ما الجديد في أمن الحوسبة السحابية ؟

بقلم: يانبي شن، فيرن باكسون، راندي كاتس ترجمة:أ. طه زروقي

تـــقـــديـــم[7]

الحوسبة السحابية Cloud Computing :هي تكنولوجيا تعتمد على نقل المعالجة ومســـاحة التخزين الخاصة بالحاسوب إلى ما يسمى السحابة، وهي أجهزة خوادم يتم الوصول إليها عـــن طريق الانترنت .لتتحول البرامج من منتجات إلى خدمات. ويتاح للمستخدمين الوصول إليها عبر الإنترنت دون الحاجة إلى امتلاك المعرفة والخبرة والتحكم بالعتاد.

وأهمّ فوائد الحوسبة السحابية جعْل أعباء صيانة وتطوير البرامج تقنيـــة علـــى عـــاتق الشركات المُزودة مما يقلل العبء على المستخدمين، ويجعلهم يركّزون علـــى اســـتخدام هـــذه الخدمات فقط.

تعتمد الحوسبة السحابية على مراكز البيانات المتطورة والتي تقدم مساحات تخزين كبيرة للمستخدمين، كما توفر بعض البرامج كخدمات للمستخدمين.

مع تطور التقنيات المتاحة من خلال شبكة الويب بظهور الويب 2,0 والويب 3,0 وتسارع تدفّق الإنترنت المتاحة للعموم، عملت الشركات على إتاحة تطبيقاتها عبر الإنترنت باســـتخدام الحوسبة السحابية. هذه التقنية أفادت المستخدمين على نطاق واسع بتوفير النفقات.

تاريخيا، كان تعبير السحابة يستخدم في البداية للإشارة إلى الإنترنت، وقد جاءت فكـــرة البرامج كخدمات في الستينيات من القرن العشرين، إذ عبّر جون مكارثي عن الفكرة بقوله: "قد تنظم الحوسبة لكي تصبح خدمة عامة في يوم من الأيام".

7 - تقديم لموضوع الحوسبة السحابية، من موسوعة ويكيبيديا بتصرف، المترجم

- تقدم بعض الشركات حاليا خدمات حوسبة سحابية مثل خدمة تطبيقات غوغل، وشبكة أمازون، وخدمات أزور لميكروسوفت،

ويستفيد المستخدمون من :

- الدخول إلى ملفاتهم وتطبيقاتهم من خلال هذه السحابة دون الحاجة لتوفر التطبيق في جهاز المستخدم،و بالتالي تقل المخاطر الأمنية وموارد العتاد المطلوبة وغيرها.
- الاستفادة من الخوادم الضخمة جداً في إجراء عمليات معقدة قد تتطلب أجهزة بمواصفات عالية.
- توفير كلفة شراء البرمجيات التي يحتاجها المستخدم الذي يكتفي فقط بحاسوب متصل بخط إنترنت سريع.
- توفير عدد العاملين على صيانة النظام والبرمجيات

لكن هذه التقنية تعاني من عدة عيوب منها:

- مشكلة توافر الإنترنت لاسيماً في الدول النامية، حيث تتطلب الخدمة الاتصال الدائم.
- مشكلة حماية حقوق الملكية الفكرية التي تثير مخاوف المستخدمين، فلا توجد ضمانات بعدم انتهاك هذه الحقوق.
- مشكلة أمن وخصوصية المعلومات فبعض المستخدمين يتخوفون من احتمالية اطلاع الغير علي معلوماتهم الخاصة.

الـــمـــلـــخـــص :

إذا صار الجانب الاقتصادي للحوسبة السحابية ضرورة، فإنّ مسـائل تأمينهـا تفـرض تحديات جديدة. وفي عملنا هذا سنلقي نظرة شاملة على القضايا الأمنيـة للحوسـبة السـحابية محاولين أن نفرّق بين المخاوف المبررة وردود الأفعال الممكنة. وسنتقصى الأبعاد التاريخية في الأوساط الصناعية والأكاديمية والحكومية والقراصنة. إذ نعتقد أن بعض الأوجه جديدة فعـلا،

بينما قد تبدو أوجه أخرى مستجدة، لكننا قد نجد لها أصلا في ما يسمى الحوسبة التقليدية، منذ سنوات.

وبالعودة إلى الماضي، فقد أثارت معظم تلك القضايا الاهتمام، ونعتقد كذلك، أنّ للأمر وجهين حديثين أساسيين في الحوسبة السحابية، هما تعدد الأطراف التي تتعقد اعتباراتها في الثقة، وضرورة قابلية التدقيق[8] المتبادل بين الأطراف.

الكلمات الجوهرية : التصميم، الحماية، الموثوقية.

1-مقدمة:

أظهرت الحوسبة السحابية تطبيقات اقتصادية كثيرة، اتّسع نطاقها، إذ يمكن لعمالقة الحوسبة السحابية بناء مراكز بيانات ضخمة بتكاليف متدنّية، معوّلين في ذلك على خبرتهم العالية في معالجة البيانات وتنظيمها وخزنها.

وهذه التكاليف المتدنّية تزيد من مردود الحوسبة السحابية، وتوفر موارد بخسة حسب الطلب، وتستجيب لطلبات المستخدمين، كل حسب حاجته، بتقاسم مرن للموارد [2،12].

وفي الوقت نفسه، يبرز الأمن عائقا أمام تسارع الاعتماد على الحوسبة السحابية وانتشارها، وهذه الآراء تأتي من جهات مختلفة كالباحثين [12]، وصانعي القرار، والمنظمات الحكومية. ولا تنصح بعض الشركات الحساسة بالحوسبة السحابية- كما هي حاليا-، بسبب مشاكل توافر الخدمة، وسرية البيانات، والمصير المشترك، وغير ذلك.

مصطلح الحوسبة السحابية فضفاض إلى حد الالتباس، كما ينتقد بعضهم [21]. فهو يضم نماذج تجارية عديدة مثل "خدمة البرامج[9]"، وأحيا مفاهيم أدوات الحوسبة حسب الطلب من حقبة نظم تقاسم الوقت[17]. وغموض مصطلح الحوسبة السحابية أعاق النقاش حول مسائل الأمن، وجعل الانتقادات الأمنية تشمل قضايا جارية وأخرى مستجدة.

