١٠٦

تكامل وتقارب التكنولوجيا الطبية وتكنولوجيا المعلومات

The Integration and Convergence of Medical and Information Technologies

Ted Cohen
Manager, Clinical Engineering Department , Sacramento Medical Center, University of California Sacramento, CA

Colleen Ward
Clinical Engineering Department, Sacramento Medical Center, University of California, Sacramento, CA

أصبحت المنتجات الطبية أكثر اعتماداً على تكنولوجيا الكمبيوتر منذ تطوير نظم الكومبيوتر الصغيرة في أوائل سبعينيات القرن الماضي واختراع وتنفيذ المُعالج الصغري في أواخر سبعينيات وبدايات ثمانينيات القرن الماضي. تعتمد بعض التكنولوجيات الإكلينيكية في الواقع (مثل ماسحات الـ CT) اعتماداً كلياً على أجهزة الكمبيوتر و لا يمكن أن تعمل بدونها. وقد أصبحت المعالجات الصغرية في الآونة الأخيرة في كل مكان في التكنولوجيا الطبية واستُخدِمت في المنتجات بما في ذلك: (١) الأسرّة الكهربائية "الذكية" التي توزن المريض وتتحسس فيما إذا كان المريض في سريره أم لا، (٢) الأجهزة المزدرعة المتطورة مثل مزيلات الرجفان المزدرعة، (٣) مجموعة كبيرة ومتنوعة من الأنظمة الطبية التي تقيس البارمترات الفيزيولوجية (في الجسم الحي أو في المختبر)، (٤) الأنظمة التي تصور تقريباً أي جزء من الجسم. لا تتضمن العديد من الأنظمة الطبية في يومنا هذا على معالجات صغرية مُدمجة فقط بل هي أيضاً قادرة على تخزين ونقل المعلومات الإكلينيكية التي تُجمعها عبر شبكات الكمبيوتر القياسية.

تطورت تكنولوجيا المعلومات في مجال الرعاية الصحية من تطبيقات التأمين والفواتير الطبية التي تعتمد على البيئة الصلبة إلى تشكيلة واسعة من أنظمة المعلومات بما في ذلك أنظمة المختبرات والصيدلة والجراحة والسجلات الطبية وأنظمة إدخال أوامر الأطباء والأشعة وأرشفة وتبادل الصور. تستخدم جميع أنظمة المعلومات مختصرات تجعلها أسهل للتذكر. على سبيل المثال، (١) CPOE من أجل أنظمة الإدخال المحوسب لأوامر الأطباء

(Computerized Physician Order Entry Systems)، (٢) PACS من أجل أنظمة أرشفة وتبادل الصور (Picture Archiving and Communication Systems)، (٣) LIS من أجل أنظمة معلومات المختبرات (Laboratory Information Systems). اعتمدت تكنولوجيا المعلومات في مجال الرعاية الصحية على تكنولوجيا تبادل المعلومات المستندة معايير الـ IT (مثل الإيثرنت والـ ATM وكابلات الفئة ٥) التي سمحت بالتنفيذ السهل نسبياً للبنية التحتية القياسية لتبادل البيانات في جميع أنحاء منشآت الرعاية الصحية الحديثة.

التكامل والتقارب
Integration and Convergence

مع تقارب التكنولوجيا الإكلينيكية وتكنولوجيا المعلومات فقد برز اتجاهين: (١) الاستخدام واسع النطاق للتجهيزات والبرمجيات التجارية الجاهزة("commercial off-the-shelf "COTS) و (٢) تكنولوجيات الاتصال التي ربطت المكتب والمؤسسة والمجتمع والعالم (مثل بروتوكول ضبط النقل/بروتوكول الإنترنتTCP/IP). قللت تكنولوجيا الـ COTS بشكلٍ ملحوظ تكاليف المُصنعين كما حسنت زمن تسويق المنتجات الجديدة بالنسبة إلى الصانعين. سمحت هذه التكنولوجيات للعديد من الأنظمة الطبية الرئيسية التي تُباع اليوم بان تعمل كجهاز كمبيوتر إضافة إلى عملها كجهاز طبي. يمكن للمستشفى الحديث أن يربط هذه "الأجهزة الطبية" باستخدام المنافذ القياسية للبيانات في مناطق رعاية المرضى والأسلاك القياسية والمحاور والمحولات والموجِّهات في حجرات البيانات. تدمج هذه الأنظمة المعلومات والتكنولوجيا الطبية ويتطلب دعم هذه الأنظمة اتباع نهج متكامل من قبل أولئك الذين هم على دراية بكلٍ من التكنولوجيا الإكلينيكية وتكنولوجيا الكمبيوتر والمُدربين على هاتين التكنولوجيتين.

تؤدي ميزات التقارب مجتمعةً إلى أنظمة مثل تلك المُبينة في الشكل رقم (١٠٦,١). تُستخدم هذه الأنظمة حالياً (والتي تشمل على كمبيوترات شخصية مُعدلة كأجهزة طبية) في طائفة واسعة من إعدادات المرضى الداخليين (مثل غرفة الطوارئ (ER)) ووحدة العناية المركزة (ICU) ورعاية الأمراض الحادة وغرفة العمليات (OR) و المرضى الخارجيين (العيادات الأولية والتخصصية) وتشمل العديد من الأجهزة والأنظمة التشخيصية والعلاجية (مثل المختبرات وتخطيط كهربية الدماغ وتخطيط كهربية القلب والإشارات الحيوية الأخرى ومضخات الحقن والتصوير الطبي).

