Multi-Factor Authentication for Public Displays using the Semantic Ambient Media Framework

David Bouck-Standen, Josefine Kipke
Kingsbridge Research Center
Hamburg, Germany
email: {dbs, jfk.student}@kingsbridge.eu

***Abstract*—In our interconnected society, public displays deliver private and personalized content. This presents the need to authenticate users in order to protect personal and private information or sensitive contexts of use. In general, authentication mechanisms on public displays are subject to a number of risks, especially, if displays offer multi-touch interfaces or grow even larger. In this contribution, we present a multi-factor authentication system for public displays using the Semantic Ambient Media Framework. In our approach, at first, users use their personal mobile devices, such as smartphones or tablets, to authenticate themselves securely. On the smartphone, a graphical code is displayed, which the user enters on a grid shown on the public display. In a last step, the user confirms the authentication on his smartphone. The code displayed on the smartphone is a one-time and location-based code and no actual credentials have to be typed in on the public display. Thus, this method protects against threads, such as shoulder surfing, thermal attacks, or smudge attacks.**

Keywords-Multi-factor Authentication; Pervasive Displays; Secure Public Authentication;

I. INTRODUCTION

Large multi-touch displays are already deployed in public spaces, such as public squares, airports, train stations, or in streets. Public displays consist of large multi-touch displays connected to a content providing system via the Internet. Today however, there is an increasing demand for public displays to offer access to personalized or context-specific content or functionalities [1]. Accessing protected data and contexts on public displays presents the need of a secure method for user authentication.

Authentication in general requires a user to enter credentials or other means for personal identification, only known to or in possession of the user himself. This could be, e.g., classically a username-password combination, or a thumbprint, iris or other biometrical information unique to the user [2].

The increasing use and functionality of public displays require providing a solution that protects against threats. These can be for example *shoulder surfing attacks* (a), where the user is observed while authenticating [3], *thermal attacks* (b), where heat traces resulting from the user's interactions are made visible revealing the sensitive authentication data [4][5], or *smudge attacks* (c) that exploit the residues from finger prints on touch-screens [6]. Research on these techniques indicate that shoulder surfing occurs in daily contexts [3]. All three attack methods have in common that displaying a digital keyboard or using a software keyboard is vulnerable to them. For this reason and to prevent possible attacks exploiting the users' interactions with the systems, systems for biometrical authentication or gaze-touch have been proposed [7].

Using additional hardware, such as bio-scanners or cameras, for public displays comes with costs and the need to retrofit most public displays currently deployed. A solution with minimal hardware requirements is more likely to be widely accepted. Thus, one of the challenges of this work is to find a solution that does not require hardware upgrades of public displays.

Modern smartphones are personal devices, equipped with different sensors and mostly more than one camera. The smartphone is still on the rise due to its connectivity, as almost 8 out of 10 Internet users in the EU surfed via a mobile or smartphone. The trend toward mobile technology and mobile Internet usage can be observed globally [8].

In this work, we present a technical solution we developed as prototype at the Kingsbridge Research Center (KRC), which addresses these challenges with a minimal technical solution. This makes use of a *multi-factor authentication* (MFA) [2]: The first factor is the *ownership* (i) of a personal mobile device, such as a smartphone. The second factor is *knowledge* (ii) of personal credentials, such as the combination of username and password. Using GPS data, we also use the users and display's *location* (iii) as third factor.

The concept of this work makes use of the interconnectedness of the devices through the Internet, using the Semantic Ambient Media Framework (SAM.F) [9] as an authoritative interface between smartphones and public displays.

In this contribution, we regard related work in Section 2, and present a practical scenario in Section 3. In Section 4, we outline the systems concept and architecture and describe our prototype implementation. In the final section, we summarize our work and illustrate future work.

II. RELATED WORK

This work takes place in the research field of public displays. Related work indicates a general increase in the deployment of public displays [10]. Today, public displays are widely connected in client-server-applications for content

 ISBN: 978-1-61208-737-5

serving purposes, and they are connected through the Internet [10]. For example, Memarovic et al. focus on interconnecting displays, e.g., with social media [11]. Our work ties onto related work through its modular client-server-based architecture. As this work depends on Web-based and modular technology, it can be integrated into existing projects.

