

SmartTrack – A Novel Approach for Online Assessment Monitoring

¹Arshna Rajeev, ²Bhagyalakshmi U, ³Jubin Mathew Joseph, ⁴Ms. Gloriya Mathew

^{1,2,3}P G Scholar, Amal Jyothi College of Engineering, Kanjirappally, 686518

⁴Associate Professor, Amal Jyothi College of Engineering, Kanjirappally, 686518

arshnarajeev@mca.ajce.in, bhagyalakshmiu@mca.ajce.in, jubinmathewjoseph@mca.ajce.in, gloriyamathew@amaljyothi.ac.in

Abstract – During past decades, the process of conducting online examinations and interviews have posed critical challenges to companies. The traditional method follows a long procedure often starting with the investing time in selecting or writing questions for interviews or recruitment tests. The proposed system SmartTrack, which alleviate the burden by using a web service. By introducing SmartTrack, companies will be able to monitor and control different people attending the examination process simultaneously. Furthermore, it can be dynamically coupled to fit in specific demands. SmartTrack can be implemented using a Kali Linux tool named Trape, which will monitor users, prevent malpractices and ensure proper authentication. Evaluation results on efficiency and proper authentication demonstrate that SmartTrack will lower security issues with higher expertise.

Index Terms – Trape, Monitoring, Online Examination, Collusion, Threats, Security

I. INTRODUCTION

Conducting online examinations are a high risks process which faced many security threats. Due to the lack of face-to-face interactions, monitoring or invigilation many threats used to occur which includes intrusion by unauthorized users and collusion by the students. One of the challenging threat is collusion, when a student invites a third party collaborator to help him/her in an online test. While all types of threats are important, the risk of collusion is increasingly challenging since it is difficult to detect such attacks. An online examination is considered a critical asset by the companies in the context of recruitment. It is delivered in a remote web-based environment which is widely open to a number of security threats.

The security threats in online examinations can be approached using SmartTrack. SmartTrack is integrated with Kali Linux tool Trape, which is written in python that can aid in tracking and monitoring users on the internet. The URL generated by Trape which is the cloned aptitude URL, will be sent to user for attending test. When the user clicks the link to take the test, it will authenticate and start monitoring the user. It also captures the user's IP address, location, and sessions of the active web services. SmartTrack monitor the user throughout

the examination. In an attempt to protect online tests this is the simple and most effective method to avoid threats during online examination.

II. LITERATURE REVIEW

The main threats which exploit vulnerabilities of assets are interruption, interception, modification and fabrication, these are reviewed in general and collusion in more detail [1]. Collusion threats is motivated by vulnerabilities in identity. These threats are classified into impersonation and abetting where impersonation happens, when a student willingly shares access credentials with a third party. Abetting happens when a student takes an online examination by taking help from a third party based in the same location or remotely. It is challenging to tracking collusion attacks after online test is completed. Paper points about the importance to mitigate such attacks in order to increase confidence of companies and enhance the credibility of online assessment.

User Security Issues in Summative E-Assessment Security explored the existing user security model of a summative e-assessment system [2]. Author pictures that the identity and authentication security goals of the existing model are insufficient to ensure security of the student against collusion threats. There is a departure from generalizing impersonation threats and have classified the threats into categories Type A, Type B and Type C. Type A threat can be avoided when the correctness of a student is not totally dependent on a human invigilator. Minimizing Type B threat rely on the strength of the authentication method adopted. However, solving Type C impersonation threat is non-trivial. An example of a biometric solution is the combination of a fingerprint and face recognition techniques. Such Multi-Biometric systems will provide security and deter Type C impersonation threats. Typical student behaviors during a test include, placing the head on a desk, leaning to a side of the desk (out of camera view), covering a face with the hand (occlusion) or looking around. Thus, a multi-biometric only system that uses fingerprint for authentication and the face for monitoring may request a re-authentication when typical behaviors are

exhibited. It should be noted there exist some unacceptable student behaviors which presents a breach in security. Authors want to guard against false re-authentication requests which suggest that the student is no longer there, when indeed the same student is still taking the test.

