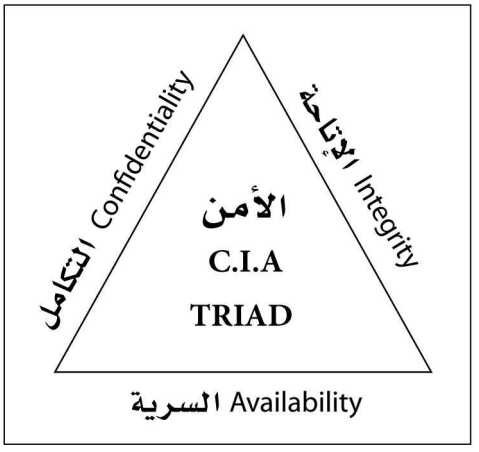
الفصل الثالث

مقوِّمات أساسيَّة في أمن المعلومات

1.3 ثلاثيَّة السرية والسلامة والتوافر



يركز هذا النموذج الشهير في حقل أمن المعلومات على تحقيق ثلاثة شروط أساسيَّة تُدعَى **ثلاثيَّة** C.I.A أو C.I.A Triad، وهي اختصار **للسريَّة** Confidentiality **وسلامة المعلومات أو تكاملها** Integrity **وتوافرها أو إتاحتها** Availability. هذا يَعني أنَّه، لكي يُحقِّق أمن المعلومات أهدافه، يَنبغي المحافَظة على سريَّة المعلومات الخاصَّة، وعلى سلامتها، وعلى تَوافرها عند الحاجة إلى استثمارها، وتَقوم معظم خُطَط وإستراتيجيَّات أمن المعلومات (مهما كان نموذج هذه المعلومات) على تحقيق ثلاثيَّة C.I.A. تُعدّ بعض المراجع ثلاثيَّة C.I.A مجرَّد مفاهيم أساسيَّة في حقل أمن المعلومات، إلا أنَّها على الأصَح مجموعة مقاييس شَرطيَّة لتحقيق أهداف أمن المعلومات.

2.3 أمن الشبكات

من الأساسيَّات في حقل أمن المعلومات حماية المعلومات الخاصَّة التي تَنتقِل عَبْر الشبكات الحاسوبية أو النقالة، وهذا الأمر هو ما يَتكفَّل به أمن الشبكات، و**أمن الشبكة** Network security هو مجموعة من الإجراءات المضادَّة التي تَكفَل إدخال المعلومات الرقميَّة الخاصَّة المشتَرَكة المعدَّة للنقل في وَضْع الأمان عند مرورها عبر شبكة غير آمنة، وتَتمثَّل مجموعة الإجراءات المضادَّة في حماية الشبكة نفسها وفي حماية المعلومات الخاصَّة التي تَمرُّ عَبْرها. وعمومًا، يُؤدِّي أمن الشبكات دوره لحماية المعلومات الخاصَّة في المحيط الإلكتروني فقط.

ويُعَدُّ تصميم الشبكة الحاسوبيَّة المناسب أمرًا فعَّالًا في حمايتها، ومن طُرُق التصميم المُثلى للشبكة تقسيم الشبكة الحاسوبيَّة إلى شبكات صغيرة Network segmentation، وتركيب الجدران الناريَّة Firewalls وتركيب أنظمة اكتشاف التطفُّل [2، 11]. وإن **تقسيم الشبكة** الحاسوبيَّة الكبيرة في بيئةٍ ما إلى مجموعة من الشبكات الصغيرة، تُدعَى كلٌّ منها **الشبكة الفرعية** Subnet، يوفر مزيّة التّحكُّم في حركة المعلومات التي تَمرُّ عَبْر الشبكات الفرعيَّة بكل سهولة. أمّا **الجدار الناري** فهو مجموعة من البرامج الحاسوبيَّة التي تَتحكَّم في حركة المعلومات الخاصَّة التي تَنتقِل بين الشبكة الداخليَّة والشبكة الخارجيَّة وفقًا لمجموعة من القواعد الموضوعة، ويُمكِن النظر إلى الجدار الناري على أنه حاجز أمني يَقَع بين الشبكة الداخليَّة الآمنة والموثوقة في بيئةٍ ما (كشبكة داخليَّة في منظَّمة ما) والشبكة الخارجيَّة (كشبكة الإنترنت) ويَتحكَّم في دخول المعلومات وخروجها بينهما، وأمّا **نظام اكتشاف التطفُّل** Intrusion detection system فهو برنامج حاسوبي يَسعى إلى اكتشاف نشاط أي متطفِّل يُحاوِل الدخول إلى الشبكة الداخليَّة في بيئةٍ ما من خلال إصدار إنذارات تُنبِّه إليه.