وهذا السياق يؤطر ورقتنا هذه، إذ نقرّ أنّ الأمن يَطرح قضايا أساسية في توسيع الاعتماد على الحوسبة السحابية. بل إنّ مسألة الحماية من عدمها في الحوسبة السحابية ستبقى لا محالة،

8 Auditability
9 Software as service

لذا سنتجاوز مسألة المصطلحات (الفصل 2) ونتطرق إلى المسائل الجديدة، مقابل ما استجد من تحديات في عصر الإنترنت. وعليه، فسنسلط الضوء على أمن الحوسبة السحابية دون غموض، وخوف من المجهول، بأن نعرض نظرة شاملة للمسألة.

وسنستعرض رأينا باستقصاء ما كتب حديثا عن الحوسبة السحابية، مقروناً بفذلكة تاريخية لنظم تشارك الوقت[10] ومراقيب الأجهزة الظاهرية[11]. فالمناقشات الحديثة لمسألة الأمن مستجدة نسبيا في الحوسبة في العقد الماضي (الفصل 3)، بينما قد تعود كثير من التحديات المعاصرة إلى مسائل تشبهها منذ عقود خلت [4].

ونشير إلى أنّ بعض المسائل في أمن الحوسبة السحابية مستجدة وتحتاج إلى حلول مستحدثة مطوّرة. وسنوفّق بين الآراء القديمة والحديثة مما سيتيح لنا الإطلاع على أبحاثَ جديرة بالاهتمام [5]. ومن جهة أخرى، نقول أنّ وجهين أساسيين حديثين إلى حد ما في الحوسبة السحابية هما تعدد الأطراف التي تتعقد اعتباراتها في الثقة فيما بينها، وضرورة قابلية التدقيق المتبادل بين الأطراف.

2.بعض التعاريف:

لا تعريف واضح متعارف عليه للحوسبة السحابية ، مما يعيق الحديث عن الحوسبة السحابية عموما. فالمصطلح فضفاض يحدده الاستعمال أكثر من الوثائق. مما يجعل المصطلح المعروف أنّ الحوسبة السحابية "تشمل كل ما نعمله فعلا". فنتيه وسط التعاريف المختلفة مما يبعدنا عن المسائل التقنية، لذا سنحاول في هذا الفصل أن نحيط بالتعاريف التي سنعتبرها فيما بعد.

وأحدث مجهود لتحديد تعريف للحوسبة السحابية مقالٌ صدرَ عن جامعة بيركلي عنوانه: "فوق السحاب: رأي جامعة بركلي في الحوسبة السحابية"، تعرضها على أنها " تتضمن البرامج التي تُقدَّم على أنها خدمات عبر الشبكة، والمعدات والنظم البرمجية في مراكز البيانات التي توفر هذه الخدمات" [12]. فالخصائص الأساسية للحوسبة السحابية تشمل التوهم بلامحدودية الموارد، واجتناب الالتزام القبلي والقدرة على دفع التكاليف حسب الحاجة فقط.

10 Time sharing
11 Virtual Machine Monitors

وقد أثار الكتاب الأبيض[12] موجة متابعة لتعريف الحوسبة السحابية، وتقارير حولها، وفيما يخصنا، فأبرزها ما قدّمه المعهد القومي الأمريكي للمعايير والتكنولوجيا[13] NIST إذ يعطي تعريفا أوسع يشمل جُلّ المصطلحات المستخدمة في النقاشات عن الحوسبة السحابية، ويشكّل أساس دليل المعهد عن أمن الحوسبة السحابية[29].

ويبدو أنّ مجهودات أخرى تتقارب نحو نفس التحديد، وأبرزها الجهود الأوربية [29]، فتقرير الوكالة الأوربية لأمن المعلومات والشبكات[14] تُعرّف الحوسبة السحابية بنفس روح تعريف المعهد الأمريكي.

ووفقا لتعريف المعهد الأمريكي، تشمل الخصائص الرئيسية للحوسبة السحابية الخدمة الذاتية حسب الطلب، والوصول الواسع إلى الشبكات، وتجميع الموارد، والمرونة السريعة، والخدمة المقننة المماثلة للأدوات.

والنماذج الخدماتية ثلاثة هي: البرنامج كخدمة، حيث يتحكّم المستخدم في إعداد التطبيق فقط. والمنصة كخدمة، حيث يتحكم المستخدم في البيئة المستضيفة. والبنى التحتية كخدمة، حيث يتحكم المستخدم السحابي في كل شيء عدا مركز البيانات.

علاوة على ذلك، لدينا أربعة تصاميم تطوير أساسية، السحابات العامة متاحة لجمهور عريض أو لتجمع صناعي واسع، وسحابيات اجتماعية تخدم منظمات عديدة، وسحابيات خاصة تخدم منظمة واحدة، أو سحابيات هجينة تمزج كل ما سبق.

وتماشيا مع التطورات، نرى أنّ تعريف المعهد القومي الأمريكي للمعايير التكنولوجية يتيح لنا الإلمام بالقضايا التي تهمنا في سائر مقالنا، لذا سنتحدث عن الحوسبة السحابية بروح تعريف المعهد الأمريكي.

3-تقييم المستجدات

في هذا القسم، سنقيّم ما يبدو جديداً على الحوسبة السحابية، وما لايبدو كذلك، لنتمكّن من التعرف على الجوانب الأكثر تحديا لأمن الحوسبة السحابية.

12 White paper
13 U.S. National Institute of Standards and Technology
14 European Network and Information Security Agency (ENISA)

1.3 ما ليس جديدا؟

مع زيادة استعمال الحوسبة السحابية، توالت الحوادث وتكررت، ووصفت بأنها حوادث أمن سحابي، لكنها في الواقع، تعود إلى مشاكل التطبيقات الشبكية التقليدية وحفظ البيانات. وتشمل قضايا مثل الاحتيال بالخداع[15] [4] والأعطال[16] [24]، وفقدان البيانات[17] [38]، وضعف كلمات المرور[18][31]، ومشاكل شبكات الآليين[19] [20].

ويعدّ الاحتيال على موقع تويتر[20]، مثالا على قضية أمن ويب التقليدية، والتي غدت اليوم من قضايا أمن الحوسبة السحابية[4]. وعلى النقيض من ذلك، نرى أنّ الحادث الأخير لشبكة آليين في شركة أمازون، جدير بالذكر لأنّه يبيّن أول حلّ معروف لموفر كبير للحوسبة السحابية[20]. مما يبرز أنّ الخوادم في الحوسبة السحابية تعمل حاليا مثل الخوادم في مراكز البيانات التقليدية آمنة أو غير آمنة.