Integrity of online testing in e-Learning: empirical study, an example of an online upper division undergraduate MIS course which has been designed and delivered over consecutive five semesters to a sample of over 200 students [3]. The same course was also delivered in a paperless course with a web-enhanced version with regular classroom lectures. Author's reports on a study, which attempts to answer numerous questions regarding impact of an e-Learning format on quality of educational experience. Specifically, in this part of the study they find out whether online testing with an open book format is compromising integrity of assessment in e-Learning by encouraging cheating among students. They also find out what is the difference in online testing and assessment between students in web-based fully online class versus web enhanced class.

There is much discussion in the literature and among teachers on how to minimize cheating, such as using multiple forms of assessment, using timed tests, and proctored tests, randomized testing, and monitoring a student's work and grades for sudden unexplained improvement [4]. The main problems associated with online testing is becoming more complicated with each passing day. If Academic Dishonesty Assessment (ADA) added over the existing problems of online cheating, the credibility of online courses could be lost forever without a sound plan for addressing these concerns in the future. In terms of being fair, the only thing that most faculty members want is some assurance about reasonable safeguards in place that protect the honest assessment of student's learning. Right now, there are some techniques that to some extent can detect whether there is cheating in online courses. The duty of every instructor is to preserve the integrity of not only the individual course, but also the University.

Distributed Education (DE) enables education, both teaching and learning, anytime, anywhere, using any media or modality, at any place. Assessment, mainly testing, is a major component in the overall evaluation of an educational program [5]. However, there still is an important component missing from most DE programs to enable its full realization in a distributed environment i.e. dependable distributed testing. The paper presents a comprehensive risks analysis that classifies seven types of risks, introduces the resultant DoDoT (Dependable observable Distributed online Testing) reference model, and examines its coverage. The vision of the DoDoT reference model is the continued pursuit, and adaptation of new, innovative technologies and more computerized, reliable, affordable and prevalent.

III. PROPOSED SYSTEM

Most companies uses online assessment for recruitment. To manage credibility of the test and to eliminate threats a new approach SmartTrack can be used. It gives many features to handle online users. SmartTrack uses Kali Linux tool Trape to monitor and authenticate user. Trape, a python based script to track anyone on the Internet.

The exam conductor have to login into Trape. Add the exam URL, it will be cloned. Once the user clicks the examination link, the recruiter will get user details and location. Details include the browser in which the link is opened, all sessions opened by user and real time location. It also provides the basic system information of the user.

The main application of SmartTrack is to reduce threats during online tests. It is an effective method to reduce collusion. Collusion threats is motivated by vulnerabilities in identity and the authentication model of the users taking exam. These threats are classified into impersonation and abetting. Impersonation happens, when a student willingly shares access credentials with a third party. Abetting happens when a student takes an online examination by taking help from a third party based in the same location or remotely. These two can be monitored and warn the user, if occurred. Trape provides a rich interface to alert users through pop up. Users can also be guided by voice messages throughout the exam. If any other sessions are opened by the user then it can be redirected by the recruiter using java scripts.

SmartTrack can reduce security threats in online examinations to a large extent. This approach can solve the traditional issues of companies while conducting online assessments and help in maintaining the credibility of the test.

3.1 Advantages

The advantages of the proposed system SmartTrack are:

- Reduce Collusion and impersonation during online assessments.
- Increase confidence of companies.
- Enhance the credibility of online assessment.
- Reduce security threats.

IV. TRAPE

The main key component of SmartTrack is Trape, a Kali Linux Tool. It is a python script. Installation and execution of Trape is simple and easy. The installation process of Trape contains different steps.

4.1 Installation of Trape

Kali Linux is one of the most powerful and widely used penetration testing platform. It is mainly used for security purposes. It is a repository of hundreds of tools which are

constantly working towards various information security tasks, like Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

Trape can be installed by cloning the GitHub repository using the commands. For using Trape, we must have an account in the ngrok and to get API in Trape, a Google account is needed.

1. Git clone <https://github.com/boxug/trape.git>
2. After cloning type:
 - cd trape
3. Then type ls

Another method is by installing all the libraries that are located in the file requirements.txt.