ويُمكِن أيضًا حماية المعلومات الخاصَّة التي تَمرُّ عَبْر الشبكة بدلًا من حماية الشبكة نفسها، ومن أكثر الطُّرُق استخدامًا لحماية المعلومات الخاصَّة التي تَمرُّ عَبْر الشبكة هي الشبكات الخاصَّة الافتراضيَّة، **والشبكة الخاصَّة الافتراضيَّة** Virtual private network، واختصارًا VPN، هي مجموعة من البرمجيَّات والعتاديَّات التي تُكوِّن شبكة خاصَّة داخل شبكة عامَّة تُضاهي في عملها شبكة خاصَّة فيزيائيَّة، وتَستخدِم الشبكة الخاصَّة الافتراضيَّة تقنيَّة التعمية لحماية المعلومات التي تَمرُّ عَبْرها، ويُمكِن النظر إلى الشبكة الخاصَّة الافتراضيَّة على أنها نَفَق (أو أنبوب ضمن الشبكة العامة) تَمرُّ عَبْره المعلومات الخاصَّة بشكلها المعمَّى.

3.3 أمن المعلومات الفيزيائي

لا يَكفي أبدًا التركيز فقط على حماية المعلومات الخاصَّة دون الالتفات إلى حماية محيط مالِكها وحماية الأفراد الذين يتعامَلون معها، فتُدعَى حماية المعلومات الخاصَّة والأطراف الذين يتعامَلون معها ومحيط مالِكها، **الأمن الفيزيائي** Physical security، ويُعدّ الأمن الفيزيائي من الاهتمامات الرئيسة في حقل أمن المعلومات؛ لأنَّ تحقيقه يُمثِّل إطار الأمان الذي يُغطِّي المعلومات والأطراف الذين يتعامَلون معها ومحيط مالِكها، ويَشمَل الأمن الفيزيائي من حيث ترتيب الأولويَّة:

1. حماية الأطراف البشريَّة الذين يتعامَلون مع المعلومات الخاصَّة.
2. حماية المعلومات الخاصَّة.
3. حماية محيط مالِك المعلومات.

تُصنَّف حماية الأطراف في الدرجة الأولى في الأمن الفيزيائي؛ لأنَّ الأطراف البشريَّة (وخاصَّةً الخبيرة منها) تُعدّ المَسْنَد الذي تَتَّكِئ عليه جميع الأعمال التي تَتَّصِل بالمعلومات، فإذا حَصَل مثلًا، وتَضرَّرت المعلومات الخاصَّة، يُمكِن استعادتها من النُّسَخ الاحتياطيَّة منها، وإذا حَصَل، وتَضرَّرت المعدَّات والتجهيزات المتعلِّقة بالمعلومات

والموجودة جميعًا داخل محيط مالِك المعلومات، يُمكِن استبدالها من خلال شراء معدَّات وتجهيزات أخرى. أمّا الأطراف البشريَّة فلا يُمكِن تعويضها إلا بصعوبة بالغة، إذْ هي المحرِّك الأول في إدارة جميع الأعمال التي تَستثمِر المعلومات الخاصَّة؛ لذا فإذا حَصَل، وتَضرَّرت الأطراف البشريَّة تَضرَّر معها جميع تِلْك الأعمال، حتى ولو كانت هذه المعلومات والمعدَّات بحالة سليمة، وتَتضمَّن حماية الأطراف البشريَّة في الأمن الفيزيائي تأمينهم من جميع أشكال الأذى الجسدي أو النفسي الذي قد يَتعرَّضون له داخل محيط مالِك المعلومات.