Another research field of interest is the field multi-factor authentication, as recently surveyed by Ometov et. al [2]. Ometov et. al outline state of the art methods for MFA, illustrate technical requirements, and identify commercial, governmental, and forensic applications as three market-related groups of applications for MFA. In context with public displays, this work can potentially be deployed in all three field, but the use in commercial applications is most likely.

One of the main challenges of MFA is the absence of a correlation between the user identity and the identities of smart sensors and systems or devices, as Ometov et. al observe [2]. They propose a user-friendly process to establish a trust relationship to gain access rights, whereas Mannan et. al [12] propose a concept to use a personal device to strengthen password authentication from untrusted computers. We apply these theoretical approaches to our technically limited setting, as outlined above, and present a feasible solution for the MFA for public displays using SAM.F.

The research field of semantic frameworks is also of value to this contribution. These frameworks are used to model data structures and interconnect media with applications, services and devices [9][13][14].

With the system called Tacita, Shaw et. al [10] demonstrate a system to personalize public display experience by utilizing proximity detection for user's mobile devices, e.g., with iBeacon technology. Tacita ubiquitously personalizes public displays' content, whereas GTmoPass proposed by Khamis et. al relies on gaze-touch detection through the smartphone and the identification of the display via a Bluetooth Low Energy (BLE) beacon [7]. These approaches are distinguished from the approach presented in this contribution, as the system we develop directly authenticates users and requires a direct user interaction on the public display. It therefore supports direct use, which features the use of public displays in both unauthenticated, as well as authenticated contexts, especially, if personal information or private functionality is displayed. In addition, the solution proposed in this article does not need any supplementary hardware, such as BLE beacons.

The following scenario illustrates exemplary use-cases for the system proposed in this article.

III. SCENARIO

Today, a system administrator is servicing the systems of a museum in Hamburg. On the front wall outside the museum, public displays are installed. To carry out his task, he needs to access the systems and log onto the administrator mode. Standing in front of the display, the administrator uses his smartphone to authenticate him. Then, on the smartphone, a code is displayed. On the public screens, the administrator now accesses the login menu and a grid of 9 symbols appears. He enters the code from his smartphone by touching the five symbols in the correct order. A stroller passes by, curiously watching him entering the code, but the administrator is not alarmed, as the public display now shows a hint indicating, that he has to confirm the login on his smartphone. Using his mobile device, the administrator sees a prompt showing the display name and location. He finds this information is correct and confirms the login. Instantly, the public display changes and shows the administrator's dashboard.

The scenario shows an exemplary use case, in which after a successful logon, the administrator can access features that are hidden from unauthenticated users and also from users, who are not assigned to the administrator group. However, this work only focuses on the authentication process. Thus, modeling the use case is subject to the application applying the login to their system.

IV. SYSTEM CONCEPT AND ARCHITECTURE

For this approach and under consideration of the technical limitations outlined above, the following is the starting point for this work:

- users are in possession of a smartphone or equivalent device connected to the Internet. They have already registered an account with credentials known to SAM.F beforehand, as this is a preliminary requirement of this work.
- public displays are connected to the Internet and run on Web-based technology, e.g., showing Web-based contents in a browser-based system.
- the user sojourns in the vicinity of a public display and intentionally starts a private context.

Figure 1 illustrates the system's architecture and the starting point. In a single location, one or more users and one or more displays can be present. A user interacts with a single display and is in possession of a personal mobile device, as depicted in Figure 1. All public displays and user's devices are connected to SAM.F through the internet. However, a direct connection between a smartphone and any public display does not exist.

 ISBN: 978-1-61208-737-5

Inside SAM.F, the *multi-factor authentication for public displays* (MFA4PD) module is hosted. Public displays and user's devices connect to the MFA4PD module through the Internet. In addition, public displays connect to external content providers, which are not illustrated in Figure 1, for simplification purposes.

The system's architecture benefits from the technical limitations outlined above. As there is no direct connection necessary between the personal mobile device of a user and the public display used for authentication, there is no need for the display provider to open up his network for foreign devices. Thus, a multi-device ecology within the network of the display provider is not required, resulting in less administrative effort. From Figure 1, it can also be observed that no additional hardware, such as, e.g., BLE beacons, is required.

