Blurry Box toont hackers alleen vaag beeld van code

mei 13, 2016 Artikel

Te midden van de aanbieders van beveiligingsoftware bevond zich in Hal 5 van de recente CeBIT technologiebeurs in Hannover een stand van het Karlsruhe Institute for Technology met een presentatie over Blurry Box. Deze baanbrekende beveiligingstechnologie zal in de tweede helft van dit jaar in de productlijn van het eveneens in Kalsruhe gevestigde Wibu-Systems worden ingebouwd. Stefan Bamberg , manager bij de Duitse beveiligingspecialist, doet het geheim uit de doeken.

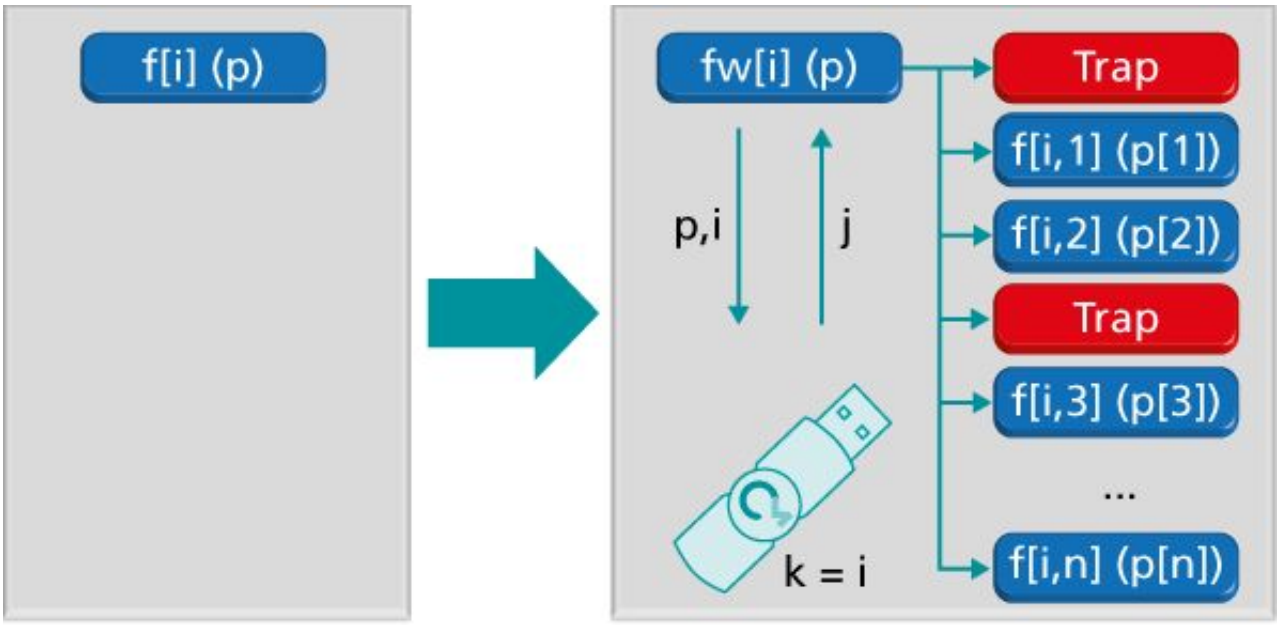
De Blurry Box Technologie is een gezamenlijke ontwikkeling van het Duitse onderzoeksinstituut FZI (Forschungszentrum Informatik), het Karlsruhe Institute for Technology en Wibu-Systems. De technologie is gebaseerd op de Wet van Kerckhoffs, vernoemd naar een 19^{e} eeuwse Nederlandse cryptograaf. Volgens diens theorie zit het geheim in de sleutel en niet in het versleutelingsysteem. Momenteel is in alle gangbare oplossingen de afscherming geheel gericht op de beveiligingmethodiek. De hacker met kennis daarvan kan inbreken. Nadeel van de toepassing van het principe van Kerckhoffs op software was het grote beslag op systeembronnen; applicaties ondervonden vertraging. Bij Blurry Box is dat niet het geval. Degene die de technologie toepast, gaat er vanuit dat potentiële hackers bekend zijn met zijn methode en tevens inzicht hebben in de te beschermen software. Ze kunnen de regels code bekijken in tekstvorm. Maar het is evenwel onmogelijk voor ze om statische code analyse toe te passen, terwijl analyse van dynamische code wordt voorkomen door toevoeging van extra beschermlagen.