التقارب: التحرك باتجاه الاتساق أو التماثل
التكامل: عملية الدمج الملائم

الشكل رقم (١٠٦,١). تعريف كل من التقارب والتكامل .

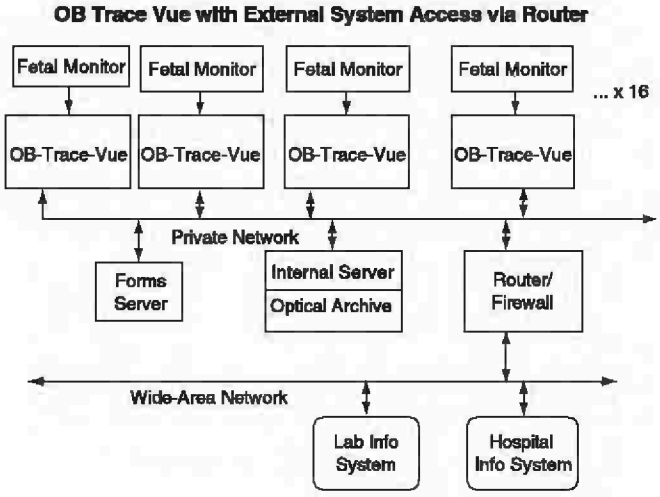
مع استخدام أجهزة الكمبيوتر الشخصية كأساس للتطوير فإن تصميم الأنظمة الطبية الحديثة يركز الآن على تطوير الأنظمة مع بذل معظم الجهد على تطوير البرمجيات والواجهات، واعتماداً على التطبيق يتم القيام ببعض أعمال التطوير الإضافية على مُبدلات الطاقة (على سبيل المثال، قياسات بارامترات المختبرات الإكلينيكية مثل غازات الدم والبوتاسيوم والصوديوم داخل الجسم الحي). ومن المطلوب بالنسبة لبعض الأنظمة القيام بالقليل من عمل البيئة الصلبة وغيره من الأعمال العرضية لدوائر ربط الواجهات. يتم بالنسبة للأجهزة الأخرى (مثل أجهزة العلاج التنفسية وآلات التخدير) إدراج كومبيوترات صغيرة ضمن المُنتَج الطبي مع ضرورة تصميم بيئة صلبة إضافية كبيرة. كما أن لهذه التجهيزات الحرجة تحديات تصميمية إضافية من أجل تلبية المتطلبات الحرجة لدعم الحياة مثل التأكد من أن تكون أزمنة إعادة تشغيل المعالج الداخلية والنظام قصيرة جداً.

سمح استخدام الـ COTS والتكنولوجيات الحديثة لتبادل البيانات للعديد من هذه الأنظمة الطبية والمعلوماتية المتكاملة من تقديم ميزات جديدة وقوية بما في ذلك الجمع والنقل والتحليل الآلي للبيانات والإعداد الآلي للتقارير وإعادة التهيئة الديناميكية للتطبيقات المختلفة دون الحاجة إلى شراء أجهزة جديدة (مثل المراقبة الفيزيولوجية للأطفال مقابل الكبار وتحديث إصدار البرمجيات عن بعد).

أما الاتجاه الآخر فيتمثل باستخدام أجهزة الكمبيوتر (سواء كانت العامة أو المتخصصة) للوصول إلى أنظمة المعلومات المتعددة. لا يمكن مع وجود عدد كبير من أنظمة المعلومات الحاسوبية في منشأة الرعاية الصحية نشر جهاز الكمبيوتر الشخصي أو المحطة بشكلٍ منفصل لكل موقع إكلينيكي ولكل نظام معلومات بسبب ارتفاع التكلفة والبنية التحتية (مثل حجرة البيانات والأسلاك والمتطلبات والافتقار إلى المكان). ولذلك فقد تم دمج تطبيقات متعددة في نظامٍ واحد من أجل السماح بالوصول المتزامن تقريباً إلى أنظمة المعلومات المتعددة.

يُصور الشكل رقم (١٠٦,٢) بيانياً نظام مراقبة جنين محوسب تم تكييفه للسماح بالوصول إلى البيانات المختبرية ونظام معلومات المستشفى وكذلك الاستمرار في جمع ومعالجة بيانات مراقبة الجنين في الزمن الحقيقي. عندما يتم استخدام الأجهزة الطبية من أجل تطبيقات متعددة من هذا القبيل فإنها تتطلب اختبار تكامل من قِبَل إما الشركة المصنعة أو المستخدم النهائي. يتطلب تنفيذ اختبار التكامل من قبل المستخدم النهائي تقديم الشركة المصنعة إجراء أو برمجيات اختبار التكامل إلى المستخدم النهائي. يتم عندئذ اتباع هذا الإجراء لاختبار التشغيل السليم للجهاز الطبي في الوقت الذي تكون فيه التطبيقات الطبية "الخارجية" المتكاملة في وضع التشغيل. على سبيل المثال، في تطبيق جهاز مراقبة الجنين المبين في الشكل رقم (١٠٦,٢) فإن الامتثال التام مع إجراء اختبار التكامل يؤكد ضمان تجميع ومعالجة وأرشفة بيانات الجنين في الزمن الحقيقي (بما في ذلك كافة الميزات الهامة مثل إنذار شذوذ معدل ضربات قلب الجنين) في حين تشغيل التطبيقات "الخارجية". كلما زادت خطورة واعتماد التطبيقات الأصلية على

الزمن، وجب على إجراء اختبار التكامل أن يكون أكثر تقييداً ومحافظةً. انظر إلى الشكل رقم (١٠٦,٣) من أجل جزء من عينة إجراء اختبار التكامل.