في الأوساط الأكاديمية، شرع أمن الحوسبة السحابية في جمع ندوات مخصصة مثل ورشة أمن الحوسبة السحابية لجمعية الحاسبات الأمريكية[21]، ومتابعات لأهم ندوات الأمن مثل مؤتمر جمعية الحاسبات الأمريكية عن الحوسبة وأمن الاتصالات.

ولحد الآن، تندرج معظم المقالات المنشورة عن أمن الحوسبة السحابية، في مسارات بحثية سابقة للبحث في الأمن، مثل أمن الويب [40،13]، والاستعانة بالمصادر الخارجية[22] وتأمينها [14،18]، ومراقيب الأجهزة الظاهرية [41،36]، وهذا المجال يظهر مزيجا من المواضيع والمجالات، بدلا عن مجموعة أوراق متخصصة في أمن السحابيات، مع بعض الاستثناءات مثل [32] التي سنناقشها فيما بعد.

كما اكتشف مجتمع القراصنة فوائد استغلال الحوسبة السحابية التي توسّع احتمالات الاختراق، مع متابعة جديدة للأمن السحابي في مؤتمر المخترقين سنة 2009 في الولايات

15 Phishing
16 Downtime
17 Data loss
18 Password weaknesses
19 Botnets
20 http://twitter.com خدمة الرسائل القصيرة
21 ACM American for Computer Machinery http://www.acm.org
22 Outsourcing

المتحدة الأمريكية. فمثلا كسر كلمات المرور بالقوة الغاشمة، وأدوات استغلال الاستيثاق ببروتوكول SSL على ديبيان Debian تعمل أيضا على الحوسبة السحابية، كما تعمل على شبكة الآليين[28]. الهجمات الجماعية لازالت فعّالة، فإحدى محاولات الاحتيال، تتم بإقناع مستخدمي شبكة أمازون السحابية بتنفيذ صورة خبيثة لجهاز افتراضي، وذلك بتقليد علامة رسمية مثل fedora_core[23] [28]. ولا تزال ثغرات الأجهزة الافتراضية مشكلة [25]، وأيضا، توليد ضعيف للأرقام العشوائية، نتيجة خلاط[24] كافٍ [37].

2.3 ما الجديد؟

تقدّم الحوسبة السحابية للمخترقين[25] إمكانيات معتبرة أكثر من شبكة الآليين، بينما يرى مقال حديث عن القوة الغاشمة[26] [28]، أنّ استعمال الحوسبة السحابية أكثر كلفة من شبكة الآليين. يقول مقال آخر عن القراصنة، أنّ سوق شبكة الآليين تعاني من مشكلة "سوق الليمون"، أي أنّ فقدان الثقة، والعجز عن التحقق من جودة السلع يؤدي إلى تقليل المبادلات[22]. إذا كانت هذه هي المسألة ، فإنّ المخترقين قد يجدون خدمة أوثق في الحوسبة السحابية بأسعار جيدة[27]، ويدّعون أن شبكة الآليين التي تعمل على الحوسبة السحابية أسهل توقيفا من شبكة الآليين العادية.

كما أنّ الحوسبة السحابية تقدّم بيئة لتشارك الموارد أيضا، مما قد ينشئ قنوات جانبية غير متوقعة(تستغل في مراقبة سلبية للبيانات) أو قنوات سرية (تستغل لإرسال نشط للبيانات). ويجدر بالذكر أن المقال [32] يعالج هذه القضية. فالثغرات المكشوفة تُسهّل وضعَ جهاز ظاهري مهاجم، على نفس الجهاز الحقيقي على أنه جهاز ظاهري مستهدف، ثم إنشاء قناة جانبية بين جهازين ظاهريين على نفس الجهاز الحقيقي، والتي تُفعِّل الهجوم المبني على مزامنة النقر على الأزرار في برتوكول ssh المبينة في [36] الذي يعدّ مثالا على البحث المهتم بالحوسبة السحابية.

23. إحدى توزيعات نظام تشغيل لينكس (المترجم)
24. سلسلة من الأرقام تستعمل لتوليد الأرقام العشوائية(المترجم)
25 Black hat.
26 Brut force
27 نلاحظ أنّ الأسعار قد تنخفض، فمثلا نقدّر أن تخفيض استغلال القوة الغاشمة [36] إل دقيقة واحدة، بدلا من 1.3 يوم حاسوبي، يتطلّب 2000 شبكة EC2 عملاقة، ما يكلّف في جانفي 2010، دولارين للاستغلال الواحد.

وتأتي قضية أخرى من المصير المشترك، الذي له نتائج مختلطة. فمن الجانب الإيجابي سيستفيد المستخدمون السحابيون من تركّز الخبرة الأمنية لدى مزودي الحوسبة السحابية، واثقين من أنّ النظام يستخدم أحسن تدابير الأمن. ومن الجانب السلبي، فإنّ خللا واحدا قد يزعج مستخدمين كثيرين.

فقد أصابت مرسلات السخام[28] شبكة EC2، وجعلت مكافح السخام[29] يستبعد قسما من عناوين الشبكة، مسببا إزعاجا للخدمات. ثم صار على من يريد المراسلة من EC2 أن يملأ استمارة، توفّر له عناوين ثابتة موثوقة، مُسجّلة. وبعد تدقيق المراسلة، ترسل شركة أمازون عناوين الشبكة التي تحققت منها لمكافح السخام، كي لا يستبعدها مرة أخرى[8].

وقد وقع حادث مصير مشترك، خلال مداهمة لمكتب التحقيقات الفدرالي FBI لمراكز بيانات تكساس، في أبريل 2009، للاشتباه في مركز بيانات يستغلّ في الجريمة الالكترونية، إذ صادر العملاء الفدراليون المعدات المشتبه بها، مما عطّل بعض النُظم المستضافة في نفس مراكز البيانات، وأغلق أخرى تماما. طلب أحد الزبائن المتضررين أمر تقييد مؤقت[30]، فرُفض طلبه، لأنّ العتاد المعني يشتبه أنه استغل في نشاطات إجرامية دون علم الزبون [6].

3.3المستجدات في تصميم الحوسبة السحابية

بجمعنا لهذه النقاشات، نرى أنّ تصميم الحوسبة السحابية يُضيف عناصر جديدة عديدة. أولا، ليست البيانات والبرامج ما يحتاج للحماية فقط، بل تصميم النشاط أيضا. فتشارك المورد يعني أنّ نشاط مستخدم سحابي، قد يظهر لمستخدم سحابي آخر، يستعمل الموارد نفسها، مما قد يُنشئ قنوات جانبية أو سرية.