- pip install -r requirements.txt
- Once the Trape and the needed libraries are successfully installed, tool can be set into action.

After successful installation of tool, we can start monitoring and authenticating the user. By using the cloned URL crack details of user's active sessions like Gmail, Facebook.

4.2 Ngrok

Ngrok gives you the token to access Trape. Ngrok is a reverse proxy tool which creates a secure tunnel from a public endpoint. It captures the traffic and uses it for detailed inspection.

1. For creating a Ngrok account go to:
 - <https://dashboard.ngrok.com/user/signup>
2. After creating an account, go to login.
3. After we log in to the account.
4. Go to Auth tab to get ngrok access token.
5. Auth token will be:
xxxxxxxEVBUxxxxxxTDDsr_4ytFLxxUSxxxxxxxxxxZF
6. After getting the access token, enter the access token in the Trape Linux console.
7. After creating a Ngrok API. Now create a Google Maps API.

4.2.1 Google API

For getting a Google Maps API, we must have a Google account.

1. Go to the link: <https://accounts.google.com/signup>
2. After creating an account in Google. Click this link: <https://cloud.google.com/>
3. Click on the console tab marked in red.
4. Go to APIs & Services and clicks on Credentials.
5. Then Click on Create Credentials and then on API key.
6. After clicking on Create Credentials, a new API key will be generated.

7. After generating both the API keys, we have to configure the Google Maps API's.
8. If the key is configured properly then we have to setup the billing account of Google Map in order to see the real-time location on the Trape control panel.

4.3 Execution of Trape

1. First move to Trape directory using a terminal.
(cd Trape)
2. Enter the Ngrok authtoken and then enter port no. 80 on the same terminal. (Figure 1)
3. Type python trape.py on a new terminal. (Figure 2)
4. After starting, we can see Lure for the user's link and the Public lure to use with the test link.
 - Rest API path show the JS that is used in cloning page.
 - We can also use the Link shortened lure to integrate with target link as it become more secure for the recruiter.
 - Link shortened lure is Google short URL.
 - The Control panel links are used in accessing the temporary (cloned) webpage of user which shows all the information which is gathered.
5. Now on user computer, we have to open the cloned page using any of the URL.
 - The public lure URL is used on the user computer.
 - As we click on Login, a user will be connected via Trape tunnels.
6. Now, the user will be connected showing his public IP address and the identifier.
7. For accessing the main features of Trape open the control panel.
8. After entering the access key. We can see the information which Trape has gathered. (Fig 3)
 - Trape has gather lot of information like operating system, CPU, local ISP, Country and city, Open ports, and the browser from which target is accessing the cloned URL.
 - One main feature of Trape is showing the location on Google Map, which will reveal the real-time location of user.
 - Or we can use the latitude and the longitude to know the location of the target.
 - Simply by searching the latitude and longitude on the Google search, and we can see its real-time location.
 - Trape will give much information about the user. This provided information reveals a lot about the activities of the user.

- Trape provides different way to monitor and control the user activities on the exam time.
- Trape can be used to send audio to user system for giving warnings.
- Trape gives many features like redirecting user forcefully when malpractice occurs. Creates the alert popup for the user.

