٩٧

إدارة أنظمة المعلومات
Information Systems Management

Elliot B. Sloane
Assistant Professor, Department of Decision and Information Technology, Villanova University, Villanova, PA

لقد أصبحت أنظمة المعلومات (IS) في نواحٍ كثيرة بنية تحتية ضرورية قياسية وأساسية في مجال الرعاية الصحية بشكلٍ يشبه اعتماد هذا المجال على الكهرباء والمياه النظيفة وأنظمة التدفئة والتهوية وتكييف الهواء الملائمة. ومن المحتمل أن يستمر هذا الدور في التوسع مُغطياً تقريباً كل العمليات التجارية وعمليات الرعاية الإكلينيكية. يوفر هذا الفصل إطار عمل للمهندس الإكلينيكي(CE) وتقني الهندسة الطبية الحيوية (BMET) لاستخدامه في إدارة المهنة في السنوات المقبلة. حاول بعض الـ CEs و BMETs النأي بأنفسهم عن أنظمة الكمبيوتر الشخصية والتجارية في تسعينيات القرن الماضي منوهين إلى عدم جدوى هذه الأنظمة في رعاية المرضى. ولحسن الحظ لم يعد هذا النقاش مفيداً باعتبار أن معظم أنظمة الأعمال التجارية والأنظمة الإكلينيكية تُشارك معظم عناصر البيئات الصلبة والبرمجيات المعروفة بغض النظر عن التطبيق. ساهمت العوامل الثلاثة الرئيسية التالية في تشكيل حالة أنظمة الـ IS الحالية: (١) الانخفاضات السريعة في أسعار تجهيزات الـ IS والزيادات السريعة في قوة الحوسبة، (٢) التوحيد القياسي وموثوقية البيئات الصلبة والبرمجيات، (٣) استقرار معايير اتصالات البيانات. يتم في أيامنا هذه تطوير العديد من الأنظمة المعقدة عن طريق استخدام مزيج من العناصر التجارية الجاهزة للبيع (COTS) أو عناصر مختلفة منها مما يجعل تطبيق تصميم النظام الموحد وتنفيذه ومهارات الدعم لكامل نظام الرعاية الصحية أسهل بكثير.

سوف يجد القارئ الذي يسعى وراء التدريب التقني العديد من المصادر المناسبة على شبكة الإنترنت وفي محلات بيع الكتب والمكتبات وكليات الهندسة وكليات المجتمع. ولذلك فقد كُتب هذا الفصل لمدير الهندسة الإكلينيكية الذي يجب عليه توفير قيادة للتكنولوجيا في مؤسسات الرعاية الصحية. تُركز المواضيع التي تتبع على المسائل الإدارية المهمة بدلاً من الموضوعات التقنية المُعمقة.

تقارب أعمال أنظمة المعلومات والتكنولوجيات الإكلينيكية في الرعاية الصحية
Convergence of Health Care's Business IS and Clinical Technologies

نظراً لانخفاض تكلفة المعالِجات القياسية والحساسات والذاكرات وأجهزة اتصالات البيانات السلكية واللاسلكية إلى بضعة دولارات لكل عنصر فإنه يتم استخدام هذه العناصر بشكلٍ مطلق ومُنتشر في جميع أنحاء المؤسسات. قد لا يكون الوقت بعيداً عندما تتمتع تقريباً كل الأجهزة الكهربائية والكهروميكانيكية بالقدرة على التقاط وتخزين وتحليل توصيل البيانات للمساعدة في تعزيز أداء وموثوقية هذه الأجهزة وإتاحة الفرصة لها للمساهمة في أداء وموثوقية النظام الكلي. إن القيمة الكامنة لهذه التكنولوجيا هي في قدرتها على تكوين ومراقبة أداء وسلامة الجهاز الذي تضبطه وقدرتها على توصيل بيانات أداء ومشاكل الجهاز والبيانات ذات الصلة بالمرضى إلى جميع أرجاء "الجهاز العصبي" لنظام الـ IS في المؤسسة. يمكن لهذا في نهاية المطاف أن يسمح بالموثوقية من خلال تبادل الآراء حول المشاكل في وقتٍ مُبكر وبشكل أكثرُ شموليةً ويمكنه أن يتحمل سلامة وتكرارية أكثر من خلال مُشاركة موارد الحوسبة عند حدوث المشاكل.

تجد مؤسسات الرعاية الصحية من الناحية العملية أن أعداداً متزايدة من الأقسام (سواء كانت إدارية أو تنفيذية أو إكلينيكية) قادرة على الربط أو المشاركة المباشرة لموارد الـ IS الكاملة أو الجزئية (مثل أجهزة الكمبيوتر والذاكرة/التخزين ومسارات الاتصالات وأجهزة الدخل/الخرج). قارَبَ ذلك بين مجموعات دعم أنظمة المعلومات ومجموعات التكنولوجيا الطبية الحيوية من الناحية الفنية ولكنه أيضاً خلق في بعض الأحيان صراعات نفوذ. تتطلب الإدارة الناجحة لهذه التكنولوجيات المتقاربة والمنتشرة تعاون جميع الأطراف لضمان تلقي المُستخدمين الإكلينيكيين والمرضى دعماً سلساً وموثوقاً بأكبر قدر ممكن من الكفاءة. يتطلب القيام بذلك التزاماً طويل الأجل للتعلم واكتساب الخبرة وفي نهاية المطاف إدارة هذه التكنولوجيات بشكلٍ مهني. يهدف هذا الفصل إلى المساعدة في جعل ذلك ممكناً من خلال تمكين المهندسين الإكلينيكيين وتقنيي الأجهزة الطبية الحيوية من فهم مجال الـ IS بشكلٍ أفضل.

يمكن في يومنا هذا التقاط لُبنات البناء الأساسية للبنية التحتية لأنظمة الـ IS في مجالات تصميم ومنهجيات إدارة أنظمة الـ IS والأجهزة والبرمجيات الحاسوبية وتخزين وتبادل البيانات. سوف تُساعد المعلومات التالية حول هذه المجالات كلاً من المهندسين الإكلينيكيين والتقنيين في المشاركة بشكلٍ أكثر فعاليةً.

تحليل وتصميم وإدارة الأنظمة
System Analysis, Design, and Management

إن الموضوع الأول الذي يجب مناقشته هو تحليل وتصميم وإدارة نظام الـ IS لأن يجب (وبحكم الضرورية) على الغرض والبيئة المقصودين للاستخدام أن يُحددان الأجهزة والبرامج التي سيتم استخدامها. ورغم أن معظمها

نصوص الـ IS تغوص عميقاً في منهجيات دورة الحياة للأنظمة بالنسبة إلى المهندس الجديد أو إلى طالب الأعمال التجارية فإن ذلك يجب ألا يكون مجالاً جديداً بالنسبة إلى تقنيين الرعاية الصحية. تشمل تقنيات تقييم تكنولوجيا الصحة وتحليل تكاليف دورة الحياة حالياً على استخدام أدوات أنظمة دعم القرار المحوسبة والمرنة. يجب على القارئ أن يفترض أن جميع المشاريع تقريباً تتطلب عدة مراحل تحليل دقيقة لفهم الجدوى والنتائج المترتبة على قرار الـ IS. ومن المرجح أن يحتاج نظام الرعاية الصحية لأن يتعايش لسنوات عديدة قادمة مع كل نظام IS يتم تثبيته وأنه من المُرجح أيضاً أن تتأثر النفقات الشاملة العامة واعتمادية وكفاءة المؤسسة لدرجة كبيرة بكل نظام IS. لا تختلف الاهتمامات الرئيسية لتصاميم أنظمة الـ IS للرعاية الصحية عن اهتمامات أي تكنولوجيا طبية. فيما يلي النواحي التي يجب الاهتمام بها بالنسبة إلى النظام الذي يتم اختياره:

- يجب تقييم النظام باستخدام مجموعة دقيقة من المواصفات التي تصف الميزات الضرورية وأولوياتها النسبية.
- يجب أن تتم تهيئته بشكلٍ صحيح لكي يتكامل بشكلٍ فعال وموثوق مع أنظمة الـ IS الحالية والمستقبلية للمؤسسة.
- يجب أن يتم تركيب النظام واختبار أداءه السليم وفقاً للمواصفات المكتوبة وذلك قبل قبوله.
- يجب أن يُدرَج في برنامج إدارة التكنولوجيا الجاري في المؤسسة لضمان أعمال الاختبار والصيانة والإصلاح الموثوقة.

تحليل الاحتياجات Needs Analysis

في يومنا هذا، لا تُعتبر عملية وضع المواصفات الكافية وإجراء التقييم الكافي مهمةً بسيطة وليس من المحتمل أن تُصبح سهلة في المستقبل القريب. في ظل غياب معايير FDA واضحة للأجهزة الطبية أو للبرمجيات الطبية أو للعوامل البشرية فقد انتهج معظم الباعة منهج التصاميم الخاصة بهم والفريدة من نوعها في أغلب الأحيان. ومن ثم فإن خيارات الـ IS المتاحة في كل تخصص لسوق الرعاية الصحية تختلف بشكل واسع في الميزات والتكلفة الإجمالية للملكية والتوافق العام. لذلك فيجب على المؤسسة أن تتبع سياسة الـ "Caveat emptor" أي مسئولية معرفة أي خلل في النظام الذي تقتنيه. ويجب أن يبدأ ذلك بإجراء تحليل دقيق للحاجة الفعلية التي ينبغي على النظام إنجازها والأنظمة الأخرى التي ينبغي أن ترتبط بشكلٍ ناجح مع هذا النظام. حتى لو كانت المؤسسة تعتقد أن الترابط غير ضروري فيجب على المرء أن يكون حذراً عند التخلي عن هذا الخيار. سوف تظهر في كثير من الأحيان الحاجة إلى التوسع في النظام و/أو دمجه في مهمة أكبر، وعند ذلك فإن تكلفة الربط الخاص في تلك المرحلة يمكن أن تكون هائلة. إضافة إلى ذلك فيجب على المرء أن يكون على يقين من إمكانية الكادر المُستهدف لتعلم هذا النظام بكفاءة وفعالية. على الرغم من إجراء البحوث المتعلقة بمجال العوامل البشرية على مدى عدة عقود، ما يزال العديد من

مطوري الـ IS لا يخصصون الوقت الكافي لفهم الأشخاص والمهارات والبيئة في مجال الرعاية الصحية. يمكن لتصاميم الـ IS المُصممة بشكلٍ سيئ أن تُسبب مشاكل تدريب كبيرة وغير قابلة للحل التي تؤدي إلى معدلات خطأ لا يمكن تحملها و/أو هجر النظام لأن استخدامه يمكن أن يكون أسوأ من عدم وجوده.

