Cyberbezpieczeństwo dla przyszłości branży motoryzacyjnej

Pojazdy definiowane programowo otwierają ogromne możliwości, pozwalając klientom końcowym cieszyć się wieloma najnowszymi funkcjami bezpieczeństwa, komfortu i wygody. Dostępne są na rynku poprzez aktualizacje oprogramowania, nawet w miarę starzenia się ich pojazdów. Ochrona tego oprogramowania podczas wdrażania i eksploatacji ma kluczowe znaczenie.

Dobrze zorganizowane zarządzanie cyberbezpieczeństwem musi iść w parze z rozwojem pojazdów definiowanych programowo. Deweloperzy oprogramowania muszą zapewnić zabezpieczenia w każdym obszarze, niezależnie od bezpieczeństwa konkretnej aplikacji.

Krótko mówiąc, deweloperzy muszą zarządzać ryzykiem. Także wyciągać wnioski z innych branż i rozwijać kompleksowe systemy zarządzania cyberbezpieczeństwem, które zapewniają podstawy do radzenia sobie z wszelkimi nadchodzącymi zagrożeniami. Współpracując z naszymi klientami, dostawcami i partnerami za pośrednictwem organizacji branżowych, Aptiv aktywnie pomaga podnosić poprzeczkę.

WYZWANIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

Cyberbezpieczeństwo jest stosunkowo nowym zagadnieniem w branży motoryzacyjnej. Gdy producenci samochodów zaczęli wprowadzać do swoich pojazdów elektronicznie sterowane układy kierownicze i hamulcowe, prawdopodobieństwo zagrożeń wzrosło, jednak łączność otworzyła drzwi do znacznie większego ryzyka.

Bezpośrednie połączenia pojazdów z Internetem wskazywane są jako źródło cyberzagrożeń, jednak zwykle pomijane są połączenia pośrednie, takie jak z telefonem komórkowym podłączonym za pomocą USB lub Bluetooth. Nawet pojazd, który wydaje się nie posiadać żadnej łączności, może być wyposażony w bezprzewodowy system monitorowania ciśnienia w oponach lub pokładowy moduł diagnostyczny, który umożliwia dostęp do informacji o pojeździe.

Łączność bez wystarczająco solidnych zabezpieczeń doprowadziła do szeroko nagłośnionego incydentu w 2015 roku, podczas którego naukowcy byli w stanie zdalnie kontrolować niektóre funkcje pojazdu. Pomimo tego, że dla wielu było to bolesne doświadczenie, incydent ten zmusił branżę motoryzacyjną do głębszego zastanowienia się nad tym, jak może wyglądać systematyczne podejście do cyberbezpieczeństwa pojazdów.

Oczywiście inne branże miały podobne doświadczenia, więc takie praktyki pomogły ukształtować ramy cyberbezpieczeństwa w branży motoryzacyjnej. Chociaż można by pomyśleć o biznesowym IT i jego ciągłej ochronie przed złośliwym oprogramowaniem, to istnieje bliższa analogia: przemysł lotniczy.

Branża ta od dawna wspiera ideę posiadania bardzo wrażliwego kodu działającego obok innego, mniej wrażliwego. W rzeczywistości klasyfikuje oprogramowanie według Design Assurance Level (DAL), systemu klasyfikacji ryzyka, który jest podobny do Automotive Safety Integrity Level (ASIL), stosowanego w branży motoryzacyjnej.

Doświadczenia innych branż w zakresie cyberbezpieczeństwa stanowiły podstawę dla nowych przepisów określających sposób tworzenia kompleksowego systemu zarządzania cyberbezpieczeństwem w branży motoryzacyjnej, takich jak UNECE. Zapotrzebowanie na zabezpieczenia sprzętowe stworzyło korzyści skali w wyspecjalizowanych mikroprocesorach, z których korzysta przemysł motoryzacyjny. Strategie obrony w głąb opracowane dla innych branż dają zaś jasną ścieżkę do zapewnienia bezpieczeństwa na wielu płaszczyznach w całym pojeździe.

