PIN Holes: Numeric Passcodes and Mnemonic Strategies

David Harley
ESET North America

About the Author

David Harley CITP FBCS CISSP has been researching and writing about security since 1989, and has worked with ESET North America – where he holds the position of Senior Research Fellow – since 2006. He previously managed the UK's National Health Service Threat Assessment Centre and is CEO of Small Blue-Green World. He is a former director of AMTSO. His books include Viruses Revealed and The AVIEN Malware Defense Guide for the Enterprise. He is a prolific writer of blogs, articles and conference papers. He is a Fellow of the BCS Institute (formerly the British Computing Society, and has held qualifications in security management, service management (ITIL), medical informatics and security audit.
Contact Details: c/o ESET North America, 610 West Ash Street, Suite 1700, San Diego, CA 92101, USA, phone +1-619-876-5458, e-mail david.harley@eset.com

Keywords

PIN, Personal Identification Number, mnemonics, keypad, memorization strategy, non-memorization strategy, ATM, handheld devices, PC keyboard, entropy, password management, passphrases, policy, education.

PIN Holes: Numeric Passcodes and Mnemonic Strategies

Abstract

Recommendations on how to select and/or memorize a four-digit PIN (Personal Identification Number) can be found all over the Internet, but while we have learned a great deal from analyses of mixed-character passwords and passphrases revealed by high-profile breaches like the highly publicized Gawker and Rockyou.com attacks, there are no exactly equivalent attack-derived data on PIN usage. However, a sample of 204,508 anonymized passcodes for a smartphone application, by ranking 4-digit strings by popularity, gives us a starting point for mapping that ranking to known selection and mnemonic strategies.

Memorization strategies summarized by Rasmussen and Rudmin include rote learning; memorization according to keypad pattern; passcode re-use from other security contexts; code with personal meaning; code written down or stored electronically (as on mobile phone) – possibly using various concealment and transformation strategies.

The data provided by Amitay allows us to assess the degree to which memorization strategies are used in relation to a standard smartphone numeric keypad, but also to engage in some informed speculation on the extent to which they might be modified on other keypads, including QWERTY phone keypads, ATM keypads, security tokens requiring initial PIN entry, and hardware using an inverted (calculator-type) numeric layout. The ranking allows evaluation of the entropic efficacy of these strategies: the more popular the sequence, the likelier it is to be guessed.

These considerations are used to assess the validity of commonly recommended strategies in a diversity of contexts and generate a set of recommendations based on the findings of this analysis. These recommendations are placed into the context of more general mixed-character passwords and passphrases. They will provide a starting point for security managers and administrators responsible for the education and protection by policy of end users and customers using the kinds of device and application that require numeric passcodes for authentication.

Introduction

There are few people in technology-rich societies who *never* have to make use of a numeric passcode or Personal Identification Number (PIN) sometimes, often in a multi-factor authentication context. (The use of the terms PIN, passcode, password and passphrase in this paper is as defined in the Appendix.)

Some examples of everyday PIN usage:

- Getting cash from an Automated Teller Machine (ATM) or cashpoint.
- Chip and PIN credit/debit card transactions
- Digital locks accessed by keypad, digital padlocks
- Handheld authentication devices where a PIN may be supplemented by a biometric technique (e.g. fingerprint scanning) or a one-time password/passcode regularly re-generated (a typical example refreshes every 60 seconds). Software that implements somewhat similar functionality is now seen on all the common smart-phone platforms, widespread enough to have attracted the attention of malware authors. For example, a recent malicious app for Android (Castillo, 2012) masquerades as a token generator allegedly

supplied by banks including Santander, and is actually intended to capture the victim's initial password before generating a 'token' which is actually just a random number. While a good passcode or PIN will not help in the case of such an attack, this attack trend is a pretty good indication of how mainstream this kind of application is becoming – and how it is transferring from the desktop to the mobile arena.