التكلفة الإجمالية للملكية Total Cost of Ownership

يجب على التقييم الدقيق للنظام أن يأخذ التكلفة الإجمالية للملكية (Total Cost of Ownership, "TCO") بعين الاعتبار (انظر الفصل ٣٠). أصبح العديد من الصناعات الأخرى يُقدر التكاليف الخفية بقدر ما يُقدر تكاليف الشراء الواضحة أو حتى أكثر. يُنصح عند القيام بتحليل الـ TCO لمشروع نظام الـ IS النظر في العواقب المترتبة على التبني الناجح ونمو الحاجة إلى الأجهزة والبرمجيات الإضافية والدعم الإضافي لفترة السنوات الثلاثة أو الخمسة التي تلي الاقتناء. ومن المثير للاهتمام أن نرى كيف فشلت الكثير من تحليلات الـ IS في التخطيط للنجاح رغم أن ذلك كان هو المأمول من عملية الاقتناء. يؤدي النجاح في كثير من الحالات إلى عدد أكبر من المُستخدمين وزيادة الاعتماد على النظام وساعات استخدام أطول وتزايد مستمر في مطالب التخزين والاسترجاع ودعم أكبر للطباعة وإمكانية الوصول عن بعد والأمن، وفي نهاية المطاف الاندماج مع موارد الـ IS الأخرى في المستشفى. يمكن تقييم وضبط قدرة الأجهزة والبرمجيات الإضافية بسهولة أكبر إذا استخدم الـ IS كميات كبيرة من أجهزة وبرمجيات الـ COTS. كلما أصبح قسم نظام الـ IS الذي لا يعتمد على الـ COTS أكبر، أصبحت التكاليف والمخاطر أكثر غموضاً. يجب على المرء ألا يستبعد برمجيات التطبيق المتأصلة من هذا التقييم، فإذا لم تعتمد هذه البرمجيات على أنظمة تشغيل ولغات وحزم برمجيات إدارة البيانات ذات معايير خاصة بهذه الصناعة، فيمكن أن تُصبح الطبيعة وحيدة المصدر للنظام مكلفة بشكلٍ متزايد ومحدودة بشكل غير مريح. إذا أدت النتيجة السعيدة لاختيار وتنفيذ الـ IS إلى الاستخدام الناجح والتبني فينبغي على المرء أن يُخطط بعناية لضمان أن ميزانية المؤسسة ستُمكّن الـ IS من تلبية المتطلبات الموثوقة للاستخدام. سرعان ما تُصبح الأنظمة الناجحة في الرعاية الصحية "أنظمة مهمة للأعمال" يعتمد عليها الكثير من الأشخاص والكثير من عمليات تقديم الرعاية الصحية. يتطلب ذلك عادة تحسين التغذية الكهربائية وضبط درجة الحرارة والرطوبة وموارد لسعة النظام والاستقرار والنسخ الاحتياطي والاسترداد وزيادة القدرة على تبادل البيانات. سوف يقلل تحليل الـ TCO الذي لا يعالج هذه القضايا بشكلٍ صارخ من تقدير الميزانية المطلوبة لدعم مشروع الـ IS. نادراً ما يوجد مُنتج IS "مثالي" لكي يتم اختياره، حيث يُقدِّم كل مُنتَج مُفاضلات مختلفة بل معقدة في بعض الأحيان. مرة أخرى، ينبغي أن يكون تحذير "Caveat emptor" راسخاً في الأذهان باعتبار أن البائع نادراً ما ينوه إلى هذه القضايا في تحليله الخاص. إذا كان مشروع الـ IS باهظ التكلفة ومُرجح لأن يُصبح ناجحاً كونه سيُصبح جزءاً من البنية التحتية للمؤسسة لبعض الوقت، فقد يكون من المفيد استخدام أحد أنظمة دعم القرار(مثل عملية التحليل

الهرمي، Analytic Hierarchy Process) (Schmoldt et al، ٢٠٠١) للمساعدة في توثيق وتثقيل الإيجابيات والسلبيات.

تثبيت وقبول النظام System Installation and Acceptance

أصبح تركيب واختبار قبول النظام في المستشفى في يومنا هذا أكثر تعقيداً وخاصة لأنه يجب على العديد من منتجات الـ IS أن تتقاسم البنية التحتية الكهربائية والبنية التحتية لتبادل البيانات، وفي الواقع تتقاسم بعض الأنظمة أموراً أكثر من ذلك بكثير بما في ذلك المحطات الطرفية والطابعات وتخزين البيانات. ينبغي على وثائق الشراء من المؤسسة أن تُلزم البائع بتقديم وسائل اختبار قبول مُحدَّدة تضمن التفصيل الكامل لواجهات الربط مع موارد الـ IS الأخرى القائمة أو المخطط لها. إذا حُذفت هذه التفاصيل فلا مفر من توجيه أصابع الاتهام كما يمكن أن يتعرض كل من الارتياح النهائي للمستخدم والتثبيت الناجح وفقاً للميزانية إلى خطر شديد. يتطور المجال الـ IS بسرعة كبيرة كما أن هناك فقط القليل من المعايير الكاملة تماماً، وإضافة إلى ذلك هناك عدد قليل من الباعة الممتثلين تماماً لجميع جوانب المعايير الموجودة. في كثير من الأحيان فإن لأفضل معايير الرعاية الصحية ثغرات ويعود أحد أسباب ذلك إلى التغير السريع في الطب وتجارة الرعاية الصحية. تستغرق كتابة معظم المعايير عدة سنوات، وفي الوقت الذي تُنشر وتُعتمد فيه هذه المعايير يكون قد تم تبني تغييرات رئيسية جديدة في البيئة مثل رعاية المرضى الخارجيين والجراحة الروبوتية والتطبيب عن بعد أو تجميعات الأدوية/الأجهزة الهجينة. إذا لم يكن نظام الـ IS الجديدة قادراً على التكيف مع النظام القائم أو المخطط له أو إذا كانت هناك تغييرات مطلوبة على النظم القائمة أو المخطط لها، عندئذ قد يحتاج تحليل الـ TCO إلى أن يعكس التكاليف الإضافية الكبيرة لكي يتم إظهار هذا الأثر بشكلٍ دقيق.

الصيانة Maintenance

من المرجح أن تطلب الإدارة القائمة لمشروع الـ IS الجديد مزيجاً من دعم الصيانة والإصلاح من المستخدمين والمهندسين والفنيين الداخليين وكذلك الاستعانة بالمصادر الخارجية. قد تقع بعض المسؤوليات (مثل تغيير الورق وخراطيش الحبر للطابعات وإعادة مُعايرة الطابعات وشحن البطاريات والحفاظ على النسخ الاحتياطية) على عاتق المستخدمين أو الأقسام التي يعملون بها. حتى لو تم ذلك فإن تكاليف التدريب وإعادة تدريب الكادر وتكاليف اللوازم الضرورية تنتمي إلى تحليل الـ TCO الدقيق. تؤسس بعض المؤسسات أو تُبرم عقداً ثانوياً لخدمات "مكتب مساعدة" (انظر الفصل ٩٩) لمساعدة المستخدمين، وإذا كان الأمر كذلك فيمكن أن تُخصَّص التكاليف النسبية الموالية (pro-rata costs) إلى مشروع الـ IS الجديد. على الرغم من أن هناك حاجة نادرة للصيانة الوقائية المقعدة لتكنولوجيات الـ IS، فإنه من الحكمة تخصيص بعض الموارد للكنس المنتظم للغبار وتنظيف المرشحات واستبدال البطاريات المهمة وإدارة وتحسين حجم قرص التخزين على النحو المطلوب من قبل النظام. إن مهمة الصيانة الأخرى

التي غالباً ما يتم تجاهلها هي إنشاء أقراص أو أشرطة النسخ الاحتياطي والفحوصات الدورية الروتينية لضمان أن هذه النسخ هي في الواقع قابلة للاستخدام. يمكن أن يكون ضمان قابلية الاستخدام أكثر تعقيداً بكثير ويمكن أن يستغرق وقتاً أطول مما كان متوقعاً في البداية لأن إجراء الفحص المناسب قد يتطلب الوصول إلى نظامٍ كامل ومماثل. وإلا فقد لا يكون للفحص فائدة كبيرة عند تعرض النظام الأصلي إلى فشلٍ ذريع. يمكن أن تكون النسخ الاحتياطية عديمة الفائدة إذا لم تكن هناك إمكانية لقراءتها من قبل نظامٍ مختلف أو إذا لم تكن هناك طريقة لتحديد أو لتجميع نظامٍ بديل مقبول وبشكلٍ سريع.

لقد كانت أعمال الصيانة والإصلاح منذ فترة طويلة ضمن مجال الـ CE والـ BMET. أدى إقرار قانون قابلية نقل ومسئولية التأمين الصحي "HIPAA" (انظر الفصل ١٠٤) إلى زيادة مسؤولية الـ CE والـ BMET لأن العديد من الأجهزة التي تتم عليها أعمال الصيانة تحتوي أو تقوم بتبادل معلومات طبية خاصة بالمرضى بسبب انتشار تكنولوجيات المعالجات الصغرية في مثل هذه الأجهزة. وباختصار، هناك حاجة لوضع ممارسات وسياسات مُحددة لضمان محي البيانات الخاصة بالمرضى قبل إرسال الجهاز إلى الخارج من أجل الخدمة وضمان المحي الكهربائي للذاكرة أو إتلافها مادياً قبل أن يتم التخلص منها أو إرسالها للإصلاح. ينبغي من أجل المزيد من التوجيه بشأن هذا الموضوع الاتصال بالكلية الأمريكية للهندسة الإكلينيكية (ACCE) في موقعها على شبكة الإنترنت (ACCEnet.org)، حيث يقوم فريق مهام الـ ACCE HIPAA حالياً بتطوير بروفيل مخاطر HIPAA لكل جهاز من أجل تسهيل تحديد الأجهزة المتضررة (انظر الفصل ١٣٠). ومع ذلك وفي حالة الشك فإنه من الحكمة أن يتجه المرء إلى جانب الحيطة والحذر واتخاذ احتياطات إضافية لمحو بيانات المرضى كلما كان ذلك ممكناً.