BEZPIECZEŃSTWO NA KAŻDEJ PŁASZCZYŹNIE

System zarządzania cyberbezpieczeństwem reprezentuje systematyczne podejście do definiowania procesów i kierowania z dbałością o bezpieczeństwo — począwszy od etapu rozwoju, poprzez utrzymanie oprogramowania w czasie, co pozwala organizacji zastosować to podejście na każdym poziomie systemu motoryzacyjnego. Oto niektóre kluczowe obszary związane z tym tematem.

Bezpieczne aktualizacje

Aby zapewnić konsumentom dostęp do najbardziej wydajnych funkcji, dzisiejsze pojazdy pobierają aktualizacje oprogramowania bezprzewodowo z chmury, dlatego aktualizacje te muszą być bezpieczne.

Większość ludzi zna ikonę kłódki w swoich przeglądarkach internetowych wskazującą, że nawiązano szyfrowane połączenie z serwerem, który został uwierzytelniony. Weryfikacja kryptograficzna kodu pobieranego do pojazdu odbywa się na podobnych zasadach.

Infrastruktura klucza publicznego (PKI) to mechanizm umożliwiający producentom cyfrowe podpisywanie oprogramowania w taki sposób, aby system odbiorczy mógł zweryfikować jego autentyczność. Używając tajnego klucza cyfrowego, producent szyfruje oprogramowanie przed jego udostępnieniem. Gdy pojazd pobiera oprogramowanie, używa innego, publicznie dostępnego klucza do weryfikacji zawartości. Złożony algorytm zapewnia, że tylko zawartość

podpisana tajnym kluczem może zostać zweryfikowana za pomocą klucza publicznego.

Bezpieczny rozruch

Nawet z bezpiecznymi mechanizmami aktualizacji, takimi jak PKI, producenci nie powinni zakładać, że całe oprogramowanie w pojeździe jest bezpieczne, ponieważ niektóre z nich mogły dostać się tam w inny sposób. Dlatego producenci muszą również zapewnić bezpieczny rozruch systemu. Po uruchomieniu pojazdu system powinien zweryfikować autentyczność i integralność oprogramowania. Oznacza to, że system musi zapewnić, że kod został stworzony przez producenta, a nie przez podmiot atakujący.

