ASK PC MAGAZINE©

A Monthly Electronic Magazine

HACKING NATIONAL SECURITY

Governments & Hardware Trojan

BRITISH COUNCIL

Breached Data Protection Act!

CLOUD COMPUTING

New Challenges

Supported by ASK PC Academy - April 2009 - Issue No. 9

BCS
REGISTERED COURSE PROVIDER

IEEE

ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

BRITISH INSTITUTE FOR LEARNING & DEVELOPMENT
ORGANISATIONAL MEMBER

ASK PC Magazine is a monthly electronic magazine published by ASK PC to enhance the information technology knowledge in Arabic language for Arabic native speakers.

ASK PC is a leading IT training company based in Egypt, UK and USA.

ASK PC Egypt:
38 Mustafa El Nahas St., Floor 5,
Nasr City, Cairo
Egypt

Tel: +20 2 22715443
Cell: +20 12 4473366
Cell: +20 10 7118587

ASK PC UK:
Dalton House, 60 Windsor Avenue,
London SW19 2 RR
United Kingdom

www.ask-pc.com

From the President | كلمة الإفتتاحية

دعوة إلى تطوير البحث العلمي!

القراء الاعزاء،

ارحب بكم جميعا في مستهل هذا العدد الجديد في ثوبه الجديد من اعداد مجلة اكاديمية ASK PC والتي يشرفنا ان نطرحها لكم شهريا ان شاء الله وبشكل دوري لزيادة المعرفة لدى القاريء العربي المهتم بتكنولوجيا المعلومات. من المعروف ان حركة الترجمة قد ساهمت وبشكل كبير في نقل الحضارات والثقافات وايضا التكنولوجيا والبحث العلمي من مكان إلى مكان عبر الازمان. ولعل ما آل اليه حالنا في الوطن العربي يرجع وبشكل كبير إلى اهمال تعلم اللغات التي لها علاقة بالتكنولوجيا كاللغة الإنجليزية وايضا توقف حركة الترجمة من هذه اللغات إلى اللغة العربية مما ادى إلى وجود فقر كبير في المعرفة التراكمية التي هي اساس العلم ووصلنا إلى ما نحن عليه من اضمحلال للفكر والعلم والثقافة! لكن مازلنا نرى الامل في شباب واناس لديهم القدرة على تحصيل وتطوير الكثير من المعارف ونقلها إلى الأخرين في وطننا العربي.
نتمنى ان نساهم ولو بشيء بسيط في تطوير الثقافة التقنية في عالمنا العربي لننتقل إلى مفهوم استخدام وتطوير التكنولوجيا بدلا من استهلاكها!

ندعوكم إلى المشاركة معنا في هذه الدعوة المفتوحة.

Contents | المحتوى

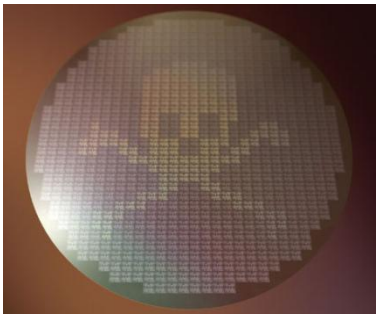
نظرة عامة عن اختراقات الامن القومي:

نشرت العديد من الصحف والمصادر الإخبارية العالمية اختراقات عديدة على صعيد الامن القومي بالولايات المتحدة الامريكية ولعل ابرزها ما نشر في اوائل ابريل 2009 عن اختراق لشبكة تشغيل الكهرباء Electric Grid وادعت الولايات المتحدة ان الهجوم قامت به مجموعة من المخترقين من روسيا والصين ودول اخرى إلا ان تحديد جهة الهجوم بشكل دقيق تعد مسألة ليست هينة وقد تكون مستحيلة في حالة استخدام المخترقون إلى طرق تغيير الهوية مثل Anonymizers Software والـ Proxy وحتى لحظة كتابة هذا المقال صدرت العديد من الاخبار الاخرى من مصادر صحفية وعلمية عن انباء اختراق منظومة لمشروع طائرة حربية بلغت تكلفتة اكثر من 300 بليون دولار! وقد اشارت نفس المصادر إلى وقوع العديد من الإختراقات الاخرى في وزارة الدفاع الامريكية كما اشارت المصادر إلى ان المخترقون قد استطاعوا سرقة كم هائل من المعلومات يحوي خرائط انظمة التحكم والتوجيه الاليكتروني الخاص بهذه المقاتلة حيث يمكنهم فيما بعد استخدامها في عمل نسخة طبق الاصل! واشارت ايضا وزارة الدفاع الامريكية إلى ان مصدر الإختراق كان من الصين إلا انه كما اشرنا ليس من السهل التأكد من مصدر الهجوم. لكن يمكننا الآن القول بان هناك حروب حقيقية تحدث في فضاء الإنترنت Cyber warfare بين العديد من الدول ولعل ابرزها الصين والولايات المتحدة والهند وبعض دول اوروبا هذا في اطار ما يعرف بالحرب الحقيقية التي تؤدي إلى ما يسمى Information Infrastructure Attacks او الهجوم الذي يستهدف البنية التحتية للبيانات. ولعل ابرز الحروب الموجودة فعليا في منطقة الشرق الاوسط هي الحرب الدائرة بين ما يعرف بالمجاهدين على الإنترنت واسرائيل . كما ان الدول النامية لم تسلم ايضا من اختراقات في امن المعلومات كإيقاف للعديد من الخدمات التي تعتمد على الإنترنت كخدمات الحكومة الإليكترونية وايضا استغلال الاجهزة المخترقة في هذه الدول في هجوم آخر على دول اخرى نظرا لغياب الوعي والكفاءات المدربة ولعل ابرزها ما حدث من اختراق للعديد من الاجهزة في مصر من قبل مخترقين من خارج البلاد واستغلالها في حرب ضد استونيا! وفي الفترة الاخيرة ايضا حدث هجوم استهدف البنية التحتية للمعلومات وخاصة DNS – Domain Name System والذي خرجت له تصريحات عديدة من جهات مصرية مسؤلة على انه قطع آخر لكوابل الإنترنت في البحر ولعل الحديث عن المشكلات التي تحدث من اختراقات للمعلومات في المنطقة العربية والحرب الإليكترونية وعلاقتها بالجريمة الإليكترونية يحتاج إلى العديد من المقالات الاخرى التي سوف نطرحها لاحقا ان شاء الله.

