot f_2 + p_3 \cdot t_3 & p_1 \cdot f_1 + p_2 \cdot f_2 + p_3 \cdot f_3 \\ p_1 \cdot t_1 + p_2 \cdot t_2 + n_3 \cdot t_3 & p_1 \cdot t_1 + p_2 \cdot t_2 + n_3 \cdot f_3 & \dots & p_1 \cdot f_1 + p_2 \cdot f_2 + n_3 \cdot t_3 & p_1 \cdot f_1 + p_2 \cdot f_2 + n_3 \cdot f_3 \\ \dots & \dots & \dots & \dots & \dots \\ u_1 \cdot t_1 + u_2 \cdot t_2 + u_3 \cdot t_3 & u_1 \cdot t_1 + u_2 \cdot t_2 + u_3 \cdot f_3 & \dots & u_1 \cdot f_1 + u_2 \cdot f_2 + u_3 \cdot t_3 & u_1 \cdot f_1 + u_2 \cdot f_2 + u_3 \cdot f_3 \end{bmatrix} \quad (2)$$

Macierz może być interpretowana jako zbiór $\mathbf{Z}$ elementów trójek par:

$$\mathbf{Z} = \{[(p_1, t_1), (p_2, t_2), (p_3, t_3)], [(p_1, t_1), (p_2, t_2), (p_3, f_3)], ..., [(u_1, f_1), (u_2, f_2), (u_3, t_3)], [(u_1, f_1), (u_2, f_2), (u_3, f_3)]\}.$$

W zbiorze $\mathbf{Z}$ wszystkich możliwych stanów bezpieczeństwa i stanów pracy można wybierać trójkę par określającą aktualny stan pracy i bezpieczeństwa urządzeń, np. pożądany stan $[(p_1, t_1), (p_2, t_2), (p_3, f_3)]$, wskazujący stan pracy włączonego urządzeń D_1 z bezpiecznym oprogramowaniem, włączonego urządzenia D_2 z bezpiecznym oprogramowaniem i wyłączonego urządzenia D_3, z bezpiecznym oprogramowaniem.

W rozważanym przykładzie pożądanymi stanami układu są tylko dwie trójki:

$$\mathbf{Z}^* = \{[(p_1, t_1), (p_2, t_2), (p_3, f_3)], [(p_1, f_1), (p_2, f_2), (p_3, t_3)]\}$$

natomiast pozostałe stany albo stanowią potencjalne zagrożenie bezpieczeństwa lub wskazują na niedopuszczalne działanie urządzeń i powinny być odpowiednio sygnalizowane lub blokowane.

W rozważanym przykładzie ze zbioru wszystkich stanów $\mathbf{Z}$ można wyróżnić, oprócz zbioru $\mathbf{Z}^*$ także zbiór $\mathbf{Z}^{**}$ stanów dopuszczalnych, w tym także stanowiących potencjalne zagrożenie bezpieczeństwa, w których D_1 i D_2 są włączone, D_3 wyłą-

czone lub też – jeśli D_3 jest w stanie „włączone", to D_1 i D_2 są wyłączone.

Przy takim założeniu macierz odwzorowującą zbiór stanów $\mathbf{Z}^{**}$ można przedstawić jako zmodyfikowane równanie (1) w postaci:

$$\mathbf{Z}^{**} = \mathbf{S}_{3^3\times 3}\cdot\mathbf{W}_{3\times 2} = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_1 & p_2 & n_3 \\ p_1 & p_2 & u_3 \\ p_1 & n_2 & p_3 \\ \dots & \dots & \dots \\ u_1 & n_2 & n_3 \\ u_1 & n_2 & u_3 \\ u_1 & u_2 & p_3 \\ u_1 & u_2 & n_3 \\ u_1 & u_2 & n_3 \end{bmatrix} \cdot \begin{bmatrix} t_1 & f_1 \\ t_2 & f_2 \\ f_3 & t_3 \end{bmatrix} \tag{3}$$

