معلومات أم بيانات .... أو كلاهما ؟

حسنا دعونا نعرج على تعريف أمن المعلومات أولا من عدة مصادر :

فلو قلنا أن أمن المعلومات هو علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها.

هذا بحسب التعريف المنشور على ويكيبيديا

تعريف اخر يقول ان امن المعلومات هو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها .

بينما نجد في بعض الكتب والمصادر الأخرى ان الامن المعلوماتي هو مجموعة الإجراءات والتدابير الوقائية التي تستخدم لتامين المعلومات ومصادر البيانات وحماياتها من أي تهديدات او تجاوزات غير مشروعة ومن مخاطر الكوارث الطبيعية المحتملة التي تؤدي الى الفقدان أو التلف أو التأثير على نوع ومستوى الخدمة المقدمة .

إذا فقد ورد هنا مصطلح معلومات وبيانات!

قد يخطأ البعض أحياناً في استخدام البيانات والمعلومات كمعنى واحد، غير أن معنى الكلمتين مختلف تماماً، فما معنى البيانات؟ وما هي المعلومات؟

وما أهمية البيانات والمعلومات؟

مفهوم البيانات !

يمكن تعريف البيانات على انها مجموعة من الحقائق والقياســات والمشــاهدات والتي غالبا ما تأتي على شــكل أرقام وحروف ورموز وأشكال خاصّة، ولا يكون لها معنى (فما معنى الرقم 25 بالنسبة لك ؟ وما معنى رمز =)

مفهوم المعلومات !

هي نتاج معالجة البيانات التي ليس لها معنى محدد بتصنيفها وتنظيمها وتحليلها، أو التعديل عليها حتى تصبح ذات معنى

مثال توضيحي .

ترفع ســماعة الهاتف لتتصــل بوحدة الأرصــاد الجوية في بلدك للاســتفســار عن حالة الطقس فيرد الموظف المختص ويخبرك بان غدا منخفض 35 شــمالية شــرقية 15 عقدة 22% 17 بار خفيفة الى متوســطة .....

حسنا مذا فهمت الان !؟

الموظف هنا قام بتزويدك ببيانات الطقس وهي دقيقة جدا بالمناسبة لكنك لم تفهم شيئا منها !!

ببساطة لأننا حينما نريد الاستفسار عن حالة الطقس ، لا يجب أن نحصل على بيانات درجة الحرارة وحركة الرياح وقياس نسبة الرطوبة وحركة الغيوم وما الى ذلك بل لابد ان نحصل على معلومة مستخلصة من كل البيانات السابقة ؟

ومن هنا يمكن معرفة ما تمثله البيانات من أهمية بالغة في عملية استخلاص المعلومات .

إذا وببساطة شديدة البيانات هي المادة الخام للمعلومات ويجب حمايتها أيضا .

أقسام الحماية

يمكن تقسيم الحماية داخل إطار أمن المعلومات الى ثلاث اقسام

أ- الحماية **الفيزيائية** Physical Security

يقصد بها حماية الأجهزة والبرامج والشبكات والبيانات من الأحداث الفيزيائية التي يمكن ان تسبب خسائر وأضرار ، مثل الحرائق والكوارث الطبيعية وعمليات السطو والتخريب وما الى ذلك ، من خلال استخدام أنظمة مراقبة وتتبع وانذار مبكر وغيرها .

ب – الحماية التشغيلية Operational security

وتعتمد بشكل كبيرة على برامج وأنظمة التشغيل كالجدران النارية ومكافح الفيروسات ومراقب النظام وعمليات فحص المنافذ وما الى ذلك .

ج –الإدارة والسياسات Management and policies

وهي مجموعة القوانين والإجراءات المعتمدة في المنشاة لتأمين البيانات والمعلومات الخاصة بها كسياسة كلمات المرور وصلاحيات الوصول وإدارة الملفات ، وكلما كانت هذه السياسات قوية كلما زادت قوة أمن المعلومات في هذه المنشاة .