كيف يحدث الإختراق؟

ربما يتسائل الكثيرون (كيف يحدث هذا الإختراق في اكثر بلدان العالم تطورا؟)

تعود القصة إلى الستينيات عندما بدأ مصنعي اشباه الموصلات Semiconductors التي تعتبر العصب الرئيسي في صناعة الـ IC او الدوائر المتكاملة إلى البحث عن بدائل لتقليل تكلفة انتاج هذه الرقائق وكان من اهم هذه الحلول هو الحصول على عمالة مدربة ورخيصة حتى لو كانت هذه العمالة خارج الولايات المتحدة وبدأت بالفعل الولايات المتحدة في التعامل مع كل من تايوان وسنغافورة وبعض الدول الاخرى عن طريق امدادهم بعمالة لتدريب العاملين هناك على تصنيع مثل هذه الرقائق واقتصر دور الولايات المتحدة على عملية Testing او الفحص بعد التصنيع. ومع مرور الوقت بدأت الرقائق والـICs تصبح اكثر تعقيدا واصبحت مسألة الفحص من الصعب جدا ان تتضمن فحصا دقيقا لآلاف الترانزيستورز وملايين البوابات المنطقية Logic Gates على الـ IC وما هي وظيفة كل جزء من هذه الدائرة الإليكترونية! فتم الإكتفاء بفحص ما يسمى How Chip will perform specific function? اي كيف ستؤدي هذه الشريحة الأليكترونية وظيفة معينة فلو اخذنا على سبيل المثال دائرة اليكترونية في الهواتف المحمولة فإنه سوف يتم فحص ما إذا كانت تعمل بشكل جيد ام لا من ارسال واستقبال وما إلى ذلك. إلا ان هذا الفحص بالتأكيد غير كافي على الإطلاق لفحص اي عملية مريبة داخل هذه الشريحة الإليكترونية!



نظرية المؤامرة:

ومع تنامي نظرية المؤامرة في كل بلدان العالم Conspiracy Theory بدأت الكثير من الدول تفكر في استغلال التكنولوجيا في هذه النظريات والحروب الخفية. ولعل ابرز هذه الافكار ما نشر من ان شركة اوروبية تختص بتصنيع الـ Chips تستخدم ما يسمى بتقنية Kill Switch لايقاف الاجهزة الإليكترونية عن العمل وقت الحاجة إلى ذلك وهي نفس التقنية التي تستخدم في برمجيات كثيرة مثل Windows Vista لإغلاق النظام عند استخدام نسخة مقرصنة Pirated Copy. إلى ان هاجس استخدام Kill Switch Technique في نظريات المؤامرة والحروب الإليكترونية لم يتم لمس اي دليل مادي حقيقي له حتى هذه اللحظة رغم ان وزارة الدفاع الامريكية تبذل الكثير من الجهد والابحاث لاكتشاف هذه الادلة.

ومن اشهر الاحداث التي القت حولها الكثير من هواجس نظرية المؤامرة هي حادثة قصف الطائرات الاسرائلية هدفا في سوريا سبتمبر 2007 اذعانا منهم بان هذا الهدف هو هدف نووي. واعلن الكثير من الخبراء ان هذا الهجوم الفجائي للطائرات الاسرائيلية على الهدف الذي ربما لم يكن نووي ولكن الامر متعلق بتعطيل اسرائيل لرادار تستخدمه سوريا للتحذير من هذه الهجمات بشكل مبكر وسبب عدم كفاءة الرادار انه تم استخدام رقائقOff-the-Shelf جاهزة في تصنيعه، بها باب خلفي Backdoor تمكنت اسرائيل من برمجته لتعطيل الرادار عن العمل بشكل صحيح وهذا نقلا عن الكثير من المصادر الإخبارية

تصريحات مسؤلي الامن القومي:

واستنادا إلى هذه الاقاويل والافكار بدأ الهاجس يدخل إلى قلب البنتاجون من انهم اصبحوا وبشكل غير مباشر وغير مقصود ايضا لا يستطيعون السيطرة على هذه الرقاقات الإليكترونية Chips ومن يصنعها واين وماذا بها بالتفصيل! ربما الغرض الاساسي من عملها معروف وربما لديهم الخرائط الخاصة بهذه الرقائق التي صنعت في بلدان اخرى وربما هم من امدوا هذه البلدان بهذه الخرائط للتصنيع ولكن من يضمن ان هذه الرقائق لم يتم اضافة عمليات خفية بداخلها او اضافة وظيفة ليست في خريطة بناء هذه الرقاقة؟ ولو سلمت فرضا وزارة الدفاع الامريكيةDoD بانه يمكنهم التدقيق وفحص هذه الرقائق، لكنهم للاسف ايقنوا انهم لا يستطيعون فحص كل جزء او طبقة اليكترونية وكل ترانسيستور او بوابة لان هذا الفحص بالتأكيد في نهايته سوف يؤدي إلى تلف الرقاقة التي تخضع للفحص مما يجعل العملية مستحيلة وغير مجدية!

وليتخيل القاريء عدد اجهزة التحكم الاليكترونية الموجودة في مشروع طائرة مثلF-35 بتكلفة تتعدي الـ 300 بليون دولا وكم يوجد من رقائق اليكترونية في هذه الاجهزة واين صنعت ومالذي وضع فيها؟ ربما تجيب وزارة الدفاع ومشروع البحث المتطور بها DARPA – Advanced Research Project Agency ان لديهم عقود مع ما يسمونهم Defense Contractors وهم موثوقون من وزارة الدفاع لتصميم مثل هذه الدوائر إلا ان وزارة الدفاع نفسها اعترفت بان البعض الآخر من الدوائر الجاهزة Off-the-Shelf قد تستخدم في بعض الاحيان وهذه بالذات من المكونات التي يصعب التكهن بما بداخلها بنسبة100%. وقد اشار البروفيسور Ruby Lee من خبراء الإليكترونيات بالجملة التالية:

”You could check the obvious possibilities, but can you test for every unspecified function“?