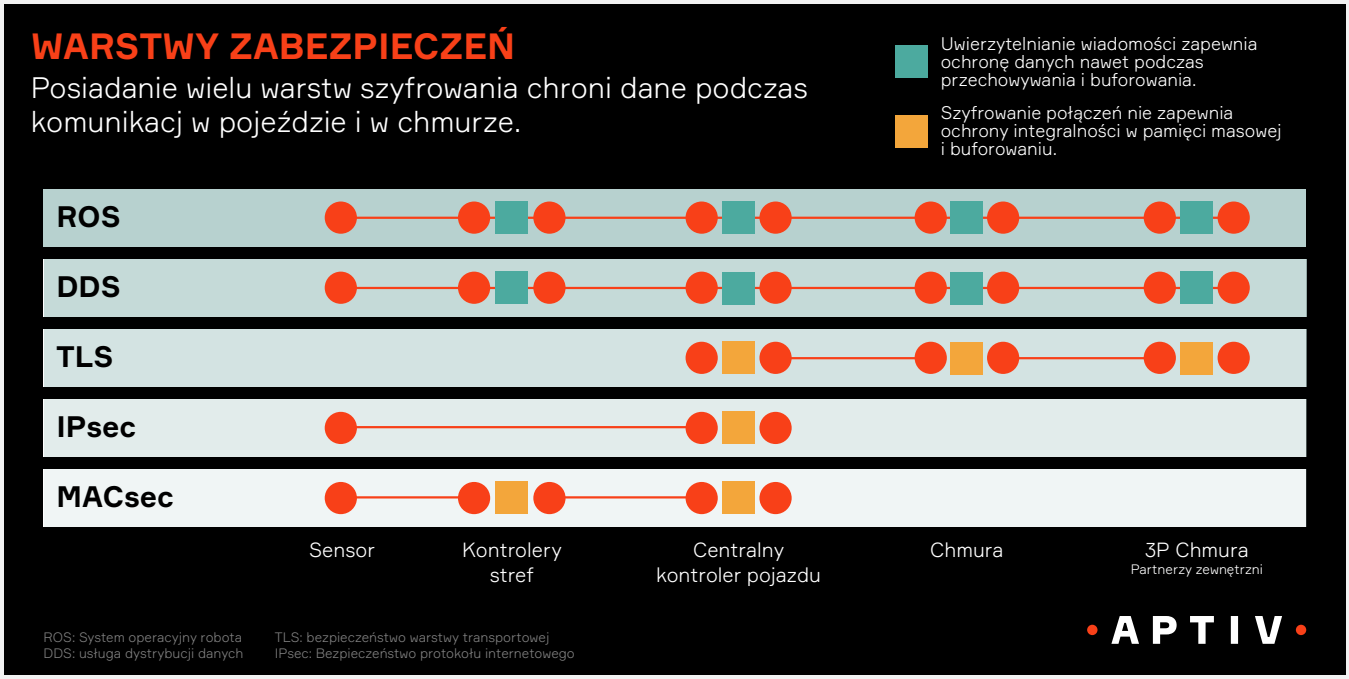
Bezpieczna sieć pojazdów

W miarę jak pojazdy stają się coraz bardziej złożone i zdefiniowane programowo, wiele działających na nich aplikacji będzie wykorzystywać te same procesory i te same sieci do przesyłania danych między różnymi węzłami przetwarzania. Na przykład niektóre aplikacje informacyjno-rozrywkowe mogą wymagać prędkości pojazdu i danych nawigacyjnych, podczas gdy inne aplikacje mogą potrzebować informacji o zarządzaniu akumulatorem.

Posiadanie sieci w pojeździe - i połączenie z siecią w chmurze za pośrednictwem sieci komórkowej i Wi-Fi - wymaga, aby pojazdy zabezpieczały te połączenia na wielu poziomach.

Najniższa warstwa to Media Access Control Security (MACsec), która ustanawia dwukierunkowe szyfrowane połączenie między dwoma bezpośrednio skomunikowanymi ze sobą urządzeniami. MACsec może działać niezwykle szybko, szyfrując i deszyfrując informacje z szybkością łącza przy użyciu specjalistycznego sprzętu.

Kolejną wyższą warstwą jest Internet Protocol Security (IPsec), który działa na warstwie sieciowej w celu uwierzytelniania i szyfrowania pakietów danych między węzłami sieci z adresami IP. Korzystanie z mechanizmu IPsec może pomóc w ochronie danych przepływających przez sieć - przez router, do chmury i tak dalej - a nie tylko na fizycznym łączu między dwoma punktami.



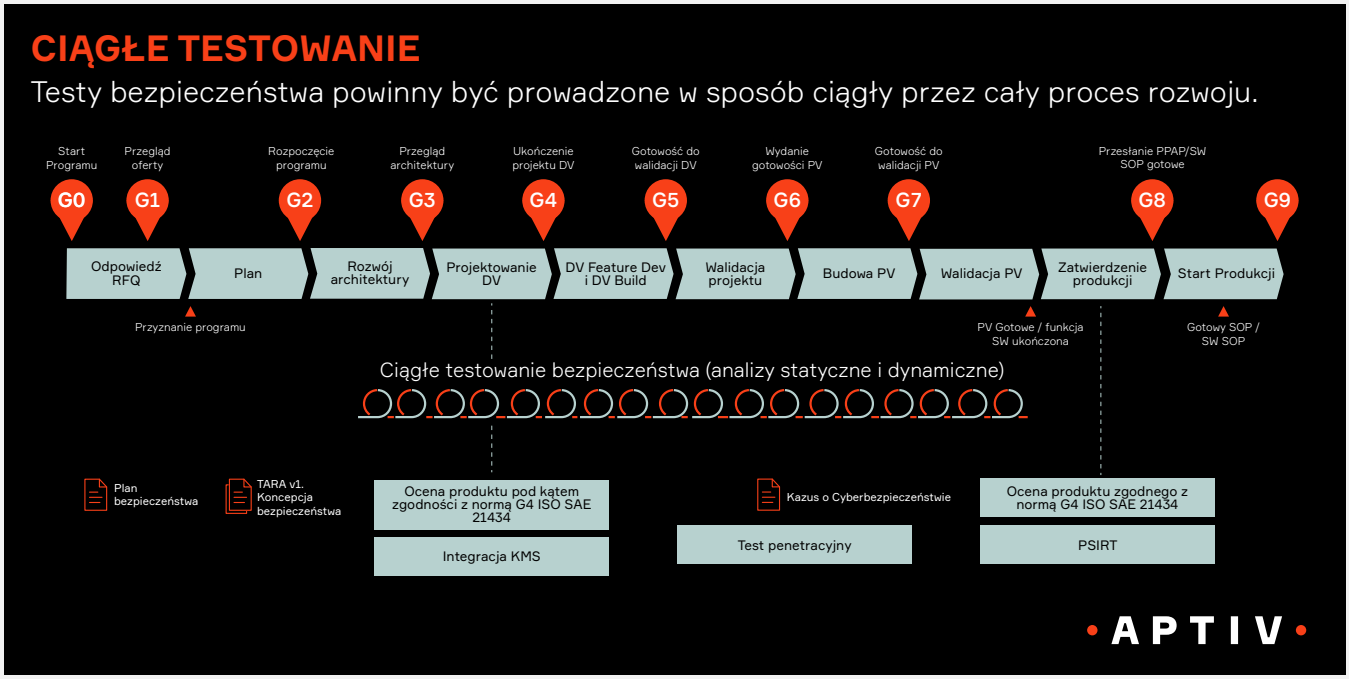
Przechodząc do góry stosu, producenci mogą korzystać z Transport Layer Security (TLS). Protokół ten działa na poziomie sieci, gdzie procesy komunikują się bez powiązania z adresami IP, dzięki czemu mechanizm bezpieczeństwa jest bardziej elastyczny. TLS jest obecnie powszechnie stosowany w komunikacji internetowej, a pojazdy powinny używać go podczas połączeń z chmurą.