والاهتمام الثاني في قائمة أولويَّة الحماية في الأمن الفيزيائي هو المعلومات الخاصَّة، وهي الحماية التي تتضمن إجراء النَّسْخ الاحتياطي لها وحماية هذه النُّسَخ، وتتضمن إتلافها وإتلاف جميع النُّسَخ بعد الانتهاء من استثمارها، و**النَّسْخ الاحتياطي للمعلومات** Backing –up information هو عملية إنشاء نُسَخ متطابقة (واحدة على الأقل أو أكثر) من النسخة الأصليَّة للمعلومات الخاصَّة بهدف استعمالها لاحقًا عند تَعرُّض النسخة الأصليَّة من المعلومات للتخريب، وتَتضمَّن هذه العملية إمّا نَسْخ أشرطة أو أقراص التخزين مرَّات عدَّة إذا كانت المعلومات رقميَّة، أو تصوير الوثائق والمستندات مرَّات عدَّة إذا كانت المعلومات ورقيَّة. أمّا **إتلاف المعلومات** Destroying information فهو عملية التخلُّص من المعلومات الخاصَّة عند الانتهاء تمامًا من استثمارها. إنَّ عملية إتلاف المعلومات ضرورية من أجل عدم استعمالها لاحقًا من قِبَل أفراد بشريَّة أخرى يُمكِن أن تَستغلَّها، وتُؤذي مالِكها، وتَتضمَّن عملية إتلاف المعلومات إمّا مَحو جميع المعلومات المخزَّنة على الأقراص الصلبة باستخدام برامج متخصِّصة، وإتلاف جميع الأشرطة والأقراص التي تَحتوي على المعلومات، وإتلاف جميع النُّسَخ أيضًا، وذلك من خلال تخريب هذه الأشرطة والأقراص وتمزيقها على نحوٍ مُحكَم، بحيث يَستحيل استعادتها أو استعادة المعلومات منها، وكلُّ ذلك بلا ريب إذا كانت المعلومات رقميَّة،

أو تمزيق الوثائق والمستندات التي تَحتوي على المعلومات الخاصَّة باستخدام معدَّات مخصَّصة لذلك أو إحراقها وإتلاف جميع النُّسَخ المصوَّرة إذا كانت المعلومات ورقيَّة.

والاهتمام الثالث في قائمة أولويَّة الحماية في الأمن الفيزيائي هو محيط مالِك المعلومات، ويَشتمِل محيط مالِك المعلومات على كلِّ المعدَّات والتجهيزات التي تَرتبِط من قريب أو من بعيد بالمعلومات، وتَتضمَّن هذه الحماية اختيار الموقع الفيزيائي المناسب للمعدَّات والتجهيزات التي سَتحتوي على المعلومات وتَقييد الوصول إليها إلا من قِبل الأطراف البشريَّة المُجَاز لها ذلك، وتَوفير الظروف البيئيَّة المناسبة للمحافظة على سلامة هذه المعدَّات والتجهيزات.

ويُمكِن تحقيق الأمن الفيزيائي باستخدام **ضوابِط الأمن الفيزيائي** Physical security controls، وهي مجموعة من الأدوات والأفراد البشريَّة والمواد الإعلاميَّة التحذيريَّة التي تُسهِم في تحقيق الأمن الفيزيائي، وثَمَّة ثلاثة أنواع من ضوابِط الأمن الفيزيائي هي: **ضوابِط رادِعة** Deterrent controls، **وضوابِط كَشْفيَّة** Detective controls، **وضوابِط وقائيَّة** Preventive controls، والضوابِط الرادِعة هي الضوابِط المُصمَّمة لتثبيط الأفراد عن السعي لانتهاك أمان المعلومات أو محيطها أو محيط مالِكها، ومن أمثلة هذه الضوابِط شارات إعلاميَّة تحذيريَّة في الأماكن الخارجيَّة لمحيط مالِك المعلومات تُنبِّه إلى أنَّ المكان مُراقَب بكاميرات التصوير. أمّا الضوابِط الكَشْفيَّة فهي الضوابِط المخصَّصة لاكتشاف أي انتهاك لأمان المعلومات أو محيطها أو محيط مالِكها عند وقوعه، ومن أمثلة الضوابِط الكَشْفيَّة أجراس الإنذار التي تُطلَق عند القيام بمحاولة اقتحام أو دخول غير مرخَّص في أحد أماكن محيط مالِك المعلومات، وأمّا الضوابِط الوقائيَّة فهي الضوابِط التي تُستعمَل لمَنْع الأفراد من انتهاك أمان المعلومات أو محيطها أو محيط مالِكها، ومن أمثلة ذلك الأقفال المركَّبة على أبواب الأماكن في محيط مالِك المعلومات والحرَّاس وكلاب الحراسة.

