Besturingssystemen beveiligen door adequate licentieregistratie

SECURE BOOT HOUDT HACKERS BUITEN HET DIGITALE MACHINEPARK

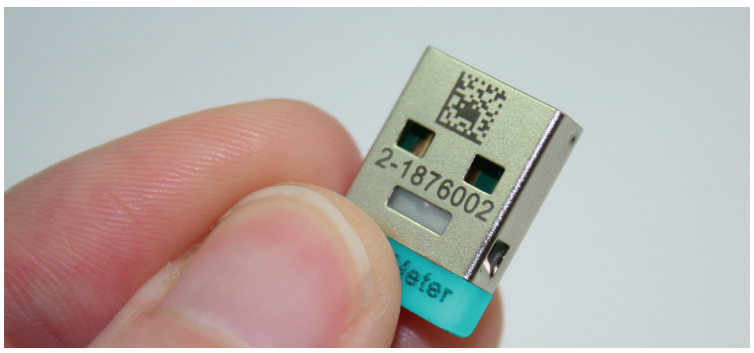
Nadat vele jaren cyber security voornamelijk was gericht op het beveiligen van de poorten van computersystemen, is nu een terugkeer naar de basis waarneembaar. Het gaat weer om het afschermen van de software tegen ongeoorloofd gebruik en ongewenste aanpassingen. Met een adequate licentieregistratie laten industriële besturingssystemen zich effectief beveiligen.

LVD koos voor de beveiliging van de besturingssoftware van de nieuwe generatie lasersnijmachines voor het CodeMeter beveiligingssysteem van Wibu-Systems

Veel moderne besturingssystemen zijn gebaseerd op standaard hardware, zoals industriële PC's, die gebruik maken van standaard operating software als VxWorks, QNX, Windows en Linux Embedded. Ook in de runtime omgevingen wordt vaak een gedeelde standaard toegepast, bijvoorbeeld Codesys. De verspreide, op het internet-protocol gebaseerde netwerken zijn afzonderlijk beveiligd via VPN's en firewalls. Voor de controllers is dat echter niet afdoende. Het is een bekend verschijnsel dat servicemedewerkers de toegangscodes voor de VPN's van hun klanten vastleggen op onvoldoende beveiligde laptops. Krijgt een kwaadwillige via de zwakke plekken in Firewall en VPN's (te korte RSA encryptiesleutels) toegang tot een netwerk, dan ligt de weg open naar alle componenten, waaronder de vitale controllers. Een fysieke scheiding van besturingssystemen en de apparaten of de productiemachines levert geen extra bescherming op. Vanuit hun laptops hebben servicemonteurs toegang tot controllers. De backups van software en data, alsmede de instellingsparameters zijn elders opgeslagen. Ze komen allemaal samen in de processor van de procescontroller (PLC). Dat is de plek waar de beveiliging cruciaal is. De controllers bevatten alleen uitvoerbare (run)code, waarvoor de configuratiegegevens en de parameters zijn vrijgegeven door daartoe gemachtigde functionarissen. De meeste besturingsmodules zijn op locatie op te waarderen met nieuwe functionaliteit, terwijl gelijktijdig tijdens die sessie bugs zijn te fixen. Als een onderhoudsspecialist toegang heeft tot software, kan een hacker er ook bij. Via een Secure Boot is misbruik te voorkomen.

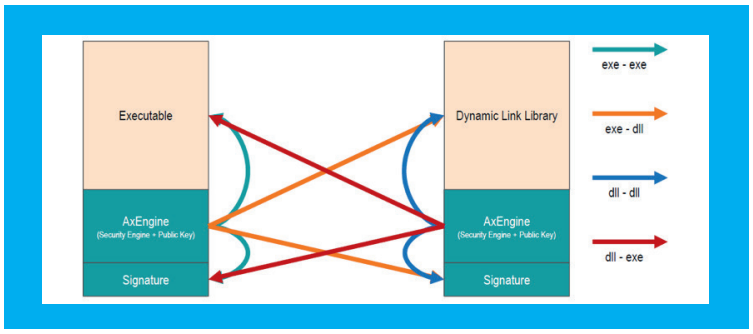
Cryptografische versleuteling

Bij een Secure Boot beveiligde opstartprocedure starten alle systeemonderdelen, inclusief de bootloader, vanuit een cryptografisch beveiligde omgeving die de betrouwbaarheid waarborgt. De afzonderlijke onderdelen van het besturingsysteem zijn voorzien van digitale handtekeningen van de producent en de