يتعلق القلق الإضافي بالنسبة إلى الصيانة والإصلاح باحتمال أن لا تكون جميع الأجهزة والبرمجيات ونظم الاتصالات متوافقة تماماً حتى عندما تزعم الجهة المُصنِّعة مطابقة معايير الصناعة. يمكن أن يمثل ذلك مشكلةً خطيرة بالنسبة إلى الأجهزة والأنظمة ذات الترتيب البرمجي لأنه قد يكون من الصعوبة بمكان الكشف عن أي عيب صغير أو تعارض أو ترتيب خاطئ غير مقصود أو عدم تناسق آخر. على سبيل المثال، قد يكون من الصعب كشف جهاز العرض المعيب والذي يبدو مُطابقاً للأجهزة الأخرى بسبب تحديد وضوحيته أو تباينه على الوضعية المنخفضة، ففي هذه الحالة فإن هذا الجهاز يمكن أن يُسبب أخطاء تشخيصية أو علاجية كارثية من خلال حذف تفاصيل هامة إكلينيكياً. كذلك يمكن لجهازٍ ما أن يُسبب حالات فشل عامة أخرى في جميع أنحاء نظام الـ IS عندما يتم وصله على الشبكة وذلك بتقييده لهذه الشبكة. على سبيل المثال، يمكن للجهاز الذي يتسبب بإعادة إرسال أو إعادة تهيئة البيانات الرقمية بشكلٍ كثيف في جميع أنحاء نظام الـ IS أن "يُقيِّد" عرض الحزمة المحدود والذاكرة و/أو موارد الحوسبة مما يؤدي إلى إبطاء أو فشل أجزاء أخرى من النظام. إن الطريقة الوحيدة لمنع مثل هذه المشاكل هي تطوير وتوثيق وتنفيذ عملية تحقق حذرة من صحة النظام أو الجهاز في وقت الصيانة أو الإصلاحات. إذا كان النظام العام

لـ IS في المستشفى هو عبارة عن مزيج معقد من تكنولوجيات مختلفة متعددة المصادر وتغطي أجيالاً عديدة من التكنولوجيا، عندئذ يمكن لعملية التحقق هذه أن تكون مرهقة ومكلفة مما يؤثر على الـ TCO.

الخصوصية والأمن Privacy and Security

توجب قوانين HIPAA قانونياً موضوعين مهمين يجب أخذهما بعين الاعتبار في إدارة أنظمة الـ IS في الرعاية الصحية وهما الخصوصية والأمان. من المطلوب قانونياً من كل مؤسسة رعاية صحية تقريباً ضمان أن يكون الأفراد الذين يصلون إلى المعلومات الطبية للمرضى أو معرفة حالتهم هم الأفراد المخوَّلون فقط. لأن الكثير من المعلومات هي الآن في شكلٍ إلكتروني فيجب استخدام البرامج والأجهزة بطريقة تمنع بشكلٍ موثوق الوصول غير المُصرَّح إلى هذه المعلومات. ليس المطلوب كلمات السر فقط، بل أيضاً التحديث الإلزامي لكلمات السر وكذلك التدريب الموثق لمنع تبادل كلمات السر أو المعلومات الخاصة. ولفرض الامتثال ولتقييد الوصول إلى المعلومات السرية أو الأنظمة الحساسة مثل الوصفات الدوائية بشكلٍ صارم، يمكن للمؤسسات أن تُنفذ بشكلٍ انتقائي المسح البيولوجي (مثل مسح القزحية أو بصمات الأصابع أو الصوت أو مسح الوجه) و/أو أجهزة ضبط الوصول الشخصي المادية (مثل البطاقات الذكية أو البطاقات الممغنطة أو بطاقات الأشعة تحت الحمراء أو الأزرار ذات الترميز الرقمي). ورغم ذلك، لا تكون هذه الإجراءات الأمنية فعالة إلا إذا كان الوصول إلى كل محطة طرفية وكل طابعة ومنفذ اتصال ومحرك الأقراص القابل للإزالة مُقتصراً بشكلٍ مادي على الأشخاص المخولين وللمدة الزمنية التي يُعتزَم استخدام هذه الإجراءات الأمنية فيها.

يوجِّه جانب الخصوصية الذي يتعلق بتقييد إمكانية الدخول إلى الـ IS هذه المناقشة إلى أحد المظاهر الهامة للأمن من حيث ضمان عدم إمكانية الأفراد غير المخولين من الدخول إلى نظام الـ IS. إن ضرورة الحماية المادية هي ليست فقط لموارد الـ IS ضمن المؤسسة وإنما هي أيضاً ضرورية لمنع احتمال الدخول من قبل الأشخاص الخارجيين. تأتي أشد المخاطر الخارجية عن طريق قنوات الاتصال إلى الـ IS بما في ذلك التنصت غير المصرح به في الشبكات السلكية أو اللاسلكية والاتصالات وشبكة الإنترنت والهاتف/المودم. يمكن معالجة الخطرين الأخيرين من خلال مزيج من جدران الحماية للأجهزة والبرمجيات إلا أن معالجة مسائل الشبكة يمكن أن تكون صعبةً بالفعل. تتعلق المسألة بالمفاضلة بين إمكانية الوصول المريح وإمكانية الوصول غير المكلف، وإعادة تشكيل محطات الشبكة السلكية ومحطات الشبكة اللاسلكية، والحاجة إلى الأمن. قد لا تترك عقوبات انتهاك قانون الـ HIPAA إلا بديل احتضان تكلفة وتعقيد القيود الرسمية للشبكة، لكنها قد تستغرق على الأرجح بعض الوقت والمراجعات لضمان عدم إهمال أو نسيان الخطوات الضرورية. قد يتطلب "التأمين الجيد" للشبكة على الأرجح الاستثمار في تقنيات التشفير ووضع سلطة الوصول إلى الشبكة وضبطها في أيدي عدد قليل من موظفي الدعم الرئيسيين وهو الأمر الذي يمكن

أن يؤثر على تحليل الـ TCO. قد يُصبح ضمان توفر هؤلاء الأفراد كلما لزم الأمر وتزويدهم بالأجهزة والبرمجيات المناسبة التكلفة الأكثر وضوحاً لمؤسسات الرعاية الصحية. ما يزال جانبين آخرين من جوانب الأمن يستحقان التنويه حيث يتعلق كليهما بضمان سلامة البيانات الطبية للمريض لأن هذه البيانات يمكن أن تؤثر مباشرةً على التشخيص و/أو العلاج. أساساً، يقع على المؤسسة عبء ضمان حماية البيانات الطبية لكل مريض من الضرر غير المقصود أو غير المرئي والتغيير أو الفقدان الجزئي أو التام. لا تُعتبر وسائل القيام بذلك بسيطة حيث تتطلب وجود مزيج صائب من الأجهزة والبرمجيات والإجراءات من أجل الامتثال. تُعتبر كل من الحماية المادية للنظام وعمليات النسخ الاحتياطي للبيانات وممارسات التعافي من الكوارث كما تمت مناقشته آنفاً جزءاً من الحل. بالإضافة إلى ذلك، قد تكون هناك حاجة إلى أجهزة وبرمجيات تحسين موثوقية النظام كما هو موضح في فقرات النظام والاتصالات فيما يلي.

مكونات أنظمة المعلومات
IS System Components

عرَّف Von Neumann المكونات الرئيسية للـ IS كلاسيكياً بأنها الدخل/الخرج والذاكرة والقدرة المنطقية/الحسابية. عندما يتم تجميع هذه العناصر الثلاثة فإنها تؤدي مهام الحوسبة باتباع متواليات من التعليمات الموضوعة بحذر التي تتمثل في البرامج التي يقدمها المطورون. يمكن من الناحية العملية توسيع الدخل/الخرج ليشمل الأجهزة المادية (مثل لوحات المفاتيح والطابعات والإظهارات) والحساسات البيولوجية (مثل تخطيط كهربية القلب وضغط الدم وقياس التأكسج النبضي) وجميع أنواع وتكنولوجيات الاتصالات التي تنقل البيانات من مكانٍ إلى مكانٍ آخر. يمكن لعناصر الذاكرة أن تكون: (١) ستاتيكية (ذاكرة PROM أو EPROM قابلة للبرمجة أو قابلة للمحي) أو (٢) ذاكرة وصول عشوائي ديناميكية (RAM) التي قد تكون إما في شكل رقائق منفصلة أو متأصلة في ضمن تغليف المُعالج الصغري أو (٣) سواقات أقراص ذات أشكال كثيرة بما في ذلك التخزين الضوئي على CD/DVD والأقراص المغنطة أو سواقات الأقراص الصلبة. أما القدرة المنطقية/الحسابية فيمكن أن تكون في شكل معالجات صغرية عامة الغرض ذات نطاق واسع ومتفاوت من حيث التكلفة والسرعة أو أجهزة منطقية متخصصة ذات تكلفة منخفضة وذات أدوار محدودة.

من المهم قبل مناقشة هذه العناصر بمزيد من العمق إدراك أن انخفاض التكلفة والتصغير من المكونات الإلكترونية قد أدى إلى الكثير من المُنتجات (إن لم يكن معظمها) بأن تكون ذات دخل/خرج وذاكرة وقدرة منطقية/حسابية مُدمجة مما أتاح لها أداء مهمتها بشكلٍ أكثر موثوقيةً ومرونةً. ومن ثم فإن التبسيط الزائد في تعقيدات تكنولوجيات الحوسبة الحالية والمستقبلية قد لا يُعتبر أمراً حكيماً لأنها في الواقع تتكون من أنظمة حوسبة متعددة

ومترابطة. تتطلب أعمال التصميم والتنفيذ والإصلاح الناجحة لمثل هذه الأنظمة فهم دور كل عنصر فضلاً عن وظيفته في إطار النظام الكبير.

تتوسع تحديات التصميم والتركيب والدعم مع تحول المزيد من تكنولوجيات الرعاية الصحية إلى الحواسيب الرقمية المتعددة المترابطة (التقارب الرقمي). ليس فقط يجب على كل جهاز أن يعمل كما تم تصميمه ولكن يجب أيضاً التحقق من أداء النظام بأكمله في كل مرة يحدث فيها تغيير. للأسف قد لا تكون هذه التغييرات مرئية حيث يمكن أن تكون على شكل تغييرات في البرنامج (مثل الترميمات والتحديثات) التي قد لا تكون موثقة أو قابلة للكشف. قد تهتم المعايير الناشئة في حقل الرعاية الصحية في إدارة هذه المشاكل، إلا أن تعددية المصادر والترابط بين التكنولوجيات متعددة الأجيال والمطلوبة في معظم المؤسسات سوف يُبقي على جزء كبير من العبء على كاهل موظفي هذه المؤسسات وليس على الشركات المصنعة أو الوكالات الحكومية.