عناصر وأهداف أمن المعلومات CIA

هناك ثلاث عناصر رئيسية لابد أن تكون في كل التدابير والسياسات والعمليات والاجراءات المستخدمة في تامين البيانات والمعلومات بحيث يتم بها تحقيق الأمن المعلوماتي .

هذه العناصر تختصر في الرمز **CIA كالتالي :**

الخصوصية او السرية : Confidentiality

وهي منع غير المصرح لهم من الاطلاع او الحصول على البيانات والمعلومات .

السلامة : Integrity

وهي منع غير المصرح لهم من التعديل على البيانات والمعلومات .

الاتاحة : Availability

يقصد بها توفر إمكانية الوصول الى البيانات والمعلومات للأشخاص المصرح لهم .

هذه العناصر الثلاث يجب أن تمر من خلال **التحقق والتفويض والمحاسبة** وهو ما يطلق عليه معيار " **AAA** "

وهذا المفهوم أيضا يجب ان يستخدم عند تصميم او بناء أي خطة امنية لان معظم بروتوكولات أمن المعلومات قائمة في الأساس على هذا المفهوم.

والان لنتوقف قليلا لفهم هذا الـ "AAA"

يعبر كل حرف من هذه الأحرف الثلاث لمصطلحات ثلاث هي Accounting / Authorization / Authentication

التحقق Authentication : هي الهوية الرقمية التي تمنح لك في عالم أمن المعلومات ولا تخلو من أن تكون

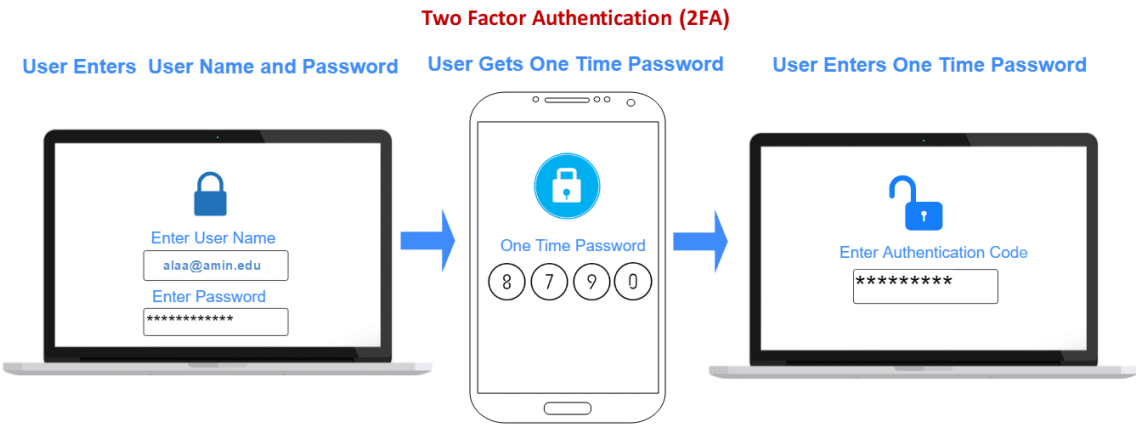
1- شيئا تعرفه ككلمة مرور أو رمز دخول
2- شيئا تملكه مثل كارت ممغنط او مفتاح مشفر
3- شيئا يعبر عنك كبصمة الاصبع او العين أو بصمة صوتية

في أمن المعلومات نستخدم أشكال عديده للوصول لمعيار التحقق كأجهزة الـ Biometric مثلا والشهادات الرقمية والبروتوكولات التي يتم التركيز عليها غالبا ، كما ان معيار التحقق نفسة هو الاخر يأتي في عده أشكال .

