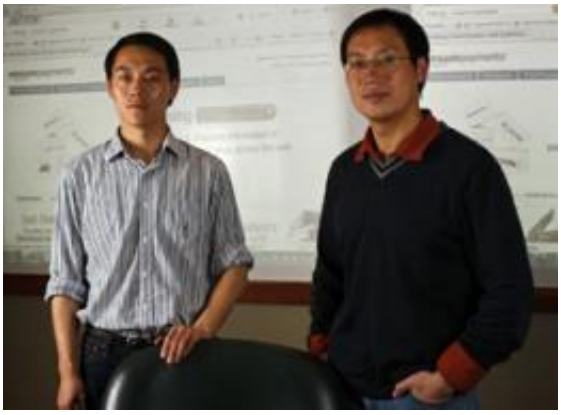
Amazon, others make fixes after IU informaticists uncover online security flaws, receive free products

March 31 2011



Informatics doctoral student Rui Wang, left, and IU associate professor XiaoFeng Wang.

(PhysOrg.com) -- Internet security researchers at Indiana University and Microsoft Research have exploited software flaws in leading online stores that use third-party payment services PayPal, Amazon Payments and Google Checkout to receive products for free or at prices far below the advertised purchase price.

The research group that included IU Bloomington School of Informatics and Computing Associate Professor XiaoFeng Wang and doctoral student Rui Wang, as the lead author, was able to receive electronics, DVDs, digital journal subscriptions, personal health care items and other

products either free or at prices the group itself determined.

Leading merchant applications NopCommerce and Interspire, cashier-as-a-service (CaaS) providers such as Amazon Payments and some popular online merchants all contained serious logic flaws that would allow malicious users to exploit inconsistencies in how payment statuses were perceived by the merchants and CaaS providers (Amazon Payments, PayPal and Google Checkout). The researchers in some cases were able to convince the web stores they had paid for an item through Amazon Payment while actually making the payment into their own merchant account at Amazon.

"We believe that it is difficult to ensure the security of a CaaS-based checkout system in the presence of a malicious shopper who intends to exploit these knowledge gaps between the merchant and the CaaS," XiaoFeng Wang said. "This trilateral interaction (between merchant apps, online stores and the CaaS) can be significantly more complicated than typical bilateral interactions between a browser and a server, which have already been found to be fraught with subtle logic bugs."

Most of the flaws were due to lapses in merchant software, they said, but responsibility also fell on the CaaSs. In one case the researchers discovered an error in Amazon Payments' software development kit that led to the company significantly altering the way it verifies payment notifications.

More troubling, the report notes, is that the preliminary study touched only on the simplest trilateral interactions and not on other real-world applications that involve even more parties, like marketplaces and auctions, which the researchers now believe could be even more error-prone.

"This calls for further security studies about such complicated multi-

party web applications," said Rui Wang. "Our analysis revealed the logic complexity in CaaS-based checkout mechanisms, and the effort required to verify their security properly when developing and testing these systems. We believe this study takes the first step in the new security problem space that hybrid web applications bring."

The research group, which also included Shuo Chen and Shaz Qadeer of Microsoft Research in Redmond, Wash., said it now hopes to explore whether similar flaws can be found that would allow malicious users to purchase two items at extremely different prices and then return the cheaper one while receiving a refund for the more expensive item.

"An interesting question might be whether we can check out a $1 order and a $10 order and cancel the $1 order to get $10 refunded," Rui Wang added.

In each case where flaws were found the researchers reported their findings to the affected parties, received acknowledgements from the parties, returned any property received, and worked with them to correct the flaws.

In January 2011 Rui Wang and XiaoFeng Wang, his doctoral adviser, and Shuo Chen, the Microsoft researcher, were part of a team that uncovered Facebook vulnerabilities that allowed malicious websites to access and share private user data. Facebook later confirmed it had repaired the vulnerabilities. XiaoFeng Wang is also acting director of the IU Center for Security Informatics and is an affiliated researcher at IU's Center for Applied Cybersecurity Research.

Their current work, "How to Shop for Free Online: Security Analysis of Cashier-as-a-Service Based Web Stores," will be formally presented in May at the Institute of Electrical and Electronics Engineers' annual Symposium on Security and Privacy in Oakland, Calif. The research

paper can be viewed here.

Provided by Indiana University