- Mobile devices such as laptops, netbooks and tablets used for access to specialist resources and databases on the move: for example, mobile healthcare specialists requiring access to patient data.
- Smartphones and other mobile devices (iPods, tablets and so on) also use PINs and other passcodes for protection and privacy by screen-locking (Amitay, 2011). And that is where the author's hunt for rational PIN selection and memorization strategies actually began. (Harley, 2011a)

The main data sources used here are a database quantifying passcode usage kindly shared with this author by Daniel Amitay (Harley, 2011b), and an analysis by Rasmussen and Rudmin (Rasmussen & Rudmin, 2010) of the results of surveys quantifying the use of various mnemonic strategies.

Big Brother is Watching (and Counting)

Amitay marketed an iPhone app called Big Brother to take photos of anyone using an iPhone or iPod Touch 4 without permission (i.e. without entering a passcode). An update added code to capture the passcodes required during setup without identifying the individual iGadget or its owner, and ran some analysis on a sample population of 204,508 passcodes. In fact, iGadgets offer a choice of passcode modes for screenlocking:

- Inactive
- Simple 4-digit passcode
- A more complex passcode

The customer's choice of passcode for Big Brother doesn't necessarily reflect either the strategy for selecting a 4-digit screenlocking passcode or general PIN selection practice – in fact, as we'll see, differences in keypad layout probably have a significant influence on selection strategies for some devices – but it seems reasonable to assume that, given the size of Amitay's sample population, there's likely to be *some* correlation, at least with respect to the same iGadget. We already know that people re-use passwords on many accounts, and high-entropy numeric strings are probably harder to remember and even more liable to re-use.

Discussion

Rasmussen and Rudmin offer a list of mnemonic strategies:

- Rote learning
- Memorization by keypad patterning
- Code re-use
- Code with personal meaning
- Numbers paired with letters
- Code written down and kept separate*

- Code stored in mobile phone*
- Code concealed in a phone number*
- Written down and kept in proximity*
- Written down but rearranged*
- Notated as a transform of the code*

The strategies marked with an asterisk are what might be described as non-memorization or memorization-avoidance strategies, and the Amitay data, being anonymized, don't give provide us with insight into the proportion of subjects who use them.

Out of a sample of 388 respondents to a survey (Rasmussen & Rudmin, 2010), however, 61% claimed to use at least one non-memorization strategy, while 38% claimed to use a code that meant something to them personally. Amitay and Rasmussen & Rudmin both cite dates as an example of such a personal meaning, but other examples might include (part of) a house or apartment number, telephone number, car number, and so on.

Murder She Rote

One straightforward memorization option is what might be called the 'take what you're given approach: that is, to accept and memorize a PIN as originally allocated by a service provider, even in the absence of a convenient strategy to make memorization of a hard-to-remember password or passcode easier. In some contexts, of course, there is no alternative: the system simply doesn't offer a way of personalizing the passcode: however, in that case, we can hardly talk about selection. On the other hand, a customer or end-user might be required to change an initially-generated passcode on activation and/or change it on a regular basis, though these requirements are far more common in the context of passwords. When offered a choice, do people prioritize security over ease of recall (in the absence of a non-memorization strategy)?

There is copious evidence that many people are continuing to use highly stereotyped password selection as aids to memorization. Or to put it another way: many, many people are using the same handful of passwords. In fact, much of the research on password use and re-use derived from the analysis of known collections of exposed passwords (Harley, 2011c) so as to see which are the most commonly used, and there's a high degree of consistency in various top ten (or top five, top 100 or even top 100) lists of 'worst passwords'. For example, the following are found somewhere in the top twenty in many such lists, though not always in the same order (What's My Pass?, 2008):

123456 [...9]
password
qwerty
iloveyou
abc123

Table 1: Common/Stereotyped Passwords

PINS, Needles and Haystacks

It seems that similar stereotyping applies in the selection of numeric passwords: it turns out that the top ten choices accounted for 15% of Amitay's sample set:

Ranking	Passcode	Incidence
1	1234	8,884
2	0000	5,246
3	2580	4,753
4	1111	3,262
5	5555	1,774
6	5683	1,425
7	0852	1,221
8	2222	1,139
9	1212	944
10	1998	882

Table 2: Top Ten Passcodes (n=204,508) (Amitay, 2011)

Perhaps we shouldn't be too surprised that the top-ranked 4-digit code is essentially the same as the top-ranked password according to many sources (Imperva, 2010): that is, the first n digits in the numeric sequence from 1 to 9. Most password authentication schemes enforce a minimum length of at least six characters: if the minimum length for passwords was four characters or the common convention for PIN length was six digits, the top-ranked password and top-ranked PIN might well be identical.

