ENDPOINT SECURITY IN ELGA ARCHITEKTUREN

Unterthiner S[1], Hafner M[1], Breu R[1] , Schabetsberger T[2]

Kurzfassung

Die elektronische Gesundheitsakte (ELGA [1]) ist eine der größten IT Herausforderungen im Gesundheitswesen. Ziel der ELGA ist es, die lebenslange Krankengeschichte der Patienten zu verwalten und den behandelnden Ärzten zugänglich zu machen. Sicherheit ist dabei ein zentrales Thema, das für die gesellschaftliche Akzeptanz der ELGA zentral ist. In diesem Beitrag betrachten wir die allgemeine Sicherheit der verschiedenen Komponenten eines ELGA Netzwerkes und gehen dabei besonders auf die Sicherheit der Endknoten, also der Rechner der Ärzte und ähnlichen Dienstleistern, ein.

1. Einleitung

Eine der grundlegenden Fragen bezüglich der Sicherheit von Informationen ist jene nach dem Wert der zu schützenden Information. Je höher der Wert der Information, desto mehr Ressourcen wird ein möglicher Angreifer bereit sein aufzubringen, um die Information zu erhalten. Wie viel ist nun die Gesundheitsakte wert?

Der Wert einer einzelnen elektronischen Gesundheitsakte (ELGA) rechtfertigt meist keinen komplexen Angriff. Dies ändert sich jedoch ab einigen hundert oder tausend Akten. Bringt ein Angriff auf ein Ziel Zugriff auf eine große Zahl an Akten, steigt damit sowohl die Wahrscheinlichkeit, wichtige Informationen zu erhalten sowie auch die Anzahl potentieller Abnehmer. Eine große Anzahl an digitalen Akten könnte z.B. für Werbung von medizinischen Produkten oder von Versicherungen oder Pharmakonzernen missbraucht werden.

Ziel eines Angriffes auf ein elektronisches Gesundheitsnetzwerk ist dabei im allgemeinen nicht die Zerstörung oder Manipulation der Datenbestände, sondern möglichst unbemerkt digitale Kopien erstellen zu können.

Bekannte ELGA Ansätze zeigen nun Architekturen auf, um die elektronischen Akten sowohl verteilt und dezentral zugänglich zu machen, als auch im gleichen Schritt zu schützen. Dies wird meist mit Verschlüsselungsverfahren, Serverarchitekturen und Protokollen realisiert.

[1] Institut für Informatik, Universität Innsbruck

[2] Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik, Hall in Tirol

1.1 Angriffspunkte einer verteilten eHealth Architektur.

Jede SW-Architektur ist nur so sicher wie ihr schwächstes Glied. In dezentralen Systemen sind drei zentrale Angriffspunkte vorhanden:

1. Das erste und wohl durch die Medien bekannteste Angriffsziel ist ein (beliebiger) Server des verteilten Gesundheitssystems. Wir sehen einen Server als den Erzeuger- und Speicherpunkt der ELGA (oder Teilen davon), während Ärzte und Patienten als Verbraucher der Akte betrachtet werden. Bedenkt man aber die Ziele eines Angreifers und die Architektur eines verteilten Systems, so scheidet dieser Angriffspunkt in den meisten Fällen aus. Die heutigen Technologien machen es schwer, einen gut administrierten und gepflegten Server zu hacken, ohne grundlegendes Wissen über die Sicherheitsarchitektur zu haben, Exploits auszunutzen oder Hilfe von Insidern (z.B. Administor) zu erhalten. Weiters hinterlässt ein Angriff auf einem Server in den meisten Fällen Spuren, ist zeit- und kostenintensiv und im Falle einer dezentralen und verteilten Speicherung der ELGA nicht zielführend, da jeder Server nur Teile einer Akte besitzt.

2. Der zweite Angriffspunkt ist die Kommunikation zwischen den verschiedenen Teilnehmern im Gesundheitsnetzwerk. Diese Kommunikation ist in modernen Systemen über verschlüsselte Protokolle wie SSL, TLS oder modellgetrieben Ansätze wie SECTET [2] abgesichert. Bedenkt man, dass ein (nicht mehr zeitgemäßer) 512 Bit RSA Schlüssel mittels eines Brute Force Angriffes [3] von einem Intel Core Duo X6800 erst nach ca. 1 Jahr geknackt würde, erscheint auch dieser Angriffpunkt für einen massiven Angriff eher ungeeignet, zumal mittlerweile Schlüssel mit 1024 bzw. 2048 Bit verwendet werden.