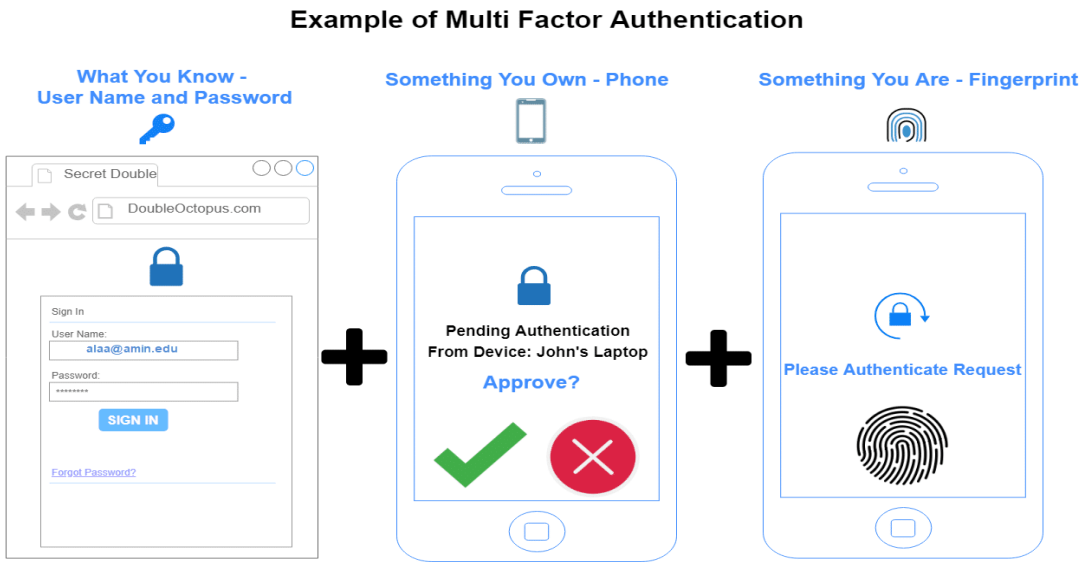
فقد يأتي الـ Authentication في صورة نوع واحد كبروتوكول (SFA) Single-Factor Authentication

والذي يعني ببساطة مطابقة الهوية بما هو موجود في قاعدة البيانات المخزنة كما في الشكل

أو بدمج نوعين معا وهو ما يعرف بـ Two Factor Authentication (2FA)



أو بتداخل الأنواع كلها معا وهو ما يعرف بـ Multi-Factor Authentication (MFA) .



التفويض Authorization : وهو المصطلح الثاني في مفهوم (AAA) ويعني التفويض ويأتي مباشرة بعد التحقق ومن خلاله يتبين ما الذي يمكن لهويتك فعله وما لا يمكن .

ثم تأتي عملية المحاسبة Accounting لتتبع وتأكيد عمليات الـ Authentication و الـ Authorization فهي تسجل وتراقب وتتابع جميع العمليات كتسجيل الدخول وأوقاتها والصلاحيات الممنوحة وتعد مرجعا واثباتا لمسئول أمن المعلومات في حالات التسلل والعبث

الآن قم بإخراج بطاقة الصراف الالي ATM الخاص بك لنطبق عليها عناصر امن المعلومات وكذلك مفهوم الـ "AAA"

- هل يمكن لأي شخص غيرك الحصول على بيانات المبالغ بداخل البطاقة ؟ ..... (التحقق) (Authentication)
- هل يمكن اجراء تعديل على كلمة السر الخاصة بالبطاقة دون علمك ؟ ..... (السلامة) (Authorization)
- هل تتمكن من استخدام البطاقة في أي وقت طالما هي معك ؟ ..... (الإتاحة) (Accounting)

سياسات أمن المعلومات

علمنا ان أمن المعلومات يتكون من عناصر ثلاث ولتحقيق هذه العناصر لابد من استخدام مجموعة من السياسات والإجراءات والأساليب التي يطلق عليها مجملا " سياسات أمن المعلومات " وهي مجموعة القواعد والقوانين التي يتم تطبيقها عند التعامل مع المعلومات وما يرتبط بها لتحقيق الأمن بالنسبة للنظام أو المنظمة أو أي كيان آخر و توضيح ما هو مسموح به وما لا يسمح به.