Podczas gdy Aptiv wdrożył MACsec, IPsec i TLS w naszych produktach, badamy również ochronę integralności wiadomości. Jest taka jak ta, którą można znaleźć w niektórych implementacjach usługi dystrybucji danych oraz w Secure Robot Operating System 2 (SROS2) - aby faktycznie powiązać ochronę z informacjami. Ochrona ta może obowiązywać nawet wtedy, gdy informacje są buforowane i przechowywane między połączeniami TLS, a nawet w przypadku przekaźników obejmujących wiele połączeń TLS w pojeździe oraz między pojazdem a chmurami i smartfonami.

Zaawansowana łączność

W miarę jak autonomiczna jazda staje się coraz bardziej powszechna, wdrażanie zabezpieczeń na jeszcze wyższych poziomach szyfrowania wiadomości może stawać się coraz ważniejsze. Przykładowo, użytkownik może wysłać wiadomość do pojazdu z prośbą o odebranie go spod określonego adresu. Wiadomość ta powinna być podpisana kryptograficznie i dostarczona w bezpieczny sposób. Nowe protokoły mogą w tym pomóc, nawet z udziałem wielu chmur, jeśli zajdzie taka potrzeba..

Ponadto, ponieważ firmy motoryzacyjne zaczynają zatrudniać więcej programistów do tworzenia różnych funkcji w oprogramowaniu, ważne staje się zapewnienie braku interferencji między aplikacjami. Dzieje się to poprzez wykorzystanie hiperwizorów, kontenerów i innych technologii w celu oddzielenia oprogramowania, nawet na współdzielonym sprzęcie.



USTRUKTURYZOWANE PODEJŚCIE

Wdrożenie wszystkich tych technologii cyberbezpieczeństwa we właściwy sposób wymaga struktury, która może pochodzić z najlepszych praktyk, zautomatyzowanych testów, audytów lub przepisów.

Organizacja Narodów Zjednoczonych ustanowiła przepisy, które zawierają wytyczne dotyczące cyberbezpieczeństwa w branży motoryzacyjnej. Jednym z nich jest UNECE R156, który określa wszystkie wymagania dotyczące bezpiecznej aktualizacji, bezpiecznego rozruchu i innych technologii. Drugim jest UNECE R155, który wzywa do wprowadzenia systemów zarządzania cyberbezpieczeństwem regulujących sposób, w jaki bezpieczeństwo jest projektowane w pojazdach. Zapewnia także ramy dla systematycznego myślenia o ryzyku dla pojazdu, poprzez analizę zagrożeń.

