Politechnika Śląska
Wydział Automatyki, Elektroniki i Informatyki

Dariusz Rogowski

METODA OCENY ZABEZPIECZEŃ KOMPONENTÓW SIECI PRZEMYSŁOWEJ NA PRZYKŁADZIE STEROWNIKÓW PRZEMYSŁOWYCH

Rozprawa doktorska
napisana pod kierunkiem
Dra hab. inż. Andrzeja Białasa
Dra inż. Artura Kozłowskiego

Gliwice, 2023

Gliwice, 2023

Streszczenie rozprawy doktorskiej:

Metoda oceny zabezpieczeń komponentów sieci przemysłowej na przykładzie sterowników przemysłowych

Autor: mgr inż. Dariusz Rogowski

Systemy sterowania i automatyki przemysłowej IACS (Industrial Automation and Control Systems) oraz ich komponenty są coraz częściej przedmiotem cyberataków, które przenikają z sieci korporacyjnych do sieci przemysłowych z powodu coraz głębszej integracji z systemami zarządzania przedsiębiorstwem.

Z tego powodu problem skutecznej ochrony urządzeń sterowania, które w wielu przypadkach kontrolują elementy infrastruktury krytycznej, staje się coraz poważniejszy, a przedsiębiorcy chcą uzyskać potwierdzenie i mieć zaufanie, że zastosowane zabezpieczenia zadziałają.

Problem, który został rozwiązany w niniejszej pracy, wynika z braku dostępnych metodyk oceny bezpieczeństwa komponentów przemysłowych, które w rezultacie takie potwierdzenie by dawały.

W doktoracie opracowano metodę oceny bezpieczeństwa informatycznego dla przemysłowych systemów automatyki i sterowania, tym samym realizując cel główny pracy.

Metodę oparto na międzynarodowym standardzie Common Criteria (ISO/IEC 15408) i wspierającej ją metodyce oceny CEM (Common Evaluation Methodology) (ISO/IEC 18045), który przeznaczony jest do oceny bezpieczeństwa teleinformatycznego. Standard jest źródłem technik kreowania uzasadnionego zaufania opartych na kontrolowanych, rygorystycznych procesach konstruowania, dokumentowania i testowania produktu oraz na wnikliwej ocenie zastosowanych zabezpieczeń. Jako jedyny standard wprowadza, tzw. miary zaufania do oceny zabezpieczeń w postaci poziomów uzasadnionego zaufania EAL (Evaluation Assurance Level).

Problemem było to, że standard CC zawiera kryteria oceny bezpieczeństwa dla typowych rozwiązań informatycznych. Jednocześnie jest to jego zaleta, ponieważ zagrożenia dla urządzeń przemysłowych są coraz częściej natury informatycznej i też w tym kontekście powinny być rozpatrywane. Problem został rozwiązany w pracy doktorskiej poprzez wytypowanie źródeł wymagań bezpieczeństwa przemysłowego, które stały się punktem wyjścia dla adaptacji standardu CC. Tymi źródłami stała się rodzina norm IEC 62443, która definiuje wymagania i procesy dla implementacji i utrzymania bezpiecznych systemów IACS i ich komponentów.

W rezultacie, opracowano zmodyfikowane zbiory wymagań i kryteriów dla Common Criteria, uzupełnione o cechy charakterystyczne dla komponentów przemysłowych, które zostały włączone do utworzonej metody oceny. Zbiory te obejmują wymagania na uzasadnione zaufanie do zabezpieczeń, wymagania na funkcjonalność zabezpieczeń oraz działania ewaluatora, który ocenia te wymagania.

Metoda oceny bezpieczeństwa dla IACS, implementująca dostosowane wymagania CC i CEM, została poddana walidacji. Walidacja polegała na weryfikacji opracowanych wymagań oraz bazowała na wynikach pilotażowej oceny bezpieczeństwa progamowalnego sterownika zabezpieczenia odległościowego wykonanej w laboratorium oceny bezpieczeństwa. Podczas oceny pilotażowej wykonano testy urządzenia na zgodność z przemysłowymi wymaganiami bezpieczeństwa. Te same wymagania przemysłowe uwzględniono w zaadaptowanej metodzie oceny. Walidacja metody pozwoliła potwierdzić w praktyce tezę pracy doktorskiej, że: *„Metodyka Common Criteria może być zastosowana do oceny zabezpieczeń komponentów sieci przemysłowych po jej adaptacji do potrzeb i realiów specyficznych dla środowiska operacyjnego tych komponentów.”*

Opracowana metoda oceny bezpieczeństwa dla IACS jest uniwersalnym narzędziem, integrującym światy informatyki i przemysłu, umożliwiającym wspólną ocenę ich zabezpieczeń oraz zwiększanie uzasadnionego zaufania do tej oceny.