ومن أشهر هذه السياسات

سياسة إدارة الشبكة

وتعني تحديد المهام والأدوار وإسنادها للأشخاص كلا بحسب اختصاصه

فمثلا تسند أعمال إدارة الخوادم والعتاد والربط والتعريف الى مهندسي الشبكة Network Engineer بينما يتولى إدارة المستخدمين و كلمات المرور ومشاركة الملفات مهندسي الدعم الفني غالبا Support Engineer أما التطبيقات وما يتبعها كالتحديثات والترقية والمتابعة فتقع ضمن مهام مهندسي النظام System Engineer ، وفيما يتعلق بالتوثيق والإجراءات ووضع الخطة التشغيلية ومراجعة السياسات ومراقبة الأداء فبالطبع تتبع مشرفي ومديري الإدارات التقنية .

وقد تختلف هذه الأدوار والمهام من جهة الى أخرى بحسب طبيعة العمل وحجم المنشأة والنشاط .

وقد تجد شخص واحد يتولى عده مهام مشتركة ومتنوعه فيما بين مهام الدعم الفني وإدارة النظام مثلا أو مهام الإشراف والمراقبة وأعمال فنية أخرى وهكذا .

سياسة التعافي من المخاطر

وهي وضع خطة لمواجهة **أي كارثة قد تحدث** ، وغالبا ما يقوم قسم إدارة المخاطر في المنشاة بالاجتماع مع افرادها المعنين لتحديد وحصر كافة المخاطر كفقدان البيانات او التعرض للفيروسات أو لهجوم قرصنة الكترونية ، أو أعمال السرقة والنهب والزلازل والبراكين والفيضانات وانقطاع التيار الكهربائي، وحتى إمكانية حدوث ثورة في البلاد يترتب عليها اعمال فوضوية او تخريبيه أخرى.

سياسة إدارة المعلومات

وهنا يتم تقسيم المعلومات وتصنيفها الى عامة وخاصة وداخلية ويحدد في هذه السياسة من الذي سيصل الى كل نوع ومن سيمنع من الوصول .

فالمعلومات العامة بطبيعتها متاحة للجميع وغالبا ما تنشر على موقع الشركة أو النشرات واللقاءات التعريفية لها

أما المعلومات التي تتعلق بالأنظمة الإدارية واللوائح والتعاميم فينحصر نشرها على نطاق محدود داخل المنشأة ولمنسوبيها ولذا سميت بالمعلومات الداخلية .

أما المعلومات الخاصة فهي التي يقيد وصولها الى عدد محدود أو قليل جدا، كأن تتاح على مستوى المدراء التنفيذيين أو الإدارة العليا فقط (يصل في بعض الأماكن إلى شخص واحد فقط)

سياسة التصميم البرمجي

يقصد بهذه السياسة إحداث توازن بين الأداء والتكلفة فلا يعقل اعتماد شراء مائة نسخة لبرنامج أو نظام ما بينما عدد الذين سيعملون على هذا النظام هم خمسة عشر مستخدم فقط ، أو اطلاق موقع الكتروني للمنشاة بأضعاف دخلها السنوي .

والحقيقة أن هذه السياسة رغم أهميتها البالغة إلا أنها قد تغيب في كثيرا من الأحيان داخل المنشآت على أختلافها من حيث الحجم أو النشاط ، وقد تطبق بشكل خاطئ تماما وتختلف المسببات في ذلك فأحيانا يعود السبب لاعتماد ميزانية في بداية العام وفرض استنفاذها قبل باية العام التالي ، أوقد يكوزن السبب هو تطبيق هذه السياسة من قبل أشخاص لا يملكون الحد الأدنى من الخبرة والكفاءة ، أو وجود بعضا من المنتفعين من وراء هذه السياستو وما الى ذلك .

