A Holistic Evaluation of E-Commerce Payment Security Through Automated and Manual Analysis

Urvashi Kishnani, Briana Whalen, Andrew Burris, Sanchari Das
Ritchie School of Engineering and Computer Science, University of Denver

ABSTRACT

With increasing online transactions, questions regarding customers' privacy and security are increasing and need to be addressed. These online transactions, by necessity, involve personal and sensitive information, including Personally Identifiable Information (PII) such as name, address, SSNs, and banking information. This information also changes hands several times from the end user, online platform, banking platform, and, if necessary, to a transportation company for shipping fulfillment.

Thus, to understand the current security and privacy aspects of these platforms, we performed a holistic evaluation of 91 e-commerce websites. We also conducted a literature review to understand better e-commerce and what is involved in a payment platform.

Through a combination of hands-on and automated tool-based analysis, along with the study of relevant literature, we evaluate the current state of online payment platforms from the view of technical security and user privacy. Our literature review highlights the most discussed privacy and security associated with e-commerce security and identifies some gaps in the literature.

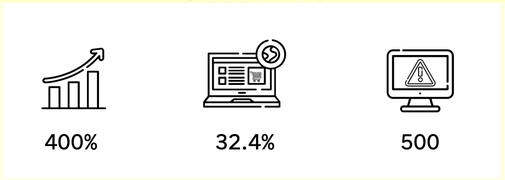
The website analysis focuses on the website's privacy policy, cookies, payment, and other security measures and highlights both the divergence from or adherence to expected outcomes. Finally, we propose suggestions for both users to make informed decisions and for companies to increase the security and privacy fronts of their e-commerce website products.

CONTACT

Contact:
Sanchari.Das@du.edu
@ DrSchariDas

Lab contact:
inspirit.lab@du.edu

MOTIVATION



- Since the start of the pandemic, the FBI has seen a **400%** rise in reports of cyberattacks.
- E-commerce platforms deal with sensitive information like name, address and banking details, about **32.4%** of cyberattacks are targeted towards e-commerce, making it the MOST attacked industry.
- In February of this year, about **500 e-commerce companies** were attacked in a single day due to vulnerabilities in an outdated software. This motivates us to understand the current state of e-commerce platforms, both from an academic and a practical perspective on the privacy and security fronts.

OVERVIEW

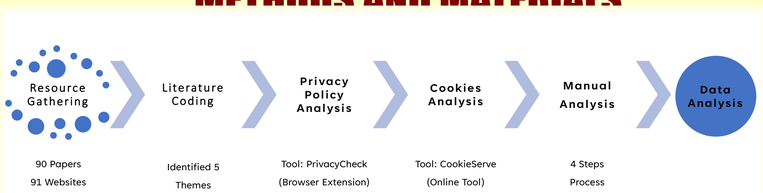
We selected and performed a thorough evaluation of 91 different e-commerce websites. After that, we looked at the security and privacy details of the website from several angles. Our analysis was performed using both automated and manual evaluation.

We utilized the PrivacyCheck tool, which collects data points for 20 different subcategories from lengthy privacy policies, 10 of which are under user control and the remaining under GDPR.

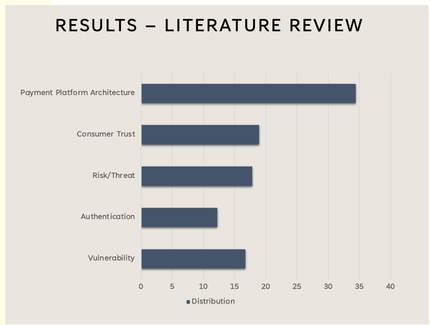
Each of these 20 subcategories has an associated question that the tool answers and gives a score of 0-10. In addition, another tool, CookieServe, was used to determine the number of default cookies used by each website and their specific purpose, whether necessary, analytical, or advertisement.

We conducted a hands-on evaluation of the payment platform's security by looking at five key factors: website security, where we looked for the use of Hypertext Transfer Protocol Secure (HTTPS) and the presence of a valid digital certificate; authentication, where we checked for Multi-Factor Authentication (MFA) options and guest checkout; payment security where we checked for the use of a secure payment processor and association with a trusted financial institution; input validation where we checked whether incorrect card details and addresses were being detected; and user confidence where we looked if the website allowed for customer ratings and reviews on their products.