فتصميم النشاط، نفسه، ينبغي أن يُحمى. فإنْ نُشِر قد يُسبب. الهندسة العكسية[31] لقاعدة المستخدمين وحجم الإيرادات، وما شابه ذلك.

28 Spammer مرسلات البريد المزعج
29 Antispam
30 Temporary restraining order
31 Reverse-engineering

كما تستحقّ السمعة التجارية الحماية أيضا، فعند تشارك الموارد في عمل حسّاس، يتعذّر تحديد نشاط مؤذٍ أو خبيث. حتى إذا كان ممكنا تحديد الجناة ومعاقبتهم، فالدعاية السيئة قد تخلق الشكّ، وتشوّه سمعة راسخة.

علاوة على ذلك، لابد من وجود سلسلة ثقة أطول، فمثلا تطبيق مستخدم طرفي قد يشغّل تطبيقا لدى مزوّد خدمات البرامج[32]، هذا المزود يشغل نظامه على مزوّد منصات[33] آخر، ومزود المنصات يُشغّل منصاته عند مزوّد بنية تحتية[34].

هذا المثال، حسب علمنا ، مُبالغ فيه حاليا، لا يُمكن أن يحدث لانعدام واجهة تطبيق كافية API. كما أنّ المثال يبيّن أنّ استخدام أي تصميم قد يجعل المعنيين بالامر في علاقة أكثر تعقيدا من علاقة مستخدم ومزوّد. قد يكون بعض المشاركين مخرّبين يتحكمون فيما يبدو سحابية مستخدمين عادية أو سحابية مزوّدين لكنهم يرتكبون جرائم حاسوبية أو هجمات.

ومن الأمثلة، المستخدمون السحابيون الذين يشنون هجمات القوة الغاشمة أو شبكة الآليين أو حملات السخام من السحابة. أو المزودين الذين يتجسسون على بيانات المستخدمين ويبيعون معلوماتهم لمن يدفع أكثر.

علاوة على ذلك، يمكن أن تعمل الشركات المنافسة داخل نفس نظام الحوسبة السحابية أو ينتهون إلى علاقة مزوّد ومستخدم، مما قد يؤدي إلى تضارب مصالح شديد، ويخلق دوافع إضافية لاختراق معلومات المنافس. هذه التعقيدات تشير إلى الحاجة إلى قابلية التدقيق في الحوسبة السحابية، وهي مطلوبة في الرعاية الصحية والخدمات المصرفية، ونظم مماثلة أخرى.والجديد في الحوسبة السحابية هو الحاجة إلى قابلية التدقيق المتبادل، لأنّ النظام يضمّ أصحاب مصالح متضاربة،ومستخدمين ومزوّدين يحتاجون إلى ضمانات من الطرف الآخر محترم للقانون (من ناحية الفواتير).

يمكن أن تساعد قابلية التدقيق المتبادل مساعدة ملموسة، في التعامل مع الحوادث والاسترجاع، نظرا لأنّ المزوّد والمستخدم كلاهما قد يكون مصدر الهجوم أو هدفه. قابلية

32 Software as a service SaaS provider
33 Plateforme as a service PaaS provider
34 Infrastructure as a service IaaS provider

التدقيق المتبادل تُمكّن من "إلقاء المسؤولية" في حالات التحري والمصادرة، وتكون أداة إثبات حيوية للهيئات القانونية في أداء واجباتها.

وأخيراً، يصعب فهم تهديدات الحوسبة السحابية لعدم دقة تعريف للحوسبة السحابية كخدمة متوفرة على الدوام. هذا الرأي، الذي نشأ من تصميم عام بالاعتماد على خدمة السلع بنكهة الأداة المساعدة، يمكن أن يخلق شعورا زائفا بالأمن، مما يؤدي للاستخفاف بتدابير الأمان، مثل نسخ البيانات الاحتياطي المنتظم عبر مزوّدين مختلفين. وهكذا، نرى أنّ السحابة تتعطّل بنفس النسبة كغيرها من النظم، ولكن أثر تعطّلها أشدّ.

4. بعض مما سلف:

سنستقرئ في هذا القسم، ثلاثة نظم حوسبة مبكّرة لها خصائص مماثلة لما نسميه الحوسبة السحابية في يومنا. ذلك أنّ كثيرا من مسائل أمن الحوسبة السحابية المعاصرة تصعب مقاربتها، وتعالج مثلما كانت تعالج مسائل تاريخية. لكن توجد بعض الفرضيات لم تعد فعّالة تماما، ويصعب تقييمنا لأمنها لأنها قضايا عفا عليها الزمن. هذه المقاربات التاريخية تمنحنا منطلقات تعتبر في أبحاث الحوسبة السحابية، وهو ما سنشرحه في القسم 5.

1.4 ملتكس :

أدخل نظام ملتكس[35] مفهوم الأداة الحسابية مبكرا منذ سنة 1965 [17]، بالمعنى نفسه الذي أخذته الحوسبة السحابية بتقديم أدوات حاسوبية. أثّرت الاعتبارات الأمينة في جوانب تصميم ملتكس [31]، وكما أثّرت آليات تأمينه في الأنظمة اللاحقة، وعليه كان أول نظام يحصل على شهادة من قبل الكتاب البرتقالي [39]. كان ابرز جوانب ملتكس مبادئ تصميم أمنه [33] التي تستحقّ التقرير اليوم.

أولا استخدم ملتكس آلية حماية تعتمد على الصلاحيات، وليس على الإقصاء، أي بلوغا لأي شيء يتفقّد الصلاحيات الحالية.

35 .Multics

ثانيا، جسّد ملتكس شكلا من مبادئ كركهوفس[36] ، وهو الحفاظ على تصميم مفتوح لآلياته، مع حماية بمفاتيح سرية فقط.

ثالثا، يعمل النظام دوما بأدنى الامتيازات[37].

وأخيرا، يُقرّ التصميم إقرارا واضحا بأهمية قابلية الاستخدام البشري، لاسيما ما يتّصل بما نريده اليوم، مع انتشار الهجمات الجماعية[38].

يُحدد تصميم الأمن ملتكس، أهمية أن نتجنّب أن يصبح مسؤولو النظام مَخْنَقا للقرارات. كما أن المستخدم سيتجاوز المديرين بالعادة (ما يصطلح عليه حاليا بنوع من الرضا) ويخرقون آليات الحماية [33]. وتذكيرا بما قلناه في القسمين 3.2 فإن الإجابة عن حادث العناوين في شبكة أمازون، ينطوي على فرض قيود على البريد الالكتروني، مما يزيد من تدخّل المسؤول، وهذا الإجراء لا يُمكن أن يُوسّع إذا ما تكاثر من يريدون إرسال بريد الكتروني.