3. Der dritte Angriffspunkt ist der Verbraucher einer ELGA. Wir betrachten dabei im Gegensatz zu anderen Publikationen nicht vorrangig den Patienten als mögliches Angriffziel sondern den Arzt, den Apotheker oder andere Gesundheitsdienstleister und deren PCs. Bedenkt man, dass auf dem Rechner eines Patienten lediglich eine (oder einige wenige) Gesundheitsakten liegen, würde ein Angriff auf eine zufällige Akte kaum dessen Aufwand rechtfertigen.

Anders als die Server des Netzwerks speichert ein Ordinationsrechner unter Umständen lokale Kopien der besichtigten Akten ab, greift auf eine relativ hohe Anzahl an verschiedenen Akten pro Monat zu und stellt neue Daten über einen Patienten in das Netzwerk. So könnte ein Ördinationsrechner einige hundert Aktenkopien gespeichert haben, welche jedoch im Gegensatz zu den Versionen auf den Servern nicht zerhackt und verschlüsselt vorliegen. Damit wird ein solcher Rechner für einen Angreifer potentiell interessant.

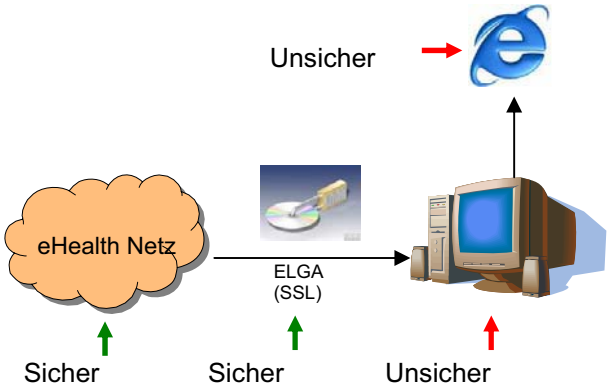

Abbildung 1: Endpunkt Sicherheit im eHealth Netz

Daraus ergibt sich die Frage nach der Sicherheit dieser Knoten des Gesundheitsnetzwerkes wie in Abbildung 1 dargestellt. Geht man außerdem davon aus, dass sowohl die Kommunikation der Kno-

ten des Netzwerkes untereinander als auch die globalen Speicher- und Verwaltungspunkte (Server) sicher sind, so muss man feststellen, dass Sicherheit an den Endpunkten schlagartig und rapide abnimmt. Anders als ein Server, der mittels rigider technischer und administrativer Mechanismen geschützt ist, wird ein konventioneller Rechner, wie ihn Ordinationen oder Apotheken verwenden, kaum die notwendige Sicherheit bieten.

1.2 Sicherheitsstatistik

Berichte der Firma Symantec [4] für die ersten 6 Monate des Jahres 2005 sprechen das Problem klar an. So entwickle sich der Trend von Schadsoftware weg von der Zerstörung und hin zum unbemerkten Kopieren von Daten. Die Studie von Symantec ergab folgendes:

- Es wurden 1.895 neue Software-Schwachpunkte ausgemacht, von denen 79% einfach auszunutzen waren und 97% mittlere oder schwerwiegende Folgen hatten.
- Ein Software-Hersteller benötigt im Durchschnitt laut Statistik 49 Tage zwischen der Veröffentlichung der Schachstelle und deren Behebung. Statistisch gesehen taucht aber ein Exploit (Virus, Wurm oder sonstiger Angriff) nur 6 Tagen nach Bekanntwerden der Schwachstelle auf. Ein Rechner ist somit durchschnittlich 43 Tage lang völlig schutzlos.
- Weiters sind laut Symantec 10.992 neue Viren und Würmer aus 170 neuen Familien alleine in den ersten 6 Monaten des Jahres 2005 entdeckt worden, was 56 Viren pro Tag entspricht.
- Darüber hinaus wurden weltweit geschätzte 7,92 Millionen Phishing Angriffe pro Tag gestartet, wobei es sich laut Symantec dabei um 97.592 verschiedene Angriffsnachrichten im Zeitraum von Januar bis Juli handelte.

