A Real Time Provider Identity Verification Service for a Trusted Telehealth Video Collaboration

Rajesh Vargheese
Cisco Healthcare Solutions
Cisco
Austin, TX
rvarghee@cisco.com

Prashant Prabhudesai
Cisco Healthcare Solutions
Cisco
Richardson, TX
pprabhud@cisco.com

***Abstract*—Video based telehealth is emerging as an important technology for effective and efficient collaboration between providers and patients. The advantages of receiving care at source not only account for convenience and cost effectiveness but also enable faster access to care. It brings access, experience and efficiencies in the care process. While there are multiple models of telehealth, in this work, we will focus on an on demand telehealth appointment between a provider and a patient. Given that the patient might not have a previous care relationship with the provider, it is extremely important to ensure that the patient is assured that the provider that he is communicating with is verified by a trusted third-party verification service. Today, basic methods such as authentication and authorization are used to verify the identity of the provider at entry. In this work, we take this model further by proposing a real-time in-session provider identity verification service. This leverages video stream analytics and computer vision models to validate the person involved in the session by a third-party verification service. We propose an architecture and method for enabling such a service, which will enhance the trust model – a critical factor in the adoption of on-demand telehealth.**

Keywords: Healthcare, TeleHealth, Video, Real time Analytics, Security, Privacy, Trust, Identity Verification, Collaboration

I. Introduction

The healthcare industry has been attempting to find new models of care delivery as a response to the escalating cost of care, shortage of medical professionals, increased number of patients with chronic diseases and inefficiencies in the current system. Telehealth is emerging as one of the innovations in healthcare industry to address the challenges of access, experience and efficiencies. Video based telehealth attempts to provide care to patients without having to travel to the hospital. Providers and patients interact with each other through video and providers provide remote consultations. Multiple models of telehealth have evolved. Few of them include the traditional models of the established primary care physician for the patient providing care over video, models where the patient can select an available provider from a list of providers and models where the patient calls into the contact center and the system assigns an available provider. These methods provide increased access, convenience and cost-effectiveness for patients and hospitals. At the same time, some of these models introduce new trust and privacy challenges and hence systems must be in place to assure the patient that he is communicating with a verified provider. Today, basic authentication and authorization methods are used to ensure providers are validated by the system at login time. In this work, we will focus only on the third model, where a patient calls into a common service and the system assigns a provider for the consultation and we will propose a real-time in session provider identity verification service to address the trust and privacy concerns in such a model.

The contribution of this paper is to propose an additional level of trust verification using real-time video parameters to ensure secure on-demand telehealth. We provide a high level architecture of such a real-time trust verification service that will provide an added level of trust verification and is built in conjunction with the existing trust mechanisms.

The layout of the paper is as follows: In section 2, we will review the different models of telehealth and how video is used in telehealth. In section 3, we will review the concept of on-demand telehealth appointments. In section 4, we will look at the state of art verification models used in telehealth. In section 5, we will introduce the concept and architecture of the automated trust verification service in telehealth.

II. Video in Telehealth

Telehealth [1] is defined as the use of technology to enable remote consultation between a provider and a patient that are geographically distant from each other. Video in an important element in telehealth and enables the interactive collaboration between the patients and the providers. Based on factors such as use cases, resolution, physical form factors, and capabilities, multiple types of videos are leveraged in telehealth. Today, with the wide adoption of mobile devices and applications, patients have the ability to access care using video from anywhere.

Based on the interaction between the providers and the patients, telehealth can be broadly classified into two categories.

Real-time Synchronous Telehealth: In this model, the patient and providers interact with each other in real time. This is primarily used in primary and specialty care consultations where the provider requires interaction with the patients to enable effective consultations.

COLLABORATECOM 2014, October 22-25, Miami, United States

DOI 10.4108/icst.collaboratecom.2014.257620

Store and Forward: In this model, the conversations at the originating end is recorded and forwarded to the provider, who reviews the case asynchronously. Store and forward method [2] is typically used in scenarios of second opinion and when a real time interaction is not required and resource constraints such as bandwidth exist.

Based on the number of participants involved in an appointment, telehealth can be classified into two categories:

Point-to-Point Appointments: If there are only two participants in an appointment – a typical scenario between a provider and the patient – video flows directly between the two endpoints. This is called point-to-point video appointment.

Multipoint Appointments: If there are more than two participants in an appointment – a typical scenario between the primary care physician, the patient and a consulting specialist – a multipoint unit is used to mix the video to enable each participant to see the rest of the participants. This is called multipoint video appointment.

