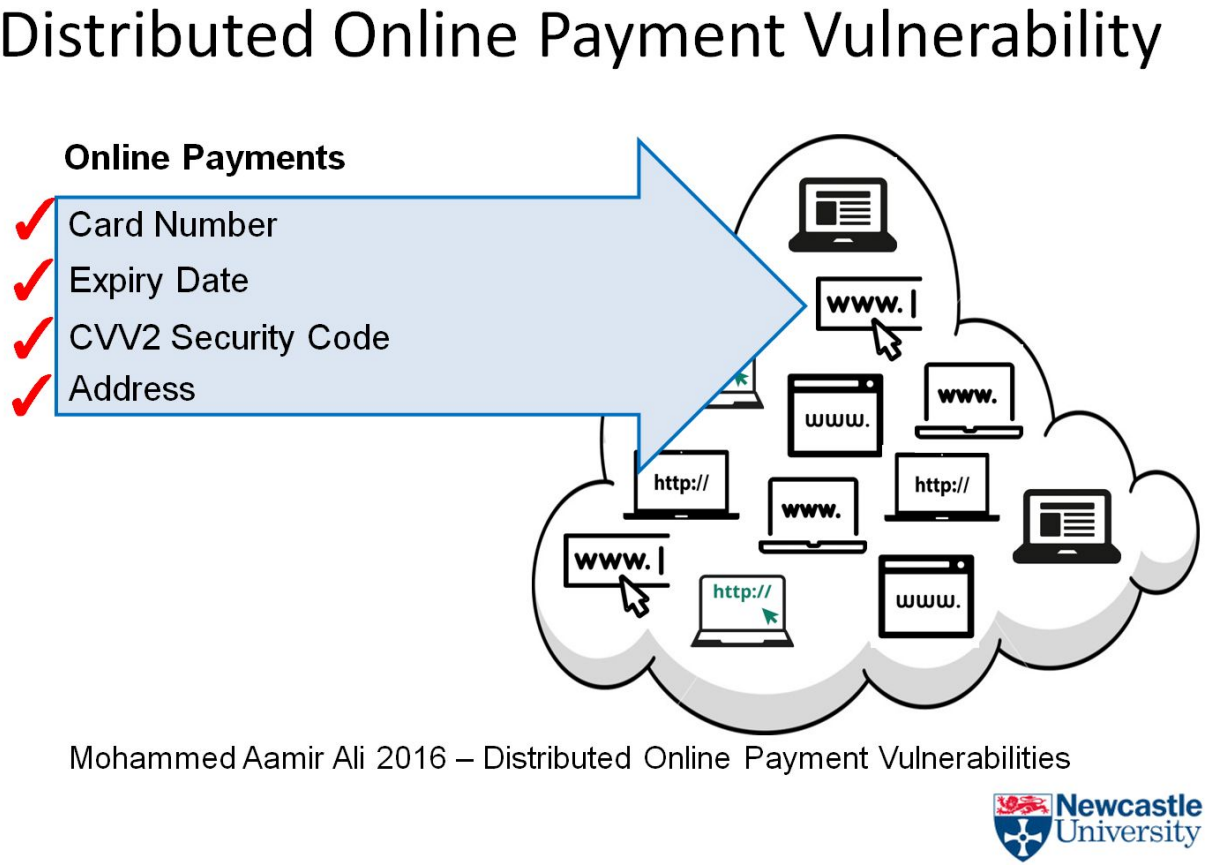
How it takes just six seconds to hack a credit card

December 1 2016



Credit: Newcastle University

Working out the card number, expiry date and security code of any Visa credit or debit card can take as little as six seconds and uses nothing

more than guesswork, new research has shown.

Research published in the academic journal *IEEE Security & Privacy*, shows how the so-called Distributed Guessing Attack is able to circumvent all the security features put in place to protect online payments from fraud.

Exposing the flaws in the VISA payment system, the team from Newcastle University, UK, found neither the network nor the banks were able to detect attackers making multiple, invalid attempts to get payment card data.

By automatically and systematically generating different variations of the cards security data and firing it at multiple websites, within seconds hackers are able to get a 'hit' and verify all the necessary security data.

Investigators believe this guessing attack method is likely to have been used in the recent Tesco cyberattack which the Newcastle team describe as "frighteningly easy if you have a laptop and an internet connection."

And they say the risk is greatest at this time of year when so many of us are purchasing Christmas presents online.

"This sort of attack exploits two weaknesses that on their own are not too severe but when used together, present a serious risk to the whole payment system," explains Mohammed Ali, a PhD student in Newcastle University's School of Computing Science and lead author on the paper.

"Firstly, the current online payment system does not detect multiple invalid payment requests from different websites. This allows unlimited guesses on each card data field, using up to the allowed number of attempts - typically 10 or 20 guesses - on each website.

"Secondly, different websites ask for different variations in the card data fields to validate an online purchase. This means it's quite easy to build up the information and piece it together like a jigsaw.

"The unlimited guesses, when combined with the variations in the payment data fields make it frighteningly easy for attackers to generate all the card details one field at a time.

"Each generated card field can be used in succession to generate the next field and so on. If the hits are spread across enough websites then a positive response to each question can be received within two seconds - just like any online payment.

"So even starting with no details at all other than the first six digits - which tell you the bank and card type and so are the same for every card from a single provider - a hacker can obtain the three essential pieces of information to make an online purchase within as little as six seconds."

How the Distributed Guessing Attack works

To obtain card details, the attack uses online payment websites to guess the data and the reply to the transaction will confirm whether or not the guess was right.

Different websites ask for different variations in the card data fields and these can be divided into three categories: Card Number + Expiry date (the absolute minimum); Card Number + Expiry date + CVV (Card security code); Card Number + Expiry date + CVV.

Because the current online system does not detect multiple invalid payment requests on the same card from different websites, unlimited guesses can be made by distributing the guesses over many websites.

However, the team found it was only the VISA network that was vulnerable.

"MasterCard's centralised network was able to detect the guessing attack after less than 10 attempts - even when those payments were distributed across multiple networks," says Mohammed.

At the same time, because different online merchants ask for different information, it allows the guessing attack to obtain the information one field at a time.

Mohammed explains: "Most hackers will have got hold of valid card numbers as a starting point but even without that it's relatively easy to generate variations of card numbers and automatically send them out across numerous websites to validate them.

"The next step is the expiry date. Banks typically issue cards that are valid for 60 months so guessing the date takes at most 60 attempts.

"The CVV is your last barrier and theoretically only the card holder has that piece of information - it isn't stored anywhere else.

"But guessing this three-digit number takes fewer than 1,000 attempts. Spread this out over 1,000 websites and one will come back verified within a couple of seconds. And there you have it - all the data you need to hack the account."

Protecting ourselves from fraud

An online payment - or "card not present" transaction - is dependent on the customer providing data that only the owner of the card could know.

But unless all merchants ask for the same information then, says the

team, jigsaw identification across websites is simple.

So how can we keep our money safe?

"Sadly there's no magic bullet," says Newcastle University's Dr Martin Emms, co-author on the paper.

"But we can all take simple steps to minimise the impact if we do find ourselves the victim of a hack. For example, use just one card for online payments and keep the spending limit on that account as low as possible. If it's a bank card then keep ready funds to a minimum and transfer over money as you need it.

"And be vigilant, check your statements and balance regularly and watch out for odd payments.

"However, the only sure way of not being hacked is to keep your money in the mattress and that's not something I'd recommend!"

Provided by Newcastle University