Example solutions and best practices for protecting consumer information via retail payment systems

April 6 2016

With attacks on America's largest retailers increasingly in the headlines, the need to better secure consumer information is critical. Credit card information is a common target for cybercriminals, and once obtained it

is often sold on the black market. However, account information is not the only customer data collected by retailers.

"When you go shopping, you leave additional information about yourself, such as where you live, your age, your birthday, purchasing habits and other loyalty card information," said Yuliang Zheng, Ph.D., professor and chair of the UAB College of Arts and Sciences Department of Computer Information Sciences. "All of this information accumulates over time. Five or 10 years down the road, an enormous amount of data has been collected, and there is no way to get it back. When you aggregate all of this information, it can be used to paint a detailed picture of a person."

Secure handling of sensitive, noncredit card consumer data, multifactor authentication for e-Commerce transactions and combating online fraud were the topics of a collaborative workshop hosted by the National Cybersecurity Center of Excellence at the UAB Hill Student Center on March 22. Cybersecurity experts and retail executives from several major retailers gathered to discuss and identify pressing retail cybersecurity issues, applicable standards, best practices, and how current and emerging cybersecurity technologies and relevant architectures can be used to address these cybersecurity business challenges.

"UAB has a national reputation for excellence in cybersecurity research and education," said Robert E. Palazzo, Ph.D., dean of the UAB College of Arts and Sciences. "As one of nine universities on the Academic Affiliates Council for the nation's first federally funded research and development center solely dedicated to enhancing cybersecurity, we are honored to have been selected to host this collaborative workshop and contribute to the creation of possible solutions to the growing challenges of retail cybersecurity."

During the workshops and breakout sessions, participants discussed the complexities of securing personal identifiable information (PII) and how it can be protected, but remain accessible to various departments such as customer service and marketing. They explored whether current security measures used to protect credit card data could also be used to protect noncredit card information. Some of the recommendations include using tokenization, format-preserving encryption or anonymization to send customer data to shipping providers and others essential to the business process.

Over the next several months, the NCCoE will take all of the recommendations and information gathered to create example solutions to the defined problems and freely share the information with the retail industry. The information will be published in a National Institute of Standards and Technology Cybersecurity Practice Guide, providing detailed guidance on how to implement the established solutions.

More information: For more information, see nccoe.nist.gov/news/retail-cyb … s-new-nccoe-projects

Provided by University of Alabama at Birmingham

Citation: Example solutions and best practices for protecting consumer information via retail payment systems (2016, April 6) retrieved 26 April 2024 from https://phys.org/news/2016-04-solutions-consumer-retail-payment.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.