سياسة الاستخدام

هذه السياسات تحدد كافة الموارد والمصادر داخل كل منشأة ، وتحدد أيضا طريقة استخدامها والاستفادة منها، وذلك عبر مجموعة من القوانين التي يجب الالتزام بها عند الاستخدام ، كعدم طباعة أوراق لا تخص العمل أو الحد من إساءة استخدام شبكة الانترنت ، و عدم استخدام منافذ الـ USB في شحن الأجهزة الشخصية او تقنين استخدام بريد الشركة على المعاملات الرسمية فقط وقد تأتي أيضا هذه السياسات متضمنة ما يترتب على عدم الالتزام بالقوانين الواردة فيها .

بروتوكولات التحقق Authentication Protocols

نحن كبشر نقوم بعملية التحقق بعدة طرق باستخدام نعم الله علينا كالسمع والبصر ، فنحن ندرك وجوه بعضنا البعض عندما نلتقي ، و نتعرف على أصوات بعضنا البعض على الهاتف أيضا ، لكن كيف سيتم الأمر مع الآلات ؟

حسنا

قد ذكرنا فيما سبق ان معيار " **AAA** " والذي يرمز الى Accounting / Authorization / Authentication يستخدم لتحقيق أهداف أمن المعلومات (**CIA**) وذكرنا أيضا ان المقصود بالـ Authentication هو عملية التوثيق أو التحقق الرقمي من الهويات والتي على ضوئها تتم عملية الـ Authorization لمنح الصلاحيات بعد ذلك .

اذا لابد حتى امنح صلاحيات ان استوثق من هويات أصحابها .... أليس كذلك ؟

هنا يأتي دور بروتوكولات التحقق Authentication Protocols

وفيما يلي سنتطرق لأشهر وأهم البروتوكولات التي تستخدم في عملية التحقق تلك .

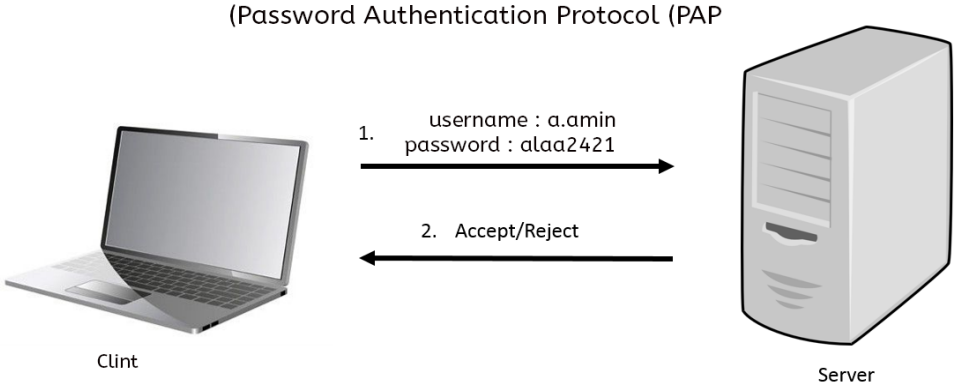
بروتوكول المصادقة بكلمة السر Password Authentication Protocol (PAP)

هو أبسط بروتوكول يستخدم في عملية التوثيق وآليه عملة ببساطة هي ان يرسل المستخدم اسم الدخول وكلمة المرور

فيرد الخادم بعد فحص المدخلات بالسماح أو الرفض .

و بروتوكول الـ PAP يقوم بتسجيل جميع تفاصيل المصادقة في نص واضح دون أي تشفير ، مما يجعل هذا البروتوكول عرضة للقرصنة، ولذلك يجب تعطيل بروتوكول الـ PAP ما لم يكن هناك حاجة ماسة للعمل به في كوسيط لا يدعم كلمات المرور المشفرة.