Hackers zelden bekend met structuur van software

In de afgelopen 20 jaar is er veel wetenschappelijk onderzoek verricht naar IT-criminaliteit; meestal in samenhang met experimenten op het gebied van software ontwikkeling. Diverse studies laten zien dat de meest gangbare software een dusdanig complexe structuur heeft, dat geen enkel mens meer in staat is de achterliggende code te doorgronden nadat hij of zij het programma heeft opgestart. Van die software past een doorsnee gebruiker maar 10 tot 20% van de functionaliteit toe, terwijl een power user komt aan 30 tot 50%. Interne kwaliteitscontroleurs hebben inzage in 80 tot 90% van de code. Onderzoeken tonen ook aan dat hackers maar zelden het uiteindelijke doel van de software of de interne structuur kennen. Wel beschikken ze over een uitstekende kennis van hackingtechnieken. Verborgen code kunnen ze zonder meer detecteren en waarden in terugkeeropdrachten wijzigen. Hun specialistische kennis stelt ze ook in staat delen van de code te combineren of om code te lezen en eventueel terug te plaatsen in het werkgeheugen van de computer.

Functionele blokken van applicaties

Door een applicatie onder te verdelen in blokken met bepaalde functiegroepen zijn binnen Blurry Box verschillende beveiligingsmethoden te combineren. Een functieblok f[i] heeft de invoerparameter pln[i] en de uitvoer parameter pOut[i]. Afhankelijk van pln[i] zal het functieblok als resultaat pOut[i] opleveren. In het Blurry Box proces zijn de afzonderlijke functieblokken vermenigvuldigd naar verschillende varianten. Zo is functieblok f[i] veranderd in de blokken f[i,1] tot f[i,m]. De functieblokken f[i,j] zijn toegankelijk via een gebundelde functie fw[i], afhankelijk van de toegangsparameter pln [i]. De uitvoer van de variant f[i,j] wordt teruggegeven als waarde pOut[i]. Daardoor zal onder besturing van de geselecteerde parameterbundel gedurende elke cyclus een minimale hoeveelheid code worden uitgevoerd.

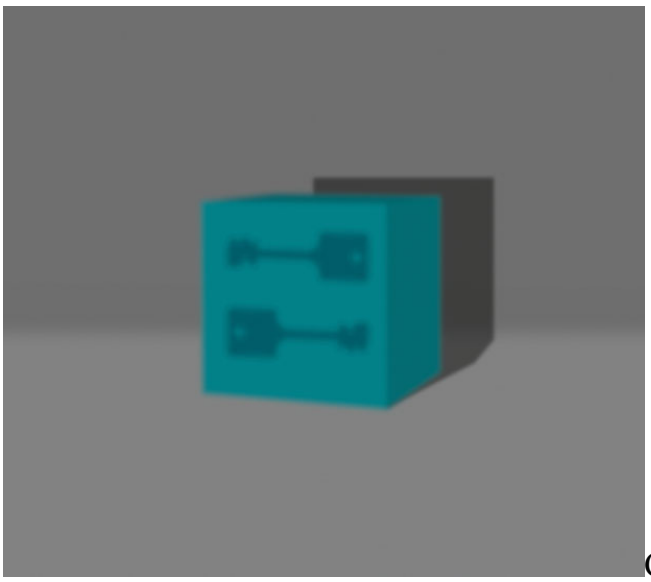


Theoretisch is het mogelijk om de varianten te omzeilen door de bundelfunctie fw[i] te manipuleren, zodat alleen een enkelvoudige variant per keer wordt uitgevoerd. Om die truc uit te sluiten, modificeert Blurry Box Technologie de varianten van een functieblok zodat ze alleen met de correcte reeks parameters kunnen werken. Zonder kennis van de interne structuur is een hacker niet in staat andere, onbekende varianten of de originele functieblokken gemakkelijk te herleiden uit enkelvoudige of zelfs meervoudige varianten. Wijzigingen aan de code, resulteren in varianten die incorrecte uitvoer leveren aan parameters die niet in hun bereik liggen. Een hacker kan zonder de specialistische kennis van de betreffende software een expres ingebouwde fout niet corrigeren. De onbekende variant is om die reden niet te vervangen door een bekende versie.

Elke enkelvoudige variant is volledig versleuteld met een sleutel die veilig is opgeborgen op een dongle met een usb-aansluiting en een eigen geheugen; in feite een in hardware uitgevoerde sleutel. Die is ook voorzien van een API functie (Application Programm Interface) waarmee versleutelde informatie in het geheugen is te laden en te decoderen. Die versie van de code wordt via een API teruggegeven en vervolgens geactiveerd als een uitvoerbare code variant. Zonder een correcte sleutel is geen enkele variant te decoderen. Het encryptie proces werkt volgens de Advanced Encryption Standard (AES). Die onderscheidt willekeurig gekozen waarden in het verwerkingsproces van de computer. Die waarden representeren blokken met dezelfde inhoud in verschillend cijferschrift.