METHODS AND MATERIALS



RESULTS – LITERATURE REVIEW

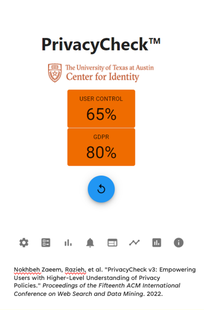


PRIVACY POLICY ANALYSIS

User Control
Email Address Security
SSN[1] Security
Targeted Advertisement
Law Enforcement
Data Control
PII[2] Security
COPPA[3] Compliance
Location Tracking
Privacy Policy Opt-Out
Data Aggregation

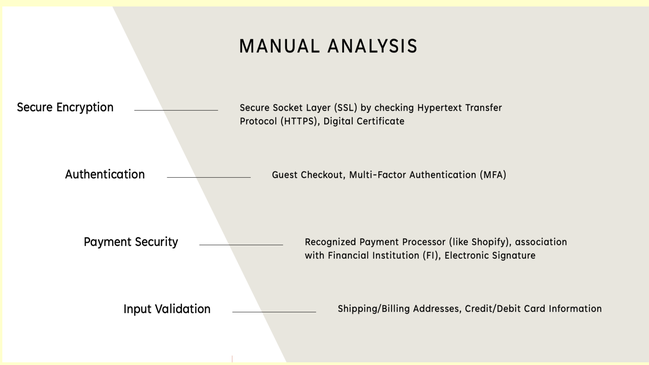
GDPR[4]
Between Site Transfer
Right to be Forgotten
Reject Usage of PII
Data Encryption
Data Protection Principles
Company Location
Data Retention Notification
Under 16 Protection
Data Processing Consent
Breach Notification

[1]SSN: Social Security Number
[2]PII: Personally Identifiable Information
[3]COPPA: Children's Online Privacy Protection Rule
[4]GDPR: General Data Protection Regulation

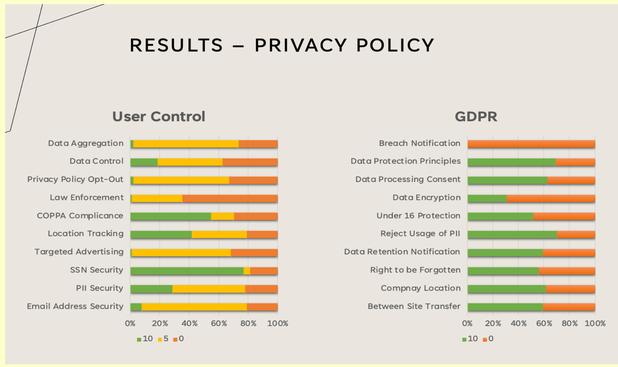


Nokhbeh Zaeem, Razieh, et al. "PrivacyCheck v3: Empowering Users with Higher-Level Understanding of Privacy Policies." *Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*. 2022.

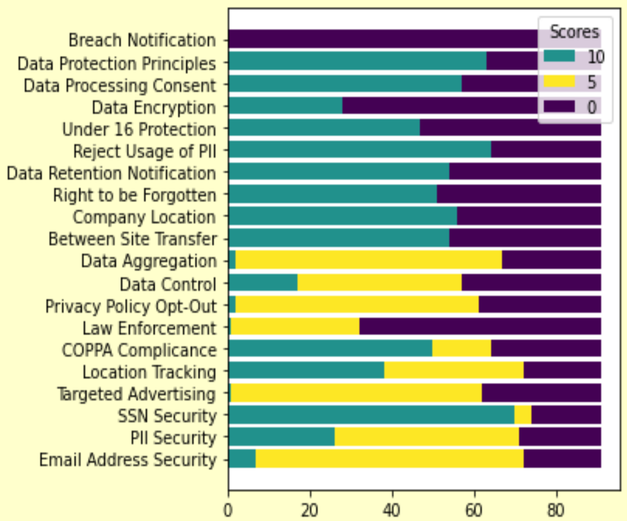
MANUAL ANALYSIS



RESULTS – PRIVACY POLICY



Each website collected about 38.5 cookies, with one having as many as 115 cookies. Most of the cookies were used for ``other" purposes, which implies they were not deemed necessary or used for analytical, functional, performance, or advertisement purposes. Necessary and functional cookies were the least in number. In the privacy policy, we note that the average score obtained for user control is only about 53.5%, which indicates that most websites only give users partial control over the data collected or tracked by them.



Shows the distribution of scores across all websites for all privacy policy categories. The maximum standard error obtained was 0.7, and the average standard error was 0.4055, indicating that the mean values obtained were within the acceptable range of 0.8-0.9.

REFERENCES & ACKNOWLEDGEMENT

1. Justine S Hastings, Brigitte C Madrian, and William L Skimmyhorn. 2013. Financial literacy, financial education, and economic outcomes. Annu. Rev. Econ. 5, 1 (2013), 347–373.
2. Jane Tighe, IC McManus, Neil G Dewhurst, Liliana Chis, and John Mucklow. 2010. The standard error of measurement is a more appropriate measure of quality for postgraduate medical assessments than is reliability: an analysis of MRCP (UK) examinations. BMC medical education 10, 1 (2010), 1–9.
3. Razieh Nokhbeh Zaeem, Ahmad Ahbab, Josh Bestor, Hussam H Djadi, Sunny Kharel, Victor Lai, Nick Wang, and K Suzanne Barber. 2022. PrivacyCheck v3: Empowering Users with Higher-Level Understanding of Privacy Policies. In WSDM '22: Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining. Association for Computing Machinery, Virtual Event - AZ USA, 1593–1596.

We thank Ashton Foster, Oscar Cerino, and Zac Abero for their initial contribution to the study. We would also like to acknowledge the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Lab at the University of Denver. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors.