Programowanie Defensywne

Przegląd wybranych standardów
część pierwsza

Arkadiusz Chrobot

Katedra Systemów Informatycznych

21 czerwca 2024

Plan

Wprowadzenie

Oprócz nieformalnych standardów związanych z wytwarzaniem oprogramowania, które omawialiśmy do tej pory, opracowano na potrzeby bezpieczeństwa (ang. *security & safety*) również standardy formalne, których spełnienie warunkuje dopuszczenie produktu do użytku. Są wśród nich zarówno takie, które są ogólne (np. standardy ISO 27000, Common Criteria), jaki i dotyczące konkretnych dziedzin, takich jak systemy automatyki przemysłowej (ang. *Operational Technology*, OT), medycyny, czy finansów. Obejmują one swoim zakresem nie tylko oprogramowanie, ale również fizyczne urządzenia i inne elementy systemów informatycznych, które mogą mieć związek z bezpieczeństwem.

Standardy ogólne

Sprawami cyberbezpieczeństwa w Uni Europejskiej zajmuje się European Union Agency for Cybersecurity — ENISA. Opublikowany przez nią dokument pt. „Advancing Software Security in the EU” [1] zawiera przegląd obowiązujących formalnych i nieformalnych standardów bezpieczeństwa, które dotyczą oprogramowania. W tym opracowaniu poruszono również tematykę związaną z tworzeniem bezpiecznych programów (wymogi bezpieczeństwa, bezpieczeństwo w inżynierii oprogramowania i w cyklu życia programów), a także wskazano największe problemy z tym związane.

Standardy ogólne

Do problemów związanych z zapewnieniem bezpieczeństwa oprogramowania zaliczono:

1. brak klarownych wytycznych, spowodowany brakiem uregulowanej współpracy między organami standaryzującymi i instytucjami opracowującymi tzw. dobre praktyki,
2. brak spójnego systemu klasyfikacji poziomu bezpieczeństwa, który byłby klarowny dla nie-ekspertów,
3. problem utrzymania poziomu bezpieczeństwa certyfikowanego oprogramowania,
4. brak związku między jakością procesu wytwórczego, a jakością produktu w kontekście bezpieczeństwa.

Standardy ogólne

Jednymi z najczęściej stosowanych standardów bezpieczeństwa są normy ISO/IEC z serii 27000 [1, 2]. Zostały one także zaadaptowane jako Polskie Normy. Dotyczą one wielu aspektów cyberbezpieczeństwa, np. ISO 27001 dotyczy Systemów Zarządzania Bezpieczeństwem Informacji. Z punkty widzenia tworzenia oprogramowania istotnymi są:

27034-3 application security management process,

27034-5 protocols and application security controls data structure,

27034-7 assurance prediction framework.

Zaletą tych standardów jest to, że są powszechnie stosowane i mają poparcie wielu podmiotów gospodarczych. Do ich wad należy zaliczyć obszerność i dostępność za odpłatnością.

Standardy ogólne

Odpowiedzią na problem z brakiem spójnej klasyfikacji poziomów bezpieczeństwa miały być *Common Criteria for Information Technology Security Evaluation* nazywane krócej *Common Criteria* lub po prostu CC [3]. W zamierzeniu miał to być międzynarodowy system oceny zabezpieczeń, który pozwalałby ustalić poziom bezpieczeństwa określonego produktu (nazywanego *przedmiotem oceny* (ang. *Target of Evaluation*)), w oparciu o konkretny *Profil Ochrony* (ang. *Protection Profile*). Profil ten jest zbiorem funkcjonalnych wymogów bezpieczeństwa i wymogów gwarancji (ang. *assurance*) dla danej klasy produktów. Może on zostać przekształcony (ang. *refined*) do *Celu Zabezpieczenia* (ang. *Security Target*), dla konkretnego produktu. Oceny profili, celów i samych produktów dokonują akredytowane laboratoria, które mogą być zarówno państwowe, jak i prywatne. W Polsce, która przystąpiła do programu CC, instytucją certyfikującą jest Państwowy Instytut Badawczy NASK.

Standardy ogólne

Ocena produktu w ramach programu CC dokonywana jest na następujących poziomach (ang. *Evaluation Assurance Level*):

- EAL1 przetestowany funkcjonalnie,
- EAL2 przetestowany strukturalnie,
- EAL3 metodycznie przetestowany i sprawdzony (ang. *checked*),
- EAL4 metodycznie zaprojektowany, przetestowany i sprawdzony (ang. *reviewed*),
- EAL5 półformalnie (ang. *semi-formally*) zweryfikowany, zaprojektowany i przetestowany,
- EAL6 półformalnie (ang. *semi-formally*) zweryfikowany projekt i przetestowany,
- EAL7 formalnie zweryfikowany projekt i przetestowany.

Większość sprawdzonych produktów dostępnych powszechnie ma poziom EAL4.

Standardy ogólne

Według Rossa Andersona problemy z CC są następujące:

- proces certyfikacji jest długi i kosztowny,
- CC pomijają wiele aspektów bezpieczeństwa, np. emisja elektromagnetyczna, funkcjonalność (ang. *usability*),
- duże firmy zgłaszają profile ochrony ryglujące rynek,
- mimo, że profil może być określony poprawnie, to jego przeniesienie na poziom aplikacji już takie nie musi być,
- CC zostały zaprojektowane z myślą o wytwarzaniu oprogramowania w modelu kaskadowym, od którego stosowania się odchodzi,
- CC są skupione na aspektach technicznych, a dla bezpieczeństwa większe znaczenie mają procesy biznesowe,
- jakość procesu oceny różni się w zależności od kraju,
- nie ma wystarczającej ochrony marki, np. pojawiają się oznaczenia CC *evaluated* zamiast CC *certified*,
- CC nie mają dobrego umocowania w prawie.

Standardy dla automatyki przemysłowej

Sieci i systemy przemysłowe, które nazywane są także automatyką przemysłową (ang. *Operational Technology*) rozwijały się równolegle, ale odrębnie od systemów informacyjnych (ang. *Information Technology*). Pod koniec ubiegłego wieku, te dwa rodzaje systemów zaczęto ze sobą integrować, co ujawniło problemy bezpieczeństwa związane z OT [4]. Są one szczególnie ważne, gdyż systemy OT stanowią znaczną część infrastruktury krytycznej kraju, a ich rosnące zastosowanie związane z rozwojem Internetu Rzeczy (IoT) oraz przemysłu 4.0 dodatkowo potęguje zagrożenia. Publicznie udostępniona wersja robocza dokumentu „Guide to Operational Technology (OT) Security" [5] opracowywanego przez NIST wymienia wiele różnic między systemami IT, a OT.

Standardy dla automatyki przemysłowej

Należą do nich:

- systemy OT są bardziej uwarunkowane czasowo (ang. *time-critical*),
- dostępność w systemach OT ma większe znaczenie,
- inne są wymagania związane z ryzykiem; w przypadku IT najważniejsza jest poufność i integralność danych, w przypadku OT bezpieczeństwo ludzi, odporność na błędy, zgodność z regulacjami, zapobieganie zagrożeniu życia i zdrowia, utracie wyposażenia lub produktu,
- systemy OT mają bezpośredni wpływ na świat fizyczny,
- systemy OT wymagają innego doświadczenia i umiejętności w obsłudze, niż IT,
- systemy OT mają często ograniczone zasoby i nie posiadają w związku z tym takich mechanizmów zabezpieczających jak systemy IT,

Standardy dla automatyki przemysłowej

- protokoły komunikacyjne używane w OT są nie tylko inne niż te stosowane w IT, ale też mogą być własnościowe,
- instalowanie poprawek jest bardziej skomplikowane; wymaga długiego i starannego testowania oraz zaplanowania przestojów systemu,
- serwis rozwiązań OT jest zapewniany zwykle przez jednego producenta; może to utrudniać instalowanie zabezpieczeń dostarczanych przez strony trzecie,
- typowy czas użytkowania wyposażania OT to 10–15 lat,
- komponenty rozproszonych systemów OT mogą znajdować się w odległych, trudno dostępnych miejscach.

Standardy dla automatyki przemysłowej

Podstawowym standardem bezpieczeństwa dla systemów OT są norma (a w zasadzie ich seria) IEC 62443 oraz „CIS Critical Security Controls for Effective Cyber Defence” [4, 6] . Wspomniana norma definiuje cztery poziomy zabezpieczeń systemu przemysłowego:

- SL1 zapobieganie nieautoryzowanemu ujawnieniu informacji przy pomocy podsłuchu lub na skutek przypadkowej jej ekspozycji,
- SL2 zapobieganie nieautoryzowanemu ujawnieniu informacji przez mało zmotywowanego intruza o ogólnych umiejętnościach,
- SL3 zapobieganie nieautoryzowanemu ujawnieniu informacji przez średnio zmotywowanego intruza o ukierunkowanych umiejętnościach,
- SL4 zapobieganie nieautoryzowanemu ujawnieniu informacji przez wysoce zmotywowanego intruza dysponującego zaawansowanymi umiejętnościami.