The iPhone and its iGadget siblings give the user ten chances to try an activated 4-digit screenlock passcode before locking them out, giving an intruder a surprisingly good chance of getting in using only the top ten passcodes as indicated in Amitay's sample set. (Harley, 2011b);

Other security applications on other platforms may less (or more) forgiving.

Bad Passwords in the Twitterverse

Twitter has its own views on what constitutes bad password selection: in 2009 it started to refuse to accept passwords submitted by its users that featured on its own blacklist. (Gawker, 2009). Further investigation showed that it was using a script along these lines.

```
    for (var i = r.length - 1; i >= 0; i--){
      twttr.BANNED_PASSWORDS.push(r[i].replace(/[a-z]/gi, function(l){
          var c = l.charCodeAt(0), n = c + 13;
          if((c<=90 && n>90) || (n>122)) { n -= 26; }
          return String.fromCharCode(n);
      }));
    };
  })();
</script>
```

Decoding the alphanumerically ordered list of proscribed passwords obscured using a simple substitution algorithm, essentially ROT13 we find the following completely numeric strings: ‘000000’,’111111’,’11111111’,’112233’,’121212’,’123123’,’123456’,’1234567’,’12345678’,’123456789’,’131313’,’232323’,’654321’,’666666’,’696969’,’777777’,’7777777’,’8675309’,’987654’.

There are, of course, also some mixed alphanumeric strings like our old friend ‘abc123’ and ‘ncc1701’, an ID indelibly associated with the USS Enterprise (Wikipedia, 2005). (In fact, since the script uses only a ROT13 algorithm, which doesn’t include substitution for digits, decoding is not actually necessary to see the purely numeric strings.)

Ergo Ergonomics

The classifications defined by Rassmusen and Rudmin include ‘Memorization by keypad patterning’. To avoid confusion with the Pattern Unlocking technology used in some Android touchscreen telephone handsets (Zwienenberg, 2012), though that has some relevance to the topic under consideration, I’ve preferred to use the term ergonomic strategy rather than patterning to describe strategies that derive from the layout of keyboards and keypads. My justification for this somewhat cavalier hijacking of the term ‘ergonomic’ is based on a definition of ergonomics by the International Ergonomics Association:

> Ergonomics (or human factors) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance. (Human Factors and Ergonomics Society, 2005-2010)

Code Re-Use

This simply refers to re-using a passcode (or indeed password or passphrase) already memorized from another security context, so could be regarded as a non-memorization strategy. It’s certainly a viable (if not secure) selection strategy, and some of the sources currently available for password stereotyping analysis indicate that it’s a very widely used in that context: for example, Troy Hunt found, during analysis of 37,608 stolen Sony Pictures passwords put out as a torrent by LulzSec, that there were over 2,000 accounts where the same email address had been registered on both the 'Beauty' and 'Delboca' databases, and 92% of passwords were found across both systems (Harley, 2011d). We don’t, however, have comparable PIN-usage data that would allow us to make a similar estimate across multiple systems.

Strategy Classification Hypotheses

Twitter’s list doesn’t tell us anything about the volume of use of these passphrases relative to other over-used passphrases on the list, but it does offer the opportunity to consider why they are used often enough to attract Twitter’s attention. We can, in fact, guess at the following selection strategies and relate them to mnemonic strategies (with some overlap):

