Two Factor Credit-card Safety for Online Transactions

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

My friend and colleague Jürgen Pabel was one of our first graduates from the Norwich University Master of Science in Information Assurance. He is an active participant in our alumni discussion group and a frequent and welcome correspondent. Here, I present his latest suggestions (entirely his with minor edits and additions):

* * *


Just a few years ago every credit-card transaction was authenticated by two factors: the actual credit card (possession) and either the correct PIN or a valid signature (knowledge / capability). The Internet broke this security scheme in that it was no longer possible to verify the possession of the actual credit card. Banks responded by adding the credit-card verification (CCV) numbers on the back of the cards, but if the card is stolen that doesn’t help stop fraud either. Adding a second factor to the login process for online banking portals is a good measure to reduce the risks of unauthorized access through compromised credentials. The SafePass program introduces the customer's mobile phone as a second factor for authentication to Bank of America's online banking portal.

However, millions of credit-card users still depend solely on the secrecy of their credit card information to guard them against online credit-card fraud. A new universal second factor would be useful, even though in most cases customers are liable only up to a certain amount in case of provable fraud; someone's got to pay the bill, and it isn’t the banks: it’s people who pay finance charges on late credit-card payments.

The problem with incorporating a second factor in online credit-card transaction processing is the backend process. Changing the data formats would require millions of vendors to adapt the new process—so expensive that it’s unlikely to be implemented. An interesting idea to overcome this massive redesign problem would be to include authenticating information for the transaction in the credit-card owner's _name_ field.

Any bank issuing credit cards would be able to extend its transaction authorizing process to either require the physical card to be present (swiped) or to require a one-time code to be included in owner's name field. These changes would not require any modifications outside of the issuing bank's infrastructure. The authenticating information might be transmitted via text-message to the customers mobile phone number - transforming the mobile phone into the second factor as in the SafePass program.

There are additional aspects to consider. First, there are going to be vendors with whom customers frequently execute online credit-card transactions and they will want to be able to save
their credit-card information in their customer profile at the vendors’ Websites. It must therefore 
be possible for customers to mark certain vendors as trusted for transactions where the 
authentication information won’t have to be present in the name field.

Under this scheme, compromised credit-card records would pose a much lower threat of 
unauthorized charges to customers because they could not be used for most transactions, as they 
would contain no usable authentication information. The exception would be unauthorized 
charges with vendors the customer has marked as trusted, but vendors could employ mechanisms 
to either prevent or to detect such fraud such as blocking deliveries to unauthorized addresses or 
by requiring confirmation from the authorized e-mail accounts and thus give customers reason to 
declare them as trusted with their bank.

A lot more nitty-gritty details would need to be worked out; for example, how do customers 
notify their bank that they are about to conduct a transaction and thus need a new one-time code? 
I welcome contacts from readers interested in pursuing discussions of these ideas. Please contact 
me via e-mail to discuss this and other solution alternatives <jpabel@akkaya.de>.

[MK adds: I’ll be happy to get a detailed proposal published.]

* * *

Jürgen Pabel, MSIA, CISSP is a consultant with Akkaya Consulting Gmbh <http://www.akkaya.de/>. He runs an interesting technical blog <http://blog.akkaya.de/blojsom/blog/jpabel/> that often includes security topics. He last wrote for 

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information 
Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of 
Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 J. Pabel & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without 
limit on any Web site, and to republish it in any way they see fit.