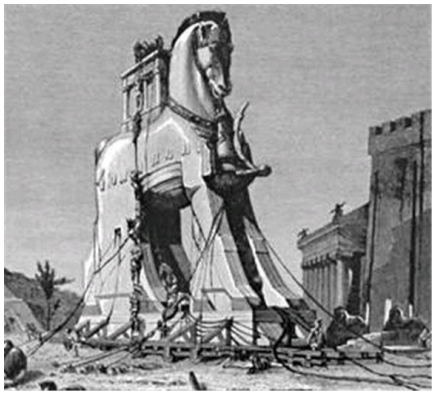
قد تستطيع التحقق من الإمكانيات الواضحة لكن هل يمكنك فحص كل العمليات الغير واضحة؟ بالتأكيد لا وهذا كما اوضحنا في مثال اجهزة الهواتف النقالة.

في السبعينيات كانت وزارة الدفاع الامريكية من اكثر الجهات استهلاكا للدوائر المتكاملة في العالم ICs إلا انها الآن لا تمثل اكثر من 1% من استهلاك العالم ككل في استخدام الدوائر الإليكترونية طبقا لمصادر من وزارة الدفاع نفسها.

وتقول NSA – National Security Agency وكالة الامن القومي بانه ليس بديهيا ان تقوم امريكا بتصنيع دوائر التشفير Encryption على سبيل المثال في الصين! إلا ان هذا لا يمنع استخدامنا لبعض الرقائق المصنعة من قبل بلدان اخرى في اجزاء محدودة من الاجهزة الحربية وهنا تكمن الخطورة التي ايقنتها وزارة الدفاع الامريكية بحدوث الحالات الاخيرة للإختراقات التي حدثت واشرنا اليها.

نظرية احصنة طروادة (السم في العسل):

لعل حصان طروادة من اشهر حيل الخداع في التاريخ وهو معروف ايضا كحيلة للإختراق في علم امن المعلومات إلا انه ببساطة برنامج ضار يضمر عكس ما يظهر للمستخدم فهو قد يظهر في صورة برنامج نافع مثل برامج الكتابة إلا انه يقوم باعمال اخرى في الخفاء مثل نقل البيانات والتجسس وارسال المعلومات إلى المخترق بطرق مختلفة. إلا اننا نتحدث هنا عن جيل جديد من احصنة طروادة يتم زراعتها في اجهزة التحكم المركزية CPU عند صناعتها من قبل مصنعي هذه الرقائق Chips الغير موثوق بهم للتحكم في الاجهزة التي يتم تركيب هذه المعالجات او الرقائق بها لاحقا. وغالبا توجد هذه الانواع من احصنة طروادة Hardware Trojan في المعالجات التي تباع بشكل تجاري في كل مكان وتصنع في بلدان مثل الصين طبقا لتصريحات علمية من داخل وزارة الدفاع الامريكية ومن قبل متخصصين في علم هندسة الإليكترونيات بـ Virginia Polytechnic Institute ويؤكدون ان هذه الاكواد التي تقوم بالتحكم في الـChip تزرع فيها اثناء عملية التصنيع او اثناء عمل خريطة المعالج netlist code وتعمل فيما بعد هذه الاكواد عند توافر شروط معينة Trigger conditions



على سبيل المثال on-chip Thermal communication حيث يتم عمل الإتصال بالـTrojan عندما تصل درجة الحرارة مثلا إلى درجة معينة نتيجة العمليات التي يقوم بها المعالج حيث ترتفع درجة حرارته في بيئة العمل. وهذا من شأنه تقليل احتمال اكتشاف هذا النوع من احصنة طروادة اثناء عملية فحص المعالج! كما اشار العلماء إلى وجود اكثر من اسلوب لزرع مثل هذه الاكواد عن طريق زيادة بوابات معينة Logic gates او Oscillators لاداء نفس المهمة. ويعتبر هذا الموضوع من اكثر الموضوعات جدلا والمتعلق بتأمين الـ Hardware وكيفية ايجاد طرق للحيلولة دون حدوث هذه المشاكل او حتى التحقق من وجود مثل هذه الاكواد ان كانت موجودة.

خطوات وزارة الدفاع نحو الحماية:

بدأت الولايات المتحدة منذ اواخر عهد بوش باطلاق حملة لدعم الامن القومي على الإنترنت تبلغ اكثر من 17 بليون دولار وفي عهد اوباما وفي ظل الازمة الاقتصادية إلا انه اشار بضرورة المضي قدما وضخ المزيد من البليونات! وذهبت ادارة اوباما إلى ما هو ابعد من ذلك حيث طلب الرئيس تعيين فرقة من وزارة الدفاع والجيش الامريكي مهمتها الدفاع عن ممتلكات الولايات المتحدة من الشبكات والاجهزة التقنية ضد الهجمات الإليكترونية. كما اشار البيت الابيض إلى ان هناك مخططات اخرى لفرض سياسات امنية معينة حتى على الاجهزة التي لا تخضع لرقابة وزارة الدفاع مثل اجهزة المؤسسات الخاصة لانها قد تستخدم في الهجوم ايضا. ومن المعلوم ان اوباما حتى قبل توليه منصب الرئيس عندما كان نائبا في البرلمان شدد على ضرورة معاملة فضاء الإنترنت وما يحدث به من هجمات على انه قضية امن قومي!