الشكل رقم (١٠٦,٢). نظام مراقبة الجنين مع إمكانية للوصول الخارجي.

OB TraceVue Archiving Functionality Test

Test Instructions Follow these instructions, marking your results on the Worksheet

Archiving Functionality
Procedure 1: Partitioning the optical drive 1. Connect the optical drive to the SCSI interface 2. Insert an optical disk into the drive 3. Start the server 4. Start Disk Administrator from the Administrative Tools menu 5. Format the optical disk 6. Create a partition on the optical disk
Procedure 2: Checking the optical drive Archive 1. With the third party running, start OB Trace Vue on the server with the optical drive and optical disk 2. Create one user and one bed using default basic alert settings 3. Assign Bed 1 to serial port A 4. Turn on the fetal monitor's recorder 5. Admit a new patient into Bed 1 6. Obtain a 5 minute trace with a fetal heart rate of 190 and toco that switches between 60 and 10. 7. Close the episode in Bed 1 8. Wait for 15 minutes 9. Retrieve the archived episode into Bed 1 10. Make a printout of the retrieved trace

الشكل رقم (١٠٦,٣). عينة من إجراء اختبار التكامل (Phillips، ٢٠٠١).

الموثوقية وضبط الجودة
Reliability and Quality Control

من أجل ضمان العمل الموثوق للأنظمة الطبية القائمة على الـ COTS فيجب أن يعمل النظام بأكمله (أي المُبدل والربط وأجهزة الـ COTS وبرمجيات الـ COTS وبرنامج التطبيق) معاً وبشكل موثوق. يمكن أن تكون أجهزة الـ COTS موثوق للغاية. عادة ما تتمثل أضعف النقاط من وجهة نظر الموثوقية في برمجيات الـ COTS (أنظمة التشغيل) وفي برمجيات التطبيق.

غالباً ما يُعبَّر عن موثوقية برمجيات نظام التشغيل بعدد من الرقم "تسعة" حيث تُمثِّل "تسعَتين" زمن جاهزية ٩٩٪. إن موثوقية Windows NT 4.0 الواردة في التقارير هي "تسعَتين". يُعادل هذا الرقم بالنسبة إلى نظام التشغيل الذي يعمل بشكل مستمر نحو ٨٠ ساعة توقف عن العمل في السنة. أما موثوقية Windows 2000 فهي ٩٩,٩٥٪ أي ثلاث تسعات (أي فترة توقف غير مُجدولة قدرها خمس دقائق في السنة). كانت الإصدارات القديمة من Windows أقل موثوقية. إن أي مقارنة كمية لموثوقية أنظمة التشغيل المختلفة (مثل UNIX مقابل Windows 2000) سوف تكون مثيرة للجدل وغير موثقة بشكلٍ جيد بسبب غياب معايير مقارنة قياسات موثوقية البرمجيات. حاولت بعض الشركات قياس عدد مرات إعادة التشغيل خلال فترة زمنية معينة، ولكن حتى هذا المبدأ كان مُشتبهاً لأن لأنظمة التشغيل المختلفة مُتطلبات مُجدولة مختلفة لإعادة التشغيل (مثل متطلبات إعادة التشغيل التي تحدث عندما يتم تثبيت تطبيقات جديدة في الإصدارات القديمة لنظام Windows). ومن المعروف والموثق أيضاً بشكل جيد أن الإصدارات الأحدث لـ Windows (مثل Windows 2000) هي أكثر موثوقية وتتطلب عدداً أقل من عمليات إعادة التشغيل مقارنةً مع الإصدارات القديمة (مثل Windows 3.1 و Windows 95 و Windows 98). كما أن نظام UNIX والعديد من متغيراته هي عموماً أكثر موثوقية من الإصدارات القديمة لـ Windows. ويبقى أن نرى ما إذا كان موثوقية Windows 2000 يمكن أن تساوي موثوقية UNIX.

تُقدم الأنظمة المتكاملة إلى مُصنعي الأجهزة الطبية التحدي المتمثل في ضمان الجودة على المستوى المطلوب بالنسبة إلى الجهاز طبي، كما توفر لهم في الوقت نفسه استخدام برمجيات نظام التشغيل COTS وأجهزة COTS التي قد لا تكون قد خضعت لمثل بروتوكول ضبط الجودة الصارم هذا. تقوم الـ FDA في الولايات المتحدة بتنظيم الشركات المصنعة للأجهزة الطبية وتفرض وجود تدابير ضبط جودة مختلفة. وفقاً لوثيقة الـ FDA ذات العنوان "استخدام البرمجيات الجاهزة في الأجهزة الطبية"(FDA، ١٩٩٩) فإن الشركة المصنعة للأجهزة الطبية والتي تستخدم البرمجيات الجاهزة "لا تزال تتحمل المسؤولية عن استمرار الأداء الآمن والفعال للجهاز الطبي". يعتمد مستوى المصادقة والتحقق اللازم للأنظمة الطبية القائمة على البرمجيات (مثل أي جهاز طبي آخر) على شدة المخاطر المحتملة

على المريض والمشغلين والمارة إذا حصل أي فشل في النظام بغض النظر عن سبب الفشل سواء كان في البيئة الصلبة أو البرامج.

