>> Jorge Dávila

Déjame entrar...

El perímetro en redes, empresas, trabajos, parejas, sociedades y naciones cada vez es más débil; si es que todavía podemos encontrar indicios de él (sólo está claro en las concertinas de las fronteras). La Globalización se ha encargado de ello, pero no contaba con que, súbitamente, los procedimientos habituales debían cambiar, debían digitalizarse. Una pandemia vírica que nos ha recordado lo delicados que somos nosotros y todos nuestros constructos, nos ha lanzado a una digitalización forzosa sobre una Internet esencialmente insegura y propiedad de unos pocos, en la que las reglas de juego clásicas no se sostienen. Es tiempo de ver de qué se está hablando en el mundo TIC en tan procelosos días, ya que no sólo son oportunistas las bacterias que acaban con nosotros cuando un virus simplón vuelve loco a nuestro sistema inmunitario. En ello tampoco podían faltar ni las Zero Trust Networks o Zero Trust Network Architectures ni su inevitable relación con la identidad, causantes directos ambos de la aparente jubilación del perímetro y las VPNs.

Después de veinte años de advertencia sobre el riesgo de reducir el hábitat de especies salvajes y junglas, después de la visita de varias epidemias víricas como la del SARS[1, 2], las sociedades occidentales y avanzadas no han querido oír esos vaticinios. Los oídos de todos y todas estaban y están taponados con mucho de antropocentrismo narcisista y una codicia enfermiza en la que sólo cuentan los beneficios económicos y financieros que esa devastación supone.

A finales del siglo pasado el capitalismo mutó pasando de la Guerra Fría –periodo que le fue muy rentable, a la Globalización de todo, de los negocios, del sistema productivo, del turismo, del ocio, de la atención y del divertimento de la población, de la cultura, de la información, etc.–. Hoy, ¿cuántas empresas son dueñas y señoras de la Web 2.0 que controla y monitoriza a más de la mitad de la población mundial en su calidad de clientes/productos? Muy pocas, en realidad Internet también se trata de un inmenso oligopolio mundial.

En quince años, las grandes plataformas de Internet se han infiltrado en todos los aspectos de la vida humana. Se coló y casi ha sustituido la dimensión física y presencial de las relaciones personales (RRSS). Se erigió en la única fuente de información universal (Google) y de conocimientos (Wikipedia). Ha permeado con eficiencia inexplicable las empresas, los bancos, las instituciones financieras y hasta las Administraciones públicas (Sedes Electrónicas y La Nube), y dentro de poco, acabará con los sistemas de enseñanza académica, presencial y humana. No tardará en llegar el día en el que esa Internet actual, que no tiene nada que ver con la que fue en sus orígenes, controle cada uno de los dispositivos físicos que nos dan la vida (IoT) y modulan nuestras libertades gracias a la mal llamada Inteligencia Artificial como artífice tenaz de la vigilancia continua y automática de todo y de todos.

Con esta globalización y virtualización de nuestras vidas ya no nos limitamos a las ofertas del comercio de proximidad, sino que además podemos comprar cualquier cosa y tenerla en cualquier sitio (Amazon). Nuestros viajes y desplazamientos ya tienen como único límite las dimensiones de este planeta. A mediados del siglo pasado lo excepcional era que los de secano, los de tierra adentro, hubiesen visto el mar antes de tener que hacer el servicio militar; ahora los adolescentes sueñan con hacerse ***selfies*** delante del sarcófago de Chernóbil[3].

El tráfico aéreo mundial[4] ha crecido de forma inusitada en las últimas décadas y España no podía ser una excepción[5] dada la importancia que tiene el Turismo en su PIB. En 2018 en el mundo volaron 4.400 millones de pasajeros y ese mismo año, el número de conexiones mediante vuelos directos fue de 22.000 pares de ciudades, más del doble de las que había veinte años antes.

Las ZTAs vienen a jubilar el recurso de un posible perímetro y también la existencia de VPNs. La idea es abandonar la quimera de algo Privado en Internet, y aceptar la esencia Pública de todo lo que en ella ocurre. En los planteamientos ZT se aboga por basarlo todo en la verificación activa de la identidad de los participantes, en la integridad de las transacciones, y en la integridad y salud de los dispositivos utilizados.

En otra dimensión nada moderna, en el bienio 2002-2004 se dio la denominada Crisis del SARS, que fue una epidemia caracterizada por presentar un síndrome respiratorio agudo (SARS-CoV-1). Su origen estuvo en una ciudad de más de siete millones de habitantes conocida como Foshan[6], en la provincia de Guangdong en China.