لا يهدف ملتكس للأمن بمعنى مطلق، بل يتيح للمستخدمين بناء نُظم جزئية محمية [33، 42]، وبالمثل، فالحوسبة السحابية تختلف فيها حاجات المستخدمين الأمنية، إذ يتيح تصميم جيد اختيار مستويات الأمان وآلياته. وقد شرع المزودون السحابيون في اتخاذ الخطوات الأولى في هذا الاتجاه بتوفير بعض سحابيات خاصة افتراضية، بموارد مخصصة، وشبكات افتراضية "تضمن" العزل [1]. "مقاربة الأمن" المنتهجة تستحق الدفاع عنها.

في هذا الصدد، كان لمفتاح ملتسيان[39]، أثر قوي في وثيقة الشهادة الصادرة عن إدارة الكتاب البرتقالي لوزارة الدفاع[40] [9، 30]. تضمّن الكتاب البرتقالي معاملة القنوات السرية تشبه ما ورد في [32، 35] عن القناة الجانبية في الحوسبة السحابية. في كلتا الحالتين، تشمل مبادرة تقييم المخاطر إجراء تقدير كمّي لمعدل البِت[41] مصحوبا بتقييم معدل البت الذي يشكل خطرا ملموسا.

36 Kerckhoffs
37 Privileges
38 Social engineering attacks
39 Multicians
40 Department of Defense Orange Book certification document
41 Bit rate

يحدد الكتاب البرتقالي معدل البت بأنه المستوى اللازم لتشغيل حاسوب طرفي [36]، معدّل البت يتطابق مع تخفيض العبء لكاسر كلمات المرور بالقوة الغاشمة[42]. لكن، حتى إن أغفلنا معدل البت، في بعض الإعدادات، فإنّ مجرّد وجود قناة سرية أو جانبية خطرٌ جدا. وكلا النوعين أوسع أنواع تسريب المعلومات ومن أهم شواغل الحوسبة السحابية.

وفي ختام مناقشة ملتكس، نلاحظ أن عددا من آليات أمن ملتكس ، وهي فذلكة تاريخية الآن، تبقى سائدة اليوم، حتى وإن كانت لا تعمل على النظم الحاسوبية الحديثة. هذه الآليات فيها قوائم ضبط الوصول ACL، وكلمات مرور مولّدة آليا وتشفير ضعيف لملف كلمات المرور [33، 39]. وهكذا، قد يوفّر لنا التاريخ أفكارا قيّمة للحوسبة السحابية الحديثة، وبطبيعة الحال علينا أن نواكبها مع مستجدات الحوسبة.

2.4 مراقيب الأجهزة الظاهرية:

ذكرنا سابقا، أنّ العمل على مراقيب الأجهزة الظاهرية (م.ج.ظ) قَيّم، لأن مختلف أنواع المحاكاة، تشكل جانيا أساسيا من الحوسبة السحابية. وهنا نستعرض الآراء المبدئية، لماذا (م.ج.ظ) أكثر أمنا من النظم الحاسوبية العادية [26]، ونحدد لماذا لم تعُدْ هذه الفرضية تصلح للأجهزة الظاهرية الحديثة؟

لهذا الرأي عدّة أوجه:

الأول أنّ المستويات الدنيا للبرمجة المتعددة (أي التنفيذ المتنافس) يؤدي إلى مخاطر فشل الأمن، وفي الحالة القصوى فإنّ لنظام تشغيل وحيد البرمجة مخاطره الأمنية أقل من نظام تشغيل يشغّل برامج متنافسة. وهكذا، نثبت أنّ (م.ج.ظ) مع مستوى منخفض من البرمجة المتعددة، اكثر أمانا من نظام تشغيل مع مستويات أعلى من البرمجة المتعددة.

ثانيا، حتى إن كان مستوى البرمجة المتعددة نفسه، فإنّ (م.ج.ظ) أكثر أمنا لأنها أسهل وأبسط في التنقيح.

ثالثا، عندما يعمل نظام تشغيل زائر على (م.ج.ظ) تعمل على جهاز حقيقي، فإنّ انتهاك الأمن يحدث فقط عندما يتعطّل كل من نظام التشغيل الزائرو (م.ج.ظ) في الوقت نفسه. وهكذا،

42 Brute force password breaker

فـ (م.ج.ظ) تشغّل عدد "ك" من أنظمة التشغيل الزائرة، كل نظام منها يُشـغّل عـدد "ن" مـن البرامج، يتعطّل أقل من نظام تشغيل يُشغّل "ن×ك" برنامجا.

رابعا، تعطُّل كل برنامج مستقلٌ، ومن ثمّ قد تتضاعف احتمالات التعطّل، وهكذا عمومـا، فأي برنامج على (م.ج.ظ) يشغل عدد "ك" من نظم تشغيل زائرة، كل منها يشغّل عدد "ن" مـن البرامج، يتعطّل بتواتر أقلّ من نفس البرنامج إذا اشتغل على نظام نشـغيل مـع "ن×ك" مـن البرامج. فأثر التضاعف يقلّل احتمال التعطّل.

هذا الرأي، يعطي ثلاث فرضيات حاسمة، **الأولى** أنّ (م.ج.ظ) بسيطة. **الثانيـة**، نظـم التشغيل لها مستوى برمجة متعددة أدنى.**الثالثة**، (م.ج.ظ) ونظم التشغيل الزائرة أعطالها مستقلّةُ. لكن الأجهزة الظاهرية الحديثة تقوّض كل الفرضيات الثلاث.

لم تعد (م.ج.ظ) صغيرةً على الإطلاق. فمثلا جهاز XEN له 1500 سطر كـودا(رمـز) برمجيا [11]، وتبقى أصغر من أي نظام تشغيل حديث (مثلا نواة لينكس 2.6.32 [7] فيها 12 مليون سطر) ما يماثل 176250 سطرا لنواة لينكس 1.0 [5]، التي شكّلت بالفعل نظـام تشـغيل متعدد الأغراض غنيا بالمزايا.