The system concept relies on the interconnection of mobile devices and public displays through SAM.F, which is described in Section A. To begin using a personal or private context on a public display, the user completes the authentication process, as illustrated in Section B. We discuss our approach in terms of security in Section C and describe the prototype implementation in Section D.

A. SAM.F

The *Semantic Ambient Media Framework* (SAM.F) we develop at KRC is a framework semantically interconnecting (a) *media*, (b) *devices*, and (c) *services*, which are enriched by digital properties in the form of semantic annotations [9].

In SAM.F, media consists of text, photos, audio, videos, animations, 3D objects, which are extended by digital properties, e.g., by classifying the media's content using the OWL Web Ontology Language in the internal model of SAM.F.

Digital properties are also Meta data from the original file, such as Meta information on MIME type or encoding. For devices, in SAM.F we model digital properties reflecting, e.g., the devices' capabilities', location, capacity or screen size.

All digital properties are used by the services in SAM.F. Using a dedicated application model, an application accesses the services in SAM.F through Web-based interfaces. Each service serves a dedicated purpose, interconnecting applications through the shared use of devices and media.

The architecture of SAM.F, although described here only with reference to the MFA4PD module, consists of a layer-based system concept, as illustrated in Figure 2. A client application, such as the display or mobile application of this work described in more detail below, connect to the SAM.F *API Web Services* through the *API Security Layer*. Data is exchanged between applications and services, which reside in the *Service Logic* layer, in the form provided by the specification of the *API Client Data Model*. Internally, SAM.F works with a dedicated *Data Model*, as illustrated in Figure 2. Any data is mapped from the *Datastore*, which includes external (semantic) databases, as well as binary data stores, to the internal Data Model, which applies a homogenous model to potentially heterogenic data. For simplification purposes, and in order to reduce the learning curve when implementing applications accessing SAM.F, the internal Data Model is only used in the *Provider Layer*, which contains, e.g., authentication or data providers to be accessed by the upper Service Layer, and in the Service Layer, as shown in Figure 2. Any data provided by a service to a client is mapped to the specific API Client Data Model before being served through the API Web Services and the API Security Layer.

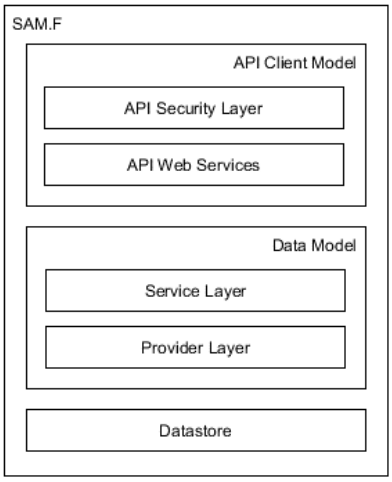

Figure 2. Architecture of SAM.F.

Applying data mapping in SAM.F produces constant overhead, but services and applications, as well as their developers, benefit from only working with data models that are specific to the requirements of the services' or applications' context, reducing overhead when loading large sets of data. Data in this respect describes media, devices and services.

In context of this work, SAM.F serves as authentication provider, which validates user credentials via its standard user service. This work extends the Service Layer of SAM.F by adding the MFA4PD module, which implements the authentication process described in the following section.

B. Authentication Process

To start a private session on one of the public displays, the user opens up the *mobile application* of MFA4PD on his personal smartphone. The user then enters his credentials

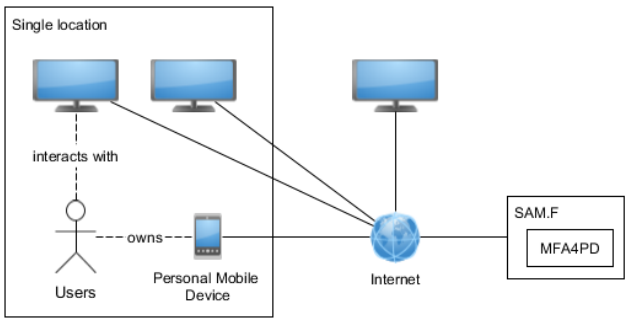

Figure 1. Illustration of the system's architecture and network.