Weiters gehen führende Experten wie der Mitentwickler von TCP/IP und „Vater des Internet“ Vint Cerf [5] davon aus, dass zur Zeit ca. 25% aller an das Internet angeschlossenen PCs weltweit in einem sog. Botnet gefangen sind, also von schadhafter Software infiziert wurden und ohne Wissen der Besitzer missbraucht werden. Berücksichtig man diese Schätzung bedeutet dies, dass auch 25% aller Ordinationsrechner infiziert sein könnten und sich völlig vom Arzt unbemerkt unter Fremdkontrolle befinden dürften. Diese Statistiken zeigen eine ernst zu nehmende Problematik auf, welche im Zusammenhang mit ELGA ein nicht zu kalkulierendes Gefahrenpotential darstellt.

Bedenkt man nun weiters, dass die meisten verteilten eHealth Architekturen Webportale zum Sichten der ELGA planen, wird die klaffende Sicherheitslücke offensichtlich. Die ELGA der Patienten eines Arztes liegen demnach zumeist ungeschützt auf dem Rechner des behandelnden Arztes. Ist dieser Rechner von einem Trojaner oder anderer Schadsoftware infiziert, verliert der Arzt unbemerkt jegliche Kontrolle. Ohne dass dies bemerkt wird, kann schadhafte Software die Akte problemlos kopieren und an den Angreifer verschicken. Die Risiken und der Aufwand für einen Angreifer sind dabei sehr gering. Nicht systematisch gewartete Rechner loggen kaum oder gar nicht den Datenverkehr mit und die Gefahr, bei einem Angriff bemerkt und belangt zu werden ist für den Angreifer vernachlässigbar. Ebenfalls äußerst bedenklich ist die Tatsache, dass es für den Angriff auf einen relativ ungeschützten Rechner kaum tief greifendes technisches Wissens bedarf. Eine Infizierung mit einem Trojaner kann über Phishing-Angriffe selbst erfahrene Benutzer betreffen und ist ohne großen Aufwand großflächig durchführbar.

Kritisch ist, dass der Arzt gesetzlich verpflichtet ist, die Daten der Kunden zu schützen. Dass er dazu aber in den meisten Fällen technisch und administrativ gar nicht in der Lage ist, wird dabei in vielen Architekturansätzen nicht berücksichtigt. Gesetzlich dürfte der Arzt jedoch haftbar gemacht werden, wenn ihm Fahrlässigkeit bei der Absicherung seines Rechners nachgewiesen wird.

Zusammenfassend kann gesagt werden, dass eine elektronische Gesundheitsakte ohne Möglichkeiten der Absicherung der Daten an den Verbraucherknoten äußerst bedenklich ist.

2. Lösungen

Prinzipiell geht der Trend in der Soft- und Hardwarebranche der nächsten Jahre eindeutig mehr auf die Absicherung der Endpunkte, also der Benutzer-PCs, ein. Trusted Computing (TC [6]) und TC-fähige Betriebssysteme wie Microsoft Windows Vista [7] oder Linux 2.6.12 [8] unterstützen diese Entwicklung. Über diese Technologien ist es möglich, mehr Sicherheit zu garantieren. So kann nicht mehr unbemerkt schadhafte Software auf einem Rechner installiert werden und Software kann keine geschützten Bereiche des Arbeitsspeichers auslesen oder gar das Betriebssystem modifizieren. Dies sind die Angriffspunkte an denen zumeist Trojaner ansetzen und die Integrität des Rechners kompromittieren. Besagte Technologien sind teils noch in Entwicklung, teilweise bereits verfügbar. Eine bestmögliche Sicherheit der Endpunkte ist durch diese Technologien durchaus erreichbar, jedoch ist davon auszugehen, dass es noch mindestens 5 Jahre dauern wird, bis diese Technologie massentauglich und weit verbreitet ist.