4.3 الولوج أو النفاذ إلى المعلومات

تَحتوي معظم المراجع في حقل أمن المعلومات على تفاصيل موسَّعة ودراسات كثيرة في طُرُق الولوج إلى المعلومات الخاصَّة والتَّحكُّم فيها، وسوف نَكتفي فيما يأتي بالحديث عن المفاهيم الأساسيَّة فقط.

تَتألَّف آلية الولوج إلى المعلومات من خمس عمليات أساسيَّة هي بالترتيب: **إثبات الهويَّة** Identification، **والتأكيد أو التحقق** Verification، **والمصادَقة** Authentication، **والترخيص** Authorization، **وضَبْط الوصول إلى المعلومات** Access control.

إثبات الهويَّة هو العملية التي يُقدِّم فيها طرفٌ ما هويَّته التي تَتضمَّن معلومات أساسيَّة عنه إلى الجهة المسؤولة عن مَنْحه إذن الولوج إلى المعلومات، وقد تَكون الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات إمّا طرفًا بشريًّا أو برنامجًا حاسوبيًّا، وإنَّ عمليَّة إثبات الهويَّة هي مجرَّد ادِّعاء حامِل الهويَّة بملكيَّة هويَّته، ولا تَقتضي بالضرورة أن تَكون معلومات الهويَّة صحيحة، أو أنَّها تَعود فعلًا لحامِلها.

أمّا التأكيد أو التحقق فهي العمليَّة التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بفَحص الهويَّة التي قَدَّمها الطرف البشري للولوج إلى المعلومات، ولا تَتضمَّن هذه العمليَّة إلا التأكُّد من أنَّ حامِل الهويَّة قد قَدَّمها فعلًا دون إثبات صحَّة ما فيها من معلومات أساسيَّة وصحَّة أنَّها تَعود فعلًا إلى حامِلها.

وأمّا المصادَقة فهي العمليَّة التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بالتَّحقُّق من أنَّ المعلومات الأساسيَّة الواردة في الهويَّة المقدَّمة إمّا صحيحة بالكامل، وأنَّها تَعود فعلًا إلى حامِلها أو أنَّها مزوَّرة، ومن ثم التقرير رسميًّا بما سَبَق.

وأمّا الترخيص فهو العملية التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بالسماح للطرف البشري الذي قَدَّم هويَّته، وتَمَّت المصادَقة رسميًّا على صحَّتها بالوصول إلى المعلومات الخاصَّة.

وأمّا ضَبْط الوصول إلى المعلومات فهو العمليَّة الأخيرة التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بتحديد مستويات الوصول لجميع الأطراف (المستخدِمين) الذين يتعامَلون مع المعلومات الخاصَّة كُلٌّ بحسب حاجته من هذه المعلومات، وتَتضمَّن هذه العمليَّة تَقييد حريَّة وصول كل طرف بشري إلى المعلومات الخاصَّة التي لا يَحتاج إلى استثمارها.

5.3 التعمية من المقومات الأساسية لأمن المعلومات

تقنية التعمية (أو التشفير) هي المكوِّن الأساسي لأي مجموعة إجراءات في أمن المعلومات، وقد بَدَأ استعمال التعمية منذ القدم عندما أراد الإنسان أن يَحمي معلوماته الخاصَّة بطريقة لا يَحتاج فيها إلى إخفائها فيزيائيًّا، وكانت التعمية (ولا تزال) الأداة الفعَّالة لتَبادُل المعلومات العسكريَّة. أمّا الآن فقد أصبحت التعمية ضرورة لحماية أي معلومات خاصَّة، سواء أكانت عسكريَّة أم مدنيَّة عند خزنها أو تبادلها، وفي حقل أمن المعلومات تُعدّ تقنيَّة التعمية الأداة الرئيسة التي تَنطوي داخل أي مجموعة من الإجراءات المضادَّة لحماية المعلومات الخاصَّة المعدَّة للتخزين أو المعدَّة للنَّقل.