Category Number	Strategy Classification Hypothesis
1	Single character repeated as many times as is necessary to meet the required length of password. Interestingly, the only numeric characters seen here in the context of this strategy are 0, 1 and 7. Topographically, 1 is the easiest to find on a standard computer keyboard, so it’s not surprising that it’s found so often in single digit passwords, while 0 is also a logical ‘starting’ digit for

	computer-oriented geeks, and also easy to find for a hunt and peck typist. But why 7? Something to do with it's being more memorable, being a 'lucky number' in Western cultures perhaps? (That would put it in the category Rasmussen and Rudin describe as 'code with personal meaning', even if it were 'personal' to an awful lot of people. However, it doesn't take a touch typist to find *any* numeric key and press it *n* times, a strategy I'd define as ergonomic.
2	Simple ordered sequence starting (logically enough) from 1 and finishing when the password length requirement is met (123456 to 123456789 in the Twitter list). The algorithm is so mnemonically obvious that it barely needs to be memorized, as such, especially in a context where input is ignored after *n* characters, as may happen with PINs. Again, these are very easy sequences on a standard computer keyboard: the group 123 is actually very easy on the top row of the main keyblock, but also on the characteristic numeric keypad at the right hand side of a standard keyboard. We also have a special case here where each digit in the sequence is immediately repeated (112233), and two instances where the starting digit is different and the sequence is descending (987654 and 654321). However, these choices can be accounted for by the fact that they're almost as easy to type as a '1-n' sequence. These would probably fall into the keypad patterning/ergonomic category.
3	Short ordered sequences repeated as necessary: 121212, 123123, 131313, 232323 in this instance, suggesting ergonomic selection. The joker in this pack is 696969, where the base sequence is still ascending but the keys are significantly further apart on the top row of the main keyblock. On a numeric keypad, the nine is immediately above the six: however, given the number of stereotyped passwords that have some sexual connotation, it's possible that there may be an association with soixante-neuf here.
4	One of these strings, 8675309, doesn't meet any obvious ergonomic criteria, but a little research establishes that it is, apparently, 'one of the most famous telephone numbers in the world' (Urban Dictionary, 2004) being part of the title of a 1980s hit for Tommy Tutone. Snopes.com, a site specializing in urban legends, notes in passing (Snopes, 2007) that the sequence actually breaks down into three upward diagonal sequences on a touch-tone telephone (86, 753, 09), but that doesn't seem particularly advantageous ergonomically, so a 'code with personal meaning' classification seems more appropriate. (Again, it's clearly 'personal' to a great many people...)

Table 3: Suggested Strategy Classifications

How well does a similar analysis work with the Amitay data in Table 2?

Several of the top ten passcodes fit into the same hypothetical strategies listed in Table 3, even though virtual keypads for screenlocking on iGadgets are like the numeric keypad on a standard keyboard as represented in Table 4 (or the numbering on a touchtone telephone or smartphone) rather than the serial layout of numbers on the main keyblock.

Num Lock	/	*	-
7 Home	8 ↑	9 PgUp	+
4 ←	5	6 →	
1 End	2 ↓	3 PgDn	Enter
0 Ins		Del	

Table 4: Numeric/Cursor Keypad (standard keyboard)

1	2	3	4	5	6	7	8	9	0

Table 5: Numeric Keys on Main Keyblock (standard keyboard)

- 0000, 1111, 5555 and 2222 are obvious candidates for category 1 (same digit repeated as often as necessary). While 1212 is, for someone of my age and nationality, inevitably memorable by association with Scotland Yard's former telephone number Whitehall 1212 (Harley, 2011a), it's more probably and commonly a case of a repeated short sequence as per category 3 (i.e. an ergonomic strategy). In fact, 121212 is regularly found in lists of breached passwords.
- 1234 is, as in category 2 above, mnemonically obvious as an algorithm and requires no specific memorization, and isn't significantly more difficult to type on a keypad than on a standard typewriter-type keyboard.
- 2580 and 0852 are almost certainly ergonomic choices: The middle column on an iGadget virtual keypad reads 2580 going down, 0852 going up.
- 1998 doesn't seem to represent an obvious ergonomic or pattern memorization strategy, but Amitay hypothesises – on the basis that the year-like strings 1990-2000 are all in the top 50 while 1980-1989 are all in the top 100 – that people use the year of their birth or graduation as an easily remembered passcode. (Code with personal meaning.) It's likely that people do use memorable dates, but it's also likely that as they get older they use other memorable dates such as the date they got married, left university, changed jobs, and so on. However, this kind of hypothesis remains unproven in the absence of supporting qualitative data.