2.1 Lösungsansatz

Unser Ansatz zur Absicherung der ELGA an den Endknoten ist ein Zwei-Phasenplan. *Schritt 1* ist die Einführung eines Digital Privacy Management Systems (DPM), ähnlich dem Digital Rights Management (DRM [9]), welches heute bereits digitale Medien wie MP3's vor illegalen Kopien schützt. Technisch sind DRM und DPM ähnlich, fachlich haben beide Konzepte aber sehr verschiedene Aufgaben und Zielsetzungen. Diese Phase wird von uns *SoftDPM* genannt. Prinzipiell ist der Gedanke der folgende: jedes Datenpaket welches das ELGA Erzeuger-Netz (Server) verlässt und auf einem Verbraucher (z.B. Ordinationsrechner) gelesen werden kann, wird in ein DPM Packet eingeschlossen. Ein DPM Packet besteht aus zwei Komponenten, einer *Policy* und einem verschlüsselten Datenpaket. In der Policy legt man den Zugriff auf das Datenpaket fest. So kann man dadurch z.B. festlegen, dass eine ELGA Akte nur für einen bestimmten Zeitraum lesbar sein soll, sich nach dem Ablauf einer Frist vom Verbraucher-PC selbst entfernen muss oder nur nach Eingabe der Bürgerkarten von Arzt und Patient lesbar sein soll (4 Augen Prinzip). Der zweite Teil des DPM Paketes ist die ELGA selbst, also die Daten die der Erzeuger dem Verbraucher zur Verfügung stellt. Das DPM Packet wird durch kryptografische Verfahren verschlüsselt und damit geschützt. Denkbar ist hier, das DPM Packet mit der Bürgerkartenumgebung zu verknüpfen, sodass der Verbraucher das DPM Packet nur entschlüsseln kann, wenn erst der Arzt und dann der Patient ihre Chipkarten in das Lesegerät geschoben haben. Prinzipiell ist unser Ansatz hier jedoch sehr flexibel und nicht an eine spezielle Prozedur gebunden.

Um jedoch eine Entschlüsselung und eine Einhaltung der Policies zu ermöglichen, muss eine spezielle Ansichtssoftware benutzt werden, vergleichbar mit Secure Viewer, welcher in der Bürgerkartenumgebung vorgesehen ist. Ein gewöhnlicher Browser bietet keinerlei Sicherheit in dieser Hinsicht und nicht die benötigte Funktionalität. Die Akte selbst kann weiters sicher auf der Festplatte in ihrem DPM Container abgespeichert werden. Es bleibt mit Phase 1 natürlich weiterhin das Problem des unsicheren PCs erhalten. Jedoch kann ein Trojaner nun nicht mehr problemlos die Akte von der Festplatte kopieren und per Web versenden, da sie auch weiterhin im DPM Container verschlüsselt bleibt. Ohne die nötigen Schlüssel, z.B. jener der Bürgerkarte, kann die Akte nicht entschlüsselt werden. Wählt man ein Verfahren, welches das DPM Packet mit einem kombinierten Schlüssel auf Arzt-Schlüssel und Patienten-Schlüssel verschlüsselt, ist jede einzelne Akte auf dem Rechner des Arztes mit einem anderen (kombinierten) Schlüssel geschützt. Ein Brute Force Angriff auf jede einzelne Akte ist somit extrem aufwändig und rechtfertigt kaum die eingesetzten Mittel.

Klar ist, dass Phase 1 nur einen Zwischenschritt auf dem Weg zu einem akzeptablen Sicherheitsstandard darstellen kann. So ist durch die DPM Lösung zwar sichergestellt, dass ein Trojaner nicht einfach unbemerkt Akten kopiert oder mitloggt, trotzdem befindet sich die Akte zum Zeitpunkt der Visualisierung ungeschützt und unverschlüsselt im Hauptspeicher des Rechners. Ein Trojaner kann also weiterhin die Akte aus dem Speicher kopieren, das Betriebssystem modifizieren oder unsere Secure-View-Anwendung ändern. Jedoch ist dazu bereits fundiertes Fachwissen von Nöten. Durch zahlreiche konzeptionelle und architekturbezogene Maßnahmen kann man die Hürden noch erhöhen, erwähnt sei hier als Beispiel eine online Software-Attestation des Viewers beim Start der Software.

