>> Jorge Dávila

La IoT y la seguridad actualizable

Todos los visionarios y apóstoles tecnológicos siguen con tesón anunciando la llegada de un futuro lleno de *gadgets* digitales domóticos, de IoTs de todo tipo y de un sistema productivo llamado Industria 4.0 que va dejar en sus manos toda la producción industrial del planeta. La seguridad de las personas y de sus sociedades sigue sin estar teniéndose en cuenta en esas campañas y convendría prestarle algo de atención. No solo son importantes por sus consecuencias, sino además por la posibilidad real o no de que esos artefactos puedan llegar a considerarse seguros.

Dialogando recientemente con un milenial [1], se me ocurrió utilizar la expresión "*...los placeres del Serrallo*" y el susodicho se quedó atónito y al instante comprendí que él había oído "*se ralló*" [2], expresión milenial para referirse a muchas cosas, y entre ellas, cabrearse, enfadarse, ofuscarse [3]. Tuve que aclararle que un "serrallo" (en turco, Saray) es un palacio o residencia de un regidor turco. En particular se refiere a los palacios de los sultanes otomanos. Desde el siglo XVIII es un término asociado en Europa a exóticas y lujuriosas fantasías relacionadas con la cultura del mencionado imperio. Un magnifico y célebre ejemplo de serrallo es el de Topkapı [4].

Aunque estábamos hablando de los nuevos *gadgets* domésticos que nos trae la IoT, hubo que aclararle al muchacho que también se conoce como "serrallo" al área residencial del palacio en el que viven las mujeres y odaliscas [5] o al propio harén de cualquier gobernante musulmán.

La razón de llegar a tener que aclarar todo esto a mi contertulio, era la de exagerar un modelo para ver hasta dónde nos llevaba. El modelo se refería al nuevo escenario que propone la IoT doméstica o domótica. Le propuse que imaginase cómo debe ser la vida de los poderosos sultanes en su palacio, siempre rodeados de innumerables sirvientes de todo tipo, y cuya única razón de existir es la buena y segura vida de su señor. Le pedí que, en ese escenario, me dijese cuál era la intimidad/privacidad que se podía esperar, y cuáles los riesgos (ventana de exposición) frente ataques de todo tipo (normalmente conocidos en ese caso como magnicidios) que debía sufrir el mencionado poderoso en su jaula de oro.

He conocido algunos usuarios de la domótica que orgullosos me han mostrado cómo es eso de llegar a casa y pedir en voz alta que se encienda la luz y que la luz se encienda como por arte de magia. Alguno me enseñó cómo a su asistente doméstico (digital) le puedes preguntar por el tiempo que hace en Sebastopol (península de Crimea), y la tal Alexa te contesta prolija en los detalles (desconozco cuál podía ser la utilidad de esa información, y en ese momento, para mi amigo).

También pude ver un magnífico "espejo virtual" [6] en el que, como si de la madrastra de Blancanieves se tratase, al ponerte delante de él se iluminaba y te mostraba un abigarrado Cuadro de Control informando sobre el estado de innumerables sensores de temperatura, humedad, estado de algunas cerraduras, etc., así como de las últimas noticias, la fecha del calendario en ese momento, la previsión climatológica y la evolución de algún extraño índice bursátil que no supe reconocer.

Terminada la visita, cuando me iba, fui pensando en cuál podría ser el encanto que encontraban en esas tecnologías sus adeptos, y sólo se me vino a la cabeza la imagen de verles llegar solos y cansados a sus casas y tener alguien que les conteste, que les haga caso y, encima, les obedezca. ¡Placeres del siglo XXI!

Es necesario poder estar seguro de que el dispositivo está ejecutando el software que se supone debe ejecutar, y también de que ese software no puede ser modificado más que por los agentes (fabricantes) autorizados para ello.

[1] Ver https://en.wikipedia.org/wiki/Millennials

[2] Rallar = Causar molestia o enfado a una persona, fastidiar con inoportunidad.

[3] Ofuscar = (ofuscarse) Perder [una persona] de forma pasajera el entendimiento y la capacidad de razonar o de darse cuenta con claridad de las cosas.

[4] Ver https://en.wikipedia.org/wiki/Topkapi_Palace

[5] Odalisca = Mujer esclava en el harén de un sultán y que está al servicio de las otras mujeres del harén

[6] Ver https://en.wikipedia.org/wiki/Virtual_mirror

La "domotización" de nuestras vidas

Desde el punto de vista de la seguridad, esta "domotización" de nuestras vidas y de nuestros entornos de trabajo (que algunos vaticinan que terminaran siendo el mismo) descarta cualquier posible idea de privacidad. Al igual que un Sultán no tiene vida privada en su serrallo, los domotizados están permanentemente expuestos a la vigilancia y escrutinio[7] de sus asistentes domésticos digitales. En el caso del regente del imperio otomano, es él quién tiene el poder para castigar a cualquiera que transgreda la intimidad propia de su harén[8] y para ello lo tenía cuidadosamente custodiado por agentes quirúrgicamente manipulados llamados eunucos.