تكنولوجيات الدخل/الخرج
Input/Output Technologies

تلعب تكنولوجيات الدخل/الخرج دوراً مهماً غالباً ما يتم إغفاله في تطبيقات الرعاية الصحية حيث إنها قد تلحق ضرراً غير مقصود في معلومات الإنسان التي يتم تمثيلها باستخدام هذه التكنولوجيات. إن هذه المشكلة هي نتيجة ثانوية للتحويل اللازمة من الإشارات التناظرية التي تُميز الحياة والطبيعة إلى الإشارات المتقطعة أو الرقمية لمكونات نظام الـ IS. يجب تحويل الإشارات التناظرية للإنسان من الشكل التناظري إلى الشكل الرقمي (A/D) قبل أن يتمكن نظام الـ IS من التعامل معها ومن ثم لا بد في كثير من الأحيان أن يتم تحويلها إلى تمثيل التناظري آخر (مثل شاشة عرض أو طباعة) الأمر الذي يتطلب شكلاً من أشكال التحويل الرقمي- التناظري(D/A). وعلى الرغم من أن تردد ومعدل التغير في معظم أشكال أمواج إشارات الإنسان هو بطيء جداً بالنسبة إلى العديد من مجالات التكنولوجيا الأخرى (مثل الراديو والرادار)، إلا أن دقة عمليات A/D و D/A تعتمد على توفُّر ما يكفي من السرعة والوضوحية والتخزين الآمن والحوسبة الآمنة لضمان عدم ضياع أو تشويه التفاصيل التشخيصية أو العلاجية المهمة. تُقدم إشارة تخطيط القلب (ECG) مثالاً بسيطاً على ذلك: إذا تم التحويل A/D إما ببطء شديد أو بوضوحية قليلة جداً، عندئذ يمكن للبيانات الرقمية التي تم الحصول عليها التي سوف تُستخدم للتداخلات التشخيصية أو العلاجية أن تكون إلى الأبد مُتضررة بسبب فقدان التفاصيل الدقيقة من البداية. والأكثر من ذلك وحتى لو كانت عملية الـ A/D صحيحة، فإذا فشل أي جزء من أنظمة التخزين والاتصالات والحوسبة (التي تتعامل مع البيانات الرقمية) في الحفاظ على (أو تفسير) كل بت (bit) في التمثيل الرقمي بشكلٍ دقيق يكمن أن يؤدي إلى فقدان دائم للمعلومات و/أو تحليل وتداخل غير دقيقين. وأخيراً، حتى لو كان التمثيل الرقمي دقيقاً داخل النظام فإن التحويل الـ D/A غير المناسب إلى صورة بيانية على شاشة الإظهار أو الطابعة يمكن أن يمنع الطبيب من رؤية تفاصيل بالغة الأهمية.

يمكن لمشاكل مرحلة تحويل الـ D/A الأخيرة أن تكون صعبة التفادي بشكلٍ كبير جداً لأنها غالباً ما تعتمد أيضاً على التفسير البصري أو السمعي أو الحسي للمراقب البشري للتمثيل التناظري. ما تزال القدرات الإدراكية وحدود الربط بين الإنسان ومخرجات الحاسوب قيد الدرس، ولكن من الواضح أنه يمكن أن يكون هناك اختلافات أداء واسعة للإنسان والتكنولوجيا يمكن أن تؤثر على النتيجة إلى حدٍ كبير. باستخدام تخطيط كهربية القلب كمثال، قد لا يرى عدداً ملحوظاً من الأطباء تشوهات معينة على الشاشة بسبب عدم قدرتهم على استيعاب حدود أو وضعيات التباين أو الشدة للجهاز. يمكن أن يكون لمثل هذا الخلل العام أن يكون صعب التحديد والإصلاح حالياً باعتبار أن العديد من الأطباء قد يستخدمون إظهارات مختلفة سواء كانت متنقلة أو ثابتة أو محلية أو بعيدة خلال اليوم الواحد.

تُعتبر الأمثلة المذكورة آنفاً بمثابة تحذيرات ينبغي على المهندس الإكلينيكي أو تقني الإلكترونيات الطبية الحيوية أن يأخذها بعين الاعتبار كلما تعامل مع أجهزة الإدخال/الإخراج. وعلى الرغم من أن معظم هذه الأجهزة قد تكون بسيطة وموثوقة جداً بحد ذاتها، فإنها عندما تُدمج في نظام الرعاية الصحية قد تُحد بشدة (ولكن بشكلٍ مخفي) السلامة والموثوقية العامة والأداء العام للنظام من خلال إخفاق الحلقة الأضعف. الخطر الآخر الجديد هو أن العديد من الأجهزة الطبية يمكن أن تُصبح أجهزة الإدخال لعملياتٍ أخرى وهو الأمر الذي لم يؤخذ بعين الاعتبار عند وضع التصاميم الأولية لهذه الأجهزة. يمكن لمنفذ بيانات من مضخة التسريب أن يُصبح مصدر بيانات لنظام تحذير التعارض الدوائي لمصنعٍ آخر أو لنظام رسم سجل المريض. يمكن للعقاقير المكتشفة حديثاً أو تخفيفات الجرعات الجديدة أو الاستخدام غير المتوقع للمضخات القائمة بحد ذاتها من دون منافذ بيانات أن تُلغي السلامة المتوقعة أو الدور الإكلينيكي أو الإداري للنظام.

وبصرف النظر عن المسائل المنهجية المذكورة آنفاً، تستحق بعض جوانب الإدخال/الإخراج الرقمي أيضاً الاعتبار الحذر. نحن نعرف من الخبرة الهندسية الكلاسيكية والإكلينيكية والكهربائية والميكانيكية أنه يجب في كثير من الأحيان تضخيم وترشيح أشكال الموجات التناظرية بعناية لضمان دقة موثوقة. يتم الآن تضمين الكثير من هذه التقنيات في معالجات الإشارات الرقمية (DSPs) التي يمكنها أن توفر مناورة غير باهظة الثمن ومرنة لشكل الموجة باستخدام الحساب بدلاً من المكثفات أو الملفات. تسمح الـ DSP بالتصاميم المعقدة للمُرشحات التي يمكن أن تكون صعبة ومكلفة بل وربما مستحيلة بالعناصر المادية. سمحت هذه المنتجات باسترجاع وتحسين الإشارات في حالات لم تكن ممكنة من قبل. وفي الوقت نفسه، ليس هناك طريقة بسيطة للتنبؤ بالتفاعلات (أو ضبطها) التي يمكن أن تحدث عندما يتم ترابط أجهزة متعددة في نظامٍ ما. تكمن النتيجة المثالية في تحقيق ميزة تراكمية للنظام، ولكن ينبغي عدم الاستخفاف بذلك. يمكن للإشارة الصنعية المُحفَّزة بشكلٍ غير متوقع (على سبيل المثال، إشارة جديدة مُحسنة التي هي أكبر من المتوقع، أو إزالة جزء من الإشارة بواسطة المُرشح الذي تم تفعيله بدون قصد) أن تتسبب بإزعاجات أو

عواقب عكسية وخيمة. من المحتمل أن تنتشر الـ DSP على نطاق واسع لأغراضٍ كثيرة وينبغي عدم تجاهلها في التصميم أو التركيب أو الصيانة.

الاتصالات
Communications

قد يتم اعتبار الاتصالات البعيدة والاتصالات الرقمية والشبكات حقلاً منفصلاً في كثير من النصوص ولكن تم تضمينها هنا للإشارة إلى القارئ أنه يمكن ويجب النظر إليها بوصفها عملية متواصلة توسِّع مسافة و/أو مرونة الدخل/الخرج بين المرضى والأطباء والأجهزة ومكونات الـ IS.

الاتصالات عن بعد Telecommunications

تجري مناقشة التطبيب عن بعد والصحة عن بعد في أماكن أخرى من هذا الكتاب (انظر الفصل ١٠١) إلا أن تزايد انتشارها يقدم مزيداً من الدعم لنهج هذا الفصل. يمكن للأطباء عند الحاجة تنزيل الـ ECGs عن بعد، وإعادة برمجة ناظمات الخطى القلبية وطلب الوصفات طبية ومُشاركة الأشعة السينية التشخيصية، ويبدو أنه يمكن تقديم المزيد من الرعاية الطبية بهذه الطريقة. إن المهندس الإكلينيكي الذي تجاهل الاتصالات عن بعد في العقد الماضي كونها كانت "مجرد" دعم لفاكسات المناقشات أو الأعمال، سوف يظهر اليوم كمن يضع رأسه في الرمال. استخدمت أنظمة الاتصالات عن بعد التقليدية المُبدلات والمفاتيح الرقمية لإقامة التوصيلات السلكية للإشارات التناظرية (أي الأصوات). بينما تُحوِّل أنظمة الاتصالات عن بعد الحديثة في كثير من الأحيان الصوت إلى بيانات رقمية باستخدام أجهزة D/A و A/D مثل تلك المذكورة آنفاً. حتى لو تم استخدام يد الهاتف القياسية للمحادثة بين شخصين، فليس هناك وسيلة لمعرفة ما إذا كان الرقمنة تحدث في نقطةٍ ما أو أكثر في مسار المحادثة. يمكن للكثير من الأجهزة الطبية أن تستخدم الاتصالات الهاتفية لتبادل البيانات وكذلك تكنولوجيات الاتصالات السلكية أو الرقمية عن بُعد التي يمكنها أن تحدث تشوهات فريدة يصعب كشفها أو تشخيصها أو إصلاحها. إذا كان المرء مسئولاً عن ضمان موثوقية الاتصالات الطبية عن طريق خطوط الهاتف فيجب عليه أن يفهم التكنولوجيات المتوفرة للاتصالات عن بعد. لا يوجد مع تلك المعرفة فصل بين التدريب والمقدرة المطلوبتين لدعم المكالمات الهاتفية التجارية والشخصية العادية.

يستخدم بث الفاكس (الفاكس) مجموعة من التقنيات الرقمية والتناظرية لنقل الصور من نقطة إلى أخرى عن طريق نظام الاتصالات عن بعد على الرغم من استخدام شبكة الإنترنت أحياناً بدلاً من ذلك. تم مع ظهور قانون HIPAA الأمني وقوانين الخصوصية استدعاء آلة الفاكس البسيطة إلى الخدمة باعتبارها إصلاح مؤقت لإرسال معلومات المرضى إلى الأطباء الآخرين أو المؤسسات الأخرى من دون استخدام المسارات الرقمية الرسمية مثل البريد الإلكتروني أو مُخدمات الشبكة. قد يبدو هذا الإجراء من الناحية الفنية بمثابة خطوة إلى الوراء لكنه يتفادى بعض القواعد والمخاطر الأكثر صرامة في قانون HIPAA. تستثني لوائح HIPAA على وجه التحديد المناقشات أو