What about 5683? Not an obvious ergonomic choice: however, in the context of a smart-phone keypad, Amitay has a likely hypothesis to fit the case, using a memorization strategy. The numbers on such a keypad (excluding 1 and 0) usually include three or four corresponding letters:

1	2 abc	3 def
4 ghi	5 jkl	6 mno
7 pqrs	8 tuv	9 wxyz
	0	

Table 6: Smartphone Keypad Letter/Number Correlation

In this case, 5683 could easily correspond to L-O-V-E: as Amitay also points out, this is a rough analogue to the 'iloveyou' string that turns up in so many Top *n* Worst Passwords lists (Imperva, 2010). This falls into the category Rasmussen and Rudin refer to as 'Numbers paired with letters.' How widespread is this category likely to be? To some extent, this depends on keypad layout. The touchpad-phone-like layout of the iGadget Passcode Lock setting dialogue suggests that PINs including 1 and 0 don't use exactly this strategy, as there are no letter pairings for these digits. However, it's likely that some people may use one of these keys as a 'dummy' value, though this doesn't altogether account for the high volume in Amitay's data of PINs that *do* include 1 or 0. In fact, manually searching for numbers in the top hundred that *are* likely to correlate to four-letter dictionary words proved fairly unproductive. However, there are many possible four-letter strings that wouldn't necessarily come up in a dictionary search yet still have meaning for the individual: for example ZIZZ, MATT, substituted digits for letters like H00K instead of HOOK, or mixed or interleaved alphanumerics like TIM7 or MI5T . The fact that these numeric strings rarely occur in the Amitay data suggests possible strategies for increasing PIN security, almost irrespective of their length.

Alphabetical String	4-Digit Equivalent	Instances
ZIZZ	9499	5
MATT	6288	10
H00K	4005	5
HOOK	4665	10
TIM7	8467	10
MI5T	6458	9

Table 7: String To PIN Mappings (n=204,508) [Amitay]

Keypad Layout is Key

While the number-to-letter mapping shown in Table 6 is very widely used on modern telephones, smart-phones and devices of a similar form factor, other layouts are possible, even on telephones, and these will impact on For example, the Blackberry 'QWERTY' keyboard layout results in this one-to-one number-to-letter mapping:

Number	Letter
1	W
2	E
3	R
4	S
5	D
6	F
7	Z
8	X
9	C

Table 8: Blackberry QWERTY number-to-letter mapping

In Tables 8 and 9, grouping of keys by row is indicated by alternating background shading.

This layout, unlike the more generally seen layout in Table 4, does offer letter mapping to the digit 1, but still not to 0, and reduces the number of letters available for a letter-to-number mapping strategy to 9. However, it's feasible that some passcodes combine a letter mapping strategy with a number-for-letter substitution strategy (f00d = 6005, for example).

Other QWERTY keyboards on handsets may use different mapping keys: for example, keyboards that include a top row of number/punctuation keys modelled on the common configuration for laptops, are likely to use the mapping shown in Table 7, further reducing the number of potential letter mappings to seven.

Number	Mapping
7	7
8	8
9	9
4	U
5	I
6	O
1	J

2	K
3	L
0	M

Table 9: Common Laptop Simulated Numeric Keypad Configuration

However, it may offer a slight ergonomic advantage to users accustomed to using numeric keypads on computer keyboards (Table 4) or common calculator configurations like Table 10:

7	8	9
4	5	6
1	2	2
0		

Table 10: Conventional Calculator Keypad Layout

There are (inconclusive) discussions on why numeric keypads on calculators and telephones are usually the opposite way round to each other at http://www.howstuffworks.com/question641.htm.

There are other ergonomic (keyboard-related) factors that are not considered here: for instance the use of Bluetooth add-on keyboards with iGadgets, and the use of alternative keyboard layouts such as Dvorak for ergonomic reasons. (Dvorak keyboards offer a surprising range of number key layouts according to context.)

