Experiment Pre-Registration
Predicting 3-D-Secure Fraud Detection Outcomes[*]

Thomas Groß
Newcastle University
United Kingdom

Mohammed Aamir Ali
Newcastle University
United Kingdom

General Purpose of Pre-Registrations

Pre-registrations are research statements of intention established before a sample is evaluated and statistical inferences are undertaken. A pre-registration asserts the aim of a study, including its research questions and statistical hypotheses, methods, incl. operationalization of independent variables (IVs) and dependent variables (DVs), sample and analysis specification.

The primary reason for a pre-registration lies in the fact that a statistical inference (Null Hypothesis Significance Testing) is only valid if the statistical hypotheses are fixed before the inference is undertaken. This is grounded in a p-value being a conditional likelihood contingent on the fixed null hypothesis assumed to be true. Furthermore, pre-registrations serve as a ward against questionable research practices, such as outcome-switching, hypothesizing after the results are known (HARKing), or p-hacking... it is meant to counteract the many temptations of researcher degrees of freedom.

Pre-registrations are typically committed confidentially under embargo, with an immutable timestamp. Once the corresponding study is published, the embargo is lifted.

This is an experiment registration form for the Open Science Framework (OSF)[1]. It is modelled according to the format of AsPredicted[2].

[*]Open Science Framework: `https://osf.io/x6yfh/`

[1]`https://osf.io`

[2]`https://aspredicted.org`

Context of this Pre-Registration

Meta-Data of Pre-Registration.

- Open Science Framework Repository: `https://osf.io/x6yfh/`
- Registered Registration File: `https://osf.io/85zs2/`—Prereg_3d_Secure.pdf
- Timestamp: **2018-09-20 05:45 PM**
- Archived Immutable Pre-Registration: `https://osf.io/4mysp`
- Timestamp: 2018-12-05 11:25 AM

Peer-Reviewed Publication. The definitive version of the study is published as:
Mohammed Aamir Ali, Thomas Groß, and Aad van Moorsel. Investigation of 3-D secure's model for fraud detection In proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust (STAST'2018), December 2018, pp. 1-11. `https://doi.org/10.1145/3361331.3361334`. The paper received the **STAST'2018 Best Paper Award**.

ArXiv Report. Mohammed Aamir Ali, Thomas Groß, and Aad van Moorsel. Investigation of 3-D Secure's Model for Fraud Detection. arXiv:2009.12390, 2020. `https://arxiv.org/abs/2009.12390`

1 Structured Abstract

Background. 3-D Secure [1] is an XML-based identity federation protocol meant to authenticate credit card transactions on the Web. The system uses a fraud detection model with a number of features extracted from the Web Browser to decide whether the user needs to be challenged with a password authentication or not.

Aim. We aim to investigate and quantify the impact of factors used by 3-D Secure in its fraud-detection decision making process and to establish a Logistic Regression Classifier for likely outcomes.

Method. In a repeated measures experiment, four different credit cards were used to run credit card transactions with two different Web sites. During that experiment the the independent variables machine_data, value, region, and website were systematically manipulated, taking two levels each.

We measured whether the user was challenged with an authentication, whether the transaction_status was declined or accepted, and whether the card was blocked as nominal dependent variables.

We establish logistic regressions as predictive model how the independent variables impact the likelihood of the response variables changing. We also seek to establish a multiple logistic regression as overall model.

Anticipated Results. We anticipate the logistic regressions to yield odds ratios as quantification for the impact of individual independent variables on the response variables.

Anticipated Conclusions. We anticipate that the logistic regression models are insightful in explaining the (probabilistic) security and fraud-detection decisions taken at the back-end.

2 State of Data Collection

Have any data been collected for this study yet?

(a) ☐ **NO** data have been collected.
(b) ☑ Some data have been collected, but not analyzed.
(c) ☐ Some data have been collected and analyzed.

If (b) or (c), please explain briefly:

At the time of this pre-registration, the card-transaction experiments have already been completed and their results encoded. However, NO data has been analyzed statistically yet, at this point.

3 Aims

Hypothesis: What's the main question being asked or hypothesis being tested?

Research Question. Which factors impact the fraud-detection decisions with what magnitude of change in acceptance likelihood?

Statistical Hypotheses. Iterating over the independent variables $X \in \{$ machine_data, value, region, website $\}$ and the dependent variables $Y \in \{$ challenged, transaction_status, blocked $\}$, we consider the following statistical hypotheses:

Alternative Hypotheses. $H_{1,X,Y}$: The independent variable X systematically impacts the likelihood of a change in the dependent variable Y.

Null Hypotheses. $H_{0,X,Y}$: The independent variable X does not yield an impact on the likelihood of change in the dependent variable Y.

Note that we, thereby, investigate 5×3 relations with corresponding alternative and null hypotheses.

Logistic Regression Classifier. The logistic regression is to establish the magnitude of impact on the likelihood on change in the response variable. The ultimate aim is a multiple logistic regression taking into account all three response variables at the same time.

4 Methods

Give a brief overview of the methods used.

The experiment is constructed as repeated-measures experiment, meaning that the four credit cards were used repeatedly with different independent variable levels.