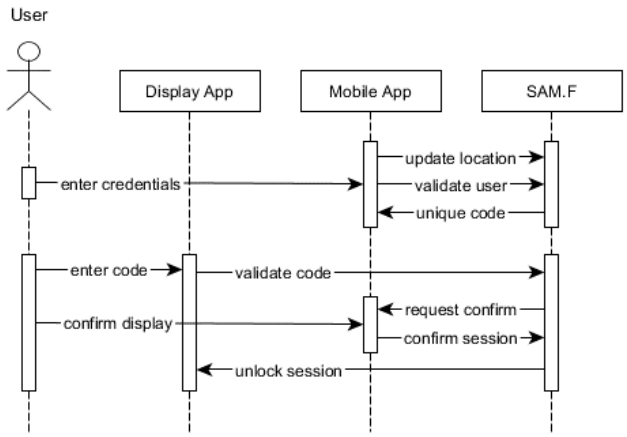

Figure 3. Sequence diagram showing the authentication of one session by a user.

previously registered with SAM.F, which the Web application submits to MFA4PD, as illustrated in Figure 3.

At this point, the process of authentication might be enhanced by further means of MFA, such as gathering biometrical data from fingerprint sensors, facial recognition, or voice sensors. These extensions however might require at least a hybrid application deployment for mobile devices, in order to access the appropriate sensor data. For this reason, in this initial approach, we focused on the Web application combining MFA with ownership and knowledge factors.

The users are identified and authenticated by MFA4PD through their credentials. During the entire process, MFA4PD continues to check the actual location of the user. The location is determined from the GPS data, which is accessible through the smartphone's Web browser API. If any location mismatch occurs, the process to establish a secure session or the session itself will be terminated immediately for security reasons. This feature might prove useful, whenever a user leaves the location of a public display. However, we did not evaluate this feature's aspect nor the accuracy required from GPS data in order to work in an everyday scenario, yet.

After the user's location and credentials are validated, SAM.F generates a code consisting of five symbols, which is shown to the user on his mobile device, as illustrated in Figure 3. The code is valid for a short period of time and the specific user only.

In order to authenticate him- or herself on a public display, the user has to enter the one-time code shown on his smartphone. The user opens up the login dialogue of the *display application* on the public display, and a grid of symbols is displayed. Within this grid, the user now selects the symbols shown on his or her smartphone. The display application communicates the code back to the MFA4PD module, as shown in Figure 3. This serves two purposes:

a. to identify the display, the user selected from the number of public displays available, and
b. to identify the user, who chose a public display.

However, the session is not yet usable. The last step to enable the session on the public display requires the user to again interact with his smartphone in using the *confirm mechanism*. As illustrated in Figure 3, the MFA4PD module sends an authentication request to the mobile application. The dialogue shown indicates a login event took place, together with the name and location shown on the public display. Without the user confirming his or her login on the public display, the session will not be unlocked.

The session on the public display is released after the user's confirmation using the mobile application.

The users can now put their smartphones away and start using the public display, until they log out.

An additional timeout mechanism prevents misuse of the session on a public display.

The users can also close the session at any time using their smartphones, e.g., in case they forgot to select the logout function on the public display. In addition, SAM.F monitors the users' location throughout the entire process and session in order to prohibit misuse of login or automatically logout a session after a user clearly left the screens location.

Now that the systems architecture and concept have been illustrated, in the following section, this approach is viewed with regard to security.

C. Security

As outlined above, related work identifies possible means to attack public display authentication, such as shoulder surfing attacks (a), thermal attacks (b), or smudge attacks (c).

Combining ownership and knowledge factors together with the confirm mechanism, only initially entering the user credentials on the mobile application is vulnerable to shoulder surfing attacks. However, once the trust relationship is established between SAM.F and the users' smartphone for the current location, another mobile application login is prohibited for the duration of that trust membership.

In our prototype, we use session cookies and device cookies to temporarily store trust relationship data. In future work, we will improve and further enhance security, possibly by integrating the Web application into a hybrid application. This way, the device ownership factor is strengthened. In hybrid applications it will be possible, e.g., to read the device's hardware id and bind session.

With regard to the one-time code displayed on the mobile application, as well as the user's input of this code on the display application, they are not vulnerable to shoulder surfing attacks. Again, the confirmation mechanism protects the theft of the session. If any irregularity occurs, the user just declines unlocking the session and generates a new code.