lub też zastąpienie tych elementów macierzy $\mathbf{Z}$, które reprezentują stany niedozwolone zerami:

$$\mathbf{Z} = \begin{bmatrix} 0 & p_1\cdot t_1 + p_2\cdot t_2 + p_3\cdot f_3 & \dots & p_1\cdot f_1 + p_2\cdot f_2 + p_3\cdot t_3 & 0 \\ 0 & p_1\cdot t_1 + p_2\cdot t_2 + n_3\cdot f_3 & \dots & p_1\cdot f_1 + p_2\cdot f_2 + n_3\cdot t_3 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & u_1\cdot t_1 + u_2\cdot t_2 + u_3\cdot f_3 & \dots & u_1\cdot f_1 + u_2\cdot f_2 + u_3\cdot t_3 & 0 \end{bmatrix} \tag{4}$$

Macierz $\mathbf{Z}$ jest macierzą rzadką, co implikuje możliwości stosowania metod numerycznych charakterystycznych dla tej grupy macierzy, ale – jak widać z powyższego przykładu – nie jest macierzą symetryczną.

3.2. Uogólnienie modelu macierzowego stanu pracy i bezpieczeństwa dla *k* urządzeń

Ogólnie, dla k urządzeń, charakteryzujących się typowymi trzema stanami bezpieczeństwa (w szczególności eksploatowanego na nich oprogramowania), z których każde może być włączone lub wyłączone, zapis przestrzeni wszystkich stanów pracy i bezpieczeństwa można przedstawić następująco:

$$\mathbf{Z} = \mathbf{S}_{3^k\times k}\cdot\mathbf{W}_{k\times 2^k} = \begin{bmatrix} p_1 & \dots & p_i & \dots & p_k \\ \dots & \dots & \dots & \dots & \dots \\ p_1 & \dots & p_i & \dots & n_k \\ \dots & \dots & \dots & \dots & \dots \\ u_1 & \dots & u_i & \dots & u_k \end{bmatrix} \cdot \begin{bmatrix} t_1 & t_1 & \dots & t_1 & \dots & f_1 & f_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ t_i & t_i & \dots & f_i & \dots & f_i & f_i \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ t_k & f_k & \dots & f_k & \dots & t_k & f_k \end{bmatrix} \tag{5}$$

Zbiór stanów pożądanych $\mathbf{Z}^*$ zawiera arbitralnie ustalone i wybrane stany, które z punktu widzenia bezpieczeństwa urządzeń i ich interakcji uznaje się za prawidłowe i bezpieczne.

Analogicznie, można – także arbitralnie – ustalić zbiór $\mathbf{Z}^{**}$, zawierający stany, które z punktu widzenia bezpieczeństwa systemu są obarczone pewnym ryzykiem wymagającym powiadomienia użytkownika, jednakże mogą być uznane przez kontroler za dopuszczalne i skutkują jedynie przesyłaniem w czasie rzeczywistym komunikatu o wykrytym zagrożeniu bezpieczeństwa systemu.

W zależności od wiedzy *a priori* o układzie można rozważać dowolne scenariusze stanów pracy i bezpieczeństwa systemów i ustalać zbiory $\mathbf{Z}^*$ i $\mathbf{Z}^{**}$. W szczególności można zakładać, że do zbioru $\mathbf{Z}^*$ mogą należeć tylko takie elementy, w których ocena stanu bezpieczeństwa jest ustalona jako prawidłowa lub też takie elementy, dla których stany pracy przyjmują wyznaczone wartości.

W identyfikacji stanu bezpieczeństwa i ustalania urządzeń IoT w systemie, dla którego są wyznaczane zbiory $\mathbf{Z}^*$ i $\mathbf{Z}^{**}$ można posłużyć się rozmaitymi metodykami, np. opisaną w pkt. 2 metodyką diagramów Ishikawy czy też wywodzącym się z tzw. dobrych praktyk frameworkiem CSA [12] posługującym się także trójpoziomową oceną bezpieczeństwa badanego systemu. Przegląd właściwości rozmaitych frameworków został przedstawiony w pracy [13].