بالإضافة إلى ذلك،فنظام تشغيل زائر حاليا، له نفس مستوى البرمجة المتعددة مثل نظـام تشغيل أصلي. فيعامل المستخدمون النظم الزائرة معاملة النظام الأصلي نفسه، مقوّضين فرضية أنّ نظم التشغيل الزائرة لها مستويات أقلّ من البرمجة المتعددة.

علاوة على ذلك، فبعض الأجهزة الظاهرية الحديثة فيها نظم تشغيل زائرة تشـتغل علـى أجهزة ظاهرية، تعمل بدورها على نظام مُضيف! [10]. في هذا السياق، يتّضـح أنّ الأجهـزة الظاهرية غير آمنة مثل النظام نفسه، كما أنّ النظام المضيف يوسّع جدا قاعدة الكود البرمجـي الموثوق به.

وقد أثار باحثون آخرون انشغالات مماثلة [23]، ولذا نحتاج في أمن الحوسبة السحابية إلى التحقق من أنّ فرضيات المحاكاة تنطبق على مستوى الشبكة ومراكز البيانات.

3.4 شركة ناشيونال سي.أس.أس:

وسننهي كلامنا عن الأبعاد التاريخية بالحديث عن شركة ناشيونال سي.أس.أس[43] ، وهي شركة قدّمت خدمات تقاسم الوقت، مثل مزودي الحوسبة السحابية في يومنا هذا. وتصوّر مؤسسوها فكرة تحويل التكاليف المتصاعدة إلى تكاليف متغيّرة. وقد نجحت الشركة لمرونتها المتزايدة في توفير موارد حاسوبية جاهزة للاستخدام [15]، وهي فوائد مماثلة لما توفره الحوسبة السحابية اليوم.

على الرغم من أنّ خبرة شركة واحدة في الماضي لا تتعمم على خبرات العقود الموالية، فإننا نريد أن نبرز حادثين على المصير المشترك، مما يثبت أنها مفيدة للحوسبة السحابية اليومَ.

أدى الحادث الأول إلى نتائج سلبية لشركة ناشيونال سي أس أس، في سنة 1979 سطا مُهاجِم على كلمة سر لمجلّد، فمسّ أمن زبائنها من الشركات [27]. فأعلمت الشركة زبائنها الثمانية آلاف عن المشكلة الأمنية، لكن لم تُفصّل، فأدى ذلك إلى ردود أفعال سلبية.

وعندما استفسر زبون، اتهمت الشركة تقنييها بعدم التستر على الحادث، وفي نهاية المطاف تدخّل مكتب التحقيقات الفدرالية FBI، مما خلق ضدها دعاية سلبية جدًا.

وعلى النقيض من ذلك، أثبت الحادث الثاني نجاحا كبيرا، إذ أضاع تعطلُ جهازٍ بيانات "مخابر بل" أحد زبائن الشركة المهمين.

وخلافا للتدابير المعتادة، لم تُنسخ البيانات احتياطيا، واعتبرت الشركة أن البيانات لن تُسترجع، فأعلمت زبونتها، بالمشكلة بأمانة، وأنها ستبذل كل ما في وسعها لمساعدتها لاسترداد البيانات. وبعد الصدمة الأولى، عملت الشركتان على كتابة البيانات من رزم الأوراق المطبوعة. هذا التجاوب أعجب "مختبرات بل"، وغدت أكبر زبائن الشركة [19].

.وهكذا، فإذا كان في الحوسبة السحابية علاقات معقّدة بين أصحاب المصالح والمصير المشترك، فإنّ هذه الحوادث ملهمة فيما يتعلق بفوائد إدارة المخاطر الأمنية، بمواءمة المصالح التجارية وبناء شراكات بين أصحاب المصلحة.

43 National CSS, Inc

.5. الفرص الجديدة:

جمعنا بين الآراء القديمة والحديثة ووصلنا إلى أنّ معظم قضايا أمن الحوسبة السحابية ليست مستجدة في الواقع، ولكن غالبا ما زالت تحتاج إلى حلول مستحدثة من حيث آليات محددة. تعمل الأبحاث الحديثة بالفعل على دراسة المجالات ذات الصلة، وهنا سنسلط الضوء على ما يهمّنا.

أولاً، ينبغي أن يُقدّم موفرو الحوسبة السحابية اختيارات لتدابير الأمن، مع إعدادات تلقائية جيدة. المستخدمون السحابيون يعلمون كثيرا عن تطبيقاتهم الخاصة، بينما يعلم المزودون السحابيون أكثر لتركّز الخبرة الأمنية في أيديهم. ومن الناحية المثالية، يختار المستخدم السحابي طيفا من مستويات الأمان، وحدود أمن النظام الفرعي. نحن نعتقد أنّ هذه المرونة يمكن أن تُثبت أنها تَحسُّنٌ كبير إن نُفّذت جيدا. ينبغي أن تكون إحدى المقاربات الممكنة، أن تصاغ تدابير الأمن حول الدفاع عن أصحاب المصالح المختلفة من تهديدات بعينها. ويمكن أن نضيف ميزة أخرى قد تدعم خدمة "التوصيل والتشغيل[44]" متوافقة مع معايير معروفة مثل HIPAA[45] وصناعة بطاقات الدفع[46].

ويهتم مجال بحث مهم آخر بتحديد ملاءمة الأجزاء للعزل، والعديد منها ممكن، مثل عزل الأجهزة الحقيقية أو الظاهرية، أو الشبكات، أو السحابيات أو مراكز البيانات. ونحن حتى الآن نفتقر إلى فهم جيد للمفاضلة بين الأمن والأداء[47] لكل من الخيارات السابقة. ولكن ما يرجح أن المزودين السحابيين يمكنهم – بشكل مثمر– أن يوفروا أشكالا من العزل، ضمن طيف من تدابير الأمن.

تشكّل القنوات الجانبية والسرية تهديدا أساسيا آخر، يتداخل مع مسألة مستويات العزلة التي ناقشناها أعلاه.

44 Plug and play
45 Health Insurance Portability and Accountability Act
46 Payment Card Industry
47 Performance

عندما لا يكون حلا، (مثلا، تؤخذ بعض البتات لسرقة كلمة السر)، فإن تحليلا مفيدا يمكن أن يشمل تقييما كميا لمعدلات البت لقناة ما، مقترنا بتقييم لمعدلات البت المطلوبة لإلحاق الضرر. المقاربة المذكورة في [32] و [36] تقدّم أمثلة جيدة.