Based on how the appointments are scheduled and initiated, telehealth appointments can be classified into two categories:

Scheduled: In this type of appointments, the time and the consulting provider is determined in advance and is recorded in an information system such as a scheduler.

On-Demand: In this type of appointments, the consulting provider is determined at the time of appointment initiation.

III. VIDEO ENABLED ON-DEMAND TELEHEALTH APPOINTMENTS

In the case of an on-demand appointment model, the selection of the provider can be initiated by the patient or by the system. For example, a patient can click on a button on a mobile app, make a payment and the system can route the call to an available provider. While these models provide convenience, the fact that the patient has not interacted with the provider can result in a trust issue. [3]

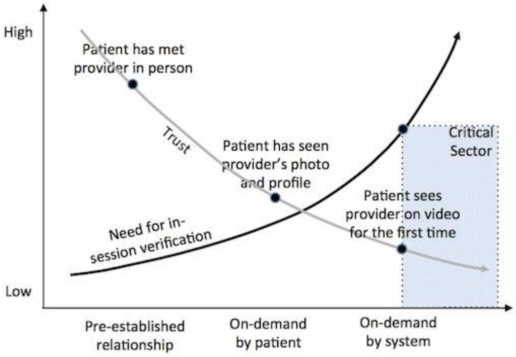

Figure 1. Trust levels of telehealth models

In the graph above, we can see that the trust level goes down as the prior relationship between the provider and patient changes. As the trust level goes down, a system that can perform the verification is needed.

In this work, we will focus on the model where the system selects a provider for the patient (indicated by the shaded area in Fig. 1 above), understand the trust issues and propose an architecture that will address the trust issues.

IV. STATE OF THE ART VERIFICATION

One of the challenges with the on-demand provider based telehealth service models is that the patient does not have a pre-established relationship with the care provider. Other case where a pre-established relationship may not exist is when a patient is referred to a specialist or a primary care physician brings in a specialist into an ongoing video session for consultation.

Today, systems rely on Authentication, Authorization and Accounting (AAA) controls to guarantee trust for a patient. Typically, systems authenticate care providers at login time using multi-factor authentication mechanisms like using basic credentials along with dynamically generated pins. [4]

However such schemes have certain drawbacks in certain scenarios such as the following:

- If the appointment details of a video session are compromised, then there can be no guarantee that the patient is seeing the provider that they expect to see and hence trust cannot be guaranteed for the patient.
- If another person joins the video session while it is in progress, there is no way to guarantee trust for the patient in that situation since authentication is done only at login or session initiation time and only for the provider initiating the session. For example, if a nurse walks into a room where a patient-provider video session is underway, there is no mechanism to verify if the nurse is authorized to be present. In such situations enterprises rely on other modes of compliance and policy controls such as allowing only authorized staff access to resources or training the staff appropriately. There is no runtime trust enforcement in such situations.
- If a care provider such as a specialist is brought in into a consultation video session on an ad hoc basis, it is generally via a simple dial out to the specialist's video device and there is no trust validation for the specialist to guarantee if the specialist is who he says he is.
- If the provider's credentials are compromised without their knowledge then there can be no guarantee that the patient is seeing the provider that they expect to see.

V. AUTOMATED TRUST VERIFICATION SERVICE (ATVS) ARCHITECTURE FOR TELEHEALTH

The primary goal of the proposed automated trust verification service in a telehealth video session is to provide assurance to the patient that the provider that they are communicating with has been verified by a trusted third party service. This enables the patient to share sensitive private health information with the provider to assist in the consultation. In addition, as additional care providers enter the consultation room or the session at the far end, the system continues to keep track of them and verifies that all the people in the communication channel are trusted.

In typical telehealth architectures, the Call Control Unit, the Media Control Unit, the Media Processing Unit (used only for multipoint video), the Firewall Traversal Agent and the various video endpoints form the standard building blocks of a unified video communications infrastructure.

A. Architecture

The Automated Trust Verification System is an overlay on top of the unified video communications infrastructure.