من الصعب اختبار البرمجيات بشكلٍ شامل. وعلى الرغم من أن البرمجيات لا تتعب أو لا تفشل بشكلٍ كارثي مثلما يحدث في الجهاز الميكانيكي أو أي عنصر من العناصر الإلكترونية، فإن مشاكل البرمجيات تحدث بانتظام. يمكن لهذه المشاكل أن تتراوح من التطبيقات التي لا تعمل كما صُمم لها أن تعمل (حيث يمكن إعادة تشغيلها بحد أدنى من المشاكل) إلى تشغيل نظام ذي توقفات واضطرابات متعددة (التي عادة ما تتطلب إعادة التشغيل على نظام داعم للحياة والذي قد يكون أمراً كارثياً). حتى عندما يتم إجراء الاختبار الشامل، يمكن للأنظمة أن تتعرض لفشل في البرمجيات لعدة أسباب ومنها: (١) مشاكل في الذاكرة التي تتطور على مدى فترات طويلة من الوقت (مثل ما يسمى تسريبات الذاكرة)، (٢) خطأ المُستخدِم أو المُشغل (مثل عملية استرجاع غير ملائمة للنظام من خلال سلسلة نقرات خاطئة على لوحة المفاتيح)، (٣) عدم وجود موارد الكمبيوتر، (٤) المشاكل التي تسببها التطبيقات الخارجية والفيروسات والاختراقات الخبيثة. يجب على الشركات المصنعة للأجهزة الطبية أن تُصمم الأنظمة بحيث تكون موثوقة لأعلى درجة ممكنة وبحيث تكون الأعطال "خفيفة" و لا تؤذي المريض. مع استمرار تطور أنظمة التشغيل فإن وظيفتها في الزمن الحقيقي وموثوقيتها تتحسنان أيضاً كما تتزايد التطبيقات الهامة والأجهزة التي تستخدم الأنظمة القائمة على الـ COTS.

أمن أنظمة المعلومات
Information System Security

يمكن اعتبار نظام أو شبكة الكمبيوتر آمنة عندما تكون مواردها متاحة للمرخَصين باستخدامها فقط وعندما يؤدي استخدام هذه الموارد إلى نتائج موثوقة. لا يمكن الوثوق بالنظام المُعرض للخطر بسبب دخيلٍ ما. كما تُشكل العيوب البرمجية (software bugs) أو أخطاء المستخدم أو الخلل في عمل نظام المرشات (sprinker system) تهديدات لأمن نظام الكمبيوتر. يمر أمن أنظمة المعلومات الإكلينيكية في مرحلة تطور. يُنظم قانون مسئولية وقابلية نقل التأمين الصحي (HIPAA) الأمن المتعلق بسرية بيانات المريض في الولايات المتحدة وقد تمت مناقشة هذا الموضوع في أماكن أخرى من هذا الكتاب (انظر الفصل ١٠٤). يُعتبر تصميم الأمن في أنظمة المعلومات الطبية سمة هامة حيث ينبغي أن تشمل على قضايا أمن توصيل الشبكة وإدارة اسم وكلمة مرور المستخدم وضبط التحديث والإصدار إضافة إلى الأمن المادي لأجهزة الكمبيوتر سواء كانت المخدمات أو محطات العمل التابعة.

يمكن تقسيم التهديدات الأمنية للكمبيوترات إلى أخطاء في الاستخدام والتصميم والهجمات المُتطفلة. تشمل أخطاء الاستخدام والتصميم على ارتكاب المستخدمين المخولين للأخطاء (مثل الحذف العرضي للبيانات) والعيوب

البرمجية المعروفة (أي: الكود الخاطئ للبرنامج أو الكود الذي لم يُختبر بشكل كامل). تشمل الهجمات الخبيثة على: (١) المستخدمين غير المخولين، (٢) مشاهدة البيانات بشكلٍ ضار من قِبَل المستخدمين المخولين أو تغيير البيانات، (٣) التصريح عن كلمات السر من قِبَل المستخدمين المخولين عن قصد أو عن غير قصد، (٤) إدخال الشيفرات الخبيثة على أجهزة الكمبيوتر عن غير قصد (على سبيل المثال، الفيروسات أو أبواب الفخاخ أو الأبواب الخلفية أو هجمات الحرمان من الخدمة أو الاعتراض الإلكتروني غير المصرح به للبيانات)، (٥) الوصول المادي غير المصرح به إلى البيانات أو الأنظمة.

يتمكن التصميم الجيد لنظام الأمن أن يمنع بعض الهجمات المُتطفلة فضلاً عن المشاكل الأمنية غير المقصودة. على سبيل المثال، يمكن للأنظمة أن تفرض كلمات سر ذات ثمانية أرقام التي تشمل على أرقام وأحرف (كبيرة وصغيرة) ورموز خاصة، ومن ثم تكون كلمة السر أكثر صعوبة من كلمات السر التي تتألف من ثلاثة أرقام.

بالإضافة إلى ذلك، تُساعد أنظمة الرعاية الصحية كما يُساعد مسؤولي الأنظمة على الحماية ضد المشاكل الأمنية عن طريق تنفيذ كافة الإجراءات التالية:

١- ينبغي على مسؤول النظام أن يضع مبادئ توجيهية أمنية توثق جميع إجراءات الأمن المادي وضوابط الدخول وسياسات وإجراءات النسخ الاحتياطي وسياسات المراجعة وبارامترات الاستخدام الرئيسي المتعلق بالأمن.

٢- ينبغي على مسؤول النظام أن يُنفذ ضبط الوصول مع ضبط مستوى امتياز الوصول إلى البيانات (مثل امتيازات العرض والإضافة والتعديل والحذف الملائمة لكل مستخدم) وفرض أسماء مستخدمين فريدة وسياسة كلمة مرور قوية بما في ذلك طلب التغييرات الدورية لكلمة المرور. ينبغي النظر في المقاييس الحيوية مثل مسح شبكية العين أوبصمات الأصابع أو طبعات الأيدي عندما يكون المستوى العالي من الأمن مطلوباً. كما ينبغي أن تُنفِّذ الأنظمة ميزة الخروج التلقائي كما ينبغي على المستخدمين عدم ترك الأنظمة مفتوحة (logged) وغير مراقبة.

٣- يجب تفعيل إدارة الأمن المادي. يجب ضبط الوصول إلى حجرات البيانات وغرف المخدمات.

٤- يجب القيام بالنسخ الاحتياطي بشكلٍ روتيني، كما يجب تخزين وسائط النسخ الاحتياطي في مكان منفصل عن نظام الحاسوب ويفضل أن يكون في مكان آمن من الحريق. يُعتبر النسخ الاحتياطي على الأرجح من أهم المهام الأمنية!

٥- يحتاج مسئولي النظام إلى تنفيذ ضبط برامج التحديث والإصدار في امتثال لتوجيهات مُصنِّع النظام الطبي. عندما يوافق المُصنعون والوكالات التنظيمية عندئذ ينبغي تحديث أنظمة التشغيل وبرامج التطبيقات بشكلٍ

دوري بالنسبة إلى تصحيحات وتحديثات الأمان المتوفرة (على سبيل المثال، كشف الفيروسات والتحديثات الصحيحة). تقع على عاتق مسئول النظام مسؤولية مستجدات القضايا الأمنية التي تؤثر على نظام التشغيل وبرامج التطبيقات. عندما يتم الإعلان عن أحد التحديثات، فيجب على المسئول تقييم تأثير هذا التحديث على النظام واتخاذ إجراءات على نحو مناسب وفي الوقت المناسب تبعاً لطبيعة المشكلة وحالة التحديث. قد تكون الاحتياطات المؤقتة (أو الحذر) لازمة حتى يتم تطوير واختبار وتحرير التصحيح من قبل الشركة المصنعة. ويجب أن تبقى الفجوة الزمنية بين اكتشاف الخلل الأمني من قبل قراصنة الكمبيوتر والوقت الذي يتم فيه اتخاذ أي إجراء لازم من قبل مدير النظام قصيرة قدر الإمكان لتقليل فرص التدخلات الأخرى أو وقوع هجمات جديدة. إلا أن التوقيت يُعتبر مشكلة بالنسبة للأنظمة الموافق عليها من قِبَل مركز الأجهزة والصحة الشعاعية للـ FDA (FDA CDRH) حيث إنه من المطلوب إجراء ضبط للإصدار واختبار كبير من قِبَل المُصنعين قبل تنفيذ التحديث.

٦- يمكن في بعض الحالات من أجل حماية الشبكة الحماية تثبيت جدار حماية أو شبكة خاصة افتراضية (VPN) لضبط الوصول من وإلى مواقع محددة عبر المجال وبروتوكول الإنترنت (IP) وغيرها من منهجيات ضبط الوصول إلى الشبكة. يمكن برمجة جدران الحماية لضبط جميع عمليات الدخول والخروج للشبكة المحلية (LAN) أو الواسعة (WAN). يمكن تنفيذ الـ VPN من أجل تغليف وتشفير البيانات الخاصة الموجودة في الشبكة العامة بحيث لا يمكن اعتراضها بسهولة.

٧- يمكن تحقيق الأمن الإضافي عندما يكون مطلوباً بواسطة تقنيات التشفير المختلفة. تُعتبر خصوصية التشفير السلكية (Wired Encryption Privacy "WEP") من إحدى معايير التشفير المعروفة بالنسبة إلى الأنظمة اللاسلكية.

٨- يجب تنفيذ عمليات تسجيل ومراجعة جميع عمليات الدخول لمسئولي النظام ومحاولات الاختراق الممكنة (مثل فشل محاولات الدخول) وغيرها من الأحداث الهامة عندما يكون ذلك متوفراً.

ما الذي ينبغي عمله بشكلٍ عام إذا تم اكتشاف انتهاك أمني كبير؟ أولاً، يجب العودة إلى السياسة الأمنية ومن ثم عمل نسخة احتياطية للنظام بأكمله على القرص في مساحة قرص ليست قيد الاستخدام حالياً (System Snapshot). إذا كان النظام مُرتبطاً بالشبكة فيمكن فصله عن الشبكة إذا كان ذلك هو المصدر المحتمل للاختراق أمني أو إذا كان مصدر الخرق غير معروف. يجب تقييم الاختراق الأمني لدرجةٍ أكبر من أجل تحديد ما الذي حدث وما هي النواحي التي تعرضت للخطر. سوف يحدد ذلك ماهية الإجراءات الإضافية التي يجب اتخاذها بهدف تصحيح أي بيانات أو برامج تعرضت للخطر (على سبيل المثال، استعادة البيانات باستخدام النسخ الاحتياطي الحديث للبيانات والأقراص الأصلية للبرامج حيث تدعو الحاجة وتصحيح الخلل الأمني بحيث يقل ترجيح حدوث ذلك في

المستقبل) ومن ثم تحديد ما إذا كان يجب اتخاذ إجراءات إضافية مثل إخطار المُدراء المناسبين أو وكالات إنفاذ القانون.