ثَمَّة نوعان من التعمية هما: **التعمية ذات المفتاح المتماثِل** Symmetric –key cryptography **والتعمية ذات المفتاح غير المتماثِل** Asymmetric–key cryptography 15. تَستخدِم التعمية ذات المفتاح المتماثِل المفتاح نفسه، ويُدعَى **المفتاح السرِّي** Secret key، من أجل تعمية النص الواضح وفك تعمية النص المعمَّى. أمّا التعمية ذات المفتاح غير المتماثِل فتَستخدِم مفتاحين مختلفين: الأول من أجل تعمية النص الواضح، ويُدعَى **المفتاح العام** Public key، والثاني من أجل فك تعمية النص المعمَّى، ويُدعَى **المفتاح**

الخاص Private key. جَاءَت التعمية بالمفتاح غير المتماثِل لحَلِّ مشكلة تَبادُل المفاتيح السريَّة في التعمية بالمفتاح المتماثِل عبر الشبكات غير الآمنة. أيضًا، ثَمَّة نموذجان للمعمِّيات التي تَستخدِم المفاتيح المتماثِلة، هما: **المعمِّيات الكتلوية** Block ciphers و**المعمِّيات التسلسليَّة** Stream ciphers، والمعمِّي الكتلوي هو المعمِّي الذي يقوم بتعمية النص الواضح كتلةً كتلة من البيانات حجمها 64 بتًّا أو أكبر. أمّا المعمِّي التسلسلي فهو المعمِّي الذي يَقوم بتعمية النص الواضح خانةً خانة (بتًّا بتًّا) من البيانات.

تُستخدَم التعمية أيضًا لأغراض غير أغراض حماية المعلومات من الاطلاع غير المشروع عليها، مثل الحفاظ على سلامة المعلومات من تغيير أي خانة أو حرف فيها، والتقنيَّة التي تُسهِم في الحفاظ على سلامة المعلومات هي **تابع البصمة أو الحشوة** Hash function، ويَأخُذ تابع البصمة كدَخْلٍ إمّا وسيطًا واحدًا هو معلومات فقط أو وسيطين هما: معلومات ومفتاح سرِّي، ويُعطي كخَرْجٍ قيمة تُدعَى **قيمة البصمة** Hash value، وعندما يَتِمّ تعديل أو إضافة أو إزالة بت واحد إلى المعلومات التي طُبِّقَ عليها تابع البصمة تَتغيَّر قيمة البصمة كليًّا، وذلك يَدلُّ بشكلٍ صريح على عملية تَلاعُب بتِلْك المعلومات.

ثَمَّة تقنيَّة مهمة من تقنيات التعمية ذات المفتاح غير المتماثِل هي **التوقيع الرقمي** Digital signature. تَستنِد هذه التقنيَّة إلى قيام مرسِل الرسالة بتوقيعها من خلال تطبيق تابع عليها باستخدام مفتاحه الخاص وإلحاق خَرْج هذا التابع (الذي يُعدّ بمنزلة التوقيع) بالرسالة، ومن ثم قيام مستقبِل الرسالة بتطبيق التابع نفسه عليها باستخدام المفتاح العام للمرسِل والتأكُّد من مطابقة خَرْج العملية مع التوقيع الملحَق مع الرسالة، والهدف الرئيس من التوقيع الرقمي هو مَنْع مرسِل الرسالة من نكرانها، إضافة إلى التأكد من شخصية المرسل، فمطابقة خَرْج تطبيق تابع التوقيع الرقمي باستخدام المفتاح العام لطرفٍ ما مع التوقيع الملحَق مع الرسالة يُلزِم مرسِل الرسالة بتَحمُّل مسؤوليات الرسالة ومضامينها ومَنْعه من نكران إرسالها.

تُطبَّق تقنيَّة التعمية على كلٍّ من المعلومات الرقميَّة والمعلومات الورقيَّة، وتطبيق التعمية على المعلومات الورقيَّة يَقتصِر فقط على استخدام المعمَّيات التقليدية، وحديثًا، وبتَطوُّر علم التعمية وتَطوُّر خوارزمياتها وتعقيدها، أصبَحَت التعمية تُطبَّق على المعلومات الرقميَّة فقط، أمّا التقنيات الأخرى مثل توابع البصمة والتواقيع الرقميَّة، فلا تُطبَّق إلا على المعلومات الرقميَّة فقط.