(Password Authentication Protocol (PAP



بروتوكول المصادقة بكلمة السر المشفرة SPAP Shiva Password Authentication Protocol

هو نسخة مطورة من الـ PAP وأعلى امانا منه حيث يتم تشفير كلمة المرر بين المستخدم وخادم التوثيق الا انه لم يزل عرضه للقرصنة حيث يمكن الوصول لبيانات المصادقة وفك تشفيرها ومن ثم استخدامها .

بروتوكول المصادقة بمصافحة التحدي CHAP Challenge Handshake Authentication Protocol

يعد الـ CHAP من البروتوكولات الأكثر امانا لقيامه بتشفير بيانات المصادقة وعدم اعتمادها الا بعد اجتياز تحدي ما يرسله الخادم المسئول عن عملية المصادقة الى العميل . وقد يكون التحدي هذا سؤالا عن العمر او النوع أو مسألة حسابية بضرب عددين مثلا او جمعهما وحتى يسمح للعميل بالدخول لابد ان يقوم أولا بالإجابة .

آلية العمل ببساطه كالتالي :

يرسل المستخدم طلبا للدخول

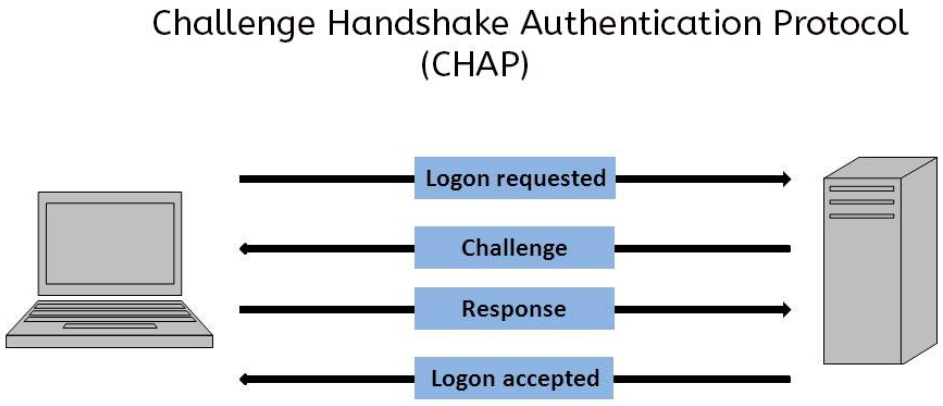
يرد الخادم بإرسال تحدي لهذا المستخدم

يستجيب المستخدم للتحدي ويرسل الطلب مره أخرى للخادم

يرد الخادم بعد التحقق من النتيجة والبيانات بالقبول أو الرفض

التوثيق بكلمة مرور لمرة واحدة Time-based One-Time Password (TOTP)

يعتبر بروتوكول الـ TOTP حديثا واكثر امانا بالمقارنة مع البروتوكولات السابقة وقد شاع استخدامه بكثره خصوصا مع انتشار الهجمات الإلكترونية وعمليات الاحتيال في الآونة الأخيرة، ويعتمد الـ TOTP على طريقة التحقق بخطوتين Two Factor Authentication (2FA) باستخدام كلمة مرور محددة بمدة زمنية .



آلية عمل **بروتوكول الـ TOTP** كالتالي :

يرسل المستخدم طلبا للدخول باستخدام بيانات اعتماده

يرد الخادم بعد التحقق من بيانات الاعتماد بإرسال كلمة مرور مؤقتة

يستخدم العميل كلمة المرور المؤقتة ويرسل الطلب مره أخرى للخادم

يقوم الخادم بعملية التحقق من صحة كلمة المرور فيرد بالقبول او الرفض

ويستخدم الـ **TOTP الان من قبل كبرى الشركات مثل جوجل وفيس بوك وميكروسوفت وغيرها الكثير .**

بروتوكول الـ Kerberos

هو بروتوكول تحقق ضمن بيئة الشبكة وهو مصمم لتوفير مصادقة قوية بين العميل/الخادم "Client/Server

وكلمة Kerberos تشير الى أسطورة يونانية قديمة لكلب حراسه بثلاثة رؤوس .