والوثائق التي يتم إرسالها عن طريق الهاتف لأنه لا يتم تخزينها ولا نقلها عن عمد بشكلٍ إلكتروني مُرقمَن. من مُسلّمات الاتصالات الهاتفية أو الفاكس هو أنها اتصال أسلاك من نقطة إلى نقطة أخرى التي تنتهي عند رقم هاتف المستلم في مكان معروف مثل مكتب الطبيب أو منزل المريض. أما الإرسال الإلكتروني عن طريق البريد الإلكتروني أو وثيقة رقمية على الإنترنت فهو غير مُستثنى من لوائح HIPAA لأنه يجب على هذه الوثائق أن تمر من خلال العديد من أجهزة الكمبيوتر العامة والخاصة في طريقها إلى مقصدها. ما لم تكن الوثائق مشفّرة بطريقة مأمونة بحيث لا يمكن لأحد الاطلاع عليها سوى المتلقي المقصود، فقد تكون عرضة للقراءة من قبل جهات غير مصرح بها مما يُشكل انتهاكً لخصوصية المريض. نتيجة لذلك فقد تم نصح العديد من الأطباء بعدم التواصل عبر البريد الإلكتروني أو مواقع الويب وهو الأمر الذي جعل الفاكس أحد البدائل القليلة المريحة. يُعاني الإرسال بالفاكس وللأسف من قيود عديدة بما في ذلك المسح الضوئي والطباعة غير المتقنتين بالنسبة لمعظم المنتجات رخيصة الثمن وعدم إمكانية التنبؤ بكيفية تعاملها مع الألوان. كما هو موضح في مثال تخطيط كهربية القلب المذكور آنفاً فإن ذلك قد يتسبب بتشوهات وضجيج صنعي غير متوقع في السجل الذي يتم تلقيه كما يتسبب الإرسال المتكرر للفاكسات بين الأطباء في تفاقم هذه المشكلة. لم تظهر هذه المسألة إلا حديثاً وقد تستغرق بعض الوقت لتُصبح موثقة ومفهومة بشكل جيد. ويكفي القول إن هذا هو مثال آخر على التكنولوجيا التي يمكن أن تؤثر على نوعية الرعاية الطبية الأمر الذي يضعها بشكلٍ قوي في نطاق اختصاص المهندسين الإكلينيكيين وتقنيي الأجهزة الطبية الحيوية. وكتنويه جانبي، قد تكون إعفاءات HIPAA باستخدام الفاكس قصيرة الأمد لأنه في الحقيقة لا يوجد أي وسيلة اليوم تمنع توجيه الفاكس خلال أي شبكة رقمية أو شبكة الإنترنت. تستخدم العديد من الأنظمة الهاتفية المتاحة مسارات وتقنيات رقمية لتوفير المال والوقت. ما لم يتمكن المستخدم من ضمان أن كلاً من المرسل والمتلقي هما في الحقيقة متصلين إلى أسلاك هاتف تناظرية، فقد تستمر قيود HIPAA بأن تكون الحكم.

الاتصالات الرقمية Digital Communications

يمكننا الآن التحول إلى مناقشة تقنية بعض الشيء عن الاتصالات الرقمية العامة والشبكات والإنترنت لتوفير مفردات للعمل وفهم للمبادئ الأساسية التي سوف تكون مفيدة في هذا المجال. كانت هناك العديد من تكنولوجيات الاتصالات والشبكات على مدى العقدين الماضيين ولكن عدداً متزايداً من الشركات يستخدم عدداً محدوداً من المعايير المُثبتة في الصناعة وهو الأمر الذي يجعل هذه المناقشة أسهل قليلاً. سنبدأ بتكنولوجيات الاتصالات السلكية وننهي بالتكنولوجيات اللاسلكية.

تتطلب الاتصالات الرقمية عموماً إرسال واستقبال موثوق لإشارات ثنائية (1/0 أو on/off) التي يمكن تمثيلها بمجموعة متفق عليها مسبقاً من جهد منخفض أو أرضي (ground) أو جهد منخفض سلبي. يمكن لأي جهازين أن

يتبادلا البيانات الرقمية ما دام أنهما يتشاركان في بروتوكول متفق عليها مسبقاً، مثل كون ٥ فولت هو "on" أو "1" و كون -٥ فولت هو "off" أو "0". العنصر الأخر اللازم للاتصالات الموثوقة هو بروتوكول التوقيت لضمان أن المتلقي يقيس الإشارة في الوقت الصحيح. لتحقيق ذلك يتم إما إرسال توقيت متزامن بالتوازي أو تضمين مشغلات غير متزامنة (إشارات التوقيت) ضمن تدفق البيانات. في الاتصالات المتزامنة، يقوم سلك إضافي أو زوج من الأسلاك بإرسال إشارة توقيت (clock signal). باعتبار أن إشارات التوقيت والبيانات ستواجه تشويهاً متماثلاً على طول المسار، فيمكن لإشارة التوقيت الصافية أن تكون بمثابة تحقق من ملائمة مسار الأسلاك. يمكن قياس الجهد الوارد في كل مرة يتم فيها التقاط نبض التوقيت وهو ما يُحدد حالة "on" أو "off" للبت. يعتمد الاتصال غير المتزامن على وجود ساعة توقيت كريستال دقيقة وموثوقة للغاية في جهاز الإرسال وجهاز الاستقبال تعملان بالمعدلات المتفق عليها رسمياً. ينتظر جهاز الاستقبال إشارة أولية تُبلغه أن الرسالة قد بدأت ومن ثم يستخدم ساعته الداخلية ليجاري معدل قياسها. اعتماداً على البروتوكول المتفق عليه، فإن الرسالة تستغرق عادةً عدداً محدداً من الفترات الزمنية أو أن الرسالة تبدأ بقيمة رقمية تُبلّغ عن طول الرسالة قبل أن يتم إرسال البيانات. قد تستفيد الكميات الكبيرة من البيانات من إرسال إشارات متعددة على أسلاك منفصلة في وقت واحد وهو ما يسمى "الاتصالات المتوازية". إن التعدد الشائع هو ٨ بت أو أسلاك الإشارات. عندما تُصمم مع سلك كهربائي أرضي لكل سلك ساعة وسلك ساعة وأرضي، فسوف يتطلب كل كابل ما لا يقل عن ١٨ سلكاً بإضافة إلى أسلاك احتياطية وتدريع كهربائي خارجي. بسبب التكلفة الكبيرة والحجم الكبير للكابلات المتوازية فإنها لا تُستخدم إلا في الحالات النادرة مثل ربط بعض الطابعات واتصالات الكمبيوترات عالية السرعة (على سبيل المثال، SCSI). تستخدم معظم أنظمة الاتصالات الحالية نظام المعلومات التسلسلية غير المتزامنة، بدلاً من الإشارات المتوازية المترافقة مع التوقيت، وإرسال إشارة بعد الأخرى باستخدام توقيت دقيق للفصل بينها. تستند كلاً من أنظمة الـ RS232/422 والإيثرنت والـ USB والـ USB-2 و الـ Firewire على الاتصال التسلسلي غير المتزامن.

حتى لو كانت اتفاقات الجهد والتوقيت موجودة فما تزال هناك حاجة لوجود التصاميم الكهربائية والميكانيكية المناسبة لضمان عدم تدهور الجهد وشكل الإشارة (أي، تضائلها أو تأخرها أو تضررها) على طول مسارها. من الصعب حتى في أفضل تصاميم أنظمة الاتصالات ضمان عدم التأثير السلبي لبعض المشاكل الخارجية الكهربائية والميكانيكية أو غيرها على الاتصالات. ولذلك تشمل معظم التصميمات تأكيدات تبادل فعالة بين الأجهزة المرسلة والمستقبلة لضمان مرور الرسالة بشكلٍ دقيق. يقوم بهذه المهمة بشكلٍ تلقائي برنامج اتصالات بسيط داخل الأجهزة.

يتطلب البرنامج عموماً من الجهاز المُرسل أن يوصف طول المعلومات التي يتم إرسالها وكذلك بارامترات لضبط الجودة. على سبيل المثال، قد تُبلّغ الرسالة المرسلة المتلقي بأنه ينبغي أن يتلقى ٢٥٦ إشارة وأنه يجب أن يكون

هناك عدداً زوجياً أو فردياً من وحدات الـ (1s) عند جمع هذه الإشارات (وهو ما يُدعى "التكافؤ الزوجي أو الفردي"). يخدم هذا النظام البسيط بشكلٍ جيد عند ضياع أحد البتات ولكنه لن يكون كافياً للبيانات الهامة لأن التدخل الذي يتسبب بمضاعفات عدد فردي من وحدات الـ 1s (التي سوف يُساء تفسيرها على أنها أصفاراً) سوف يُعطي تكافؤاً صحيحاً. لذلك تُستخدم أنظمة الترميز الأكثر تطوراً بالنسبة لمعظم الاتصالات عالية السرعة. تعمل هذه الأنظمة عن طريق تنفيذ المزيد من العمليات الحسابية على البيانات التي يتم إرسالها ومن ثم إرسال البيانات حول خصائص الرسالة التي ينبغي أن تصل في نهاية المطاف. إذا نفذ الجهاز المستلم العمليات الحسابية نفسها على البيانات الواردة ووجد أنها لا تتطابق مع تلك التي أرسلت مع الرسالة فيستنتج وجود مشكلةٍ ما. يُعطى جهاز الاستقبال في بعض الحالات معلومات كافية لإصلاح الأخطاء البسيطة، ولكن كثيراً ما يُستخدم بدلاً عن ذلك بروتوكول الاتصالات بالمصافحة.

إذا كان جهاز الاستقبال راضياً عن نوعية ودقة الرسالة فبإمكانه إرسال رسالة تأكيد وجيزة من تلقاء ذاته (ACK) إلى جهاز الإرسال، وإذا كانت الرسالة معطوبة فبإمكانه إرسال رسالة سلبية بدلاً من ذلك (NAK). قد يوفر بروتوكول المصافحة عندئذ سلسلة من الخطوات التصحيحية لإعادة إرسال وإعادة فحص الرسالة بما في ذلك (إذا لزم الأمر) الاختيار التلقائي لمعدل نقل أبطأ أو حتى قناة اتصال مختلفة. تم في تصاميم إشارات الـ RS232 القديمة تخصيص أسلاك منفصلة لإرسال إشارات المصافحة هذه ذهاباً وإياباً ("أجهزة المصافحة") إلا أن التصاميم الحديثة توفر بيانات ثنائية الاتجاه وأزواج إشارات كما تستخدم رسائل مشفرة لنفس الغرض ("برمجيات المصافحة").

يسمح برنامج المصافحة بتدفق رسالة ورموز إضافية بين المرسل والمتلقي مثل إشارة "مشغول" عندما امتلاء المخزن المؤقت للطابعة أو رسالة "خرطوشة حبر فارغة" عندما يكون ذلك مناسباً، وقد تختلف هذه الإشارات مع اختلاف الأنظمة مما يُسبب عدم توافق إضافي. على سبيل المثال، لم تستخدم طابعات HP (Hewlett-Packard) القديمة نفس الرموز التي استخدمتها الطابعات الأخرى مما تسبب بمشاكل في الطباعة. يُعتبر ذلك جزء من السبب وراء الحاجة إلى "سواقات" وبرامج فريدة للطابعات المختلفة والماسحات الضوئية والمحطات الطرفية بحيث يمكن للنظام تفسير الرموز التي يتلقاها واتخاذ الإجراءات المناسبة. تقوم اليوم رقائق الاتصالات الرخيصة (UARTs وUSARTS) بمعالجة الكثير من أمور التوقيت والمصافحة بشكلٍ تلقائي تاركة قرارات المستوى الأعلى (مثل التنبيه عند جفاف خرطوشة الحبر الملوّن) إلى برمجيات الجهاز لإعلام المُشغِّل بضرورة تصحيح المشكلة.