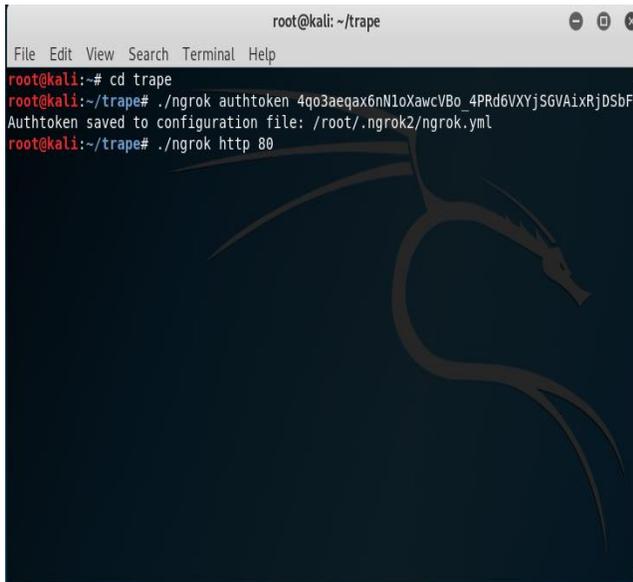


Figure: 1

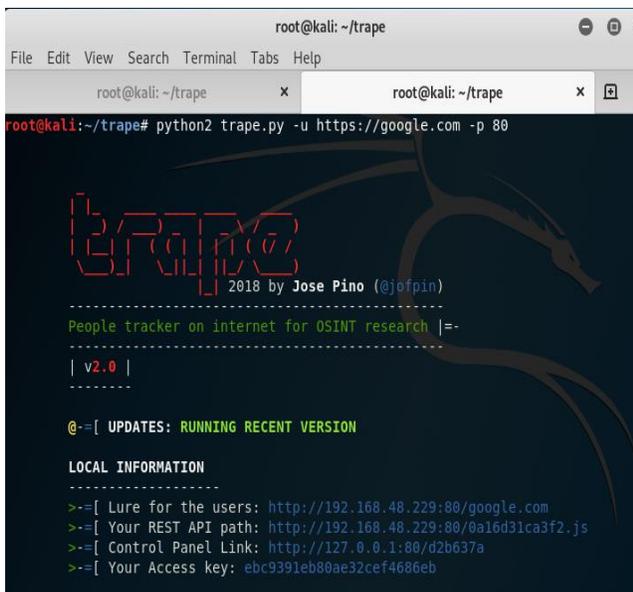


Figure: 2

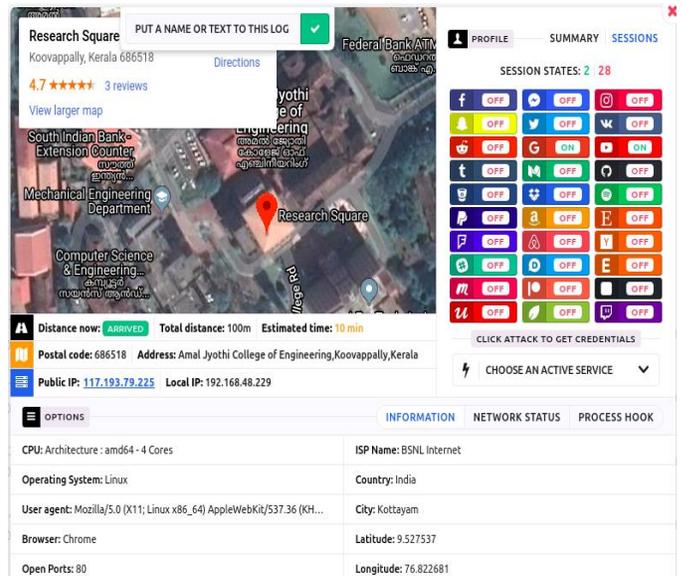


Figure: 3

V. IMPLEMENTATION

SmartTrack is an efficient method to reduce threats during online exams. SmartTrack is implemented using Trape, a python tool. Trape help in authenticating the user and monitoring the user throughout the test. Trape URL which is the cloned test link, on clicking this link test will start and details will be shown in the Trape panel. Due to lack of face-to-face interactions, invigilation many threats occurs, which includes intrusion by unauthorized users and collusion by the students.

1. When the user clicks the test URL, the details will be shown in the Trape Control Panel.
2. The online exam page will be opened for the user and the Trape page, for monitoring will be opened at the recruiter's side.
3. Once the exam started the entire control will be given to the exam coordinator. They can authenticate, monitor and prevent the collusion.
4. Once the exam ends, access to the Trape will also be terminated.
5. During the online exam time the coordinators will be provided the power to control the user by forcefully redirecting the user if they share access credentials with a third party.
6. Coordinators can create alerts to warn users.
7. They can even send voice messages to guide the users.

It is challenging to track collusion attacks after online test is completed. This method reduce impersonation and abetting to a large extent. SmartTrack is the best method to keep credibility of online assessments.