Conclusion

Amitay's data are interesting and suggestive enough to point to some strategies for increasing entropy that can be shared with customers and end-users: however, there is a limit to how far we can go without more qualitative data directly solicited from users on what strategies they actually use. The study by Rasmussen and Rudin clearly indicates that many people don't use just one strategy, and that follows from the different styles of initial passcode allocation used in different contexts.

- Easy default PIN e.g. 0000. The need to change a default may vary according to context: you may never need to change the PIN on your cordless handset at home, but the News of the World scandal clearly demonstrates that if the privacy of your voicemail matters to you, setting another PIN is a sensible precaution. (Rogers, 2011)
- Difficult (high-entropy) PIN allocated for example by a credit card provider. Caveat: if a PIN is allocated (truly) randomly, it may actually hit on an over-used, 4-digit sequence that *should* be changed. However, financial institutions often filter out over-used sequences like 1234 and 7777, presumably when allocating an initial PIN, but certainly when a customer tries to change it. (MBNA, 2012; Bank of America, 2012)

What should we tell the end-users?

Strategies for generating secure PINs are not so different to those often suggested by the security community (Harley & Abrams, 2009). While the heavily randomized passphrase mixing

alphanumeric and punctuation characters so beloved of the security community (Butler, 2012) is not an option (thankfully for those who find it difficult to remember quasi-random sequences of unrelated character, alternative memorization strategies based on number-to-letter mapping or pattern unlocking (Zwienenberg, 2012) are legion. But which offer the best privacy? Let's revisit the mnemonic classifications used by Rasmussen and Rudin that count as memorization strategies.

Rote Learning

The trick is to select passwords or passcodes that are easy to remember for the legitimate user of a service, but hard for an attacker to guess. Learning a reasonably secure 4-digit PIN isn't too hard, though it may be harder for specific age groups and anyone can forget a PIN that has no personal meaning for them if they don't use it often enough to refresh the engram. Users who are confident of their ability to retain a pre-allocated passcode may be well-advised to check that such sequences aren't too obvious. A credit card is unlikely to arrive with a PIN like 0000, but that's a very common default sequence in telephony.

Memorization by Keypad Patterning

It's easier to tell people which passcodes and passcode strategies *not* to use, and some could be said to overlap categories. Here are some dubious strategies:

- Any string consisting of an ascending or descending sequence (1234, abcd, 9876). The risk might decrease, however, if the starting digit isn't 1, 0 or 9, as usage statistics drop sharply. In fact, descending sequences seem noticeably less used that ascending sequence. Fibonacci sub-sequences work better with longer strings and not starting too early in the sequence: 0112 isn't a great choice.
- Any string consisting of a single character repeated (this applies just as definitively to passwords as to passcodes). For instance, 0000 or 7777.
- Strings that consist of a short sequence repeated (especially 1212). 2121 is less popular, but still a high scorer. Again, starting with a different digit and descending rather than ascending is less popular. Palindromes are popular, but increasing the interval between adjacent digits is less popular.
- Two of the most common patterns on the conventional smart-phone keypad are 2580 and 0852: in other words, the middle column going down and going up. Their popularity is probably explained by the fact that this is the only row with four keys in a straight line, but that popularity makes them a poor choice for a PIN. 1470 is the 51st most popular choice, and 3690 is the 68th: in each case, the pattern is downward, finishing with 0. The reverse pattern seems very much less popular.

While Android Screenlock Patterning hasn't been discussed here, some of the same considerations apply. Patterning allows you to define a personally recognizable pattern by joining 9 dots in a pattern recognized by the device as equivalent to a password. To quote Zwienenberg (Zwienenberg, 2012):

"You can swipe your finger on the screen over a 9 point square and draw your favorite little line-picture to unlock it. The line-picture should not be too easy to guess, so if your name is Lisa or Lewis, using the "L" shape may not be the safest in the world."

Code Re-Use

Re-use of a known passcode (which could be described as a special case of a code with personal meaning) might be a good strategy under some circumstances: after all, if it's a good (i.e. less popular) choice in one context, it probably is in other contexts. The drawback is that if it becomes known in one context, the risk increases that an attacker will try it in other contexts.