[1] Ver https://en.wikipedia.org/wiki/Severe_acute_respiratory_syndrome
[2] Ver https://en.wikipedia.org/wiki/2002-2004_SARS_outbreak
[3] Ver https://www.eldiario.es/consumoclaro/viajar/turismo-chernobil-riesgo-radiacion-cancer_1_1370376.html
[4] Ver https://www.iata.org/contentassets/f8d2fbbfe2664612a1e4e65a22422dc3/2019-07-31-01-sp.pdf
[5] Ver https://es.statista.com/estadisticas/540917/movilidad-internacional-del-transporte-aereo-de-viajeros-en-espana/

En ese caso el número de afectados fue pequeño, unas 8.000 personas, pero repartidas **en 29 países**[7]. El resultado de esta epidemia fue la muerte de 774 personas (letalidad del 9,6 %) por todo el mundo[8]. Pasó el tiempo y el SARS se nos olvidó, pero poco más tarde, en diciembre de 2019, el SARS-CoV-2, una nueva versión de ese mismo coronavirus apareció en otra ciudad, esta vez con once millones de habitantes y conocida como Wuhan, en la provincia de Hubei también en China. Este último caso lo tenemos todos aún muy presente, y se le conoce como la **pandemia Covid-19**[10].

En esta nueva versión el virus presenta unas **admirables capacidades infecciosas**. Por lo que sabemos, ese nuevo ejemplar de una amenaza en nada nueva, es inespecífico, **es multisistema** y puede atacar a cualesquiera de los sistemas vitales de nuestro organismo. Además de ser muy infeccioso, **es tremendamente discreto** y en muchos casos no suele dar síntomas de su presencia (pacientes asintomáticos), lo que le permite propagarse en cualquier población "*inmuno-ausente*" a sus anchas, con eficacia y a gran velocidad.

Sin duda alguna, nuestra forma de vida globalizada y el transporte aéreo de pasajeros han ayudado y ayudan a que este coronavirus y cualquier otra enfermedad infecciosa se extienda por todos los rincones del planeta, y habría que preguntarse qué es lo que se está haciendo para evitar que el Turismo, el Ocio y el Transporte Aéreo sean parte de la cadena de circulación de este y otros virus. Una respuesta inmediata y bastante clara es la caída de la actividad aérea, que actualmente ronda el 90%.

La no-presencialidad

Una de las consecuencias directas de una Pandemia es que nos tenemos que quedar quietos y, a poder ser, en casa, si queremos frenar el éxito de este coronavirus hasta que tengamos una vacuna eficaz disponible. Eso significa que muchas de nuestras actividades cotidianas que impliquen contacto personal, trabajar, ir al colegio o a la universidad, comunicarse con los amigos, comprar, etc. deberían pasar a ser no-presenciales, es decir, a través de Internet.

Esta Pandemia ha arrojado a gran parte de la humanidad (la que tiene ordenadores y teléfonos inteligentes) en las manos de un reducido número de empresas y oligarcas. Ahora, deprisa y corriendo tenemos que tele-trabajar, tele-estudiar, tele-enseñar, tele-comprar, etc., y está claro que Internet no está preparada (ni lo ha estado nunca) para respetar derechos humanos de sus usuarios (privacidad), la propiedad industrial (confidencialidad) de las empresas y el trabajo de sus usuarios (normativa laboral digital inexistente).

En los sistemas informáticos empresariales su concepción perimetral se ha desvanecido por completo, los equipos que se conectan a sus cada día más difusas redes no son necesariamente suyos y, desde luego, no están en una sede física controlada y accesible por ellos. Por otra parte, la concepción "*tierraplanista*" de las redes empresariales en las que administradores omnipotentes son capaces de ver y hacer de todo, deberán cambiar y desaparecer por los riesgos que conllevan. Si alguien entra indebidamente en una red donde alguien puede ser omnipotente, está claro que cualquier atacante localmente agazapado aprenderá pronto el modo de serlo sin que nada se lo impida.

La Identidad Digital no pueden ser PKIs, ni eDNIs como tales, la Identidad no puede ser simplemente certificados y firmas digitales de cualquier tipo que actúan del mismo modo que las Téseras del Imperio Romano. La identidad digital habrá que llevarla al dato, al proceso, al tiempo, al entorno, a la relación causal y probatoria si queremos realmente hablar de escenarios seguros de desconfianza mutua.