VII. FUTURE SCOPE

In the upcoming scenario, most companies uses online assessment for recruitment. To manage the credibility of test and to eliminate threats are important factors to be considered. SmartTrack gives many features which can be used in authenticating and monitoring users. It can also be used to understand and identify the nature of all threats. Kali tool used in SmartTrack, Trape shows the real-time location which directly attacks on any user privacy. Trape can also be used to provide awareness among internet users about hidden threats. SmartTrack can be used for monitoring and authenticating all kinds of online assessments.

VIII. REFERENCES

- [1] Ullah, A., Xiao, H., & Barker, T. (2016). A classification of threats to remote online examinations. 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). doi:10.1109/iemcon.2016.7746085
- [2] Apampa K. M., Wills G., Argles D. "User security issues in summative e-assessment security." International Journal of Digital Society (IJDS). 2010;1(2):1-13
- [3] Wielicki T., editor. "Integrity of online testing in elearning: Empirical study". Fourth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06); 2006: IEEE.
- [4] Colwell J. L., Jenks C. F., editors. "Student Ethics in Online Courses". 35th Annual Conference Frontiers in Education (FIE '05) 2005; IN, USA: IEEE.
- [5] Frank A. J., editor. "Dependable distributed testing: Can the online proctor be reliably computerized?". E-Business (ICE-B), Proceedings of the 2010 International Conference on; 2010: IEEE.

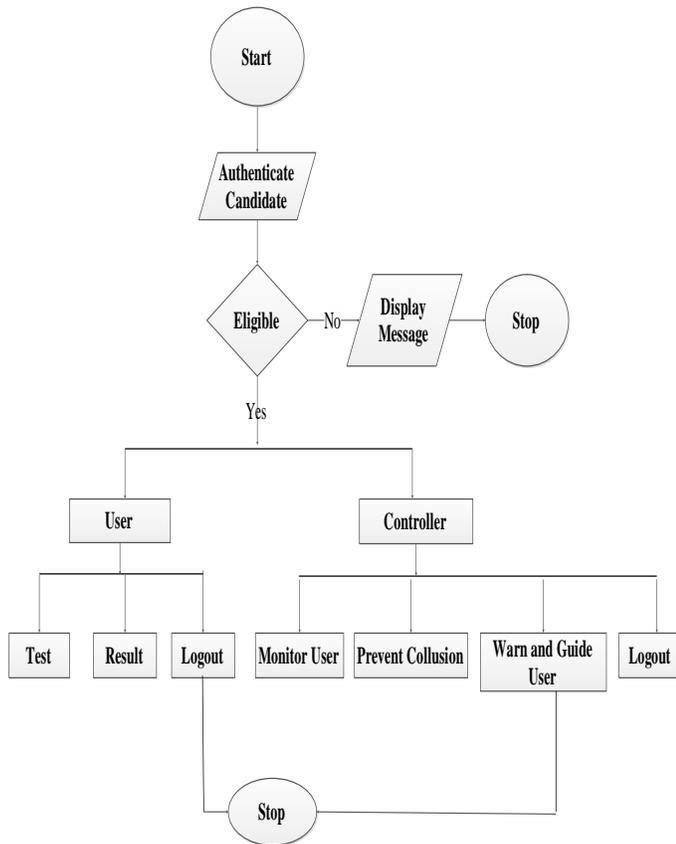


Figure 3: Flow Chart of Proposed System

VI. CONCLUSION

It is challenging to track collusion attacks when an online test is completed. To overcome this problem SmartTrack is introduced. It avoids threats to online examination collusion. Collusion threats is motivated by vulnerabilities in identity and the authentication model of the users taking exam. These threats are classified into impersonation and abetting. SmartTrack uses a Kali Linux tool, Trape to reduce these threats. Trape helps to authenticate and monitor users throughout the examination. It can also forcefully quit the exam or redirect the users back to exam if any malpractice occurs. SmartTrack will start controlling and monitoring users from the point of time they click the test link and also prevents impersonation and abetting. However, it is important to eliminate such attacks to enhance the confidence of recruiters and credibility of online assessment. One limitation of this method is that in some cases Google Maps will not load in Trape, that might be the slow internet otherwise check Google API key.