Code with Personal Meaning

This approach eases memorization, but there are two main caveats:

1. If it's based on something like a memorable date, it shouldn't be too obvious a memorable date: for example, one that might easily be deduced from information on your Facebook profile.
2. If the code is one that's among the most popular, the fact that you didn't choose it for the same reason as everyone else doesn't make it any safer. For instance, if you chose 1234 for the fairly obscure reason that your uncle's cat had kittens on the 4th March 2012, that doesn't make it any more secure than if you'd chosen it because it was a stereotypical ascending sequence.

Numbers Paired with Letters

Many of the same considerations apply to number-to-letter mapping as to the strategies above, and indeed, there is the same likelihood of overlap. In particular, a text string used as a memory jogger for a PIN is also likely to have a personal significance. In the example MATT (6288) given in Table 5, it's easier for an attacker to guess at the strategy used if the subject's name is Matt, even though it's not a heavily used PIN according to the Amitay data. However, if the name Matt doesn't have any obvious connection with the subject, it becomes much more secure.

Number-to-letter mapping also offers the opportunity to take advantage of mixed alphanumeric characters, since even where a keypad doesn't have a direct mapping from a number to one or more letters, since numbers can be used in a memory jogger text string even though there is no corresponding letter. Examples in Table 5 included H00K and MI5T, which also feature the kind of substitution of numbers for letters often favoured in passwords.

Education, Policy and Technical Issues

You can take a horse to water and an end-user (or even a home user) to the Pierian Spring (Pope, 1709), but you can't make any of them drink. As ever, while some people will respond appropriately to advice and training and will be guided by policy, it's incumbent upon service providers to impose restrictions where possible to prevent the use of stereotyped passcodes.

Such services are not restricted to those furnished over the Internet by third-party providers: in the age of Bring Your Own Device (BYOD) where unauthorized or inappropriate access to a device may give an attacker access to internal resources, there's also a need within the enterprise to find ways to encourage and enforce sensible, security-aware behaviour when it comes to PIN selection strategy.

Inside and outside the workplace, it's critical that those who've embraced the 'share everything and don't worry about privacy or security' philosophy of social media are encouraged to recognize that the ready availability of so much personal and even sensitive data makes it less safe as a source of passcodes and passwords with personal meaning.

Appendix 1: Glossary

iGadget: informal blanket term for a mobile device, especially one marketed by Apple under the names iPod, iPad, or iPhone.

Memorization strategy: a mnemonic technique for remembering a pre-allocated passphrase or passcode, or replacing a pre-allocated passphrase or passcode with one the individual is likelier to remember.

Mnemonic: describes a technique for aiding memory or, as used here, avoiding the need for memorization of a context-specific token. For example, if I were always to use the number of my apartment as a PIN (I don't!) I would still have to remember my address, but wouldn't have to memorize anything in the context of a specific application, such as a new credit card.

Multi-factor authentication: the use of more than one layer of authentication. Factoring is normally described in terms of:

- Something you have (a key, a credit card, a handheld authentication device).
- Something you know (a password or passcode, the answer to a 'secret question').
- Something you are (a physical feature authenticated by fingerprint or retinal scanning, for example).

Non-Memorization Strategy: implementation of a means of access to a passphrase or passcode that avoids the need to memorize it, such as storing it in some (possibly obfuscated) form.

Passcode: a more general term for a numeric password, often used interchangeably with the term PIN. (http://www.rsa.com/glossary/default.asp?id=1092)

Password: a word or character string used to authenticate a service user to the service, often but not invariably in tandem with a unique identifier such as an account name. Where only a numeric character string is accepted, it reduces confusion to use the term passcode.

Passphrase: essentially, a longer version of a password that may or may not include single words as tokens separated by spaces as a delimiter. Passphrases may be preferred to simple passwords (Harley, Abrams) subject to other considerations, but their superiority in terms of entropy may be overestimated (Harley, 2012; Bonneau, 2012), especially for simple sentences and well-known quotations.

PIN (Personal Identification Number): a numeric password. ISO 9564, the international standard for PIN management and security in retail banking, (ISO, 2011) historically specifies a PIN length between 4 and 12 characters. However, many devices default to four digits, and may not accept more than six (or even four) characters.

