Reverse Proxy

Seamless Web-Based Anti-Proxy Attendance System

The Team

Team Unproxy

We are batchmates and are also good friends, knowing about each other's technical skills. We did a few projects together and decided to join for the Imagine Cup.

Aditya Mitra (Team Leader), VIT-AP University, Computer Science and Engineering, 2024 – "Some call it the reality, some call it the simulation. In the end, it's all a piece of code."

Anisha Ghosh, VIT-AP University, Computer Science and Engineering, 2024 – "Make it or break it but never fake it."

Anjani Samhitha Jasti, VIT-AP University, Computer Science and Engineering, 2024 – "Keeping it real since <year>."

Rishita Shaw, NIT Durgapur, Electrical Engineering, 2024 – "Trying to be the nicest and hardest working person in the room."

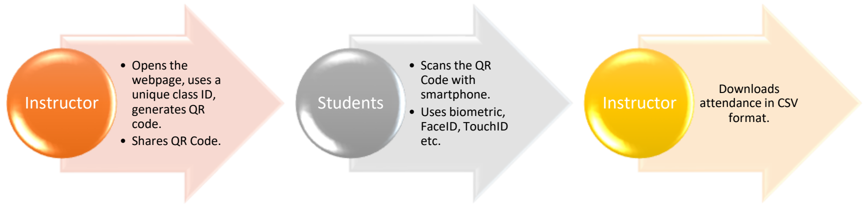
The Concept

Maintaining student attendance has been a problem in various educational institutions. Some have resorted to using manual attendance, which is very vulnerable to proxy attendances. Some are using biometric attendance systems which is not efficient and so on.

Under the theme of education, this project is a web-based framework that can be used to handle student attendance in an institution which is more seamless than the currently used digital attendance systems. It can be used in both online education and offline education modes seamlessly.

Moreover, this project is completely inexpensive. The institutions using this does not have any upfront costs like purchasing biometric attendance systems and so on.

Drawbacks of existing methods	
Methods	Drawbacks
Biometrics (Fingerprint)	Single biometric capture device being used by an entire class makes the process slower. Also, in COVID times, everyone touching the same surface is not recommended.
Forms and QR Codes	One student can easily provide proxy for another.
Manual attendance	Takes a lot of time, vulnerable to proxy attendance.


Instructor
• Opens the webpage, uses a unique class ID, generates QR code.
• Shares QR Code.
Students
• Scans the QR Code with smartphone.
• Uses biometric, FaceID, TouchID etc.
Instructor
Downloads attendance in CSV format.

Workflow flowchart

Target Audience or Market:

The target market for the project is various educational institutions. However, with minor changes, the market can be increased to various corporate organizations as well who would use this maintain the attendance record of their employees. It is to be noted that this project can replace all sort of digital attendance systems that previously existed because it provides a better method for the same.

Feedback

A major point that we received as feedback after pitching to a few of the university professors is that the attendance QR code or link should not be kept alive for a longer time after taking the attendances. Hence, we decided to add the feature of allowing the instructor to disable the link after a stipulated time.

How it works:

System Requirements:

Student side: Smart phone with internet connectivity (Android 7+, iOS 7.0+), or in other words Google Pixel 3 with Titan chip or later, Samsung devices with Knox or later, iPhone 5s, iPad Air with Secure Enclave or later etc. Also, a computer with a TPM can be used (Camera and a QR scanning application is needed). Going by the system requirements of Windows 11, most Windows Hello compatible devices and all Windows 11 devices can be used as well.

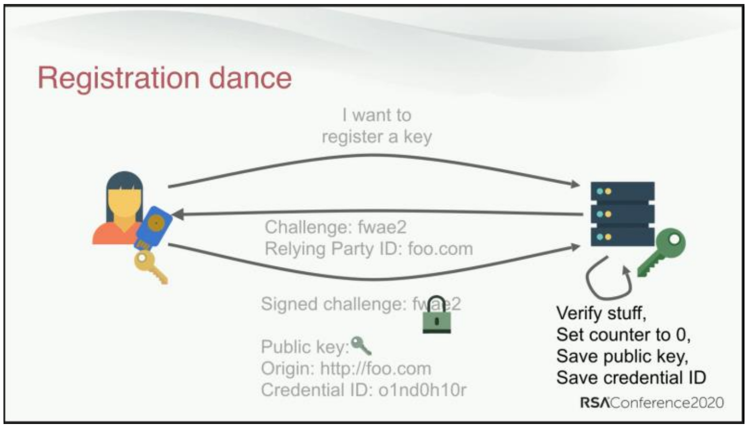
Instructor side: Any device with internet connectivity and provision to share the attendance QR code with students (Screenshare in online classes or sharing the screen in projector in case of offline classes or circulating a printout).

