NC3 THE NO-COMPROMISE CHARGE CARD
What Merchants don't have, Crooks can't steal.

Can NC3 be cracked?

Cracking is the process of taking a consumer's authorization code, creating another authorization, and charge the legal account holder (which is illegal).

Human Capable Passwords

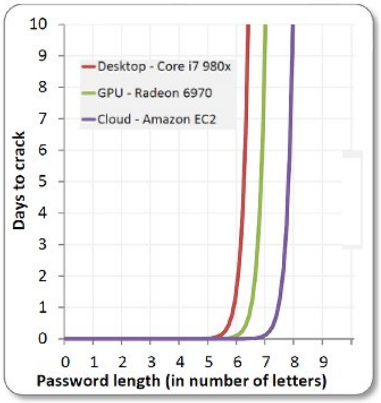
Passwords for human use require humans to be able to remember them. These are usually short and often pet names, birthdays, or other guessable, or easily determinable[1] items.

NC3 Encryption Use

NC3 uses *asymmetric encryption* designed for non-human use. *Asymmetric* means that the key used to lock is *not* the same key to unlock. Having one does not get you the other. An NC3 consumer holds only the encryption keys.

The vulnerability of a key pair is dependent on its complexity (mixed case, inclusion of numbers, special characters, non-dictionary words etc.) and length. All other elements being equal, the longer the key the more resistant to unauthorized decryption.

There is a "wall"[2] at which the *best available* computing power takes exponentially more time to hack a password of a specific length. As of mid-2012 that wall was at a password length of about eight characters. As the NC3 keys are not required to be human usable the keys can be considerably longer and farther beyond the wall making for very difficult unauthorized decryption.



Remember: Something out of sight is generally found absent only when it is sought. Cell phones are sought more often than charge cards so criminals have to crack each unique code before that consumer disables the account. By 2020 more computing power has moved the wall further out. Mass-compromise is simply not possible because each consumer has their unique code.

Even if the keys were cracked, the proper construction of requests and authorization is not generally known so re-creating an authorization has difficulty. How difficult? See next page.

[1] As for how easy, see http://arstechnica.com/security/2012/08/passwords-under-assault/
see also FIDO (Fast IDentity Online) Alliance program to replace passwords
see http://threatpost.com/en_us/blogs/darpa-fido-alliance-join-race-replace-passwords-021213

[2] The wall is the rapid rise in required processing time. One ethical hacker's experience, see http://erratasec.blogspot.com/2012/08/common-misconceptions-of-password.html << still active 10/2020

Summary

In the table below the degree of difficulty is from 1 (low) to 5 (high), or

1 trivially easy to do, so easy as to barely notice
2 barely difficult to do, requiring easily existing resources
3 moderately difficult to overcome requiring time and existing equipment
4 very difficult to overcome tending toward barely possible with considerable resources
5 extraordinarily difficult tending toward nearly impossible to overcome

Step	**Degree of Difficulty / Described**
Obtain QR-c from Consumer	2 / An NC3 Consumer payment authorization code (QR-c) is too complex for a human to eyeball and remember it. To obtain the QR-c requires surreptitious recording of a consumer's device as it is presented to the merchant.
Or Obtain QR-c from Merchant	3 / A miscreant may obtain a copy of the QR-c by hacking the merchant's records prior to approval, or a window generally under one minute. It may also be obtained by diversion-duplication, a process of directing a QR-c copy to a storage facility under miscreant control for later processing. A merchant should keep the QR-c code only as long as it takes to get an approval. After authorization the QR-c has no value.
Read	1 / The QR-c is a QR code and such readers are freely available.
Decrypt	4 / Once the QR-c is visible it appears as plain text (if there was any) followed by crypto text[3]. Because the encryption is of more than one generation the full crypto text won't appear as plain text even with a partial success. Further, not all elements are as they appear to be. << this material regarding additional specific security measures complicating decryption efforts was redacted from public version of this document >>.
Re-Crypt	5 / Given a successful decryption the same effort needs to be expended to find the encryption key. As the original code contains 'salt' (misleading constructions) and there are multiple crypto text values for the same plain text character this becomes more difficult. << this material regarding additional specific security measures complicating re-encryption efforts was redacted from public version of this document >>.
	= = = Additional Complications for Unauthorized Access = = =
Time	5 / Each QR-c contains a self-invalidating date/time in the most encrypted section. After that time the authorization is invalid. Given two days as a reasonable transaction time, it becomes unlikely all the preceding steps can be accomplished before expiration.
Consumer Re-Provisioning	5 / This is very hard to overcome for the crooks, but very easy for the consumer. Because the NC3 code is *not* the underlying charge code a consumer may obtain a new NC3 code with great ease. With the new code comes new keys, or multiple keys, and prior exposure is reduced to zero as old keys are no longer valid.

[3] See also NC3-PDE_for_the_web which describes the novel “partial dual encryption” design.