إحدى المجالات الهامة التي لم تلق اهتماما هو القابلية للتدقيق المتبادل. إمكانات القابلية للتدقيق في الأنظمة الحالية تركز على القابلية للتدقيق من جانب واحد. في الحوسبة السحابية قد يحتاج كل من المستخدمين والمزودين أن يظهروا الثقة المتبادلة، في نمط ثنائي الاتجاه، أو متعدد الأوجه. وكما ناقشنا سلفا، فإنّ تبادل الضمانات له فائدة كبيرة فيما يتعلق بتقاسم المصير، ففي حالات التحري والمصادرة يمكن للمزودين أن يقدّموا الأدلة والقرائن اللازمة للهيئات القانونية، وأن يضمنوا للمستخدمين أنهم قدّموا الأدلة والقرائن الكافية فقط، دون أي شيء آخر. وتشير الأبحاث الحالية إلى أن تنفيذ آلية القابلية للتدقيق المتبادل ليس بالأمر الهين، حتى في خدمات الوب المباشرة [16].

ولايزال في الحوسبة السحابية تحد مفتوح لتنفيذ آلية القابلية للتدقيق المتبادل، دون التأثير في الأداء.ولتعقد الأمور قليلا، ينبغي أن يكون المدقّق للعمل طرفا ثالثا مستقلا، مما سيتطلب إعدادات تختلف عن التدابير الحالية التي يسجّل حسبها المزودون سجلات التدقيق ويحفظونها. وباختصار، تحتاج القابلية للتدقيق المتبادل إلى عمل كبير .على الجانب الايجابي ، وتحقيق ذلك فعليا سيشكل ميزة أمنية هامة.

وبشكل عام، نرى الحاجة إلى البحوث التي تسعى إلى فهم عالم التهديدات. العمل الحالي في الأدبيات، عموما، يركّز على جانب واحد من مسائل أمن الحوسبة السحابية. وكما شرعنا في فهم المسائل بمعزل عن غيرها، فلابد أن نشرع في فهم كيفية تفاعل مختلف المسائل والتهديدات، فعلى سبيل المثال، نحاول أن نفهم في أمن الويب، مسائل الأمن على مستوى عال، باعتبارها نظاما بيئيا تتفاعل فيه الديدان[48] والآليين والحيل[49] والبريد المزعج، والخداع والمحتوى النشط[50] والمتصفحات، وقابلية الاستخدام[51] والعامل البشري. ونرى أنّ الأبحاث المستقبلية بشأن أمن السحابية عليها أن تضع حدودا للموضوع.

48 Worms
49 Scam
50 Active content.
51 Usability

وفي الختام، فإنّ اختراق السحابيات يُقوّيها، فهذه الدراسات تنطوي على مسائل أخلاقية واضحة، لكنها تقدّم نتائج مقنعة أكثر بكثير من مجرد كسر نظري للسحابيات. فمثلا فدراسة تسرب معلومات شبكة EC2 قي [32]، أدّت إلى جهود أمنية واضحة جدا في "خدمات ويب أمازون"، وقدّمت نموذجا لأبحاث أكاديمية مماثلة. وبالمثل، فتحسينات تدابير الأمن في ملتكس القوات الجوية[52] [42] جاء من جهود شريك في البحث عن ثغرات الأمن.

كل من الهجوم والدفاع يقدّمان تصورات لمشاريع تأمين السحابيات الحكومية، حاليا. وعلى المزودين السحابيين أن يتكاتفوا لتمويل الأبحاث الداخلية للكشف عن الاختراقات، قبل أن توضع قيد العمل. وغنيٌّ عن القول، أن على أصحاب المصالح أن يتابعوا تطلعات المخترقين. وأخيرا ننوّه بأن على أصحاب المصالح أن يتشاركوا في تمويل البحوث المختلفة لفائدتها في النهوض بهذا المجال.

6. خواطر ختامية:

ومما سبق، يتبيّن أنّ الأمن سيكون أبرز ميزة لأعمال الحوسبة السحابية. كما يعلمنا التاريخ، مع مراجعة مقاربات قضايا الأمن في الحوسبة التشاركية، أنّ تطوير بنية الأمن مبكرا، يقلل الكلفة إلى حد كبير، مع تطور النظام، وتراكم الوظائف المتباينة.

من ناحية أخرى، بّين لنا تاريخ عروض الانترنت التجارية مرارا، أنّ تقليل زمن التسويق، وخفض الأسعار يمكن أن يؤثر جدا في الزبون، حتى في غياب أسس أمنية سليمة. قد يكون الحال مختلفا إلى حدا ما هذه المرة، ومع ذلك، فاستهداف جل الحوسبة السحابية لعملاء لهم شركات كبيرة (ويخشون من تجارب سابقة) يؤدي إلى اعتبار الأمن من أولى الأولويات.

ونختتم مقالتنا، بالقول بأن ما وجدناه مثيرا للاهتمام، أن شركات مثل ناشيونال سي.أس.أس. بدأت في تقديم خدمات حاسوبية مثل تقاسم الوقت رخيصة للشركات، فأفسحت المجال أمام الحواسيب الشخصية بأسعار معقولة للجمهور. وفي نفس السياق تُقدّم الحوسبة السحابية حاليا حوسبة رخيصة على نطاق واسع للشركات. وإذا ساد هذا النموذج التجاري، فإننا لا نجد أي شيء ، ولا حتى انشغالات الأمن، سيمنع الحوسبة السحابية أن تصير سلعة استهلاكية.

52 Air Force Multics security

وكما استفادت الحواسيب الشخصية والإنترنت من ثورة المعلومات، وجعلت المعلومة متاحة للعموم، مفيدة ومعقولة السعر، فهل ستستفيد الحوسبة السحابية من ثورة الحوسبة لتجعل الحوسبة متاحة للعموم، مفيدة و معقولة ورخيصة. فنتمنّى أن تثرى هذه الآمال، بأن تكون آمنة بدرجة معقولة.

7. المراجع:

[1] Amazon virtual private cloud. http://aws.amazon.com/vpc/.

[2] Amazon web services economics center. http://aws.amazon.com/economics/.

[3] Cloud computing risk assessment. European Network and Information Security Agency. November 20, 2009.

[4] Gone phishing. Twitter Blog. January 03, 2009.

[5] Linux kernel. Wikipedia.

[6] Liquid Motors, Inc. v. Allyn Lynd and United States of America. U.S. District Court for the Northern District of Texas, Dallas Division. April 2009.

[7] Summary of Linux 2.6.32. h-online.com.

[8] Thread 37650: Email changes. Amazon Web Services Discussion Forums.