UNECE R155 powołuje się na międzynarodową normę ISO/SAE 21434, która, oprócz wielu innych cennych elementów, pomaga określić wytyczne dotyczące oceny ryzyka w oparciu o możliwość wystąpienia ataku i jego potencjalny wpływ, gdyby doszło do zagrożenia. Norma ta wprowadza również pojęcie poziomu cyberbezpieczeństwa (CAL), który może wskazywać, jak krytycznie system musi być chroniony przed atakami.

Organizacja może skalować swoje działania w zakresie cyberbezpieczeństwa - to znaczy może stosować większy lub mniejszy rygor - w oparciu o CAL.

Firmy motoryzacyjne przygotowują się obecnie do wprowadzenia przepisów UNECE, które mają stać się obowiązkowe w Unii Europejskiej w połowie 2024 r., przeprowadzając audyty swoich procesów inżynieryjnych w celu zapewnienia ich zgodności. Gdy przepisy wejdą w życie, regularne audyty mogą zapewnić stałą zgodność.

Zgodność to oczywiście nie wszystko. Zautomatyzowane testowanie jest również niezbędne do utrzymania wysokiego poziomu odporności na zagrożenia. Aptiv wprowadził już ciągłe testowanie bezpieczeństwa w naszą infrastrukturę ciągłej integracji i wdrażania (CI/CD) i dodaje kolejne formy testowania.

Aptiv wykorzystuje kilka sposobów testowania kodu w trakcie jego rozwoju. Statyczne testy bezpieczeństwa aplikacji (SAST) sprawdzają kod źródłowy pod kątem błędów, a dynamiczne testy bezpieczeństwa aplikacji (DAST) przeprowadzają symulowane ataki. Wykraczając poza SAST i DAST, narzędzia do fuzz testów lub fuzzingu mogą pomóc w testowaniu bezpieczeństwa kodu w miarę jego dojrzewania w trakcie tworzenia oprogramowania, zamiast czekać do końca procesu, gdy brakuje czasu na dotrzymanie terminów. Fuzzing obejmuje bardzo szeroki zakres potencjalnie nieoczekiwanych danych wejściowych. Generuje dane wejściowe automatycznie i w dużych ilościach, szybko dając programistom informacje zwrotne, których potrzebują. Nawet czasem co noc, aby wzmocnić swój kod przed wszystkim, od zniekształconych pakietów po losowe dane.

KOLEJNE KROKI

Wiele zagrożeń w branży motoryzacyjnej nie jest unikalnych dla jednej firmy, ale raczej wspólnych dla całej branży. W miarę ewolucji cyberbezpieczeństwa w branży motoryzacyjnej, producenci i dostawcy będą musieli otwarcie rozmawiać o zagrożeniach i współpracować w celu opracowania najlepszych praktyk w zakresie ich zwalczania. Będą musieli dzielić się informacjami o tym, co dzieje się w krajobrazie zagrożeń i współpracować, aby rozpoznać, kiedy branża motoryzacyjna może być zagrożona. Duża część tej współpracy może odbywać się za pośrednictwem istniejących organów, takich jak Automotive Information Sharing & Analysis Center (Auto-ISAC).

Aptiv jest dumny z tego, że jest członkiem Auto-ISAC. Będziemy nadal ściśle współpracować z naszymi klientami, partnerami i kolegami z branży. W końcu wszyscy dążymy do stworzenia systemów zarządzania cyberbezpieczeństwem, które umożliwią następną generację innowacji w pojazdach definiowanych programowo.

O AUTORZE

Brian Witten
Vice President & Chief Product Security Officer

Dzięki ponad 20-letniemu doświadczeniu w zakresie cyberbezpieczeństwa, od elektroniki użytkowej po wojskowe systemy lotnicze, Brian Witten ponosi globalną odpowiedzialność za cyberbezpieczeństwo produktów w Aptiv. Nadzoruje politykę i procesy cyberbezpieczeństwa, planując i prowadząc rozwój różnorodnych narzędzi i infrastruktury dla firmy. Przed dołączeniem do Aptiv, Brian pełnił funkcje kierownicze w zakresie inżynierii i badań w Defense Advanced Research Projects Agency (DARPA), Symantec, United Technologies Corporation (UTC) i Raytheon Technologies, a także służył w Siłach Powietrznych Stanów Zjednoczonych. Przez lata Brian pomagał budować zabezpieczenia w milionach samochodów i miliardach urządzeń.