Standardy medyczne

Znaczenie cyberbezpieczeństwa w medycynie rośnie wraz z pojawianiem się takich koncepcji jak medycyna zdalna. Współcześnie stosowane urządzenia medyczne zawierają komponenty oprogramowania i sieciowe, które mogą być obiektem ataku informatycznego. Standardem dla cyberbezpieczeństwa w medycynie jest np. norma IEC 80001-1 [7]. Unia Europejska opracowała z kolei regulacje dotyczące urządzeń medycznych — 745/2017 (MDR) – i urządzeń stosowanych w diagnostyce *in vitro* — 746/2017 (IVDR). Zostały one przedstawione w dokumencie „MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices” [8]. Obejmują one nie tylko fazę opracowywania urządzenia, czyli czas przez wprowadzeniem go na rynek, ale również wymuszają na producentach sprzętu i innych stronach zainteresowanych podejmowanie działań związanych z zapewnieniem bezpieczeństwa funkcjonowania tych urządzeń, po ich dostarczeniu. Równocześnie autorzy regulacji wskazują, że poszczególne przypadki użycia sprzętu mogą nieść różne wymagania odnośnie zabezpieczeń.

Standardy medyczne

Norma ISO/IEC 62366-2 jest próbą regulacji zasad bezpieczeństwa w kwestii, która jest ignorowana zazwyczaj przez inne standardy związane ze sprzętem medycznym. Chodzi o interakcję człowieka ze sprzętem, lub o funkcjonalność sprzętu (ang. *usability*). Problem ten został też dostrzeżony przez grupę badaczy zaangażowanych w projekt CHI+MED [9]. Według Rossa Andersona brak spójności w interfejsie użytkownika pomp infuzyjnych powoduje taką samą liczbę zgonów w Wielkiej Brytanii i Stanach Zjednoczonych jak wypadki samochodowe. Rozbieżności w obsłudze mogą dotyczyć nawet tego samego modelu urządzenia produkowanego przez tego samego producenta. Co więcej, nawet próby uspójnienia lub zapobieżenia przypadkowym pomyłkom prowadziły do jeszcze większych problemów. Jeden z producentów oznaczał litry dużą literą L, aby nie była ona mylona z cyfrą 1, ale mililitry oznaczał już jako *ml*. Poprawnie sytuacji nie sprzyja fakt, że certyfikacja takich urządzeń zazwyczaj polega na ocenie ich dokumentacji projektowej (!) i trwa bardzo krótko.

Podsumowanie

W ramach wykładu dokonano przeglądu wybranych standardów związanych z cyberbezpieczeństwem, poczynając od tych najbardziej ogólnych, po przez te związane z dziedzinami automatyki przemysłowej i medycyny. Przyszły wykład będzie dotyczył standardów obowiązujących w dziedzinie aplikacji finansowych.

Literatura I

Krzysztof Liderman. "Ochrona informacji sterującej w sieciach i systemach przemysłowych — propozycja podstaw edukacyjnych". W: *Przegląd teleinformatyczny* 1-4 (2020), 3-30. DOI: 10.5604/01.3001.0015.0604.

Advancing Software Secrity in the EU. URL: https://www.enisa.europa.eu/topics/standards (term. wiz. 15. 06. 2023).

Piotr Dzwonkowski. *Wymogi norm* ISO *seria 27000*. 2013. URL: https://mf-arch2.mf.gov.pl/c/document_library/get_file?uuid=e3607969-79d0-46c5-8e82-85e27331d5a3&groupId=764034 (term. wiz. 14. 06. 2023).

The Common Criteria Portal. URL: https://www.commoncriteriaportal.org/ (term. wiz. 14. 06. 2023).

Literatura II

- Keith Stouffer i in. *Guide to Operational Technology (OT) Security. Initial Public Draft.* URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (term. wiz. 21.06.2024).
- Tom Phinney. *IEC 62443: Industrial Network and System Security.* URL: https://www.isa.org/getmedia/b75b5611-1fa8-4807-99e5-d8707b7cff18/Phinneydone.pdf (term. wiz. 14.06.2023).
- *IEC 80001-1 International Standard.* URL: https://webstore.iec.ch/preview/info_iec80001-1%7Bed2.0%7Db.pdf (term. wiz. 14.06.2023).
- *MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices.* URL: https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf (term. wiz. 14.06.2023).

Literatura III


Ann Blandford i in. *CHI+MED: Making Medical Devices Safer.* URL: https://www.chi-med.ac.uk/ (term. wiz. 14. 06. 2023).

Pytania

?

Koniec

Dziękuję Państwu za uwagę!