بات من الواضح من الشواهد السابقة ان هناك فعلا حرب خفية بين مصنعي الرقائق الإليكترونية Chips وبين الاجهزة الحكومية والجهات التي تتعامل معها رغم انه ليس هناك دليل مادي تم اكتشافه على ذلك إلا اننا لا نستطيع ابدا انكار عدم وجود مثل هذا الخطر من وجهة نظرنا. ومما يعتبر دليلا على وجود مثل هذه الإختراقات هو قرار وزارة الدفاع الامريكية وتحديدا DARPA بالتوجه مرة اخرى إلى onshore chips والتي تعبر عن انتاج هذه الرقائق وتحديدا الـ CPU بداخل وزارة الدفاع الامريكية او مع جهات معتمدة من وزارة الدفاع فقط على ان تستخدم هذه الـCPU في الاجهزة التي تعمل في اجزاء هامة وحيوية من البنية التحتية للمعلومات في الدولة والجهات المهمة Critical Infrastructure ايمانا من وزارة الدفاع بانه من الصعب زرع ما يسمى Hardware Trojan او احصنة طروادة داخل الـ CPU اثناء تصنيعها لعمل ما يسمى Kill Switch او حتى باب خلفي للتحكم بالاجهزة backdoor. ويعتبر موضوع زرع Hardware Trojan في جهاز تقني من اكثر الهواجس التي تزداد يوميا خصوصا بعد تمثيلها عمليا فامضت حقيقة لا جدال فيها فهي ليست نظرية المؤامرة وانما هي واقع تعيشه الدول المتقدمة الآن وربما تكون الدول النامية هي الضحية الكبرى! إلا ان الخبراء يذهبون إلى ابعد من ذلك حسب تقرير خبراء الامن في وزارة الدفاع وهو ان يكون الـ CPU كجزء مادي Hardware آمن بدرجة كبيرة جدا إلى آخر طبقة به Mask Layer ولا يعمل إلا من خلال برامج خاصة لضمان عدة نقاط:

- ضمان ان الـ CPU حتى ان تسربت بشكل ما وتم عمل هندسة عكسية لها Reverse Engineering فسوف تصبح عديمة المنفعة بدون معرفة مفاتيح التشفير Encryption Keys المستخدمة داخلها او عدم وجود برامج التشغيل

- فرض قيود صارمة على البرمجيات التي سوف تستخدم في تشغيل هذه الاجهزة الجديدة

انهم مقتنعون بان فرصة وقوع مثل هذه الاجهزة في يد الآخرين محتملة ويدللون على ذلك بطائرة الاستطلاع الخاصة بالبحرية الامريكية التي سقطت في الصين عام 2001 لم يتم اعادتها إلى الولايات المتحدة إلا قطع مفككة بعد 3 اشهر! مما ادى إلى الغاء هذه الطائرة من سلاح البحرية وخسارة ملايين الدولارات. لهذا هم يشددون على ضرورة تأمين الـCPU لاقصى درجة حتى ان تم تفكيكها إلى نانوميترز!

وجهة نظر:

على الرغم من امكانية توافر هذا التامين إلا ان الكثيرون من الخبراء يشككون بامكانية الوصول إلى هذه الدرجة من التأمين للمعالج حيث ان الهندسة العكسية ليست الحل الوحيد لكسر الحماية او معرفة كيف يعمل هذا الجزء اوChip فأيجاد مفتاح التشفير الذي يقوم بالعمليات الرياضية من احد الحلول الاخرى فحصولك على المفتاح يعني وصولك إلى حل اللغز! وهناك العديد من الطرق العلمية المتبعة من قبل الخبراء ومن قبل المخترقون على السواء في الحصول على هذا المفتاحKey مثل Cold boot attack هجوم التبريد عن طريق تبريد الذاكرة للحصول على مفتاح التشفير اوDRAM Attack
وهذا الرابط يوضح بالفيديو كيف تتم هذه العملية ويمكن الإضطلاع على البحث الخاص بهامن هنا

نعتقد من وجهة نظرنا المتواضعة في هذا المجال ان الامر بات صعبا السيطرة عليه وان فرضنا ان الدول الكبرى مثل الولايات المتحدة قد يكون بالفعل لديها الحلول لمثل هذه المشكلات (ونعتقد ذلك) لان لديهم العلم التراكمي والعمالة المدربة والتقنية والادوات والتمويل ففرصة ايجاد الحل ليست مستحيلة. لكن ماالذي سوف يحدث لبلدان مثل بلداننا نستخدم بلا رقيب شتى انواع التكنولوجيا (او نستهلك) ان صح التعبير دون الاخذ ايضا في الإعتبار ان هذه التقنيات ربما تحوي العديد من الاساليب للإختراقات التي نتحدث عنها والكل يعلم ان الدول النامية اصبحت تستخدم وتعتمد على التقنية بشكل كبير في اجهزة الحكومة وظهور ما يعرف بالحكومات الإليكترونية وربط المؤسسات والمصالح العامة بشبكة الإنترنت ناهيك عن استخدامoff-the-shelf devices لاننا لا نصنعها ولا نعرف حتى كيف تعمل بشكل دقيق وانا اتحدث هنا عن الاجزاء المعقدة مثل تصنيع الـCPU وليس ما يدرسه طلاب الهندسة في جامعاتنا.

مناهجنا التعليمية في مراحل التعليم المختلفة حتى الجامعة تحتاج إلى تطوير واعادة نظر، البحث العلمي بات فقيرا جدا ويحتاج إلى تطوير وتمويل وامكانات اكبر من الدول والحكومات، نظرتنا في تطبيق التقنية في شتى المجالات دون تأهيل واستعداد تحتاج إلى اعادة النظر، اعتمادنا على دول اخرى في تصنيع كل ما هو تقني ليس حلا جيدا ولا فرصة جيدة لنا في هذا العالم، امن المعلومات كعلم يحتاج إلى الإهتمام من قبل الحكومات العربية كقضية امن قومي وليس رفاهية!

اعتقد اننا في حاجة إلى وقفة قبل فوات الاوان واننا لسنا في معزل ابدا عن ما يحدث حولنا
You're connected, you are affected! بما انك متصل فأنت متأثر لا محالة.

British Council Data Loss | المجلس البريطاني وضياع المعلومات

19- ابريل – 2009 – Computer World UK

خرق المجلس البريطاني قانون حماية المعلومات للمملكة المتحدة Data Protection Act حيث اعلن المجلس البريطاني رسميا عن ضياع قرص مدمج يحوي اكثر من 2000 سجل لموظفين يعملون في المجلس ويحوي اسماؤهم ومعلوماتهم الشخصية ورواتبهم وحساباتهم في البنوك وما إلى ذلك. حيث فقد القرص اثناء عملية الشحن عن طريق خدمة TNT واعلن المجلس البريطاني عن هذه الواقعة رسميا وانه اتخذ اجراءات صارمة فور تأكده من ضياع هذا القرص تشمل تشفير البيانات على كل الاجهزة المستخدمة في نقل وتخزين البيانات والتي يتم تداولها في نقل البيانات من وإلى المجلس البريطاني. وتعد هذه الحادثة في بريطانيا خرقا لقانون حماية المعلومات قد توقع عقوبات على المجلس البريطاني ان تكررت مثل هذه المشكلات!