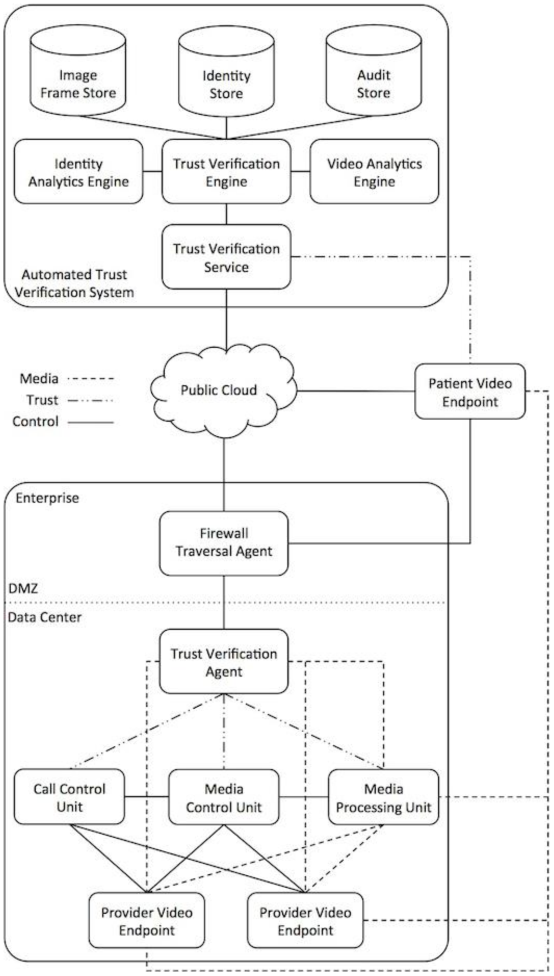

Figure 2. Automated Trust Verification System (ATVS) Architecture

The various architectural components of the ATVS shown in Fig. 2 and their functions are:

Trust Verification Service (TVS) – frontend of the system: Receives requests from the consumers of the service and is responsible for notifying the trust state of the video session and any changes to it to the appropriate entities in the session, namely the patients.

Trust Verification Engine (TVE) – 'brain' of the system: Responsible for evaluating and making decisions about the trust state of a video session using the available trust information, its algorithms and decision support systems.

Identity Analytics Engine (IAE): Responsible for verifying the identities of various entities involved a video session using the identity information available to it and techniques like analytical pattern matching.

Video Analytics Engine (VAE): Responsible for runtime analysis of the sampled image frames captured during the video session and retriggering trust verification if required.

Identity Store (IS): Database of all the care provider user identities along with the information needed for their identity verification like biometrics information and images.

Image Frame Store (IFS): Digital image database for the sampled video images captured during the video session.

Audit Store (AS): Journal of transactions handled by the trust verification system and is used for tracking, audit and reporting purposes.

Trust Verification Agent (TVA): Enterprise on-premise entity that is responsible for initiating and maintaining trust verifications and mediating the trust states between the entities involved in the video session.

B. Operational Flow

The operational flow of trust verification process is made up of two parts – 1) the onboarding of a care provider before they can be associated with a trust state and 2) trust verification and trust state establishment during a video session with a patient.

During onboarding, which is an offline process, a care provider (or an enterprise on their behalf) provides their trust identifiers to the TVS provider. The trust identifiers can be biometric [5] identifiers like facial, iris, and thermal scans as well as behaviometrics [6] identifiers like voice scans. Some of these identifiers are used during initial trust verification and some are for ongoing trust verification while the video session is in progress. The identifiers that need to be provided to establish an identity depend on which biometric and behaviometrics scanners and readers are available to the provider and can be verified during a video session. The TVS provider then verifies the identity of the provider independently and uploads the identity to the IS. The TVS uses multi-factor authentication when verifying identities.

Trust verification during a video session consists of two parts – 1) initial trust verification just before entering a video session and 2) ongoing trust verification during a video session.

Just before entering a video session requested by a patient, the video endpoint requests the care provider to provide their trust identifiers which it sends to the TVA. The TVA collects these identifiers and orchestrates the trust verification by forwarding the identifiers and the image captures from the video endpoint to the TVS. The TVS invokes the TVE which validates the care provider by running the IAE and the VAE against the identifiers of the care provider in the IS and the IFS. If multiple care providers join the video session from the same video endpoint, the VAE detects the condition using its face detection algorithms and triggers the verification procedures in the TVE to be carried out for all the care providers joining the session. [7]

Once the video session is established, the TVA captures the image frames from the video session periodically on an ongoing basis and sends them to the TVE for running through the VAE to ensure that the care providers in the video session can continue to be trusted. If the VAE detects, using its face detection algorithms, that a new participant has entered the video session, (for example, a nurse enters the room while the video session is underway), it triggers the TVE to validate the identity of the new participant. [8]

C. *Trust State Transitions*

The trust state transitions for a single patient-provider video session are depicted in the figure below.