En el caso del milenial domotizado, además de él, sus agentes domésticos los puede controlar el fabricante, y quien sabe cuántos más que hayan sabido aprovechar los muy abundantes fallos de seguridad que suelen tener esos dispositivos pretendidamente tan avanzados. El sultán no tenía intimidad, pero no la necesitaba porque era él quien podía cortar cabezas. El milenial domotizado tampoco puede esperar ni un ápice de intimidad, pero su poder no va más allá (y no de forma exclusiva) que encender y apagar luces o poner o quitar la música en su solitaria casa.

Los dispositivos IoT y sus parientes mayores, los dispositivos industriales conocidos como OT, en principio, deberían se desarrollados con niveles de seguridad muy superiores a los que se siguen en el desarrollo del software actual. La razón de ello está en (1) la repercusión, a veces critica, que tienen sobre personas, procesos e instalaciones, (2) por el hecho de que tienen que operar de forma autónoma, todo el tiempo (*non stop*) y, (3) en el caso de los sistemas OT, con ciclos de vida activa medidos en décadas. Sin embargo, la realidad comercial no parece ir por esos derroteros y lo que conocemos es tan frágil como el resto del software (en algunos casos lo es más) y esos dispositivos sólo van acompañados de un secretismo beligerante por parte de los fabricantes, lo cual nunca augura nada bueno.

Desde hace tiempo, gran parte de la comunidad hardware se pasó al mundillo de los microcontroladores[9] y las FPGAs[10]. En ambos dispositivos sus funcionalidades son programables y dependen de un programa o conexionado que se puede cambiar en aras a corregir errores o modificar funcionalidades. Esos dispositivos tienen que ser "arrancados" o puestos en marcha, o incluso "actualizados" para cambiar su programa, por lo que los procesos de encendido (*boot*) y de actualización son críticos en general, y por su seguridad en particular.

Para intentar aportar algún tipo de seguridad a los procesos de arranque y de actualización, la comunidad ha desarrollado lo que se conoce como *Trusted Execution Technology* para 1) intentar poder probar la autenticidad de una plataforma hardware y del sistema operativo que corre en ella, 2) para asegurar la autenticidad del sistema operativo que arranca (*boot*) en un entorno en el que se puede confiar, y 3) proporcionar un sistema operativo (*bootloader*) confiable con capacidades de seguridad no disponibles en los sistemas operativos habituales.

Partiendo de un elemento en el que se confía a priori, para comprobar la integridad y autenticidad del siguiente módulo ejecutado, se trata de que los procesos de arranque seguro sean una cadena de ejecuciones de sistemas operativos que parten de un origen común, seguro por definición, y terminan dando un sistema completo de autenticidad e integridad comprobadas/certificadas.

La ejecución adecuada

Los problemas de arranque y de actualización en este tipo de dispositivos son prácticamente los mismos desde el punto de vista de su seguridad. Es necesario poder estar seguro de que el dispositivo está ejecutando el software que se supone debe ejecutar, y es necesario poder estar seguros de que ese software no puede ser modificado más que por los agentes (fabricantes) autorizados para ello.

La aproximación general al problema es partir, a modo de axioma, de un punto o elemento en el que se confía *a priori*, por definición (un TMP o *Trusted Platform Module*[11]), y se intenta que sea éste el que compruebe la integridad y autenticidad del siguiente módulo ejecutado, tanto en lo que al hardware como al software se refiere. Este proceder hace que los procesos de arranque seguro sean una cadena de ejecuciones de sistemas operativos cada vez más complicados y potentes, que parten de un origen común, seguro por definición, y terminan dando (se supone) un sistema completo de autenticidad e integridad comprobadas/certificadas.

Errores muy sonados en el diseño y uso

A pesar de todas esas precauciones, esos puntos iniciales pueden no ser tan seguros y se han cometido errores muy sonados en el diseño y uso de este tipo de tecnologías. Un caso muy conocido es el del procesa-

[7] **Escrutinio** = Del latín *scrūtinium* ("examen"), también origen de escudriñar (var. escrudiñar). Inspección, revisión, examen o investigación cuidadosos con el fin de comprender en detalle o formar un criterio o juicio sobre algo o alguien.

[8] **Harén** (del árabe: حَرِيم harīm, «lugar sagrado e inviolable lugar". Conjunto de miembros femeninos de la familia y lugar donde viven.

[9] Ver https://en.wikipedia.org/wiki/Microcontroller

[10] Ver https://en.wikipedia.org/wiki/Field-programmable_gate_array

[11] Ver https://en.wikipedia.org/wiki/Trusted_Platform_Module

dor Tegra X1 [12] de Nvidia, en el que sus desarrolladores olvidaron limitar la longitud de una variable a los 8 bytes que tenía en el módulo encargado del control de la puerta USB del dispositivo. Con ese "despiste" se podía copiar código arbitrario en cualquier lugar de la memoria del dispositivo, y con ello sobrescribir y anular el comando de verificación de firmas de lo que se instalaba a partir de ese punto en el dispositivo.