Why hackers need old Nokia phone? | لماذا يحتاج الهاكرز إلى هاتف نوكيا القديم؟

22- ابريل – 2009 – GEEK.COM

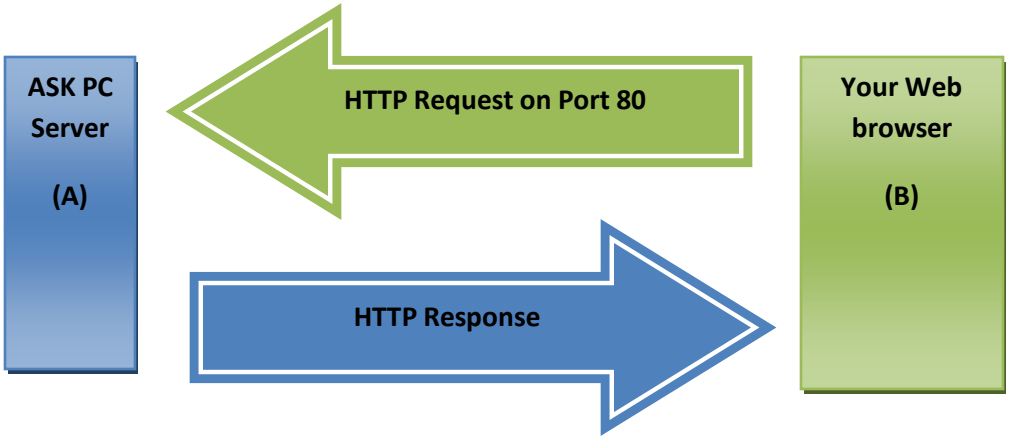
اعلن احد المخترقون Hackers عن احتياجة لهاتف نوكيا موديل 1100 مقابل مبلغا ضخما من المال وصل إلى 22 الف جنيه استرليني! والهاتف تم تصنيعه خصيصا في عام 2003 كأحد المنتجات للدول النامية وكان يباع باقل من 100 يورو. وتم بالفعل رصد تحويل مبلغ ضخم من المال مقابل هذا الجهاز العتيق! وبدأت الشبهات تحوم حول ما هي المشكلة في طلب مثل هذا الجهاز القديم بهذا المبلغ الضخم من المال؟ كشفت التحقيقات من قبل الخبراء ان الهاتف المطلوب هو فقط المصنوع في Bochum في المانيا لانه على حد قول الخبراء يحوي مشكلة في البرنامج الخاص به تمكن الهاكرز من تعديل البرمجة واستغلاله في هجوم يسمى Caller ID Spoofing او بمعنى ادق يستيطع الشخص التحدث برقم شخص آخر وانتحال شخصيته مما يعد احد انواع الاحتيال عن طريق Social Engineering Attack هجوم الهندسة الإجتماعية باستخدام تقنية المحمول. ويضيف الخبراء ان نوكيا لم تستطع حتى هذه اللحظة اقناع المسؤلين والمحققين لماذا يدفع مبلغ كهذا في مثل هذا الموديل دون ان يكون به مشكلة امنية. واشار احد الخبراء في شركة Ultrascan لامن المعلومات بان هذا الهاتف يستخدم في التحايل على انظمة امنية في البنوك في بعض دول اوروبا مثل المانيا والتي تستخدم تقنية ارسال mTAN او Mobile Transaction Number Authentication وهو رقم يرسل إلى الهاتف النقال الخاص بالشخص الذي يريد تحويل ارصدة من بنك إلى بنك أخر عن طريق الإنترنت للتحقق من هوية الشخص الذي يقوم بالتحويل حيث يدخل الشخص هذا الرقم الذي يصله على الموبايل في موقع البنك لتأكيد العملية. ويقول الخبير ان هذا الهاتف يمكن استخدامه للحصول على هذه الارقام عن طريق الدخول لحسابات العملاء لدى البنك عن طريق احد حيل الخداع مثل Phishing ومن ثم التعامل على انه الشخص صاحب الحساب باستخدام هذا الهاتف برقم الشخص صاحب الحساب البنكي!

يعتبر برتوكول HTTP هو المسؤل عن تبادل صفحات الإنترنت بين الاجهزة خلال شبكة الإنترنت وله اختصار شائع يطلق عليه Hypertext Transfer Protocol إلا ان بعض الخبراء اطلقوا عليه ايضا Hypertext Transport Protocol ربما يتسائل الكثيرون وما الفرق بين Transport و Transfer فالاثنان تقريبا نفس المعنى!

إذا رجعنا إلى تاريخ البرتوكول فسوف نجد انه تم ابتكاره عام 1990 بواسطة Tim Berners-Lee واستخدم البروتوكول في نقل او تحويل اكواد HTML التي تكتب بها صفحات الإنترنت Hypertext Markup Language من كمبيوتر إلى كمبيوتر آخر عبر شبكة الإنترنت. ويعرف ايضا بانه بروتوكول Request/Response او Client-Server حيث يتم طلب الصفحة الخاصة بالموقع على سبيل المثال من الخادم Server عن طريق كمبيوتر متصل بشبكة الإنترنت Client وتسمى العملية (الطلب – الرد) Request/Response وله عدة اصدارات من اشهرها شيوعا HTTP 1.1 المسجل لدى Internet Engineering taskforce تحت رقم RFC2616 او Request for Comment ولكي نشرح لك ببساطة فكرة العمل فهي تتلخص في ارسال واستلام صفحات او اكواد HTML عبر هذا البرتوكول من نقطة إلى نقطة اخرى في فضاء الإنترنت.

ولنصبح اكثر دقة فأن الإتصال يحدث ما بين متصفح الإنترنت لديك Web Browser الذي يطلق عليه الـ Client او Agent وبين الـ Web Server الذي يستضيف الصفحة او الموقع المراد الحصول عليه.