Kontroler, analizujący stany pracy, musiałby dysponować odpowiednimi zasobami w celu zapamiętywania macierzy $\mathbf{Z}$ oraz $\mathbf{Z}^*$ i wykonania operacji porównania stanów w czasie rzeczywistym w celu zezwolenia lub zablokowania przejścia do kolejnego stanu układu.

Zależność (4) można uogólnić dla n stanów bezpieczeństwa i m stanów pracy urządzeń zapisując je w postaci:

$$\mathbf{Z} = \mathbf{S}_{n^k\times k}\cdot\mathbf{W}_{k\times m^k} = \begin{bmatrix} s_{1,1} & \dots & s_{1,i} & \dots & s_{1,k} \\ \dots & \dots & \dots & \dots & \dots \\ s_{2,1} & \dots & s_{j,i} & \dots & s_{2,k} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n,1} & \dots & s_{n,i} & \dots & s_{n,k} \end{bmatrix} \cdot \begin{bmatrix} w_{1,1} & w_{1,1} & \dots & w_{1,1} & \dots & w_{m-1,1} & w_{m,1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ w_{1,i} & w_{1,i} & \dots & w_{p,i} & \dots & w_{m,i} & w_{m,i} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ w_{1,k} & w_{2,k} & \dots & w_{m,k} & \dots & w_{m,k} & w_{m,k} \end{bmatrix} \tag{6}$$

gdzie:

$s_{j,i}$ – stan (poziom) bezpieczeństwa j dla urządzenia i, $j = 1, 2, \dots, n$; $i = 1, 2, \dots, k$

$w_{p,j}$ – stan (poziom) pracy p dla urządzenia i, $p = 1, 2, \dots, m$; $i = 1, 2, \dots, k$.

Moc zbioru $\mathbf{Z}$ zależy wykładniczo od liczby urządzeń k i wymaga znacznych zasobów pamięci, jednakże dysponując informacjami o stanach pożądanych i o stanach dopuszczalnych można redukować problem budowy i zapisywania macierzy stanów bezpieczeństwa i pracy do określenia pożądanego zbioru $\mathbf{Z}^*$ lub dopuszczalnego zbioru $\mathbf{Z}^{**}$ i analizy przez kontroler, czy stany rzeczywiste lub stany, do których system opisywany macierzą $\mathbf{Z}$ ma przejść, występują w zbiorze $\mathbf{Z}^*$ lub $\mathbf{Z}^{**}$. Rozważanie zbiorów $\mathbf{Z}^*$ i $\mathbf{Z}^{**}$ zamiast zbioru $\mathbf{Z}$ skutkuje także możliwością korzystania z oprogramowania stosowanego do obliczeń macierzy rzadkich, co istotnie zmniejsza zapotrzebowanie na zasoby kontrolera.

3.3. Podział zadań kontrolera na zadania we mgle i w chmurze

Zasoby wymagane do zastosowana proponowanego modelu macierzowego Z mogą być udostępnione w chmurze. Za takim rozwiązaniem przemawia skalowalność rozwiązań chmurowych, jednakże w warunkach konieczności podejmowania w czasie rzeczywistym decyzji o ocenie bezpieczeństwa stanu istniejącego i stanu, do którego ma przejść system, krytycznym parametrem staje się czas przesłania danych, wypracowania decyzji i przesłania jej do urządzeń. Czasy transmisji danych do chmury sięgają co najmniej setek milisekund i mogą być nieakceptowalne.

Rozwijana w ostatnich kilku latach koncepcja przetwarzania danych we mgle rozszerza model rozwiązań chmurowych przez możliwość wykonywania obliczeń rozproszonych, lokalnie, w różnorodnych środowiskach i wypracowywanie decyzji z mniejszymi opóźnieniami w porównaniu do tradycyjnego podejścia przetwarzania danych w chmurze. Propozycja obliczeń we mgle zaproponowana w dokumentach CISCO [14] została sformalizowana w dokumencie NIST SP 500-325 [15].