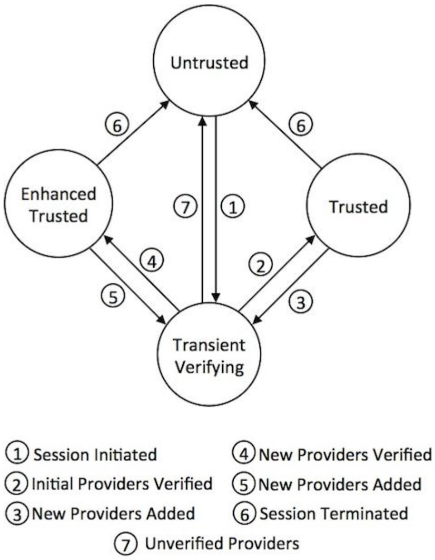

Figure 3. Trust State Transitions

A trust state machine begins in the *Untrusted* state with the patient waiting for the provider to join the video session.

As the provider is joining the session and their identifiers are being verified, the trust state transitions to the *Transient Verifying* state (Visual indication on patient’s screen: spinner).

Once the provider’s identity is verified, the trust state transitions to the *Trusted* state indicating that all the providers in the video session are who they say they are (Visual indication on patient’s screen: locked padlock).

If the system detects new entrants into the session, the trust state transitions back to the *Transient Verifying* state.

Once the identities of the new entrants are verified the trust state transitions to the *Enhanced Trusted* state (Visual indication on patient’s screen: double locked padlock).

If at any time the system is unable to verify the identity of the providers, the trust state transitions back to the *Untrusted* state indicating that one or more providers in the session could not be verified (Visual indication on patient’s screen: unlocked padlock).

D. *Differences From Traditional Approaches*

This trust verification architecture creates a trust model using concepts of the Public Key Infrastructure (PKI) such as 3rd party validation and trust. It builds on top of that model by incorporating concepts like face recognition and real time video analytics to guarantee trust for the patient in a video session. It differs from the PKI in ways wherein the system becomes an integral part of the video communication infrastructure and inserts itself into the path of the media.

Compared with traditional approaches, it makes validating trust a continuous and ongoing process throughout the video session rather than something done only at initiation time. It also introduces dynamic and adaptive elements wherein changes to ongoing sessions are detected and trust states are reevaluated and trust is guaranteed for a patient at every instant during a telehealth session.

Conclusion

Establishing trust is extremely critical in delivery of care via telehealth. Current systems do basic validation but fall short in new models of services such as dynamic on-demand access to care. Our proposed model takes the validation further and provides an enhanced trust model leveraging in-session real time video real time analytics. The key benefits of this approach are improved patient satisfaction, increased trust on behalf of the patients and enhanced compliance.

References

[1] Kareem, S.; Bajwa, IS., "A virtual telehealth framework: Applications and technical considerations," Emerging Technologies (ICET), 2011 7th International Conference on , vol., no., pp.1,6, 5-6 Sept. 2011

[2] Oberleitner, R.; Laxminarayan, S.; Suri, J.; Harrington, J.; Bradstreet, J., "The Potential of a Store and Forward Tele-Behavioral Platform for Effective Treatment and Research of Autism,"

[3] Qian Liu; Shuo Lu; Yuan Hong; Lingyu Wang; Dssouli, R., "Securing Telehealth Applications in a Web-Based e-Health Portal," Availability, Reliability and Security, 2008. ARES 08. Third International Conference on , vol., no., pp.3,9, 4-7 March 2008

[4] Mirkovic, J.; Bryhni, H.; Ruland, C.M., "Secure solution for mobile access to patient's health care record," *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on* , vol., no., pp.296,303, 13-15 June 2011

[5] Gleni, S.; Maple, C.; Yong Yue, "Security Issues of a Biometrics Health Care Information System: The Case of the NHS," *Computing, Engineering and Information, 2009. ICC '09. International Conference on* , vol., no., pp.279,284, 2-4 April 2009

[6] Crandall, A.S., “Behaviometrics for Multiple Residents in a Smart Environment” Ph.D. dissertation, Dept. of Elect. Eng. and Comp. Sci., Washington State Univ., Pullman, WA, 2011

[7] Qiuyan Jin; Woongryul Jeon; Changwhan Lee; Youngchul Choi; Dongho Won, "Fingerprint-based user authentication scheme for home healthcare system," Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on , vol., no., pp.178,183, 2-5 July 2013

[8] Ping Zhang, "A video-based face detection and recognition system using cascade face verification modules," *Applied Imagery Pattern Recognition Workshop, 2008. AIPR '08. 37th IEEE* , vol., no., pp.1,8, 15-17 Oct. 2008