De CodeMeter dongle is leverbaar in diverse uitvoeringen met een USB of (micro) SD of CD-card connector. Wibu levert tevens de interface software (API) voor het versleutelen van beveiligde berichten via 128 bits AES, 224 bits ECC of 1024 bits RSA versleutelingsalgoritmen.

www.wibu.com/nl
sales@wibu-systems.nl
(074) 750 14 95



Cross-checks waarbij de eerste executable de tweede test en vice versa hebben zich in de praktijk bewezen

technische manager van het productiebedrijf dat de PLC's toepast. In het controleproces verifieert elke laag in het systeem of de volgende mag worden opgestart. De bootloader controleert het operating system, dat op zijn buurt de runtime omgeving controleert, waarna van daaruit de applicaties inspectie ondergaan (applicatie runtime, applicatie configuratie data). In deze controleketen is het van belang dat de publieke sleutel van de eerste laag geen verandering ondergaat. Daarmee is de beveiliging van de gehele keten verankerd. Een pre-bootloader in de vorm van een 'system-on-a-chip' (SOC) is het meest optimaal. Minder kostbaar is het toepassen van een tweevoudige bootloader, waarvan het deel met het initiële laadprogramma niet is te wijzigen. Aanvullende beveiligingsvoorzieningen zorgen ervoor dat een laag nagaat of de bewerking in de vorige laag correct is verlopen. De controle moet beide kanten op kunnen gaan. Voor de teruggaande controle volstaat een dongle met een usb-connector, (micro) SD-kaart of CF-kaart. Op dit externe, goed afgesloten blokje elektronica, is een zogeheten 'state machine' aangebracht, die met een daarmee corresponderende,versleutelde code de status van het opstartproces registreert. De ontcijfering voor het opstarten van de volgende laag vindt alleen dan plaats, wanneer is vastgesteld dat het voorgaande proces correct is verlopen en de status op de dongle is vastgelegd. De diverse software onderdelen laten zich dus nooit afzonderlijk en in samenhang door hackers simuleren.

Door het opnemen van script met hash-codes tussen de instructieregels, is met zekerheid vast te stellen of bepaalde programma's nog dezelfde kenmerken hebben als toen ze voor het eerst werden geactiveerd. In de industriële wereld is het heel gebruikelijk om door middel van encryptie via hash-codes en handtekeningcertificaten de verschillende lagen te controleren. De meeste moderne besturingssystemen voor embedded applicaties hebben de mogelijkheid om op het niveau van de bootloader de integriteit van het OS te laten checken alvorens deze te activeren.

Applicatie

Het Belgische LVD, producent van machines voor de bewerking van metalen platen, maakt al gebruik van geavanceerde softwarebeveiliging. De markt waarop het bedrijf opereert kent veel concurrenten. Dus is het afschermen van de besturingslogica een must. LVD voorziet de machines van een besturing via Touch-L, een combinatie van touchscreen met besturingssoftware, waarmee zich alle NC-machineprocessen laten instellen en controleren via intuïtief te activeren grafische instructiesymbolen op het schermpaneel. De beveiliging van de embedded software mag de functionaliteit niet beïnvloeden. De machines worden wereldwijd ingezet om met zo min mogelijk operatorhandelingen essentiële productieprocessen uit te voeren.

LVD koos voor een beveiligingsmethodiek van Wibu-Systems met usb-dongles, een stukje elektronica met geheugen waarin de correcte status van de diverse registers in diverse lagen vanaf de bootloader tot en met de applicatie wordt bijgehouden. De effectiviteit van deze beveiligingsvorm wordt versterkt door een voorziening waarmee de licentierechten zich op een centraal punt laten aanmaken, distribueren en beheren. elektro DATA