يُعتبر وصول البائع إلى نظام المعلومات الطبية من أجل كشف الأعطال والتحديثات سمة متزايدة وشائعة لكنه يُمثل تحدياتٍ أمنية. تشمل الطرائق المعروفة لدخول البائع على مودم الطلب الهاتفي والدخول من خلال الشبكة (على سبيل المثال، شبكة الـ WAN) والوصول إليها عبر الشبكات الخاصة الافتراضية. توفر أجهزة المودم عندما يكون الكادر موجوداً طريقة اتصال بسيطة كما تسمح للمستخدمين النهائيين بفصل المودم عندما لا يكون قيد الاستعمال. ولكن عندما يكون نظام المعلومات موجوداً في مكان آمن أو بعيد أو في موقع لا يوجد فيه كادر، عندئذ فإن تشغيل وإيقاف المودم يُعتبر أمر غير عملي مما يجعل المودم في هذه الحالة مصدراً لمخاطر أمنية. يُعتبر الوصول إلى الـ WAN بسيط ولكنه يمكن أن يكون غير آمن ما لم يتم ضبط الوصول باستخدام جدار الحماية أو غيره من أساليب التصريح. يوفر تركيب تجهيزات الـ VPN طريقة أكثر أمناً لأنها تستخدم البنية التحتية العامة ولكنها تتيح الضبط من خلال الـ IP على غرار جدار الحماية كما أنها تقوم بتغليف وتشفير البيانات. بطبيعة الحال، مع كل أساليب الوصول الخارجي هذه فإن إدارة اسم المستخدم وكلمة السر تُعتبر مهمة أيضاً. كما يُشكل ترك اتصال الإنترنت الثابت (non-VPN) مفتوحاً بشكلٍ مستمر مع اسم مستخدم عام وكلمة سر عامة دعوة إلى التدخل غير المرغوب فيه.

في الخلاصة، تتمثل أكبر التحديات الأمنية بعدم امتثال الصانع أو المستخدم النهائي بالتصميم الأمني والممارسات الأمنية الجيدة للكمبيوتر على النحو المذكور أعلاه. تشمل الممارسات السيئة التي يمكن أن تؤدي إلى أنظمة تالفة على: (١) السماح للمستخدمين ومسئولي النظام باستخدام أسماء مستخدمين "عامة"، (٢) عدم استعمال كلمات المرور أو استعمال كلمات المرور سهلة الكشف، (٣) عدم وجود أمن مادي مما يجعل الأنظمة متاحة للأفراد غير المصرح لهم بالدخول من أجل القيام بأنشطة غير مرخص بها، (٤) اتصالات مع شبكة الإنترانت التي هي في الواقع اتصالات إنترنت عامة من دون جدران حماية أو غيرها من التدابير الأمنية التداخلية، (٥) الأنظمة المرتبطة مع الشبكات من دون برمجيات تفحص للفيروسات، (٦) غياب أو عدم كفاية مسارات المراجعة، الأمر الذي يمنع إجراءات المتابعة الكافية للخرق الأمني. وبالطبع فإن النسخ الاحتياطي الدوري يُخفف ألم التعافي من أي فقدان للبيانات سواء كان ذلك تطفلياً أو غير مقصود.

دعم الأنظمة الطبية المحوسبة
Support of Computerized Medical Systems

توفر الأنظمة الطبية المحوسبة مزايا دعم عديدة لكل من الصانع والمستخدم النهائي. تُتيح اختبارات النظام الذاتية المُدمجة إمكانية قيام الأجهزة باختبار أنفسها وتحديد ما إذا كانت تعمل بشكل سليم أم لا. وبذلك تقوم بعض

الأجهزة المتصلة بالشبكة بتنفيذ الاختبار الذاتي، وفي حال وجدت نفسها أنها لا تعمل بشكلٍ صحيح فإنها تلقائياً تتصل بالشركة الصانعة وتُخبر عن وجود المشكلة. يمكن عندئذ استخدام الوصول عن بعد (التلقائي أو اليدوي) لعلاج مشاكل البرمجيات. تشمل المزايا الأخرى على الأنظمة التي تعمل على شبكة الإنترنت الآمنة من الفشل و"عالية التوفر" والتي تحتوي على كمبيوتر ثانٍ يعمل باستمرار و"يعكس" تشغيل النظام الأساسي حيث يتولى عمليات التشغيل في حال حدوث مشكلة.