الشبكات Networks

تعتمد الشبكات والإنترنت عموماً على بروتوكولات برمجيات المصافحة غير المتزامنة المذكورة آنفاً كما أنها تُضيف بعض الشكليات إلى العملية. أصبح الإيثرنت على سبيل المثال بروتوكول شبكة غير تزامني شامل يُستخدم

على نطاق واسع في جميع أنحاء المستشفيات. إلا أن طبيعة الشبكة تتطلب من العديد من الأجهزة أن تكون قادرة على مشاركة سعة الإشارة الرقمية ذات مجموعة الأسلاك الواحدة الممتدة في جميع أنحاء المبنى. يقلل ذلك من تكلفة إرسال الإشارات في جميع أنحاء المبنى ولكنه يتطلب أن تضم الأجهزة وسيلة لتمييز الرسائل التي تنتمي إليها وتلك التي ينبغي تجاهلها. لتحقيق ذلك ينبغي توفر مزيج من الأجهزة والبرمجيات.

يتوفر قدر كبير من المعلومات التفصيلية المحددة عن الشبكات في كتب المقررات الدراسية ومصادر الإنترنت مثل wwwcisco.com ، ولذلك يتم هنا تقديم لمحة موجزة فقط عن هذا الموضوع. على صعيد البرمجيات ، فإن أحد المفاهيم الأساسية في تصميم الشبكات هو أن يتم إرسال البيانات إلى المُتلقي بحزم من البتات ذات طول محدَّد مع عنوان رقمي في بداية الحزمة. إن إحدى القواعد الأساسية للشبكات (بغض النظر عن تفاصيل الشبكة) هي أنه ينبغي على جميع الأجهزة الأخرى تجاهل الرسائل غير الموجه إليها. إلا أن ذلك لا يعني عدم قدرة الأجهزة الأخرى عن كشف وقراءة الرسائل الأمر الذي يخلق تحديات أمنية كبيرة وتحديات كبيرة للخصوصية في محيط الرعاية الصحية. إن لكل جهاز كمبيوتر على الشبكة بطاقة ربط مع الشبكة داخلية (بطاقة ربط مع الشبكة Network Interface Card, "NIC") تقوم بالتعامل مع التصميم الكهربائي وبروتوكولات الاتصال (أسلوب الوصول إلى الشبكة Network Access Method "NAM") للشبكة التي يتصل معها. كما أن لتلك البطاقة رقم تعريف فريد (ID number) يُعرف باسم "MAC address" (ضبط أسلوب الوصول إلى الشبكة ، network Method Access Control).

الطوبولوجيات Topologies

يمكن استخدام ثلاثة تصاميم عامة للكابلات تُعرف باسم "الطوبولوجيات" وهي التصميم النجمي والحلقي والناقل. يُمثل كل تصميم مُفاضلة بين تكلفة الأسلاك وسرعة الاتصال والوثوقية. يستخدم الترتيب النجمي سلك منفصل لكل جهاز وهو ما يوفر وثوقية عالية وعرض كبيرة للإشارة ولكنه ذو تكلفة عالية لأنه يجب تمديد أسلاك خاصة بكل جهاز في المبنى. يمكن لشبكة الناقل أن تستخدم سلك واحد يمتد في جميع أنحاء البناء ويمكن لكل جهاز أن يوصَّل إلى السلك في أي مكان قريب. ولكن إذا حدث أي قطع في السلك الناقل فلا يمكن عندها تمرير الرسائل بعد نقطة القطع. وعلاوة على ذلك ، إذا كانت جميع الأجهزة التي تتشارك في الناقل تحاول إرسال الكثير من البيانات الهامة فقد تحدث تصادمات كثيرة تتداخل فيها الحزم مع بعضها البعض. على الرغم من أن طوبولوجيا الناقل يمكن أن تكون رخيصة جداً إلا أنها يمكن أن تبلغ الحمل الزائد بسهولة. أثبتت شبكة الناقل البسيطة غير المزودة بالتصاميم والعناصر البرمجية والأجهزة الخاصة بأنها غير كافية بالنسبة للتطبيقات المهمة.

تستخدم الطريقة الثالثة وهي طريقة "حلقة التذاكر ، token ring" سلك مستمر يمتد خلال البناء بأكمله ويعود إلى نقطة الانطلاق. تكون فراغات الرسائل التي تُدعى بالتذاكر مخصصة زمنياً على السلك ويمكن لأي جهاز أن يضع معلومات في فراغ أي تذكرة غير مستخدمة مع عنوان الـ MAC للمتلقي. مع مرور التذاكر على كل جهاز

مُتصل مع الحلقة فإن الجهاز يقوم بقراءة محتوياتها ويتخذ قراراً: إذا كانت التذكرة موجهة إليه فإن الجهاز يقرأ محتوياتها ثم يقوم إما بتخزين الرسالة الخاصة به لإرسالها أو يقوم بمسح التذكرة لكي يتم استخدامها من قِبل الأجهزة الأخرى. أما التذكرة التي تمر بكامل الحلقة من دون أن تتم قراءتها فتمُحى لافتراض أن الجهاز المتلقي غير متصل بالشبكة ثم يقوم جهاز الإرسال باتخاذ إجراءات تصحيحية أخرى حسب الحاجة. الميزة الأخرى لحلقة التذاكر أنه في حال تعطل الحلقة في أي نقطة فإن الإشارات تستمر بالانتقال إلى كافة الأجهزة.

في واقع الأمر لا تُعتبر أي واحدة من هذه الطوبولوجيات مُفضلة بشكلٍ شامل أو حصري. غالباً ما يتم في معظم المؤسسات استخدام مجموعات من الطوبولوجيات الثلاثة توازِن بين التكاليف والأداء والاعتمادية حسب الاقتضاء. تتصل كل شبكة فرعية مع الشبكات الفرعية القريبة ببوابة تحول إشارات البيانات والبروتوكولات حسب الحاجة. تعمل البوابات مع نظام إدارة نظام الشبكة (مثل Novell Netware™) لتتبع موقع كل جهاز من خلال تخزين عنوان الـ MAC الخاص به والشبكة الفرعية المتصل معها. يتم توجيه الرسائل خلال البوابات المناسبة حتى يتم الوصول إلى الشبكة الفرعية المرجوة. عندما توجد مجموعة الشبكات الفرعية في مبنى واحد أو في منطقة واحدة من المبنى فإنها تُسمى عادة بالشبكة المحلية (Local Area Network, "LAN"). بينما تُسمى الشبكات الأكبر التي تمتد إلى عدة مبان في حرم التصنيع أو البحوث بالشبكات الواسعة (Wide Area Network. "WAN")، أما الشبكات التي تمتد على مستوى المدينة فيُشار إليها بشبكات المدينة أو شبكات المتروبوليتان (Metropolitan Area Network, "MANs"). كلما بعدت المسافة ارتفع عرض الحزمة الكلي اللازم وازداد احتمال استبدال أو استكمال أسلاك الشبكة بوصلات ميكروويف أو وصلات ألياف ضوئية باهظة الثمن. هناك ضرورة للـ NIC المتخصصة وللبوابات لاستيعاب هذه التحسينات ولكن يمكن تطبيق البنية العامة الموصوفة آنفاً بغض النظر عن وسط أو حجم الشبكة.

الإنترنت Internet

إن الإنترنت هي شبكة متخصصة تم تصميمها من قبل وكالة مشاريع أبحاث الدفاع المتطورة التابعة لوزارة الدفاع (Defense Advanced Research Projects Agency, "DARPA") بوصفها شبكة عالمية موثوقة يمكن أن تتحمل أضرار مادية كبيرة من دون التوقف عن تلقي الرسائل. تعمل الإنترنت بطريقة مماثلة للشبكات العامة الموصوفة آنفاً باستثناءين مهمين. أولاً، أن لكل جهاز موصل إلى شبكة الإنترنت عنوان بروتوكول إنترنت (Internet Protocol, IP) يختلف تماماً عن عناوين الـ MAC لشبكات LAN/WAN/MAN.

إن عنوان بروتوكول الإنترنت (IP) عبارة عن رقم يتألف من أربعة أجزاء ويُعرف بالرقم "الرباعي المنقط". يتألف الرقم الرباعي المنقط من أربعة أرقام مفصولة عن بعضها بنقطة عشرية (على سبيل المثال، 174.201.33.101). يعمل كل رقم فريد كعنوان MAC أو كرقم هاتف، ويُمثل عنوان الـ IP الرباعي المنقط العنوان لجهاز مُحدَّد أو لمُستخدم مُحدَّد. تُخصَّص بعض الأرقام بشكلٍ دائم لجهازٍ ما، مثل مخدِّم الشبكة الرئيسي للشركة. كما توجد أرقام

أخرى تُشكل عناوين IP ديناميكية تُخصَّص لأجهزة الكمبيوتر الفردية أو تُخصص للأجهزة بمجرد اتصالها بالإنترنت. يتم الاحتفاظ بعناوين الـ IP في مجموعة دولية من كمبيوترات الـ DSN (Domain Name Server) متصلة بشبكة الإنترنت لغرض الاحتفاظ بعدة أجزاء من معلومات عنونة شبكة الإنترنت بتزامن عالمي (وهي عنوان الـ IP الصحيح والاسم النصي المُسند إلى هذا العنوان (مثل www.att.com) والموقع المادي للجهاز بالنسبة إلى أقرب نقطة وصول إلى شبكة الإنترنت).

تُعرَف المصفوفة العالمية لمواقع الشبكة المُتصلة بواسطة شبكة الإنترنت "بالشبكة العنكبوتية العالمية، World Wide Web" (ومنها أتت البادئة www على معظم عناوين الإنترنت). تُقسم المعلومات التي يتم إرسالها عبر الإنترنت إلى حزم حيث يكون لكل حزمة عنوان IP لجهازي الإرسال والتلقي ومعلومات التسلسل لكل حزمة ووقت الإرسال. يتم إرسال كل حزمة إلى أقرب نقطة وصول إلى الإنترنت ومن ثم تتم قراءتها من قبل أقرب محطة إنترنت لإرسال الحزم. تتم إدارة هذه المحطات من قبل المؤسسات العسكرية والحكومية والأكاديمية والتجارية بناءً على العقود والاتفاقات الدولية.