Phase 2 beinhaltet die Einführung der TC-Hardware und eines geeigneten Betriebssystems. Dies erfolgt sobald die Marktdurchdringung der Technologien groß genug ist und etwaige Kinderkrankheiten ausgemerzt sind. Wir nennen diese Phase HardDPM, da nun das Betriebssystem dank der zugrunde liegenden Hardware nicht mehr unbemerkt modifiziert werden kann. Damit ist das Betriebssystem eine vertrauenswürdige Basis. Das Betriebssystem kann mittels eines signierten Hashwertes des Viewers vor dessen Start feststellen, ob dieser verändert wurde. Ist dies der Fall, wird der Benutzer darauf hingewiesen und das Betriebssystem weigert sich, die Applikation zu starten. Weiters schützt das nunmehr nicht mehr unbemerkt modifizierbare Betriebssystem den Speicherbereich der verschiedenen Applikationen. Damit kann eine Applikation nicht mehr den Speicher einer anderen Applikation auslesen. Interessant ist bei dem kombinierten Ansatz von DPM und TC vor allem der stufenlose Übergang, da sich beide Technologien gegenseitig vervollständigen.

So kann man natürlich auch Ärzten und anderen Dienstleistern freistellen, ob sie direkt auf die sichere Variante in Form von Phase 2 setzten wollen oder noch warten. Das Sicherheitsgrundgerüst ist jedoch bereits bei Einführung der ELGA vorhanden.

3. Ergebnisse

Das Ergebnis unserer Sicherheitsanalyse hat gezeigt, dass Sicherheit die Endbenutzer mit einbeziehen muss. Unserer Meinung nach ist auch mittels handelsüblicher Technologie ein hohes Niveau an Sicherheit möglich, allerdings nicht ohne zusätzliche Sicherheitsmaßnahmen und ohne bereits die Architektur einer verteilten Gesundheitsakte zur Entwurfszeit an diese Erfordernisse anzupassen. Ein DPM Container kann demnach eine sichere Aufbewahrung sowie Zugriffsrechte der Akte gewährleisten, TC und ein geeignetes Betriebssystem den Speicher, die Kommunikation und die Applikation vor Schadsoftware schützen.

4. Diskussion

Völlige Sicherheit ist nicht realisierbar, aber ein höchstmögliches Maß stets erstrebenswert. Der von uns vorgestellte Ansatz bringt den Vorteil, dass wir die Sicherheit stufenweise erhöhen können und dabei die aktuelle Technologieentwicklung berücksichtigen.

Es sind auch andere Ideen zur Endpunktabsicherung denkbar, welche aber entweder völlig auf Hardwarelösungen oder auf reine Softwarelösungen setzen, was uns jedoch als nicht ziel führend oder zu kostenintensiv erscheint.

5. Referenzen

[1] Arbeitsgemeinschaft ELGA. [zitiert;Quelle: http://www.arge-elga.at/index.html.

[2] M. Hafner, B.A., R. Breu, A. Nowak, SECTET -An Extensible Framework for the Realization of Secure Inter-Organizational Workflows. Emerald Press, Inc, 2006.

[3] Brute force attacks on cryptographic keys. [zitiert;Quelle: http://www.cl.cam.ac.uk/~rnc1/brute.html.

[4] Symantec. Symantec Internet Security Threat Report Tracks Notable Rise in Cybercrime Activity. 2005 [zitiert;Quelle: http://www.symantec.com/about/news/release/article.jsp?prid=20060307_01.

[5] Cerf, V. Vint Cerf: Ein Viertel der Internet-PCs ist Mitglied eines Bot-Netzes. 2007 [zitiert;Quelle: http://www.heise.de/newsticker/meldung/84317

[6] Trusted Computing Group. [zitiert;Quelle: https://www.trustedcomputinggroup.org/home.

[7] Microsoft. Windows Vista und Trusted Plattform Module. 2006 [zitiert;Quelle: http://www.microsoft.com/germany/technet/prodtechnol/windowsvista/library/29201194-5e2b-46d0-9c77-d17c25c56af3.mspx.

[8] Linux 2.6.12 unterstützt TC. [zitiert;Quelle: http://www.golem.de/0506/38712.html.

[9] Digital Rights Management and Privacy. [zitiert;Quelle: http://www.epic.org/privacy/drm/.