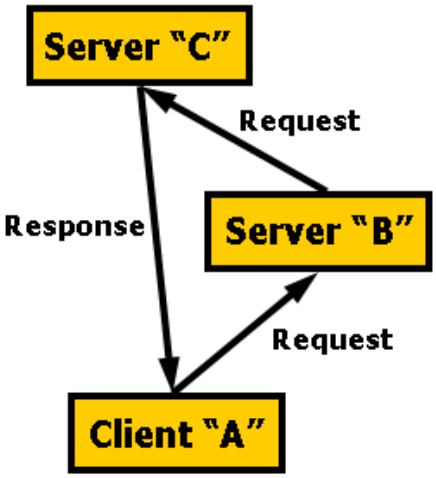
لاحظ ان الـ Web Browser يطلب الـHTTP عبر TCP او Transmission Control Protocol بالإتصال بمنفذ معلوم على الخادم وهو Port 80 الخاص بخدمة HTTP. لاحظ ايضا ان HTTP يطلب الصفحات عن طريق العنوان IP – Internet Protocol Address والذي يتم تحويله إلى حروف او ما يسمى Domain عن طريق خدمة DNS او Domain Name System التي تقوم بالتحكم بها منظمة ICANN ويعرف الاسم الكامل بـ URL او Uniform Resource Locator على سبيل المثال http://www.ask-pc.com



كما ترى الامر في غاية البساطة انتقال الصفحة من A إلى B

إلأ ان خبراء الإنترنت اشاروا إلى مصطلح Transport إضافة إلى Transfer في تعريف HTTP لانهم يرون انه اشمل في ظل احتواء صفحات الإنترنت على محتويات اخرى تتطلب وجود اتصال مستمر Constant Connection بين النقطتين حتى يتم اكتمال الحصول على الصفحة مثل الصفحات التي تحوي صورا واصوات وبرمجيات اخرى مثلActiveX و Java و XML فكل هذه التقنيات الجديدة تستخدم HTTP كاحد وسائل النقل Transport للإنتقال من النقطة A إلى النقطة B لهذا اطلق عليه ايضا Hypertext Transport Protocol. إضافة إلى ان الـ HTTP في اصداره الجديد بدأ يعرف انواع الملفات التي يتم نقلها عن طريق Internet Media Types حيث يرسل الخادم A معلومات عن نوع الملفات فيما يسمى Header في الـ HTML ليعلم B

GET http://example.com/images/splash.png HTTP/1.2



ما هو نوع الملف وما هي الطريقة المثلى للتعامل معه ان كان ملف صوت او صورة. ويطلق عليه ايضاMIME Type

اضف إلى ذلك ان الإصدار الجديد من HTTP وهو HTTP 1.2 يشمل ايضا ما يسمى HTTP Request Forwarding حيث يمكن ارسال الطلب من خادم إلى خادم آخر عند معلومية وجود الـResource المطلوب على الخادم الآخر مثل الصورة Splash.png عن طلبها في عنوان معين وهي ليست موجودة على الخادمB فأنه يوجه الـ HTTP Request إلى الخادم C

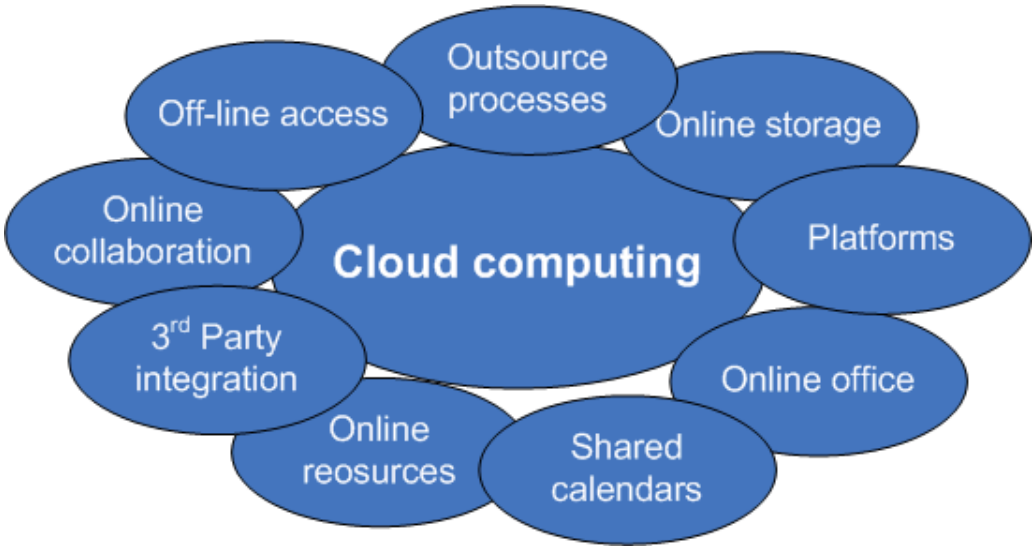
كما ان هناك ابحاث كثيرة على مايسمى SOAP او Simple Object Access Protocol وعلاقتها بنقل XML عبر الـ HTTP

كل هذا يجعل برتوكول HTTP يشمل ايضا Transport Layer او طبقة نقل للمعلومات وليس فقطTransfer فلهذا يعتبر مصطلح Hypertext Transport (Transfer) protocol اكثر شمولا في تعريف HTTP

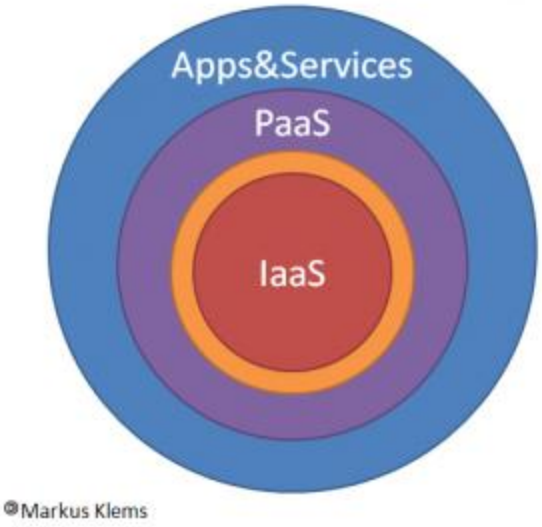
انتشر في الفترة الاخيرة مصطلح جديد في علم الكمبيوتر وهو Cloud Computing رغم اننا لا نحبذ ترجمة المصطلحات الأصلية إلى اللغة العربية ولكن يمكننا تبسيط الامر إلى القاريء بانه سحابة الحواسب او حواسب السحابة. ولكن ماذا تعني هذه التقنية تحديدا؟