Con este fallo impreso en el hardware (memoria ROM) se rompe la cadena de confianza y nada de lo que venga detrás (el software) puede considerarse seguro, auténtico e íntegro. Este incidente abrió la puerta al "*hackeo*" de esos dispositivos y eso causó importantes pérdidas a los que utilizaron este chip para el desarrollo de sus productos ya que, al ser el fallo parte del hardware, no había modo de arreglarlo sin retirar todos los ejemplares del mercado, lo cual es imposible.

Arranque seguro

Algo semejante pasa en el mundo netamente hardware de las FPGAs en las que es el modo de conexionado interno es lo que determina cómo funcionan y, por tanto, de su seguridad. En este caso también es esencial conseguir que sea seguro el arranque, las posibles actualizaciones del dispositivo, y la constante integridad del mismo mientras esté en funcionamiento.

Dentro de algunos procesadores modernos existe un área considerada segura por construcción, en la que tanto el código ejecutable como los datos almacenados en ella están protegidos en cuanto a su confidencialidad e integridad. Esas áreas que corren en paralelo y de forma independiente al sistema operativo principal de la máquina se conocen como *Trusted Execution Environments* (TEE [13]).

Para prevenir la simulación del hardware de seguridad con software desarrollado por los atacantes, en el TEE se abraza el enfoque denominado "*hardware root of trust*". Este paradigma consiste en un conjunto de claves privadas ("*endorsement keys*" o "*provisioned secrets*") que se generan e instalan directamente en el chip cuando es fabricado (escritas en memoria WORM o quemando eFuses), lo cual permite la autenticación del módulo y la protección de la confidencialidad e integridad de las comunicaciones que se tengan con él.

A pesar de ser capaces de montar "zonas seguras" en las obleas de silicio de los procesadores modernos, el problema no está del todo resuelto porque asegurar la pureza del sistema operativo que arranca no asegura la pureza del mismo pasado cierto tiempo. Además, la cadena de confianza se puede romper si se consigue ejecutar algo que no es exactamente lo que se autentica con el TEE.

Un ejemplo europeo de esta preocupación es el **Proyecto ALESSIO** financiado por el **Ministerio Federal de Educación e Investigación** (**BMBF**) alemán, que ha contado con un presupuesto de 3,9 millones de euros, comenzó en el año 2016 y ha finalizado el pasado 31 de diciembre de 2019.

Los participantes en ese proyecto han sido Infineon Technologies, el Instituto Fraunhofer para la Seguridad Integrada y Aplicada (AISEC), Giesecke & Devrient, Siemens, la Universidad Técnica de Munich y la compañía WIBU-SYSTEMS. Los resultados de ese proyecto se han presentado en el Forum VDMA en SPS (*Smart Production Solutions*) para un público netamente germánico.

A pesar de estos esfuerzos locales cuyos resultados todavía están por ver, lo que sí está claro es que todavía queda mucho por hacer en el mundo de los dispositivos digitales IoT y OT seguros, certificados y certificables. Sin embargo dichos dispositivos **están llegando a nuestras realidades sin unos niveles mínimos de seguridad** sobre los que podamos decidir si nuestra privacidad está o no está protegida con todos ellos a nuestro alrededor.

El mundo que se nos viene encima me hace recordar a Algernon, un entrañable ratón de laboratorio de la especie *Mus musculus* [14], que era un personaje especialmente significativo en la película "Charly" [15] de 1968, y que está basada en la magnífica novela corta de ciencia ficción que es *Flowers for Algernon* [16] de Daniel Keyes [17]. Con esa película ganó un Ós-

Algo semejante pasa en el mundo netamente hardware de las FPGAs en las que el modo de conexionado interno es lo que determina cómo funcionan y, por tanto, de su seguridad. En este caso también es esencial conseguir que sea seguro el arranque, las posibles actualizaciones del dispositivo, y la constante integridad del mismo mientras esté en funcionamiento.

car al mejor actor principal Clifford P. Robertson [18] encarnado a un hombre de inteligencia muy limitada al que hacen competir con un ratón de laboratorio especialmente tratado para aumentar su inteligencia.

La vida de los milenials y no milenial domotizados terminará siendo como la de esos ratones de laboratorio en la que todo está dirigido para hacerlos crecer sanos y felices para luego poder hacer experimentos con ellos. El ratón Algernon no sabía que estaba siendo continuamente observado para poder cuantificar su inteligencia aumentada y con ello el éxito o fracaso de un experimento en el cual él era su personaje principal y única víctima. ■

[12] Ver https://en.wikipedia.org/wiki/Tegra#Tegra_X1

[13] Ver https://en.wikipedia.org/wiki/Trusted_execution_environment

[14] Ver https://es.wikipedia.org/wiki/Mus_musculus

[15] Ver https://en.wikipedia.org/wiki/Charly

[16] Ver https://en.wikipedia.org/wiki/Flowers_for_Algernon

[17] Ver https://en.wikipedia.org/wiki/Daniel_Keyes

[18] Ver https://en.wikipedia.org/wiki/Cliff_Robertson

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es