تحصل محطات إرسال الحزم على معلومات الـ DNS للمتلقي وتتخذ قراراً بإرسال الحزمة إلى محطة إرسال أخرى مجاورة. إذا كانت محطات الإرسال أو خطوط الاتصالات في الاتجاه العام الذي يجب أن تذهب فيه الرسالة مشغولة فسوف يتم إرسال الحزمة في اتجاهٍ آخر. تُحرِّك كل محطة إرسال الحزمة في أفضل مسار يمكنها تحديده مع كون الهدف النهائي تسليم الحزمة حتى إذا اضطرت إلى الرجوع باتجاه عكسي عبر رحلة طويلة حول العالم حتى تصل إلى وجهتها. يجب على جهاز الاستقبال الانتظار حتى تصله كل الحزم المتوقعة في الرسالة ومن ثم توضع في التسلسل الصحيح. إذا كانت الرسالة مُرضية فيمكن لجهاز الإرسال أن يبعث برسالة إلى المُرسل تؤكد استلام الرسالة. إذا كان هناك عيب أو إذا كانت أحدى الحزم (أو أكثر) مفقودة، فإن المتلقي يبعث بعد فترة محددة مسبقاً طلباً إلى المرسل بإعادة إرسال المعلومات اللازمة. إذا فشل ذلك الطلب فيجب على جهاز الاستقبال افتراض أن المرسل لم يعد يعمل ويُعلم المتلقي أن ربط الاتصال قد فشل. بالإضافة إلى ذلك، إذا وجدت محطة إرسال الحزم أن الحزمة قد تحركت لفترة طويلة دون أن تشق طريقها إلى المتلقي، فيمكن للمحطة أن تُلغي هذه الحزمة بهدف عدم الهدر الإضافي لموارد الإنترنت. لقد أثبت هذا النهج قوة وموثوقية كبيرتين وهو من أحد الأسباب التي جعلت الإنترنت ناجحة بهذا الشكل.

إلا أن النظام الناجح لمحطات الإرسال التي تستخدمها شبكة الإنترنت هو أيضاً من أهم نقاط ضعفها بالنسبة للسرية والأمن. يمكن لأي محطة من محطات الإرسال أن تقرأ وتُخزن و/أو ربما تُغير الحزم التي تُرسلها. ما لم يتم تشفير كل حزمة بطريقة تمنع جميع المحطات ما عدا المرسل والمتلقي من قراءتها أو تغييرها، فإن المعلومات تكون مفتوحة لعامة الناس. بالإضافة إلى ذلك، فإنه من المعتقد أن العديد من الوكالات الحكومية في جميع أنحاء العالم

تقوم بمسح الحزم بما يخص المحتوى الإرهابي أو المحتويات غير المشروعة الأخرى. وقد قضت حكومة الولايات المتحدة على وجه الخصوص حصولها على مفاتيح التشفير لأي حزمة تشفير تجارية، وبذلك يمكن حتى للمعلومات المُشفرة أن تكون واضحة للحكومات. يعني ذلك أنه لا يمكن للمعلومات الصحية غير مشفرة الخاصة بالمرضى بما في ذلك الملفات والبريد الإلكتروني والصور وأشرطة الفيديو ونتائج المختبر أن تجتاز قواعد الخصوصية والأمان للـ HIPAA. وعلاوة على ذلك، يبدو أن إرسال الوثائق بالفاكس عن طريق شبكة الإنترنت لن يكون مقبولاً أيضاً لأنها ليست مشفرة ويمكن أن تُطبع بسهولة باستخدام برمجيات عرض الفاكس. كانت متعارضات HIPAA هذه وراء اقتصار الكثير من الأطباء على استخدام الفاكس العادي والهاتف و/أو البريد العادي في التعامل مع المعلومات الخاصة بمرضاهم. قد تكون هناك في نهاية المطاف طرق للالتفاف حول ذلك بما في ذلك البريد الإلكتروني المشفر أو الشبكات الخاصة الافتراضية (Virtual Private Networks, "VPNs") التي تَستخدم ضوابط التشفير والكلمات السرية للتحكم بالوصول إلى مواقع الويب وخصوصية المعلومات التي يتم إرسالها عبر الإنترنت. في حين أن الـ VPNs ليست معقدة بالضرورة إلا أنها تُضيف نفقات جديدة لأن إدارة مثل هذه الخدمات تتم عن طريق الشركات الخاصة التي تتقاضى رسوماً مقابل هذه المقدرة.

إن الاستعمال الآخر الناشئ لعنونة الـ IP هو ما يسمى بالمكالمة الهاتفية باستخدام بروتوكول الصوت عبر الإنترنت (Voice over Internet Protocol, "VoIP"). إنها تقنية مثيرة للاهتمام لأنها تستخدم عرض الحزمة العالمي الحر والموثوق للإنترنت للاتصالات الصوتية. إنها أساساً أحد أنواع الاتصالات الصوتية الرقمية المتخصصة التي تؤيدها بعض الشركات مثل Cisco Systems. قد توفر شبكة الهاتف VoIP داخل المؤسسة تركيباً مرناً وحركة للهواتف كما قد تسمح لأجهزة الحاسب المجهزة بالميكروفونات بأن تكون بمثابة هواتف. كما قد يُخفض الاستثمار في نظام الـ VoIP في المستشفى بعض تكاليف الأسلاك وتعقيداتها من خلال إلغاء بعض أو جميع أسلاك الهاتف. على أية حال، إذا كان لابد من تثبيت الأسلاك الرقمية في كل مكان، فلماذا لا يُنظر في استخدامها لتلبية احتياجات الهاتف أيضاً؟ قد تحتاج مثل هذه التركيبات أسلاكً منفصلة من أجل تطبيقات شبكة الـ LAN، إلا أن اختيار أسلاك الـ VoIP قد يُسهل نشر المنتجات اللاسلكية أيضاً.

تسمح الـ VoIP بتوجيه المكالمات الهاتفية بعيدة المدى عبر خدمات الـ VoIP مما يُقلل المكالمات الهاتفية بعيدة المدى ورسوم الخدمة المدفوعة إلى شركات الهاتف المحلية وإلغاء التكاليف التجارية بعيدة المدى. إلا أن للـ VoIP حدود على المكالمات بعيدة المدى. عند استخدام الـ VoIP داخل المنشأة فإن إشاراته نادراً ما تُرهق عرض الحزمة المتاحة. ولكن ما إن يتم إرسال حزم الصوت الرقمية عبر شبكة الإنترنت حتى يَحدث لكل حزمة تأخير لا يمكن ضبطه. وقد يتسبب ذلك بنوعية متقطعة للصوت التي قد لا تكون مفاضلة مقبولة. ولكن إذا كان لدى كلا الجهتين على طرفي الاتصالات أنظمة VoIP فيمكن للبرمجيات والأجهزة الخاصة أن تُقلل من هذه المشاكل. وبذلك فقد تكون

الـ VoIP مناسبة أكثر لأنظمة الصحة الإقليمية أو الوطنية التي يمكنها أن تستخدم توفير المكالمات بعيدة المدى للمساعدة في تغطية تكلفة تركيب أنظمة متوافقة مع الـ VoIP.

كما تُستخدم العديد من أجهزة الكمبيوتر المبنية على الشبكات للوصول إلى الإنترنت. يتم تيسير هذا الوصول بواسطة مُنتَج بوابة شبكة خاص لديه القدرة على الاحتفاظ بقوائم عناوين الـ MAC والـ IP التي هي قيد الاستخدام. يتم توجيه جميع عناوين الـ IP الواردة أو الصادرة إلى (أو من) عنوان الـ MAC الصحيح بواسطة البوابة ونظام إدارة الشبكة (NMS). يتم في معظم الحالات تعيين عنوان IP ديناميكي لكل جهاز كمبيوتر عندما بداية اتصاله بالإنترنت من أجل الحفاظ على وصلات الإنترنت المتاحة للمستخدمين الفعالين. على النقيض من ذلك فإنه يتم تخصيص عنوان IP ثابت لخدمات الإنترنت التي يتعين عليها أن تكون متصلة بالإنترنت بشكلٍ مستمر بحيث يتمكن نظام الـ DNS من توجيه الطلبات الواردة للخدمة.

الاتصالات اللاسلكية Wireless Communication

أصبحت الاتصالات اللاسلكية (انظر الفصل ١٠٣) موحدة المقاييس لدرجةٍ أكبر وهي غالباً ما تُصبح مجرد امتداد للشبكة السلكية. من أكثر البروتوكولات شيوعاً لتحقيق ذلك هو سلسلة IEEE 802.11. إن البروتوكول 802.11a هو الأقدم والأبطأ بينما يُتيح البروتوكول 802.11b المزيد من عرض الحزمة أما البروتوكول 802.11g فهو أحدث وأسرع وأكثر البروتوكولات مرونةً في التوافق. من الممكن حدوث توافق جزئي أو كلي بين كل من هذه السلاسل وذلك تبعاً لدرجة تطور مكونات الـ 802.11. أما من وجهة نظر الكمبيوتر والشبكة فتتم عنونة كل جهاز كمبيوتر على وصلة لاسلكية تماماً كما لو كان متصلاً بالأسلاك.

يُتيح معيار الـ 802.11 فرص اتصال جديدة لم يسبق لها مثيل. على سبيل المثال، تم تجهيز الآلاف من محلات قهوة Starbucks بشبكات802.11. يمكن للزبائن الذين يدفعون مقابل دخول شبكة الإنترنت أن يتصلوا مع الشبكة في أي وقت يكونوا فيه ضمن نطاق الإرسال الراديوي لـ Starbucks في أي مكان في الولايات المتحدة. إلا أنه توجد بعض التحديات الأمنية الخاصة نظراً لتمكن المُستقبلات المجهزة تجهيزاً مناسباً من نسخ جميع هذه البيانات اللاسلكية. إذا لم يتم استخدام برمجيات تشفير كافية خلال الاتصالات السرية فيمكن لأي شخص الاطلاع عليها. يُشكل ذلك كشفاً خطيراً لمواقع الإنترنت ومستخدمي البريد الإلكتروني وذلك من خلال كشف هوية المُستخدمين وكلمات السر وجميع المعلومات الخاصة بهم. إضافة إلى ذلك إذا كانت كلمات السر تسمح بالوصول إلى قواعد بيانات البريد الإلكتروني الداخلي للمؤسسة وملفاتها عندئذ يمكن للإفشاء العلني أن يُعرِّض المؤسسة للتطفل وهجمات القرصنة وغيرها من الانتهاكات الأمنية الخطيرة الجارية. للأسف، على الرغم من أن لمعظم أجهزة الكمبيوتر المحمولة والمكتبية وأجهزة الكمبيوتر اللوحية قدرات تشفير كافية إلا أن العديد من أجهزة المساعدة الشخصية الرقمية "PDA" (مثل وحدات الـ Palm Pilots™ والـ Handspring™ البسيطة) غير مزودة بمثل هذه القدرات

مما يجعل التنفيذ والرقابة أمراً صعباً إن لم يكن مستحيلاً. لا يمكن تجاهل مزايا الراحة وقابلية الحمل ووثوقية وانخفاض تكلفة تكنولوجيات الـ 802.11 اللاسلكية في الرعاية الصحية، ولكن قد يتطلب كل استخدام تخطيطاً دقيقاً وضوابط تشفير لضمان الامتثال مع لوائح الـ HIPAA.