W pracy [17] wskazano, że obliczenia we mgle mogą być rozważane jako nowa warstwa między warstwą procesów produkcji i warstwą nadrzędnego sterowania procesami. Dobre praktyki ochrony automatyki przemysłowej dla infrastruktury krytycznej, np. opublikowane przez Rządowe Centrum Bezpieczeństwa [18] wskazują, że wymagane czasy reakcji są rzędu milisekund. Zasadnicze znaczenie dla spełnienia tego wymagania ma czas opóźnienia pakietów transmitowanych w sieci.

Zagadnienia szacowania opóźnienia dla obliczeń we mgle zostały przedstawione w pracy [19]. Przyjęto typowo, że sumaryczna wartość opóźnienia transmisji pakietów wyraża się zależnością:

$$D_{\text{end-to-end}} = N \cdot (d_{\text{proc}} + d_{\text{queue}} + d_{\text{seri}} + d_{\text{prop}}) \tag{7}$$

gdzie:

d_{proc} – opóźnienie związane z przetwarzaniem pakietu w węźle sieci,
d_{queue} – opóźnienie związane z kolejkowaniem,
d_{seri} – opóźnienie związane z serializacją,
d_{prop} – opóźnienie związane z propagacją,
N – liczba segmentów sieci, jakie pakiet przebywa w ekosystemie IoT.

Wskazano, że aktualnie wartości d_{proc} oraz d_{seri} są rzędu mikrosekund na węzeł, d_{prop} – około 5 µs/km. Wartość opóźnienia d_{queue} może być optymalizowana dzięki stosowaniu lepszych polityk niż FIFO i zastosowaniu technik QoS. W konsekwencji, skoro dla obliczeń we mgle w porównaniu do obliczeń czasu opóźnienia dla transmisji chmurowych można zmniejszyć liczbę segmentów do jednego, a czas propagacji ze względu na fizyczną bliskość węzłów jest najmniejszy z możliwych, czas odpowiedzi na żądanie elementu wykonawczego spełni warunek opóźnienia rzędu milisekund i jest akceptowalny.

W przypadku gdy węzły mgły nie sąsiadują ze sobą, do oszacowania opóźnienia można stosować przeanalizowane w [19] algorytmy NCS (ang. *Network Coordinate System*), takie jak GNP (ang. *Global Network Positioning*), NPS (ang. *Network Positioning System*), Vivaldi i Pharos, jednakże ze względu na dużą zmienność położenia węzłów poszukiwane są nowe algorytmy, które umożliwią precyzyjniejsze szacowanie opóźnień w ekosystemach IoT. Dla uzyskiwania wyników dobrze przybliżających wartości rzeczywistego opóźnienia, obliczane w algorytmach NCS istotne są węzły o stałych lokalizacjach, np. serwery aplikacji, w tym aplikacji kontroli poprawności stanu bezpieczeństwa i pracy urządzeń.

Dla rozważanego modelu macierzowego zbiory $\mathbf{Z}^*$ i $\mathbf{Z}^{**}$ mogą być umieszczane na kontrolerach w warstwie mgły, w stałych lokalizacjach, co pozwala na ocenę stanu bezpieczeństwa i pracy w czasie „jednego skoku", a zatem z względnie stałym opóźnieniem rzędu pojedynczych milisekund.

Jeżeli stan rzeczywisty lub przyszły jest elementem zbioru $\mathbf{Z}^*$, kontroler zezwala na pracę lub przejście do przyszłego stanu (np. nie podejmuje żadnej akcji). Jeżeli przyszły stan jest elementem zbioru $\mathbf{Z}^{**} - \mathbf{Z}^*$, do użytkownika wysyłane jest ostrzeżenie, przejście jest wstrzymywane, a jednocześnie do chmury wysyłana jest informacja o przyszłym stanie w celu wypracowania przez kontroler w chmurze decyzji o zezwoleniu lub blokadzie przejścia układu do stanu przyszłego. Jeżeli decyzja podejmowana przez kontroler w chmurze zezwala na przejście do przyszłego stanu, to stan ten jest dopisywany do zbioru $\mathbf{Z}^*$, przy czym decyzja użytkownika, która co do zasady jest podejmowana po czasie dłuższym niż czas podjęcia decyzji przez kontroler w chmurze, ma najwyższy priorytet.

