SecTelMed â€“ sichere Kommunikation Ã¼ber Ã¶ffentliche Leitungen

Aufbau und Entwicklung einer sicheren und frei verfÃ¼gbaren TelemedizinlÃ¶sung

M. KÃ¤mmerer, G. Klos, P. Mildenberger
Klinik und Poliklinik fÃ¼r Radiologie des UniversitÃ¤tsklinikums Mainz

Aus dem Bedarf heraus radiologische Bilddaten zur Telekonsultation zwischen der Diakonie Bad Kreuznach und der Uniklinik Mainz auszutauschen entstand das Projekt SecTelMed. Ein wichtiger Punkt war die Integration der bereits vorhandenen IT-Infrastrukturen. Das bedeutet, die LÃ¶sung musste sich unproblematisch in bereits vorhandene Strukturen eingliedern lassen. Dies erleichtert die Installation und Administration und ist somit kostengÃ¼nstig. Sicherheit und Datenschutz sind bei der Kommunikation medizinischer Daten eine Grundvoraussetzung. Um das Rad nicht neu zu erfinden wurde hierfÃ¼r auf Standardsoftware aus dem Open Source Bereich beziehungsweise auf frei verfÃ¼gbare Software zurÃ¼ckgegriffen. Dies war auch notwendig, um eine Schnittstelle zum unkomplizierten Datenaustausch mit anderen Telemedizinprojekten zur VerfÃ¼gung zu stellen.

1 Material und Methodik

1.1 Programme und Programmbibliotheken

Die verwendeten Programme und Bibliotheken ergeben sich aus den praktischen Notwendigkeiten. Als Datenaustauschplattform wird uns Zugang durch die Netzwerkgruppe der Uniklinik Mainz zu dem bereits bestehenden SSH-Server in der Demilitarisierten Zone (DMZ) gewÃ¤hrt (Abb. 1). Der Zugriff auf den Datenserver erfolgt durch einen SSH-Tunnel gesichert aus dem Internet heraus. Der definierte Durchgang durch die Firewall kommt durch ein Portforwarding Ã¼ber einen VPN-Router zustande. Eine VPN-Verbindung wird nicht aufgebaut. FÃ¼r die Kommunikation mit diesem Server ist eine SSH-Verbindung notwendig. Die eigentliche DatenÃ¼bertragung erfolgt durch Secure Copy [1, 2]. Dazu wurden zunÃ¤chst die freien Implementationen Putty (SSH) und PuttySCP (SCP) [3] verwendet. Aufgrund der schnelleren Ãœbertragungsgeschwindigkeit wurden diese durch die OpenSSH [1] Bibliothek ersetzt. Damit ist zunÃ¤chst der DatenÃ¼bertragungsweg gesichert. FÃ¼r eine ausreichende Datensicherheit, wie sie im Bundesdatenschutzgesetz [4] gefordert wird, ist zusÃ¤tzlich eine hinreichende VerschlÃ¼sselung der Ãœbertragungsdaten notwendig. Wir verwenden hierfÃ¼r den quasi Standard fÃ¼r VerschlÃ¼sselung â€žPretty Good Privacyâ€œ (PGP) in der frei verfÃ¼gbaren Variante GnuPG aus dem OpenPGP Projekt [5]. Da Bilddaten in grÃ¶ÃŸerer Anzahl und GrÃ¶ÃŸe zu verschicken sind mÃ¼ssen die Daten noch zusammengefasst und verlustfrei komprimiert werden. Dazu werden die Standardbibliotheken tar und bzip2 verwendet. â€žTarâ€œ ist ein Archivierungsformat, welches ausschlieÃŸlich eine gegebene Dateistruktur in einer Datei zusamm fasst (Archivdatei). Die Kompression erfolgt verlustfrei durch den bzip2 Algorithmus [6]. Der Empfang der Bilddaten wird durch StoreSCP aus dem DICOM Toolkit von OFFIS [7] geregelt. Da die telemedizinischen Daten auch wieder in einer anderen DICOM/ PACS Umgebung gespeichert werden, wird nach dem Empfang, getriggert durch Store- SCP, die Patientenidentifikationsnummer (PatientID, Tag 0010:0020 des DICOM Headers) mit einem frei wÃ¤hlbaren Prefix versehen. Als letztes Programm kommt fÃ¼r den Datentransfer noch StoreSCU zum Einsatz. Hiermit kÃ¶nnen nach erfolgreichem Empfang der DICOM Daten diese wieder in einem gegebenenfalls vorliegenden DICOM-Netzwerk an die entsprechende Arbeitsstation weitergeleitet werden. Damit eine RÃ¼ckmeldung an den Benutzer erfolgen kann verwenden wir zusÃ¤tzlich noch eine Email-Bibliothek, welche Emails optional nach erfolgtem Versand/Empfang den Erfolg/Misserfolg an beliebige Email Adressen Ã¼ber einen SMTP-Server verschicken kann.