If a user accidentally confirms a session for a code that was used on another display or by anyone else, the simplest way is to just close the session from the user's smartphone immediately. However, this case is unlikely to occur due to the one-time code concept and the narrow time frame in which a code can be used.

Both thermal attacks and smudge attacks cannot be used on public displays in this approach. Once the one-time code has been used, it is invalidated. The statistical possibility of guessing a one-time code can be decreased by a higher

 ISBN: 978-1-61208-737-5

number of symbols used in the one-code, a larger symbol inventory, or a larger grid.

The users are identified and authenticated by MFA4PD through their credentials. During the entire login process and, in concept, during the entire authenticated session, MFA4PD continues to check the user's location. The location is determined from the GPS data, which is accessible through the smartphone's browser API. If any location mismatch occurs, the process to establish a secure session is aborted. Also, in theory, any ongoing session will be terminated immediately for security reasons. This feature might prove useful in case a user leaves the location of a public display without logging out. However, the evaluation of this feature or the accuracy required from GPS data in order for this concept to work in an everyday scenario will be carried out in future work. For Android and iOS devices, we note that continuously monitoring the user's location requires background activity privileges for an application, which a Web browser application usually does not have. Thus, to enhance security by these means currently requires implementing a hybrid app for smartphones.

In summary, with regard to security, the system's concept offers protection against shoulder surfing attacks, thermal attacks, or smudge attacks. In future work, we will also address the question of whether the server can be compromised. We will also focus on possible security issues with regard to client-server communication, in this case the communication between the display application, the mobile application and SAM.F.

D. Prototype Implementation

The prototype consists of three components: (1) the MFA4PD module extending the services of SAM.F, (2) the mobile application and (3) the display application.

SAM.F is developed as Internet Information Services (IIS) application for Windows Servers, as outlined above. The MFA4PD module is implemented as ASMX Web service and a backend-only application, which adds an ASMX Web service to the framework and interfaces with SAM.F.

The mobile application is also developed as IIS application and interfaces with the MFA4PD service. It consists from an ASPX form using JavaScript and AJAX to interact with the frameworks service, whereas the graphical user interface can be customized using HTML and CSS.

The display application consists of a graphical component including the necessary HTML, CSS and JavaScript code. It interfaces with the MFA4PD module via JavaScript through AJAX. The display application also comes with a lightweight backend for session management, that also interfaces with the MFA4PD module. This is currently implemented in ASP.NET.

In order to incorporate the display application into an existing application, we provide code snippets that can be integrated into any application. If a target project does not run ASP.NET, the required server-side code can be translated for other frameworks.

We plan to make the prototype available for non-commercial use later this year.

E. Results and Future Work

We tested the prototype under laboratory conditions with mobile devices running Android with Firefox, Edge and Chrome Web browsers. In all tests, we were able to complete the authentication process. However, an evaluation in an everyday setting with a heterogenic group of users is still pending. In addition, the system still has to be evaluated quantitatively with a larger number of users, for example with regard to system's performance, usability, the user's acceptance, or security.

In order to detect if user's change their location, we currently detect their GPS position through the Web browsers API on their mobile device. We have not evaluated the accuracy of this feature as part of this work. Known issues using this approach are, e.g., the lack of accuracy of GPS in buildings, or that this approach cannot be used under lock screen mode of smartphones. Although the latter issue may be resolved by using a hybrid app, we will also look at other approaches to detect if users leave the location of the public display without logging out of their session, without using additional hardware in the installation next to the public display.

V. CONCLUSION

Public display authentication is vulnerable to various attacks and technically presents a challenge, whenever public displays are connected to protected networks that are inaccessible for other devices and public displays are not equipped with dedicated user authentication hardware.

In this contribution, we present a technical solution we developed at the Kingsbridge Research Center (KRC), which addresses these challenges with a minimal technical solution. This makes use of a multi-factor authentication (MFA) applying the factors of ownership, knowledge and location. Not requiring any hardware upgrades for public displays, the solution implemented as a prototype makes use of the personal mobile devices of users, connecting them, as well as public displays to the Semantic Ambient Media Framework (SAM.F). Through a dedicated Web service module multi factor authentication is provided for public displays in three steps. In the first step, the user is authenticated using his smartphone. In the second step, the user enters a one-time code on the public display, which is displayed on his smartphone. In the third and final step, the user confirms his session on that particular private display on his smartphone.