تحديات الدعم Support Challenges

يُقدم تكامل الأنظمة مجموعة جديدة من التحديات أمام المصنعين وموظفي الدعم لهذه الأنظمة المعقدة. يجب وضع وسائل جديدة لإدارة ودعم هذه الأنظمة. على سبيل المثال، تحتاج مؤسسات الرعاية الصحية كما يحتاج المصنعين إلى تتبع وضبط إصدارات البرامج والتحديثات على نحو أكثر فعالية بما في ذلك برمجيات وبرامج تطبيقات الـ COTS التي تقدمها الشركات الصانعة. هناك تعارض بين متطلبات الـ FDA لضبط الإصدارات وإصدارات وحزم الدعم المتغيرة باستمرار لـ COTS. يؤثر هذا التعارض على أنظمة المعلومات المتصلة بالشبكة (وجميع فروعها) وبشكلٍ خاص على تحديثات التحسينات الأمنية لأنظمة التشغيل وبرنامج تفحص الفيروسات.

هناك المزيد من الوصف في الفقرات التالية عن التحديات الأخرى للبنية التحتية للمستشفيات والتدريب والتعليم والتوثيق.

البنية التحتية Infrastructure

تُتيح الأنظمة الطبية القائمة على معايير تكنولوجيا المعلومات بالاتصال عبر الـ TCP/IP وعبر معايير أخرى تُعجِّل عملية التواصل. كما تسمح الأنظمة القائمة على المعايير بتثبيت البُنية التحتية العامة للبيانات أثناء البناء وقبل معرفة النظام الإكلينيكي المُحدد الذي سوف يتم شرائه. وتشمل المزايا الأخرى على تركيب أجهزة الكمبيوتر في حجرة البيانات وتوفير المساحة في الموقع الإكلينيكي. تشمل التحديات على بناء حجرات البيانات بمساحات كبيرة بحيث تكفي لإيواء العدد المتزايد من التجهيزات ذات الحساسية العالية وكذلك الترميز اللوني (أو التحديد) للكابلات وغيرها من الأجهزة في حجرة البيانات لا سيما بالنسبة للأنظمة الطبية التي تعمل بالزمن الحقيقي وذلك لفصلها عن التطبيقات المكتبية وغيرها من التطبيقات غير الهامة. يجب توفير تغذية الطاقة غير المنقطعة (UPS) أو طاقة طوارئ إلى هذه الأنظمة في حال انقطاع التغذية من أجل ضمان التشغيل المستمر أثناء اختبارات مولدات الطوارئ. يجب ضبط الوصول إلى حجرة البيانات مع السماح لكادر دعم الأنظمة الطبية بالوصول إليها.

لقد اخترقت العديد من التقنيات اللاسلكية سوق الرعاية الصحية بما في ذلك: (١) 802.11b في تطبيقات القياسات الإكلينيكية عن بعد، (٢) أنظمة الهاتف الخلوي الصغرى لداخل المستشفى، (٣) المساعدات الشخصية

الرقمية اللاسلكية (PADs) للطاقم الطبي. من المطلوب وجود إدارة للترددات وإدارة لموقع نقطة الوصول (الهوائي) من أجل تجنب التداخل بين جميع أصناف التقنيات اللاسلكية التي تتنافس حالياً على سوق الرعاية الصحية. إن عملية التوحيد القياسي للتكنولوجيات اللاسلكية المختلفة هو أمرٌ مهم من أجل الحد من البنية التحتية اللاسلكية ولكنه يُعتبر صعب التحقيق في الوقت الراهن نظراً لاستخدام عدد كبير من المعايير اللاسلكية المختلفة (مثل IEEE 802.11a و IEEE80211b).

التدريب والتعليم Training and Education

إن لدى مهنيي تكنولوجيا المعلومات والهندسة الإكلينيكية وتكنولوجيا التجهيزات الطبية الحيوية الذين يدعمون هذه الأنظمة الطبية والمعلوماتية المتقاربة احتياجات تدريبية جديدة، حيث يحتاج كادر تكنولوجيا المعلومات إلى المزيد من المعرفة الإكلينيكية كما يحتاج مجتمع الهندسة الطبية الحيوية/الإكلينيكية إلى المزيد من التدريب على الكمبيوترات وتكنولوجيا المعلومات. يجب أن يشمل تدريب المهندسين الإكلينيكيين وفنيي التجهيزات الطبية الحيوية على التكنولوجيات الأساسية للكمبيوترات بما في ذلك: (١) أنظمة التشغيل مثل Microsoft Windows و UNIX، (٢) قواعد البيانات، (٣) التطبيقات، (٤) تكنولوجيات الاتصالات مثل الإيثرنت و TCP/IP والإنترنت ونمط النقل غير المتزامن (ATM) واللاسلكية، (٥) التكنولوجيات الجديد ة للكمبيوترات مثل شبكة منطقة التخزين (SAN)، (٦) تعلُّم نظام المعلومات الإكلينيكية. كما يجب على الجميع فهم مواضيع الأمن وسرية بيانات المريض وغيرها من القضايا العامة المرتبطة بتبادل البيانات بشكلٍ أفضل.

التوثيق Documentation

يضم النتاج العلمي للهندسة الإكلينيكية على العديد من المقالات المتعلقة بالتوثيق المطلوب لخدمات الأجهزة الطبية. إلا أنه لم يكتب إلا القليل عن سبل توثيق التجهيزات الطبية المعقدة التي تستند إلى الكمبيوتر وبخاصة الأنظمة المحوسبة للبيانات. من إحدى أساليب التوثيق هو أن يتم طلب ما يلي: (١) المخططات المطابقة للواقع، (٢) كتيبات التشغيل والمواصفات لكل عنصر من العناصر، (٣) كتيبات الخدمة ومعلومات كشف الأعطال لكل عنصر من العناصر المهمة، (٤) الأدوات البرمجية التي تُساعد في كشف الأعطال.