Boobytrap komt na valluik

Via Blurry Box laten zich in softwaresystemen verschillende valluiken inbouwen. Zo wordt voorkomen dat aanvallers alle varianten op de dongle ontsleutelen zonder dat de applicatie correct opstart. Die valluiken bestaan uit versleutelde varianten die de betreffende sleutel als ongeldig verklaren als ze door de dongle worden gedecodeerd. Omdat die ook moeten werken bij hackers die de betreffende broncode trachten te analyseren, bevat deze code links die direct leiden naar ’boobytrapped’ blokken. Bij geoorloofd gebruik van de software worden die nooit geopend. Ze worden immers alleen benaderd door varianten die niet opstarten wanneer de applicatie normaal draait.



Code moving is een proces dat alleen software, geladen op een beveiligde sleutel activeert. Dit proces maakt de applicatie te traag. Zelfs het draaien van een deel van de code op de dongle is geen optie. Het maakt de beveiliging onnodig complex. Een alternatief is het laten draaien op de hardware sleutel van uitsluitend code die de processtappen uit een selectie van de functieblokvarianten uitvoert. Dat neemt niet veel tijd. De selectie en implementatie van de betreffende variantencode kan automatisch verlopen zonder daar de oorspronkelijke software ontwikkelaar bij te betrekken.

Het proces werkt als volgt: de index van de bundelfunctie (i) en de relevante parameter pln[i] worden overgebracht naar de dongle. Daarin vinden de berekeningen op de varianten plaats en het resultaat wordt teruggestuurd (j). Op deze manier is het voor hackers onmogelijk te voorspellen welke varianten (of valluiken) al dan niet zijn gekozen. De volgorde waarin de blokken worden gedecodeerd in operationele omstandigheden is niet willekeurig gekozen. Een blok wordt altijd gevolgd door een specifieke selectie uit de andere blokken. In het geheugen van de dongle onderscheidt Blurry Box een geldige en een niet geldige volgorde. In het laatste geval wordt de operatie afgesloten.

Bestendigheid Blurry Box Technology

Hackers zijn experts in het gebruik van verschillende aanvalsmethoden. Zij hebben echter geen kennis van de interne structuur en werking van de applicatie. Alle vormen van hackers aanvallen zijn door het wetenschappelijke team achter de Blurry Box technologie beproefd. De praktijktesten omvatten ook inbraakpogingen, waarbij de aanvallers op de hoogte waren van de versleutelingmethode. Door vast te houden aan het principe van Kerckhoffs liet de beveiligingsmethode zich onafhankelijk testen en valideren.

Alternatief voor USB-dongle

Wie voor referentiefunctionaliteit geen hardware sleutel in de vorm van een dongle wil gebruiken, bijvoorbeeld wanneer in een project met Internet of Things (IoT) de aangesloten apparaten geen USB poort hebben, kan ook gebruikmaken van een Trusted Platform Module (TPM). Meer en meer systemen en apparaten worden standaard uitgerust met dit stukje extra elektronica met een eigen processor en geheugen waarin de correcte status van de diverse registers in diverse lagen vanaf de ’boat loader’ tot en met de applicatie wordt bijgehouden. In de praktijk blijkt een TPM echter niet altijd voldoende functionaliteit te bieden. Zo kan het ook voor de beveiliging wenselijk zijn om het gebruik van de software alleen toe te staan aan houders van licentierechten. Het is dan zinvol om die rechten op een centraal punt aan te maken, te distribueren en te beheren.

Wibu-Systems levert hiervoor Protection Suite, waarmee een complete set van programmacode zich in zijn geheel laat versleutelen en integreren met een licentieregistratie (CmLicense Central). Gecombineerd met de CodeMeter API is daaraan specifieke functionaliteit toe te voegen. De encryptie gaat tot op het niveau van de ‘executable’ code, waardoor ’reverse engineering’ (herleiden van code naar functiestappen) onmogelijk is. In 2017 komt CmCloud beschikbaar, een variant die zich eveneens goed laat combineren met de Blurry Box encryptie technologie.

Stefan Bamberg is Senior Key Account & Partner Manager Wibu-Systems

Blurry Box, Wibu-Systems

Geef een reactie

Het e-mailadres wordt niet gepubliceerd. Verplichte velden zijn gemarkeerd met *

Reactie

Naam *

E-mail *

Website

Reactie plaatsen