In the first prototype, authentication on the smartphone is carried out by entering a username-password combination.

Although this work does not focus on implementing more factors at this stage, together with the knowledge factor, the system can be extended with *biometrical* factors, using supplementary sources for multi-factor authentication, such as fingerprint scanners, facial recognition, or voice biometrics.

We have technically validated our approach under laboratory conditions. In the future, we plan to evaluate the system with a large number of users under everyday conditions, in the best case together with a project partner and by using publicly accessible public displays. Research

 ISBN: 978-1-61208-737-5

questions in this area also relate to the degree of security measures, that users are willing to accept in their everyday dealings with digital systems, as well as the question of how they perceive security issues with regard to their use of personal and private data and contexts on public displays.

The Kingsbridge Research Center is a non-profit research company based in Hamburg, Germany. With our research it is one of our goals to strengthen the use of digital technology in public environments in our digital society. We achieve this goal through our scientific and project-oriented work. Currently, our non-profit activities and the development of new future-oriented projects is funded privately. At a time, when many are confronting digitization with skepticism and uncertainty, we are committed to communicating security in the mindful use of these technologies and through fostering awareness.

REFERENCES

[1] T. Kubitza, S. Clinch, N. Davies, and M. Langheinrich, 'Using Mobile Devices to Personalize Pervasive Displays', *SIGMOBILE Mob Comput Commun Rev*, vol. 16, no. 4, pp. 26-27, Feb. 2013.

[2] A. Ometov et al., 'Multi-Factor Authentication: A Survey', *Cryptography*, vol. 2, pp. 1-31, 2018.

[3] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, 'Understanding Shoulder Surfing in the Wild: Stories from Users and Observers', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2017, pp. 4254-4265.

[4] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, 'Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2017, pp. 3751-3763.

[5] K. Mowery, S. Meiklejohn, and S. Savage, 'Heat of the Moment: Characterizing the Efficacy of Thermal Camera-based Attacks', in *Proceedings of the 5th USENIX Conference on Offensive Technologies*, Berkeley, CA, USA, pp. 6-6, 2011.

[6] E. von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, 'Making Graphic-based Authentication Secure Against Smudge Attacks', in *Proceedings of the 2013 International Conference on Intelligent User Interfaces*, New York, NY, USA, 2013, pp. 277-286.

[7] M. Khamis, R. Hasholzner, A. Bulling, and F. Alt, 'GTmoPass: Two-factor Authentication on Public Displays Using Gaze-touch Passwords and Personal Mobile Devices', in *Proceedings of the 6th ACM International Symposium on Pervasive Displays*, New York, NY, USA, 2017, pp. 8:1-8:9.

[8] Eurostat, 'Internet use by individuals', 260/2016, Dec. 2016.

[9] D. Bouck-Standen, 'Introducing SAM.F: The Semantic Ambient Media Framework', in *AMBIENT '19*, Porto, Portugal, *In Press*, 2019.

[10] P. A. Shaw, M. A. Mikusz, P. T. Nurmi, and N. A. J. Davies, 'Tacita-A Privacy Preserving Public Display Personalisation Service', *UbiComp 2018*, pp. 448-451, 2018.

[11] N. Memarovic, I. Elhart, A. Michelotti, E. Rubegni, and M. Langheinrich, 'Social Networked Displays: Integrating Networked Public Displays with Social Media', in *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, New York, NY, USA, 2013, pp. 55-58.

[12] M. Mannan and P. C. van Oorschot, 'Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer', in *Financial Cryptography and Data Security*, Berlin, Heidelberg, 2007, pp. 88-103.

[13] D. Bouck-Standen, 'Construction of an API connecting the Network Environment for Multimedia Objects with Ambient Learning Spaces', Master Thesis, 2016.

[14] D. Bouck-Standen et al., 'Reconstruction and Web-based Editing of 3D Objects from Photo and Video Footage for Ambient Learning Spaces', *Int. J. Adv. Intell. Syst.*, vol. 11, pp. 91-104, 2018.

 ISBN: 978-1-61208-737-5