ومن هنا جاءت تسمية هذا البروتوكول ، حيث أن لديه ثلاث خطوات هامه " تشير الى الثلاث رؤوس " للمصادقة على كل عمليه من خلال

اولاً - Key Distrbution center KDC

ثانيا - Authentication Service

ثالثاً - Ticket Granting Server TGS

حيث يجب على المستخدم ارسال هويته للخادم والذي يقوم بالتحقق من صحة هذه الهوية و يرسل تذكرة دخول أولية مشفرة مع مفتاح فك الشفرة ، فيقوم المستخدم بعد ذلك بالدخول باستخدام هذه التذكرة الممنوحة له .

تتكون آلية عمل kerberos على الشكل الأتي :

1- يطلب المستخدم المصادقة على هويته بإدخال كلمة المرور واسم الدخول الخاص به

2- يتحقق خادم المصادقة من وجود هذا المستخدم في قاعدة البيانات لديه ثم يحيله لمركز التوزيع

3- يضع مركز التوزيع شفرة ومفتاح سري على الطلب ويحيل الطلب لمركز التذاكر

4- يقوم مركز التذاكر بتصدير تذكرة TGT و مفتاح بين المستخدم والخادم .

3- يقوم المستخدم بعد ذلك باستخدام هذه الـ تذكرة للحصول على إذن الدخول لخدمة ما .

4- باستخدام تذكرة الدخول يمنح المستخدم تذكرة جديدة للوصول للخدمة المطلوبة وجميع هذه العمليات تكون مشفرة تماما.

حسنا جدا الان سنتعرف معا على المخاطر والتهديدات الوارد حدوثها والتي يجب ان نستخدم سياسة أمن المعلومات

وبروتوكولات التحقق للحد منها وتحجيمها ، **لكن دعونا نراجع أولا ما تعلمناه .**

مـلخص ما سبق

ذكرنا فيما سبق ان البيانات هي المادة الخام للمعلومات وان عملية التامين تنطبق على كلاهما ، وفي أمن المعلومات يوجد ثلاثة اقسام رئيسية للحماية هي الفيزيائية والتشغيلية والإدارة والسياسات ، وقلنا ان هناك ثلاث عناصر رئيسية تعد بمثابة أهداف لـ أمن المعلومات يرمز لها بالرمز CIA هي

الخصوصية او السرية : Confidentiality

وهي منع غير المصرح لهم من الاطلاع او الحصول على البيانات والمعلومات .

السلامة : Integrity

وهي منع غير المصرح لهم من التعديل على البيانات والمعلومات .

الاتاحة : Availability

يقصد بها توفر إمكانية الوصول الى البيانات والمعلومات للأشخاص المصرح لهم .

وقلنا ان تلك الأهداف يجب ان تمر من خلال ما يطلق عليه معيار "AAA" المصادقة والتفويض والمحاسبة Authentication / Authorization / Accounting

وذكرنا ان التحقق أو المصادقة في معيار الـ "AAA" له أشكال عديدة كأجهزة الـ Biometric والشهادات الرقمية وله طرق مختلفة ما بين تحقق بخطوة (SFA) أو خطوتين (2FA) أو التحقق المتنوع (MFA) ويستخدم لعملية التحقق تلك بروتوكولات تناولنا أشهرها مثل الـ SPAP –**KERPROS** – PAP – CHAP

أما الصطلح الثاني في معيار الـ "AAA" هو Authorization ونعني به عمليات التفويض والتصاريح التي تمنح لمن يتم التحقق من هوياتهم الرقمية والسماح لهم بالوصول ، ثم تأتي عملية المحاسبة Accounting لتتسجل وتراقب وتتابع جميع العمليات التي يقوم بها صاحب الـتفويض وتعد مرجعا واثباتا لمسئول أمن المعلومات في حالات التسلل والعبث .