The conditions on machine_data, value, region, and website were established, a 3-D Secure protected credit card transaction attempted and the outcome of the transaction recorded. If the card was blocked, the bank contacted to unblock/reset the card.

5 Independent Variables (IVs)

Describe the conditions (for an experimental study) or predictor variables (for a correlational study).

The following independent variables (with two levels each) were systematically manipulated.

machine_data: The machine data recorded by 3-D Secure (incl. the cookie) was either left intact or overwritten (changed by a proxy, manipulating the application data, changed with arbitrary values on browser version and operating system).

- **0=** The machine data/cookie was left intact.
- **1=** The machine data/cookie was overwritten.

value: The monetary value of the transaction as either low ($13) or high ($406).

- **0=** Low monetary value.
- **1=** High monetary value.

region: The region of the transaction was either a specific city in the UK or a specific city in Germany.

- **0=** UK (home region for the credit card).
- **1=** Germany (foreign region for the credit card).

website: The Web site used for the credit card transaction was either argos.co.uk or bnstores.co.uk.

As a convention, we encode the control condition (that is, a state of the transaction not being influenced) as 0.

6 Dependent Variables (DVs)

Dependent variables: Describe the key dependent variable(s) specifying how they will be measured.

The following dependent variables were measured:

challenged: The user was either challenged with a password authentication or not.

- **0=** The card was accepted without password authentication.
- **1=** The user was challenged with a password authentication.

transaction_status: The transaction was either accepted or declined.

- **0=** The card was accepted.
- **1=** The card was declined.

blocked: The card was blocked or left active.

- **0=** The card stayed active.
- **1=** The card was blocked.

As a convention, we code a negative outcome (being challenged, transaction declined, card blocked) as 1.

7 Mediator Variables

Describe any variables you expect to mediate the relationship between your IV's and DV. Specify how they will be measured.

N/A

8 Moderator Variables

Describe any variables you expect to moderate the relationship between your IV's and DV. Specify how they will be measured.

N/A

9 Data Preparation

Describe what measures will be taken to check assumptions and label outliers.

We check the data for completeness and correct transcription to the results table.

Given that we are dealing with nominal data we do not have pre-analysis outlier detection.

10 Main Analyses

Describe what analyses (e.g., t-test, repeated-measures ANOVA) you will use to test your main hypotheses.

We intend to establish contingency tables and corresponding analyses as preliminary tests.

The main analyses are logistic regressions between the given independent and dependent variables.

The ultimate main analysis will be one multiple logistic regression, with all three response variables as dependent variables.

11 Secondary Analyses

Describe what secondary analyses you plan to conduct (e.g., order or gender effects).

N/A

12 Validation

Describe what diagnostics or validation methods you plan to employ to check the soundness of the analyses.

Model Diagnostics. For the logistic regression models, we perform post-analysis diagnostics on the distribution of the residuals. We further analyze for variance inflation, influential cases, etc. We will use the R-package `car` co-created by John Fox for the typical regression diagnostics [2].

Accuracy Validation. To validate the classifier obtained, we execute a random sub-sampling of 80% the overall video sample and test the derived classifier on the remaining 20% sample. We intend to evaluate the Receiver Operating Characteristic (ROC) as well as the Area Under the Curve (AUC) for these re-samplings.

13 Sample

Where and from whom will data be collected? How will you decide when to stop collecting data (e.g., target sample size based on power analysis or accuracy in parameter estimation, set amount of time)? If you plan to look at the data using sequential analysis, describe that here.

The sample was collected from credit-card transactions on home appliance Web sites offering 3-D Secure fraud detection.

14 Exclusion Criteria

Who will be excluded (e.g., outliers, participant who fail manipulation check, demographic exclusions)? Will they be replaced by other participants?

We would only exclude datasets if they were incomplete.

15 Exception Handling

Should exceptions from the planned study occur (e.g., unexpected effects observed), how will they be handled?

Should we observe effects not anticipated in this pre-registration, we will treat them as exploratory effects and advise on further investigation.

16 Change Management

2018-09-20 : The predictor cookie was eliminated as it was aliasing machine_data, that is, the cookie is always manipulated when the machine data is manipulated, and therefore not a separate predictor.

2018-09-20 : The exact definition of the independent and dependent variable encoding was included.

2020-07-26: The pre-registration was amended with author disclosure and project acknowledgment; references were added.

17 Sign-Off

Pre-registration written by (initials): T.G.
Pre-registration reviewed by (initials): M.A.

Acknowledgment

This work was in parts supported by a grant of the National Cyber Security Centre (NCSC) on "Pathways to Enhancing Evidence-Based Research Methods in Cyber Security" in its approach to research integrity and reproducibility. Thomas Groß was supported by ERC Starting Grant CASCAde (GA n^{o}716980).

References

[1] M. A. Ali and A. van Moorsel. Designed to be broken: A reverse engineering study of the 3d secure 2.0 payment protocol. In *International Conference on Financial Cryptography and Data Security*, pages 201–221. Springer, 2019.

[2] J. Fox and S. Weisberg. *An R companion to applied regression*. Sage publications, 2018.