Za podziałem zadań kontrolera na warstwy mgły i chmury przemawia także istotne poprawienie bezpieczeństwa systemu w sytuacji utraty łączności z chmurą, gdyż zadanie notyfikacji użytkownika o potencjalnym zagrożeniu jest realizowane w warstwie mgły, a zadanie podjęcia decyzji przez kontroler w warstwie chmury jest realizowane po odzyskaniu łączności. W sytuacji utraty łączności z chmurą kontroler w warstwie mgły może zmieniać algorytm pracy w ten sposób, że jeśli stan przyszły jest elementem zbioru $\mathbf{Z}^{**} - \mathbf{Z}^*$, to następuje wstrzymanie decyzji do odzyskania łączności z chmurą lub też do podjęcia przez użytkownika decyzji o możliwości przejścia układu do stanu przyszłego.

Za umiejscowieniem kontrolera dla systemów urządzeń IoT w warstwie mgły i rozproszeniu jego zadań przemawia również przesłanka możliwości dekompozycji macierzy $\mathbf{Z}^*$ i $\mathbf{Z}^{**}$ dla takich systemów, w których można wyróżnić podzbiory urządzeń, których stany pracy oddziałują na siebie w danym podzbiorze, lecz nie wpływają na stan pracy urządzeń w innych podzbiorach.

4. Podsumowanie

Zaproponowany macierzowy model pozwala na opisanie stanu bezpieczeństwa i stanu pracy systemów urządzeń IoT charakteryzujących się dowolną liczbą stanów bezpieczeństwa i stanów pracy. Określanie macierzy $\mathbf{Z}^*$ stanów pożądanych oraz macierzy $\mathbf{Z}^{**}$ stanów dopuszczalnych upraszcza zagadnienie przechowywania i przeszukiwania macierzy Z opisującej przestrzeń wszystkich hipotetycznie możliwych stanów systemu. Identyfikacja jakościowa stanów bezpieczeństwa każdego urządzenia może być realizowana zaproponowaną metodą analizy uszczegółowionej i poszerzonej o zagrożenia środowiskowe listy OWASP TOP-10 dla urządzeń IoT przy zastosowaniu diagramu Ishikawy.

Bibliografia

1. Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015. [www.gartner.com/en/newsroom/press-releases/2014-11-11-gartner-says-nearly-5-billion-connected-things-will-be-in-use-in-2015].
2. Kouicem D.E., Bouabdallah A., Kakhlef H., *Internet of things security: A top-down survey*, "Computer Networks", Vol. 141, 2018, 199–221, DOI: 10.1016/j.comnet.2018.03.012.
3. Quarta D., Pogliani M., Polino M., Maggi F., Zanchettin A.M., Zanero S., *An Experimental Security Analysis of an Industrial Robot Controller*, [www.ieee-security.org/TC/SP2017/papers/20.pdf].
4. Zu T., Sekar V., Seshan S., Agarwal Y., Xu Ch., *Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things*. Proceedings of the 14th ACM Workshop on Hot Topics in Networks, November 2015 Article No. 5, DOI: 10.1145/2834050.2834095.
5. OWASP TOP10 Internet of Things 2018, [www.owasp.org/index.php/OWASP_Internet_of_Things_Project].
6. [www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf].
7. Pałęga M., Knapiński M., Rydz D., *Identyfikacja i ocena zagrożeń bezpieczeństwa informacji za pomocą wybranych*