طبقا لتعريف الموسوعة الحرة فأن Cloud Computing هي عبارة عن جيل جديد من تقديم خدمات الكمبيوتر بشكل متفاعل معتمدة على التقنيات الإفتراضية Virtualization كما انها لا تعتمد على بنية تحتية لدى المستخدم Infrastructure ويمكن الحصول عليها من اي مكان حول العالم ولعل من اكثر هذه التقنيات وضوحا والتي تعتمد على Cloud Computing هي تقنية Web 2.0 التي تحوي الكثير من المواقع المتفاعلة مع المستخدم وقد توفر خدماتها من اكثر من مكان او خادم Server على الإنترنت وكمثال ايضا خدمات Google الجديدة SaaS او Software as a Service والتي لا تتطلب ان يقوم المستخدم بتركيب اي من البرمجيات على جهازه الخاص لكنها تعمل من مكان اخر او من عدة اماكن مختلفة يطلق عليها السحابة.

ويطلق مصطلح السحابة تحديدا على الإنترنت حيث تعطي شكلا عاما لما هي عليه الإنترنت الآن من تشعب وتشابك للعديد من الخدمات ومن اشهر هذه الامثلة الخدمات المقدمة من Microsoft والتي تشتهر بـ AZURE



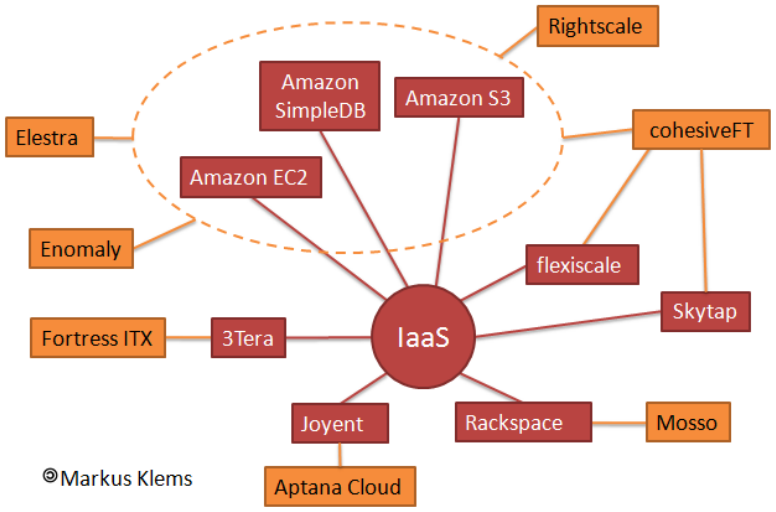
والتي تتيح للمستخدمين او حتى المطورين استخدام البنية التحتية الخاصة بميكروسوفت لاستخدام البرمجيات مثل Online Office وايضا لغات البرمجة ومنصات تطوير البرمجيات دون تركيب هذه البرمجيات على اجهزة المستخدمين ودون الحاجة لأى عناء لادارة مثل هذه البنى التحتية وكما اشرنا في المقال السابق بخصوص Simple Object Access Protocol فإن تقنية Cloud Computing تعتمد عليها ايضا. ويمكننا تقسيم انواع الـ Cloud Computing إلى 3 مستويات حسب نوع الخدمات المقدمة وربما ايضا حسب الشركات التي بدأت تتحكم في هذه الخدمات مثل Microsoft و Amazon



يوضح الشكل السابق 3 مستويات من الـ Cloud Computing حسب هذه الطبقات التي قام بعملها Markus Klems من الداخل إلى الخارج:

- البنية التحتية كخدمة Infrastructure as a Service

ويمكننا القول بان هذه الطبقة هي قلب اونواة السحابة والتي تعتمد عليها الطبقات الاخرى ولعل ابسط تعبير عن هذه الطبقة هي العصب الرئيسي الذي يوفر المساحات التخزينية وايضا خدمات Virtualizations التي يتم تقسيمها إلى اجزاء صغيرة.

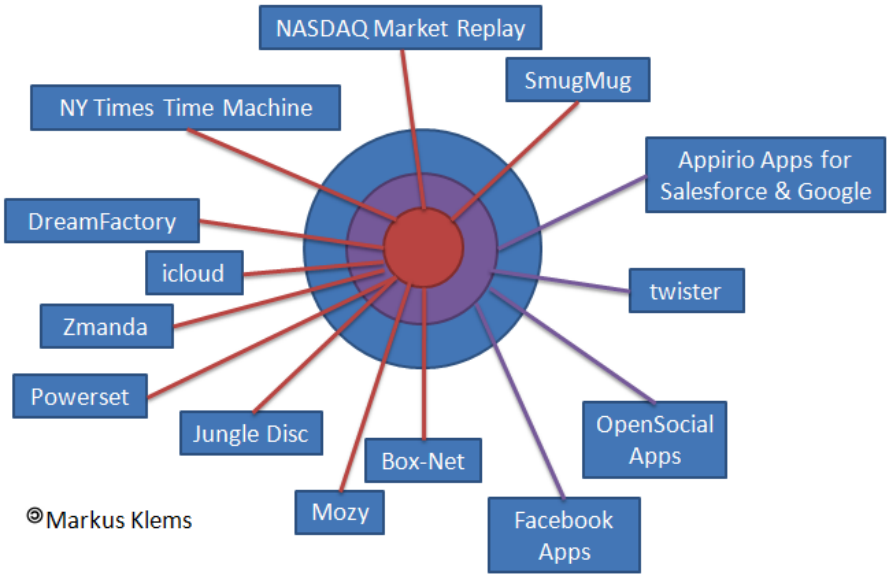


- الطبقة التي تليها تسمى Platform اومنصة العمل والتي يطلق عليها هنا Platform as a Service – PaaS

في هذه الطبقة نجد اكثر منصات العمل تعقيدا والتي تتيح البيئة الخاصة بالخدمات او الطبقة التي سوف تعمل عليها الخدمات ولعل من اشهرها Google App Engine او Salesforce.com ويطلق عليها ايضا الجزء الذي يمكن تطويره وبرمجته بواسطة مطورين في اماكن اخرى بعيدة عن هذه الطبقة اي انها تتيح للمطورين استخدامها كأداة لتطوير برمجيات السحابة!