توفر المخططات المطابقة للواقع وسيلة لتوثيق النظام بعد تثبيته حيث أنها تُبين جميع الأسلاك والمحاور والموجهات والمخدمات ونقاط الدخول ومحطات العمل. تُعتبر المخططات المحوسبة المطابقة للواقع المستندة إلى ملفات Adobe Acrobat و PDF إحدى سبل رسم المخططات المطابقة للواقع. يمكن أن تشمل مخططات الشبكة هذه على الروابط السرية "hot links" للطابعات ومعلومات طرفية أخرى كما يمكن أن تتضمن على معلومات بخصوص الموقع المادي للتجهيزات وطرازها ومسارات تبادل البيانات وعناوين الـ TCP/IP وأرقام هواتف المودم وأكثر من ذلك.

من المطلوب توفر كتيبات المُستخدم التقليدية التي تحتوي على معلومات الإعداد والتهيئة حيث يتم تزويدها بشكلٍ عادي. يُعتبر الحصول على كتيبات الخدمة أمراً صعباً ولكنها تُعتبر ضرورية بالنسبة لجميع الأنظمة والمكونات غير الجاهزة التي يكون استبدالها صعباً و/أو باهظ الثمن. يجب أيضاً الحصول على أي أدوات برمجية لكشف الأعطال التي سوف يوفرها البائع إلى العميل كما ينبغي تزويد الوثائق المناسبة واللازمة لعمل هذه الأدوات.

استنتاج
Conclusion

تتغير تكنولوجيا المعلومات بسرعة، وعلى الرغم من أن التكنولوجيا الطبية تتغير بشكلٍ أبطأ من سرعة تغير تكنولوجيا المعلومات إلا أنها تتطور بسرعة. في المستقبل القريب، سوف تشمل التكنولوجيات الطبية الجديدة والناشئة التي تعتمد على تكنولوجيا المعلومات على شبكات لاسلكية جديدة مثل: (١) شبكات البلوتوث الشخصية، (٢) الروبوتات الجراحية ذات الحساسات اللمسية، (٣) الأطراف الاصطناعية "الذكية"، (٤) التعرف المتطور على الكلام، (٥) الصوت عبر هواتف الـ IP، (٦) بث الفيديو الرقمي عالي الجودة وبأسعار معقولة، (٧) مناظير الفيديو القابلة للبلع. سوف يسمح التكامل المبني على المعايير للتكنولوجيا الطبية وتكنولوجيا المعلومات بتواصل محطات العمل مع أنظمة متعددة دون اختبار خاص للتكامل ودون القلق بشأن مشاكل الأداء الهامة. سوف تستمر معدلات نقل البيانات في الزيادة مع استمرار انخفاض التكاليف (مثل غيغابايت إيثرنت وخط DSL أسرع). سوف تندمج البنية التحتية للبيانات والصوت كما سوف تُصبح منافذ البيانات منتشرة في كل مكان مثل منافذ الطاقة الكهربائية. سوف تستمر حجرات البيانات والبنية التحتية للبيانات بالنمو من حيث الحجم والتعقيد مع ازدياد معدل انتقال التجهيزات من الأماكن الإكلينيكية إلى هذه الحجرات بشكلٍ أسرع من سرعة انخفاض حجم هذه التجهيزات.

سوف يتحرك المختبر الإكلينيكي في اتجاهين. سوف تُصبح الاختبارات في نقطة تقديم الرعاية والحساسات الملازمة للمريض في مسكنه أكثر شيوعاً. أما بالنسبة إلى المختبر الرئيسي فسوف يتم إجراء مزيد من الاختبارات عبر المختبرات الآلية المستندة إلى الروبوتات. سوف تُصبح المحطات المركزية لوحدة التمريض أقل أهميةً نظراً للإرسال المباشر لإنذارات جهاز المراقبة الفيزيولوجية وطلبات التمريض وغيرها من المعلومات الهامة إلى مقدمي الرعاية المخصصين. سوف يستمر مستوى تفهم وأهمية المرضى الداخليين بالازدياد كما سوف تنتقل التكنولوجيا إلى غرف المرضى الداخليين بدلاً من أن يتم نقل المرضى إلى التكنولوجيا.

من المطلوب توفر التعليم المستمر لكامل الكادر الإكلينيكي وكادر الدعم من أجل مواكبة هذه التغيرات. كما أنه من المطلوب توفر نماذج جديدة في قيادة تكنولوجيا الرعاية الصحية من أجل إدارة التكنولوجيا الإكلينيكية والمعلوماتية المتكاملة.

المراجع

References

FDA. Off-the-Shelf Software: Use in Medical Devices. Bethesda, MD, FDA, 1999.
OB Trace-Vue Integration Test Protocol. Andover, MA, Philips Medical Systems North America, 2001.

مواقع على الإنترنت

Internet websites

Adobe Acrobat: www.adobe.com
Bluetooth: www.bluetooth.com
Windows 2000 Server Family: Delivering the Level of Reliability You Need. Available at http://www.microsoft.com/windows2000/server/evaluation/business/overview/reliable/default.asp
Klaus CW, Wireless LAN Security 802.11b and Corporate Networks, Internet Security Systems. Available at www.iss.net/wireless