1.2 SecTelMed Control Center

Die oben genannten Programme und Bibliotheken sind in der manuellen Verwendung recht kompliziert zu bedienen, da umfangreiche Kommandozeilenparameter zu Ã¼bergeben sind. Deswegen werden diese durch unsere Eigenentwicklung SecTelMed als Frontend gesteuert. Die Applikation ist als Serverprogramm zu verstehen das normalerweise im Hintergrund (Backend) arbeitet. Sobald die Konfiguration abgeschlossen ist besteht keine Notwendigkeit mehr mit dem Programm in Interaktion zu treten. Die gesamte Kommunikation mit dem SecTelMed Server findet Ã¼ber jedes beliebige DICOMSend und -Receive fÃ¤hige Programm sowie die optionalen BestÃ¤tigungs-Emails statt.

1.2.1 Verbindungsverwaltung

Das Control Center verwaltet die zuvor genannten Applikationen und Bibliotheken. DarÃ¼ber hinaus werden aber auch die notwendigen Kommandozeilenparameter durch das SecTelMed verwaltet. HierfÃ¼r kommt zusÃ¤tzlich die OpenSSL Bibliothek [8] zum Einsatz, um so die notwendigen Login/Passwortkombinationen verschlÃ¼sselt ablegen zu kÃ¶nnen. Diese und andere Einstellungen werden nach den AE-Titeln [Abb. 2. 1] getrennt gespeichert. Weiterhin findet die OpenSSL Bibliothek Verwendung fÃ¼r die Generierung von MD5 und SHA1 Summen zur IntegritÃ¤tsprÃ¼fung der verschiedenen von SecTelMed verwendeten Programmteile und der Ã¼bertragen Daten.

Die Steuerung des StoreSCP erfolgt Ã¼ber eine durch das Control Center generierte Stapeldatei (Batch) [Abb. 2. 2], die zum Beispiel durch Ablage in dem Autostartverzeichnis automatisch mit dem Anmelden eines Benutzers startet...

Dokumentinformationen zum Volltext-Download
Â
Titel:
SecTelMed â€“ sichere Kommunikation Ã¼ber Ã¶ffentliche Leitungen
ArtikelÂ istÂ erschienenÂ in:
TelemedizinfÃ¼hrer Deutschland, Ausgabe 2004
Kontakt/Autor(en):M. KÃ¤mmerer, G. Klos, P. Mildenberger
Klinik und Poliklinik fÃ¼r Radiologie des UniversitÃ¤tsklinikums Mainz
Seitenzahl:
4,5
Sonstiges

8 Abb., 2 Diagr. Dateityp/ -grÃ¶ÃŸe: PDF /Â Â 2.870 kBÂ Click&Buy-PreisÂ inÂ Euro: kostenlos

Â

Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschlieÃŸlichÂ zum persÃ¶nlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. Â
Hier gehts zum freien PDF Download...