- الطبقة الاخيرة وهي المنتجات والخدمات التي تتاح للمستخدم Apps & Services

وهي التطبيقات التي بنيت اما على IaaS او Paas وتندرج تحتها الكثير من التطبيقات مثل تطبيقات Social Networks ومجموعة برمجيات المكتب مثل Online Office كما ترى في الشكل بالاسفل.



إلى ان الكثير من الخدمات قد تحوي ايضا API – Application Programming Interface تتيح للمطورين تطوير برمجيات خاصة بهم في بيئة الخدمات والبرمجيات اعتمادا على اي من الطبقات التي اشرنا اليها مستخدمة البنية التحتية كخدمة IaaS

يبقى ان نشير إلى ان الـ Cloud Computing تقنية جديدة تنطوي على الكثير من المميزات ولها ايضا العديد من العيوب كما سوف تظهر لنا ايضا الكثير من مشاكل امن المعلومات والتي سوف تعتبر تحديا امام هذه التقنيات الحديثة إلا انها كتقنية تعتبر نقلة كبيرة في مجال علوم الكمبيوتر Computer Science وسوف نفرد لها الكثير من المقالات في اعداد قادمة ان شاء الله.

تعتبر تقنية النانو او الجزيئات من اكثر التقنيات اثارة للجدل في الآونة الاخيرة ومن هذا المنطلق رأينا ان نلقي الضوء على هذه التقنيات في لمحة سريعة في هذا العدد.

تكنولوجيا الـ nanotech اختصارا تتعامل مع تأثيرات المادة على مستوى الذرة والجزيء وبشكل بسيط فأن تقنية النانو تتعامل مع كل جزء يمثل100 نانومتر او اقل وتشمل ايضا تصنيع مادة معينة او حتى جهاز في هذا الحيز من المساحة!

وتشمل تقنية Nanotech تصنيع اي جزء اومادة او جهاز في افرع العلوم المختلفة في الحيز الذي اشرنا عليه مثل مجالات الطب والإليكترونيات إلا انها تتعامل مع الجزئيات على مستوى الذرة وما يمكن ان يتم عمله بها. على سبيل المثال ان قمنا بجمع بعض الذرات Atoms ورتبناها ترتيبا معينا في الفحم فسوف تنتج ماس! ونفس الشيء ان قمنا بترتيب مجموعة من الذرات في الرمل باضافة ذرات اخرى من مواد اخرى قد ننتج رقاقة كمبيوتر Chip

وهكذا فهذا العلم يتحدث عن طبيعة الجزيئات داخل الذرة وما يمكن ان يفعله ترتيب الجزيئات داخل الذرة الواحدة وخصائص كل جزيء منفردا وما يمكن ان تمثله هذه الخصائص. ولعلنا يمكننا ان نشير إلى هذه التقنية بهذا المسمي molecular nanotechnology او molecular manufacturing بمعنى ابسط التصنيع بدءا من الجزيئات المكونة للمادة!

ومع زيادة استخدام تقنيات الكمبيوتر في مثل هذه التقنيات الجديدة فاننا من البديهي ان نشهد ثورة قد لا يصدقها العقل في العلوم المختلفة مثل الفيزياء والطب على مستوى الجزيئات والذرة.

كما ان هذه التقنية Nanotech سوف تتيح اشياء مهمة من شأنها ايجاد التطوير الذي تحدثنا عنه:

- ترتيب الذرات في مكانها الصحيح او في اماكن اخرى حسب الحاجة
- تطبيق قوانين الفيزياء على اجزاءصغيرة جدا وتحديدا الجزيئات وتفاصيلها المختلفة
- لن تتعدي التكلفة المطلوبة للتصنيع سوى توفير المادة الخام والطاقة اللازمة!

وتتشعب افرع هذا العلم إلى الكثير من التخصصات مثل الضوء و الإليكترونيات وخصائص المواد ولعل هذا العلم من العلوم التي تحتاج إلى اهتمام كبير في الدول النامية والتي يتوقع العلماء ان الدول النامية يمكنها تحقيق الكثير من هذه التقنية ان استطاعوا استغلالها في تطوير امكانياتهم!

يمكنك تخيل هذا العلم وامكانياته بهذا المثال البسيط " ماذا لو امكننا ارسالRobot إلى داخل جسم الإنسان وتخيل اننا نراقبه تحت المجهر الإليكتروني على ان يقوم هذا الـRobot بالتوجه إلى خليه مريضة بالسرطان والقضاء عليه واخراجه كمخلفات في الدم"

انه ليس خيالا علميا ولكن هذه حقيقة التحكم في الجزيئات وما هو في حجم النانوميتر!

سوف نخصص لهذه التقنية العديد من المقالات ان شاء الله لكن فيما يخص تكنولوجيا المعلومات والكمبيوتر لانها بدأت تدخل وبشدة في هذا المجال وسوف تؤدي إلى ابتكارات خارقة في الفترة القادمة. للمزيد عن الـNanotech بشكل عام يمكنك الأضطلاع على هذه الروابط:

http://www.nanotech-now.com
http://www.crnano.org/whatis.htm
http://en.wikipedia.org/wiki/Nanotechnology

ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

منظمة امن نظم المعلومات
الآن في مصر...

Training Tomorrow's Security Professionals...

The largest organization for IS Security Professionals
More than 140 chapter in 35 countries
Now in Egypt!

امن المعلومات يبدأ بالتوعية والتدريب
دورات متخصصة ومعتمدة عالميا
شهادات معتمدة من اعرق المؤسسات العالمية

ASK PC

Founding Sponsor & Course Provider

BRITISH INSTITUTE FOR LEARNING & DEVELOPMENT
ORGANISATIONAL MEMBER

BCS
REGISTERED COURSE PROVIDER

IEEE

ISSA in Egypt:
38 Mustafa El Nahas Street,
Floor 5, Nasr City, Cairo

+20 2 22715443
+20 12 4473366
+20 10 7118587

www.issa-eg.org
heba@issa-eg.org