كما توجد تقنيات لاسلكية أخرى قيد الاستخدام، ولكل منها مزاياها وعيوبها. إن لتقنية الاتصال بالأشعة تحت الحمراء IR التي غالباً ما تُستخدم مع أجهزة الـ PDA وبعض أجهزة الكمبيوتر المحمولة ميزة انخفاض التكلفة ومحدودية كمية ضبط أمن خط البصر. وللأسف فإنه من النادر ما يتم استخدام التشفير في هذه التقنية مما يُتيح تطبيقها في مجال الرعاية الصحية على البيانات غير السرية فقط. أما التكنولوجيا الأخرى فهي المعروفة باسم "بلوتوث" هي عبارة عن وصلة لاسلكية راديوية منخفضة الطاقة ومحدودة المسافة ويجب أن تكون منخفضة التكلفة. تتوفر حتى الآن تطبيقات قليلة للبلوتوث ولكن قد تسمح هذه التكنولوجيا في نهاية المطاف بمناطق تحميل وتنزيل مادية حيث يمكن للأطباء والممرضات والعائلات الوصول إلى موارد الشبكة أو الإنترنت من دون إحداث تداخل لاسلكي للأجهزة الأخرى المجاورة. أيضاً قد يكون التشفير لمثل هذه الرسائل محدوداً أو غير موجودة بحيث لا تكون المعلومات التي تضبطها لوائح HIPAA مناسبة لتطبيقات البلوتوث.

أما التقنية الرقمية الداخلية اللاسلكية الثالثة الجدير بالذكر فهي نظام عنونة بروتوكول الإنترنت (IP). ما دام يتم اختيار تردد راديوي متوافق مع ترددات المستشفى فيمكن لبعض الأجهزة استخدام شكلاً من أشكال العنونة اللاسلكية لـ IP بدلا من شبكة الـ LAN. ويكون الفرق الأساسي في هذه الحالة هو أن هذه الأجهزة لا تستخدم عنوان الـ LAN MAC بل تستخدم العنوان "الرباعي المنقط" الذي يتألف من أربعة أجزاء والمذكور سابقاً. إن ميزة هذا الأسلوب هو تمكن الأجهزة من استخدام الأدوات القياسية المتوافقة مع الإنترنت مثل المتصفحات أو برامج نقل الملفات. إضافة إلى ذلك فإن تركيب مقدرة الـ IP اللاسلكية يمكن أن يُسهِّل تطبيقات الـ VoIP. قد يسمح ذلك في نهاية المطاف بالمكالمات الهاتفية الداخلية والخارجية اللاسلكية الآمنة في جميع أنحاء المستشفى ما دامت قيود الـ VoIP المذكورة سابقاً لا تُشكل عقبة رئيسية.

اعتبارات الخصوصية والأمن
Privacy and Security Considerations

لا تكتمل أي مناقشة للاتصالات في عالم الرعاية الصحية بدون بضع كلمات عن تأمين الاتصالات لمنع الوصول غير المصرح به أو العبث. ساهم التطور السريع في معايير الاتصالات السلكية واللاسلكية في تسهيل تدريب الموظفين واقتناء الأجهزة والبرمجيات وتركيب واختبار وتشغيل الأنظمة القائمة على التكنولوجيا الرقمية. إلا أن ذلك لم يأت من دون ثمن حيث أصبحت نفس المكونات والبرمجيات القياسية مُتاحة لأي شخص يرغب في اختراق النظام.

لا يمكن لهذا الفصل أن يتطرق بشكلٍ كامل لهذا المجال المُتعمق بالتقنية والمُتقدم بشكلٍ سريع، ولكن ينبغي التطرق إلى بعض النقاط. أولاً، يُعرِّض الوصول إلى شبكة الإنترنت النظام بأكمله لهجمات أنواع عديدة من قراصنة الشبكة. على سبيل المثال، يتم بسهولة إرفاق الفيروسات مع رسائل البريد الإلكتروني والملفات والتطبيقات مثل برامج المحادثة الفورية أو الدردشة (Instant Messenger, "IM"). قد لا يكون هناك مفر من التثبيت المفروض والآلي لبرامج الحماية من الفيروسات ومنهجيات التحديث. وللأسف فإن للبرامج المتاحة تكلفة مادية كما أن لكل برنامج مُفاضلات (مثل استهلاك كبير في سرعة جهاز الكمبيوتر) مما يتسبب أحياناً بعدم توافق في الأجهزة والبرمجيات التي يمكن أن تكون مُعطّلة بشكلٍ شديد. ومع ذلك، لا يمكن بسهولة تبرير العمل بدون مثل هذه البرامج.

جدران الحماية Firewalls

بتعرض كل مستخدم للإنترنت لهجمات البرامج التي يمكن أن تتلف الملفات أو تعدل البيانات أو تسرق المعلومات السرية خلال اتصال هؤلاء المستخدمين بالإنترنت وذلك بسبب ظهور عنوان الـ IP الخاص بهم بالنسبة إلى جميع المواقع التي تُرسل حزمها. يمكن للبرامج الخبيثة أن تستخدم هذا العنوان لإرسال تعليمات خفية لجهاز المستخدم. لذلك يجب بالنسبة إلى كل منشأة تثبيت مجموعة خاصة من أجهزة وبرامج جدران الحماية لإدارة حركة المرور داخل وخارج المنشأة. إلا أن جدران الحماية هي منتجات غير مستقلة وتحتاج إلى تطبيق تحديثات محددة بصورة منهجية كما أنها تحتاج لأن يقوم أحد الأشخاص بتقييم حركة الـ IP لكشف ومواجهة العدد الكبير من التهديدات المحتملة. وعلى الرغم من أن التهديدات لا تكون خارجية فقط، فإن التهديدات الخارجية تتطلب تمحيصاً دقيقاً للكشف عن أنماط المتسللين الذين يحاولون التسلل أو التداخل مع جدار الحماية أو غيره من الموارد. إن آخر شيء تحتاجه المنشأة هو أن يسرق المتسلل الأقراص أو موارد الحوسبة والاتصالات بهدف اللعب أو الخبث. إن لبعض البرامج المتسللة تأخير زمني مُدمج يسمح لها بالاختفاء بصمت بعد أن يتم تثبيتها.

يمكن لعمليات الاقتحام القصيرة المتعددة والمعزولة أن تسمح بمهاجمة نظام المؤسسة من الداخل عندما يكون عدد الكادر منخفض مما يُحدث ضرراً داخلياً أو خارجياً كبيراً. من إحدى الاستخدامات الخارجية هو إحداث حجب الخدمة (denial of service, "DoS") أو هجمات البريد المُزعج على أجهزة الكمبيوتر الخارجية الأخرى. يمكن في هجوم حجب الخدمة تهيئة عدد كبير من أجهزة الكمبيوتر لتقوم بإرسال رسائل ضخمة في وقت واحد إلى أحد المواقع التجارية أو العسكرية المُستهدفة أو طلب خدمات مكثفة الوقت والموارد من هذه المواقع. وبشكلٍ مشابه يمكن لهجوم البريد الإلكتروني المزعج أن يستخدم أنظمة البريد الإلكتروني لمؤسسة واحدة أو أكثر لإرسال آلاف الرسائل الإباحية أو السياسية أو الإعلانية باستخدام قوائمها الخاصة و/أو قوائم البريد الإلكتروني للمستشفى. لهذا السبب يقوم بعض مديري جدران الحماية بتقييد عدد نسخ البريد الإلكتروني التي يمكن لأي مستخدم داخلي أن يُرسلها

كما يمكن لهم أن يحددوا عتبات على نوع وتردد وكمية رسائل الإنترنت التي يمكن لأي مُستخدم أن يُرسلها. يمكن تغيير هذه الحدود حسب اليوم والوقت.

كما يمكن أن يكون هناك المزيد من تدابير إدارة حركة الـ IP بما في ذلك تتبع أو الحد من استخدام البريد الإلكتروني ومسح محتوى البريد الإلكتروني لانتهاكات الخصوصية والتحرش ومنع الدخول إلى المواقع الإباحية للأطفال وغيرها من انتهاكات السياسات المؤسسية المكتوبة. قد يكون هناك ضرورة لنشر جدران حماية وإستراتيجيات مماثلة داخل منظومات الـ LAN أو الـ WAN أو MAN لمنع (أو لكشف) خروق الخصوصية والخروق الأمنية الداخلية المماثلة.

ضوابط الوصول المادي Physical Access Controls

يجب أيضاً أخذ ضوابط الوصول المادي بعين الاعتبار. ورغم أن أنظمة عنونة الـ IP و MAC يمكن أن تسمح في كثيرٍ من الأحيان لأي مستخدم بتوصيل أي جهاز كمبيوتر بشكلٍ مرن في أي منفذ سلكي متاح أو أي نقطة وصول لاسلكية، إلا أن ذلك قد لا يكون مدعوماً في معظم المؤسسات. تتضمن البدائل على سياسات قوية بالنسبة إلى كلمة السر وفرض تنفيذ هذه السياسات واقتصار تصريح صلاحية تنفيذ وصلات جديدة أو تغيير بعض التوصيلات في شبكة المستشفى على الكادر الرئيسي للصيانة والدعم التقني. لا تكون عملية المفاضلة في هذا السياق بسيطة. إن السماح للشبكات بجعل أي شخص لديه محول إيثرنت لاسلكي أو محول 802.11 لاسلكي قادراً على الوصول إلى اتصالات أو موارد الحوسبة قد لا يكون مقبولاً من منظور الأمن والخصوصية ولكنه بنفس الوقت يجعل تثبيت وتحريك الأجهزة المُعتمَدة في محيط المستشفى أمراً أسهل بكثير بالنسبة للكتبة والممرضين والفنيين أو حتى المرضى. وبالمقابل فإن تحديد مثل هذه التحركات على شخص واحد قد لا يكون عملياً بالأخذ بعين الاعتبار أنه لا يمكن تأجيل النقل الطارئ للمريض (وجميع الأجهزة المرافقة له) الذي يعتمد على الشبكة إلى وحدة الـ ICU بسبب عدم إمكانية الوصول إلى هذا الشخص. يمكن حل هذه المشكلة من خلال توفير عدة أشخاص مخولين في كل مجموعة عمل مع الأخذ بعين الاعتبار ضرورة التوثيق الواضح والاتصالات لتجنب المشاكل.

تكنولوجيات الذاكرة/التخزين Memory/Storage Technologies

تُشكل الذاكرة أو بشكلٍ أعم تقنيات التخزين تحديات وفرص فريدة في مجال الرعاية الصحية. والخبر السار هو أن تكنولوجيات التخزين أصبحت غير مكلفة وموثوقة للغاية بحيث يمكن حل معظم المشاكل بشكلٍ معقول.

المراجع

References

Schmoldt D, Kangas J, Mendoza GA, et al. The Analytic Hierarchy Process in Natural Resource and Environmental Decision Making. Dordrecht, Germany, Kluwer Academic Publishers, 2001.