instrumentów zarządzania jakością. Materiały z konferencji: Innowacje w Zarządzaniu Jakością, 2018, 283–295.
8. Dobrynin I., Radivilowa T., Maltseva N., Ageyev D., *Use of Approaches to the Methodology of Factor Analysis of Information Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links*, 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, DOI: 10.1109/INFOCOMMST.2018.8632022.
9. Wawak S., *Zarządzanie jakością. Podstawy, systemy i narzędzia*, Helion, Gliwice 2011.
10. Frustaci M., Pace P., Aloi G., Fortino G., *Evaluating Critical Security Issues of the IoT World: Present and Future Challenges*, "IEEE Internet of Things Journal", Vol. 5, No. 4, 2018, 2483–2495, DOI: 10.1109/JIOT.2017.2767291.
11. Khan S., Parkinson S., Qin Y., *Fog computing security: a review of current applications and security solutions*, "Journal of Cloud Computing, Advances, Systems and Applications", Vol. 6, No. 19, 2017, DOI: 10.1186/s13677-017-0090-3.
12. CSA Guide to the IoT Security Controls Framework, CSA IoT Controls Framework, https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework, 03.05.2019.
13. Ammar M., Russello G., Crispo B., *Internet of Things: A survey on the security of IoT frameworks*, "Journal of Information Security and Applications", Vol. 38, 2018, 8–27, DOI: 10.1016/j.jisa.2017.11.002.
14. *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are*, 2015, [www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf].
15. https://csrc.nist.gov/publications/detail/sp/500-325/final, marzec 2018.
16. Gurunath R., Agarwal M., Nandi A., Samanta D., *An Overview: Security Issue in IoT Network*, Proceedings of the Second International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2018), IEEE Xplore Part Number:CFP18OZV-ART; ISBN:978-1-5386-1442-6, 104–107.
17. Matt C., *Fog Computing – Complementing Cloud Computing to Facilitate Industry 4.0*, "Business & Information Systems Engineering", Vol. 60, No. 4, 2018, 351–355, DOI: 10.1007/s12599-018-0540-6.
18. *Standardy i dobre praktyki ochrony infrastruktury krytycznej. Automatyka przemysłowa w sektorze elektroenergetycznym*. Rządowe Centrum Bezpieczeństwa, 2019, https://rcb.gov.pl/wp-content/uploads/Standardy-i-dobre-praktyki-ochrony-infrastruktury-krytycznej-%E2%80%93-automatyka-przemys%C5%82owa-w-sektorze-elektroenergetycznym.pdf.
19. Li J., Zhang J., Jin J., Yang Y., Yuan D., Gao L., *Latency Estimation for Fog-based Internet of Things*, 27th International Telecommunication Networks and Applications Conference (ITNAC) 2017, DOI: 10.1109/ATNAC.2017.8215403.

Identification of Threats in the Matrix Model of the State of Work and Security of IoT Devices

Abstract: The paper presents selected issues of Internet of Things security. The classification of threats in the environment of cooperating IoT devices in the 5M + E model is presented. The TOP-10 OWASP classification for IoT was adopted as the basic one and was adapted to the needs of the analysis using the Ishikawa diagram. Threats were mapped to cause groups and the Ishikawa diagram was used to qualitatively assess the threats. A matrix security model of the ecosystem of devices operating in accordance with the IFTTT principle was proposed. A typical three-state model for assessing the safety status of each device was adopted and the usefulness of the matrix model for assessing the state of work and system security was justified. The possibilities of dividing tasks in the matrix model into fog computing and in the cloud were pointed out.

Keywords: Internet of Things, network threats, matrix model, Ishikawa diagram

dr inż. Władysław Iwaniec
wiw@pwsztar.edu.pl
ORCID: 0000-0002-5253-7710

Adiunkt w Katedrze Automatyki i Robotyki Państwowej Wyższej Szkoły Zawodowej w Tarnowie, w której był prorektorem w latach 1998–2007. Autor kilku publikacji naukowych, ma bogate doświadczenie praktyczne w zakresie systemów informatycznych. Odznaczony m.in. Złotym Krzyżem Zasługi i Srebrnym Medalem za Obronność Kraju. Zainteresowania naukowe obejmują zagadnienia kryptografii i bezpieczeństwa sieci i systemów komputerowych oraz identyfikacji układów sterowania.