Identidad digital y ZTAs

Nunca los defensores de las redes virtuales privadas (VPNs) podrían haber imaginado ser tan populares como lo son en estos últimos meses, pero está por ver que esas VPNs actuales sean realmente inviolables por un tercero que ataque desde la misma red. Sin embargo, aunque las VPNs fuesen buenas/seguras, **aún nos queda saber quién está al otro lado de la conexión, tanto desde el punto de vista del servicio como del trabajador humano** dispuesto a desarrollar su jornada. Aquí están empezando a frotarse las manos **los vendedores de Identidad Digital** pero, como en el caso de las VPNs, todavía está por ver que lo que ese sector vende sea realmente bueno y seguro.

En 2004 el escritor sueco **John Ajvide Lindqvist** publicó una conmovedora novela[11] de amores infantiles que tituló "*Låt den rätte komma in*" ("*Let the Right One In*" o "Déjame entrar", como se tituló en castellano). En 2008 el director Tomas Alfredson la llevo al cine con una película[12] muy recomendable que tenía el mismo título. En ella se cuenta la conmovedora historia de amor infantil entre un acosado niño de 12 años, y una secular vampira de su misma edad.

En tan peculiar obra, se utiliza la creencia propia de las culturas vampíricas de que un vampiro no puede entrar en tu casa a menos que tú le des permiso para ello (después atente a las consecuencias). Sin embargo, **lo realmente importante para el protagonista es descubrir quién es su misteriosa vecina**, cuya compañía le hace sentirse bien y seguro. (Lo de que sea una vampira al final resulta muy positivo).

De siempre, **el problema principal de los sistemas TIC es precisamente el de la Identidad**, saber quién es el que está al otro lado o qué es a lo que se está accediendo. Ahora ya no se puede simplificar el problema recurriendo a "perímetros" (reales o virtuales) que hablan de "dentro y fuera", ni reposar nuestra angustia sobre intensos sistemas monitorizadores de redes. No vamos a extendernos aquí en qué es la identidad, aun siendo un tema extremadamente polimórfico, interesante y muy recomendable, pero si lo resumiremos diciendo que, para lo que nos ocupa, **la Identidad son aquellos mecanismos que nos permiten establecer la responsabilidad de los hechos y resolver las disputas ante los tribunales de justicia**. Esta forma tan concreta de verlo está relacionado con algo que, sin ser moderno, se está poniendo muy de moda en nuestros entornos TIC, el **Zero Trust**.

[6] Ver https://en.wikipedia.org/wiki/Foshan
[7] Ver https://www.who.int/csr/sars/country/table2004_04_21/en/
[8] Ver https://www.businessinsider.com/deadly-sars-virus-history-2003-in-photos-2020-2?IR=T
[9] Ver https://en.wikipedia.org/wiki/Wuhan
[10] Ver https://en.wikipedia.org/wiki/COVID-19_pandemic
[11] Ver https://en.wikipedia.org/wiki/Let_the_Right_One_In_(novel)
[12] Ver https://www.filmaffinity.com/es/film666185.html

Las **Zero Trust Networks** o **Zero Trust Network Architectures** (ZTA) son conceptos utilizados para describir un nuevo paradigma en el diseño e implementación de redes telemáticas, aunque habría que extenderlo más allá de las redes y llevarlo a todas las dimensiones digitales de nuestra realidad. La idea básica es sencilla, por defecto, **no te puedes fiar de los equipos que componen tu red**. En realidad hay que ampliar el objetivo del Zero Trust y llevar esa filosofía de desconfianza mutua perfecta más allá de los equipos, e **incluir a los usuarios, los agentes, los servicios, los datos y los resultados**.

Las ZTAs vienen a jubilar el recurso, aunque fuese somero, de un posible perímetro, y también vendría a jubilar la existencia de VPNs. La idea es **abandonar la quimera de algo Privado en Internet, y aceptar la esencia Pública de todo lo que en ella ocurre**. En los planteamientos ZT se aboga por basarlo todo en la verificación activa de la **identidad de los participantes** (*user authentication*), en la **integridad de las transacciones** (e*Signature*), y en la **integridad y salud de los dispositivos** utilizados (*Trusted Execution Environments*).

La Internet original (que hoy todavía transitamos) se diseñó e implementó con la ingenuidad propia del planteamiento más naíf posible: que todo elemento iba a hacer siempre lo que tenía que hacer y ninguna otra cosa, y lo iba a hacer siempre bien. Era la Arcadia de la confianza mutua perfecta. Dada la simetría que (casi siempre) impera en la naturaleza, también se podría haber optado por el planteamiento completamente contrario, la desconfianza mutua perfecta: nada ni nadie puede confiar en que los demás harán lo que tú estás esperando que hagan. En este punto es donde aparecen los inventos ZT que ahora se ponen de moda.