Technology on Server Side:

- The backend is developed on Azure. Azure VM is used for the web backend and Azure SQL Server is used for storing the attendance records. Disks connected to Azure VMs are used for storing the cryptographic keys.
- FIDO2 Library to be used to uniquely identify the device of the user. Here, the authenticator attachment used is 'Platform' (not cross platform) which forces to capture keys from the device instead of any physical security key.

Student Enrollment:

The institute requests all students to register their devices against their enrollment numbers. This leads to a webpage where the students can use their smartphone and enter their enrollment numbers. The server uses the FIDO specifications and stores the cryptographic keys generated by the smartphone against the roll number. The roll number of the student is also added to the browser cookies of the student's smartphone. (The slide is taken from RSAConference 2020, presentation by Jen Tong.)



Registration dance

I want to register a key

Challenge: fwae2
Relying Party ID: foo.com

Signed challenge: fwae2

Public key:
Origin: http://foo.com
Credential ID: o1nd0h10r

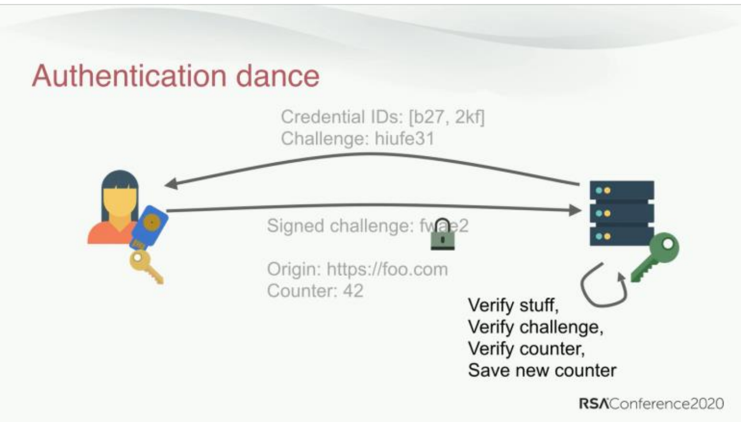
Verify stuff,
Set counter to 0,
Save public key,
Save credential ID

RSAConference2020

Student attendance:

The instructor opens the attendance webpage and requests a QR Code. The backend generates a unique class code and forms an URL and QR Code. The instructor can share this QR Code.

The students, on scanning the QR Code, lands on the webpage to mark attendance. If the enrollment number exists in the browser cookies, the identity of the device is tallied against it with FIDO specifications. Otherwise, the student first goes to a form where the enrollment number is added to the cookies and then the process is followed. (The slide is taken from RSAConference 2020, presentation by Jen Tong.)