[9] Trusted Computer System Evaluation Criteria (Orange Book). Department of Defense Standard. DoD 5200.28-STD. December 1985.

[10] VMware Workstation. http: //www.vmware.com/products/workstation/.

[11] Xen hypervisor. http://xen.org/products/xenhyp.html.

[12] Michael Armbrust et al. Above the Clouds: A Berkeley View of Cloud Computing. Technical report EECS-2009-28, UC Berkeley, http://www.eecs.berkeley.edu/Pubs/ TechRpts/2009/EECS-2009-28.html, Feb 2009.

[13] Robert Biddle, P. C. van Oorschot, Andrew S. Patrick, Jennifer Sobey, and Tara Whalen. Browser interfaces and extended validation ssl certificates: an empirical study. In CCSW '09: Proceedings of the ACM workshop on Cloud computing security.

[14] Kevin D. Bowers, Ari Juels, and Alina Oprea. Hail: a high-availability and integrity layer for cloud storage. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security.

[15] P. Ceruzzi. An Interview with Robert E. Weissman. Charles Babbage Institute. May 3, 2002.

[16] Anton Chuvakin and Gunnar Peterson. Logging in the age of web services. IEEE Security and Privacy, 7(3):82–85, 2009.

[17] Fernando J. Corbató and V. A. Vyssotsky. Introduction and overview of the multics system. IEEE Ann. Hist. Comput., 14(2):12–13, 1992.

[18] Chris Erway, Alptekin Küpçü, Charalampos Papamanthou, and Roberto Tamassia. Dynamic provable data possession. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security.

[19] H. Feinleib. A Technical History of National CSS. Computer History Museum. April 2005.

[20] M. C. Ferrer. Zeus in-the-cloud. CA Community Blog. December 9, 2009.

[21] G. Fowler and B. Worthen. The internet industry is on a cloud—whatever that may mean. Wall Street Journal. March 26, 2009.

[22] C. Herley. Economics and the underground economy. Black Hat USA 2009.

[23] P. Karger. Securing virtual machine monitors—what is needed. Keynote address, ASIACSS 2009.

[24] E. Knorr. Gmail follies and Google's enterprise pitch. InfoWorld. September 8, 2009.

[25] K. Kortchinsky. Cloudburst—a VMware guest to host escape story. Black Hat USA 2009.

[26] Stuart E. Madnick and John J. Donovan. Application and analysis of the virtual machine approach to information system security and isolation. In Proceedings of the workshop on virtual computer systems. ACM, 1973.

[27] V. McLellan. Case of the purloined password. New York Times. July 26, 1981. http://www.nytimes.com/1981/07/26/ business/case-of-the-purloined-password. html.

[28] H. Meer, N. Arvanitis, and M. Slaviero. Clobbering the cloud. Black Hat USA 2009.

[29] P. Mell and T. Grance. Effectively and securely using the cloud computing paradigm. National Institute of Standards and Technology. October 7, 2009.

[30] P. Mell and T. Grance. NIST definition of cloud computing. National Institute of Standards and Technology. October 7, 2009.

[31] D. Raywood. The twitter hacking incident last week should be a call to better security awareness and not about cloud storage. SC Magazine. July 20, 2009.

[32] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security.

[33] Jerome H. Saltzer. Protection and the control of information sharing in multics. Commun. ACM, 17(7):388–402, 1974.

[34] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. Hot Cloud 2009. http://www.usenix.org/event/hotcloud09/ tech/full_papers/santos.pdf.

[35] S. Shankland. HP's Hurd dings cloud computing, IBM. CNET News. October 20, 2009.

[36] Dawn Xiaodong Song, David Wagner, and Xuqing Tian. Timing analysis of keystrokes and timing attacks on SSH. In

SSYM'01: Proceedings of the 10th conference on USENIX Security Symposium.

[37] A. Stamos, A. Becherer, and N. Wilcox. Cloud computing security—raining on the trendy new parade. Black Hat USA 2009.

[38] J. Stokes. T-Mobile and Microsoft/Danger data loss is bad for the cloud. Ars technica. October 2009.

[39] T. van Vleck. How the Air Force cracked multics Security. multicians.org. May 21, 1993.

[40] K. Vikram, Abhishek Prateek, and Benjamin Livshits. Ripley: automatically securing web 2.0 applications through replicated execution. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security.

[41] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, and Peng Ning. Managing security of virtual machine images in a cloud environment. In CCSW '09: Proceedings of the ACM workshop on Cloud computing security.

[42] J. Whitmore, A. Bensoussan, P. Green, D. Hunt, A. Robziar, and J. Stern. Design for multics security enhancements. Technical report ESD-TR-74-176, Air Force Systems Command, http://csrc.nist.gov/ publications/history/whit74.pdf, Dec 1973.

المقال الأصلي للدراسة :

What's New About Cloud Computing Security?,

Yanpei Chen, Vern Paxson, Randy H. Katz, CS Division, EECS Dept. UC Berkeley, Technical Report No. UCB/EECS-2010-5 , January 20, 2010

http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

8. مسرد المصطلحات الواردة في المقال:

إنجليزي	عربي	شرح
worm	دودة	أحد أنواع البرامج الخبيثة
Bot	آلي	برنامج يعمل بطريقة آلية على الشبكة
Botnet	شبكة آليين	شبكة من البرامج الآلية، تستعمل في القرصنة
scam	حيل	القرصنة باستخدام الحيل
spam	سخام	بريد إلكتروني مزعج
Cloud computing	الحوسبة السحابية	شبكة حاسوبية تقدم خدمات للزبائن حسب الطلب
Time-to-market	زمن التسويق	زمن الانتقال من المصنع إلى السوق
Fishing	الخداع	القرصنة بخداع المستخدم
Mutual auditability	القابلية للتدقيق المتبادل	قدرة الطرف على التحقق من الطرف الآخر.
multiprogramming	البرمجة المتعددة	برامج تعمل في الوقت نفسه

Concurrent execution	التنفيذ المتنافس	تنفيذ البرامج في وضع متنافس
debugging	التنقيح	تدقيق الأخطاء في البرامج
Virtual machines monitors	مراقيب الأجهزة الظاهرية	برامج تحاكي الآلات الحقيقية
Plug and play	التوصيل والتشغيل	القدرة على تشغيل جهاز ما بمجرد توصيله
Payment Card Industry	صناعة بطاقات الدفع	معيار لصناعة البطاقات المالية للدفع والائتمان
Performance	الأداء	قياس كفاءة النظام