Que Internet sea naíf, se explica porque seguir el modelo de la desconfianza mutua es mucho más difícil de hacer, y todavía está por ver que sea realmente posible. Por este motivo hay que tomar todas las propuestas ZT con mucho cuidado.

El primer objetivo ha sido revivir el palabreo sobre la **Identidad Digital**[13] que en su forma de claves criptográficas asimétricas privadas (supuestamente secretas) y de Certificados Digitales[14] (PKIs[15]) ya tienen la friolera de 32 años de edad. En ese tiempo han aparecido todo tipo de certificados, de tiempo[16], de código[17], de autenticación, Autorización[18] y Accounting[19], etc.; y todos ellos han dado problemas. En concreto, los fallos en lo que se ha dado en llamar **Trusted Execution Environments** (**TEE**)[20] están detrás de los fracasos más sonados en el intento de **asegurar la integridad y autenticidad de lo que se ejecuta** en un determinado hardware de propósito general (consolas de juego, teléfonos móviles inteligentes, etc.).

Otro de los problemas es que uno podría verificar correctamente una identidad digital en un determinado momento pero tiene que ser capaz de extender esa verificación a múltiples procesos posteriores creando cadenas causales públicamente verificables. Aunque se ha hablado mucho de un *blockchain* que ha quedado en nada, esto de tener **cadenas de relaciones causales verificables** es algo que todavía está muy lejos de que lo podamos ver.

Quizás un ejemplo sencillo de entender lo difícil que es llevar la identidad/propiedad de los datos/procesos hasta sus últimas instancias lo sean los ataques **Meltdown** y **Spectre**[21] y derivados o similares. Por la forma de organizar la ejecución de programas en los procesadores actuales, el procesador central realmente no sabe quién ostenta la propiedad de lo que están calculando (*owner*), por lo que se han encontrado formas de que unos usuarios/procesos puedan copiar, con cierto éxito, los datos y operaciones que están procesando para otros usuarios/procesos. La razón de ello es sencilla, **las CPUs actuales realmente no son multitarea, y desde luego no son multiusuario**. Por tanto, cualquier "propiedad" relacionada con el titular legítimo de un proceso/dato no llega a la CPU que es donde se está haciendo todo. **La propiedad/identidad digital dentro y debajo de los sistemas Operativos actuales, es imposible**.

Lo peor que puede pasar en nuestro **escenario de digitalización brusca y atropellada** es que los que juegan en el sector de las TIC cierren en falso este trauma recurriendo a tecnologías, planteamientos y modelos con más de tres décadas de incapacidad manifiesta y documentada. La Identidad Digital no pueden ser PKIs, ni eDNIs como tales, la Identidad no puede ser simplemente certificados y firmas digitales de cualquier tipo que actúan del mismo modo que las **Téseras**[22] del Imperio Romano. La identidad digital habrá que llevarla al dato, al proceso, al tiempo, al entorno, a la relación causal y probatoria si queremos realmente hablar de escenarios seguros de desconfianza mutua.

Si las futuras redes, procesos digitales y realidades virtuales tienen que ser un territorio Sin Dios –probablemente será así–, es preferible que lo sepamos y limitemos el riesgo que corremos al utilizarlas, pero en ningún caso dejemos que sacerdotes/apóstoles de ninguna creencia vengan a convencernos de que todo está bien, de que todo se resuelve con su doctrina, y de que con ellos y sus liturgias no te pasará nada.

Si tengo que vivir entre vampiros quiero saber –si eso es realmente es posible– a quién dejo entrar… en mi alma. ■

Las CPUs actuales realmente no son multitarea, y desde luego no son multiusuario. Por tanto, cualquier "propiedad" relacionada con el titular legítimo de un proceso/dato no llega a la CPU, que es donde se está haciendo todo. La propiedad/identidad digital dentro y debajo de los Sistemas Operativos actuales, es imposible.

[13]Ver https://en.wikipedia.org/wiki/Digital_identity
[14]Ver https://en.wikipedia.org/wiki/Public_key_certificate
[15]Ver https://en.wikipedia.org/wiki/Public_key_infrastructure
[16]Ver https://tools.ietf.org/html/rfc3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[17]Ver https://en.wikipedia.org/wiki/Code_signing
[18]Ver https://en.wikipedia.org/wiki/RADIUS
[19]Ver https://en.wikipedia.org/wiki/AAA_(computer_security)
[20]Ver https://en.wikipedia.org/wiki/Trusted_execution_environment
[21]Ver https://meltdownattack.com/
[22]Ver https://es.wikipedia.org/wiki/Tésera

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