Authentication dance

Credential IDs: [b27, 2kf]
Challenge: hiufe31

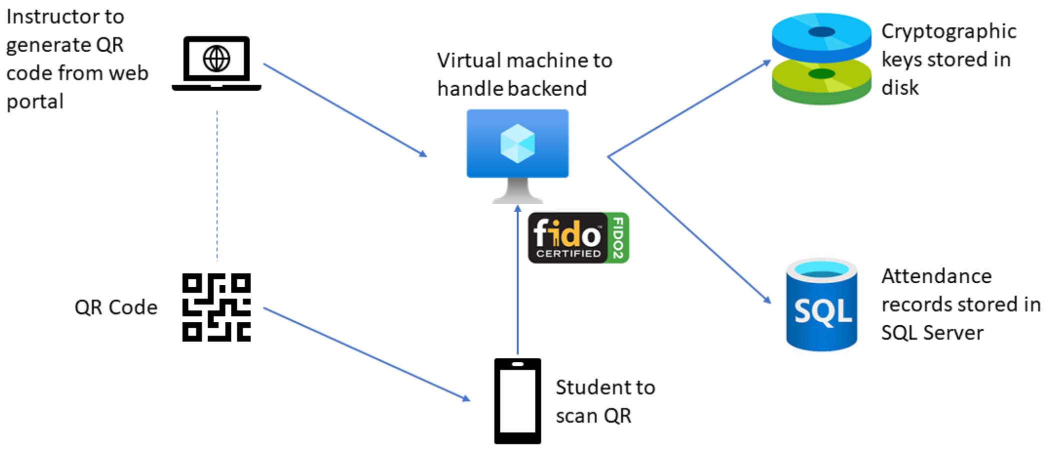
Signed challenge: fwae2

Origin: https://foo.com
Counter: 42

Verify stuff,
Verify challenge,
Verify counter,
Save new counter

RSAConference2020

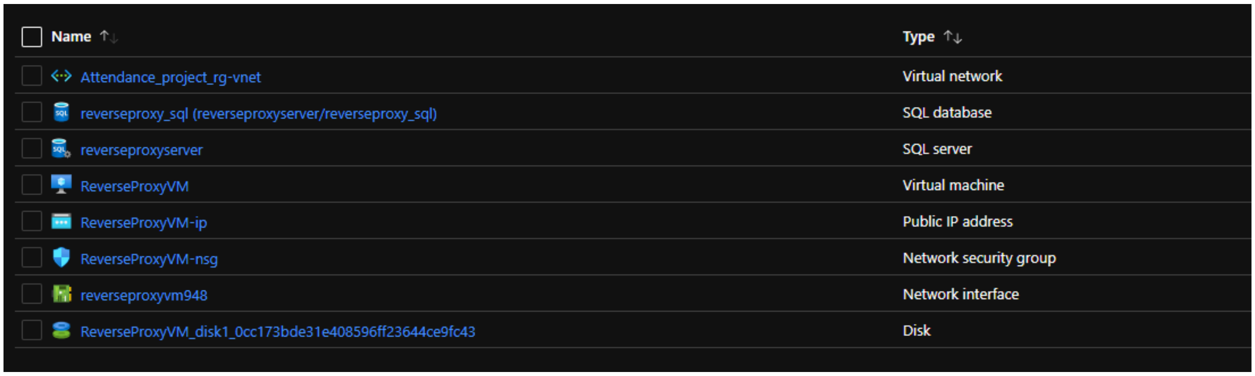
The attendance records are maintained in a SQL database. The webpage on instructor's page has an option to download the attendance in CSV format. The backend queries the SQL database to generate the attendance report in CSV format.


Instructor to generate QR code from web portal
Virtual machine to handle backend
Cryptographic keys stored in disk
fido CERTIFIED FIDO2
QR Code
Attendance records stored in SQL Server
SQL
Student to scan QR

Core Technologies

The following core technologies are used:

- Azure VMs: Azure Virtual Machines is used for the compute operations, mainly for running the web server. The program has been developed and tested on Flask libraries, then deployed on Apache2 WSGI. The SSL Certificates are signed by 'Let's Encrypt' CA.
- Azure Disk: It is attached to the VM. Premium SSD has been used. Apart from the OS and other necessary stuff of the VM, it is mainly used to store the cryptographic keys for FIDO. It saves the authenticator data for the students which is an array of objects encapsulating the Public Cryptographic keys and the credential identity.
- FIDO2: FIDO2 is a specification published for simple and strong authentication by FIDO Alliance (Fast Identity Online) of which Microsoft is a Board Level member. It mainly comprises of the W3C WebAuthn and FIDO Alliance CTAP protocols. The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation. However, here FIDO2 specifications are used to uniquely identify each student instead of authentication. Also considering the fact about System requirements of Windows 11 and Microsoft's promise to a Passwordless future, FIDO2 specifications are going to be used in a major portion of the authentication and identity technologies will be revolving around FIDO2 and Windows Hello in the future.



□ Name ↑↓	Type ↑↓
□ Attendance_project_rg-vnet	Virtual network
□ reverseproxy_sql (reverseproxyserver/reverseproxy_sql)	SQL database
□ reverseproxyserver	SQL server
□ ReverseProxyVM	Virtual machine
□ ReverseProxyVM-ip	Public IP address
□ ReverseProxyVM-nsg	Network security group
□ reverseproxyvm948	Network interface
□ ReverseProxyVM_disk1_0cc173bde31e408596ff23644ce9fc43	Disk

Resources used for deployment of this project

The Business Plan:

The rough business plan of the project is:

Competition:

FIDO2 is a relatively newer concept when it comes to the field of authentication and identity. Also going by the facts that W3C WebAuthn was published on April 8, 2021, and FIDO CTAP standard was proposed on June 15, 2021, it can be said that FIDO2 has a huge scope for development and projects. It has only been implemented in only a few numbers of websites and apps for authentication. Implementing it for checking identity for class attendance is an innovative idea, without any precedents.

It is agreed that it may not be creating a new category of products or service, but it is remarkably different and uses a different technology than the existing ones.

However, most online platforms that is used to maintain student and employee attendance are our competitors. We have still mentioned the how our project is better than the existing ones.

Business Model

As the target market of the project, this can be offered as a SaaS (Software as a Service) model for various institutions and corporate organizations who would like to maintain their student or employee attendance records using our project. Also, partnerships with the institutes will be instrumental in growth of the project. Though the option of using ad-services on the website exists, we have decided against it because the project is to be used in educational institutions where ads might distract the students. Our primary revenue channels are the institutions and organizations who make a partnership and/or use our project on the service model.

Additional Information:

Proposed plans for the future of the project:

The application may be expanded from being just an attendance maintaining system to being a student authentication system as well. It is indeed a good idea to use FIDO2 based Passwordless authentication for examination portals. Being students ourselves, we have seen cases where someone shares his login credentials with another who takes the exam on his behalf. Also, the issue of forgotten passwords and taking time to recover it just before examinations is nerve-wrecking as well, considering the exam pressure. For this, we can have a partnership with some online examination platform like Codetantra which is used by major universities across India. As the students already have their devices keys saved into the server from the attendance application, no additional setup is needed.