References

Amitay, D. (2011). Most Common iPhone Passcodes. Retrieved 19 March, 2012, from http://amitay.us/blog/files/most_common_iphone_passcodes.php

Bank of America (2012). Card Security. Retrieved 19 March, 2012, from http://www.bankofamerica.co.uk/credit-cards/security/

Bonneau, J. (2012). Some evidence on multi-word passphrases. Retrieved 19 March, 2012, from http://www.lightbluetouchpaper.org/2012/03/07/some-evidence-on-multi-word-passphrases/

Butler, D. (2012). Retrieved 19 March, 2012, from https://twitter.com/#!/david_a_butler/status/181640506873352192/photo/1

Castillo, C. (2012). Android Malware Pairs Man-in-the-Middle With Remote-Controlled Banking Trojan. Retrieved 19 March, 2012, from http://blogs.mcafee.com/mcafee-labs/android-malware-pairs-man-in-the-middle-with-remote-controlled-banking-trojan

Cluley, G. (2011). The top 10 passcodes you should never use on your iPhone. Retrieved 19 March, 2012, from http://nakedsecurity.sophos.com/2011/06/14/the-top-10-passcodes-you-should-never-use-on-your-iphone/

Gawker (2009). The 370 dumbest passwords as compiled by Twitter. Retrieved 19 March, 2012, from http://gawker.com/5435621/the-370-dumbest-passwords-as-compiled-by-twitter

Harley, D. (2011a). Hearing a PIN Drop. Virus Bulletin, September 2011, 12-14. Retrieved 19 March, 2012, from http://macviruscom.files.wordpress.com/2010/06/dharley-vb201109.pdf

Harley, D. (2011b). Passcodes and Good Practice. Retrieved 19 March, 2012, from http://macviruscom.wordpress.com/2011/06/15/passcodes-and-good-practice/

Harley, D. (2011c). Good passwords are no joke. Retrieved 19 March, 2012, from http://www.scmagazine.com/good-passwords-are-no-joke/article/204675/

Harley, D. (2011d). A nice pair of breaches. Retrieved 19 March, 2012, from http://blog.eset.com/2011/06/07/a-nice-pair-of-breaches

Harley, D. (2012). Passwords, passphrases, and big numbers: first the good news… Retrieved 19 March, 2012, from http://blog.eset.com/2012/01/17/passwords-passphrases-and-big-numbers-first-the-good-news

Harley, D. and Abrams, R. (2009). Keeping Secrets: Good Password Practice. Retrieved 19 March, 2012, from http://go.eset.com/us/resources/white-papers/EsetWP-KeepingSecrets20090814.pdf

Human Factors and Ergonomics Society (2005-2010). Definitions of Human Factors and Ergonomics. Retrieved 19 March, 2012, from http://www.hfes.org/Web/EducationalResources/HFEdefinitionsmain.html

Imperva (2010). Imperva Releases Detailed Analysis of 32 Million Breached Consumer Passwords. Retrieved 19 March, 2012, from

http://www.imperva.com/news/press/2010/01_21_Imperva_Releases_Detailed_Analysis_of_32_Million_Passwords.html

ISO (2011). ISO 9564-1:2011 Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems. Retrieved 19 March, 2012, from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=54083

MBNA (2012). Credit Card Security. Retrieved 19 March, 2012, from http://www.mbna.co.uk/protection-security/credit-card-security/#tab:we-protect-you

Pope, A., (1709). Essay on Criticism. Retrieved 19 March, 2012, from http://poetry.eserver.org/essay-on-criticism.html.

Rasmussen, M. and Rudmin, F. (2010). The coming PIN code epidemic: A survey study of memory of numeric security codes. Electronic Journal of Applied Psychology. 6(2):5-9. Retrieved 19 March, 2012, from http://ojs.lib.swin.edu.au/index.php/ejap/article/viewPDFInterstitial/182/220

Rogers, D. (2011). How phone hacking worked and how to make sure you're not a victim. Retrieved 19 March, 2012, from http://nakedsecurity.sophos.com/2011/07/08/how-phone-hacking-worked/

Snopes (2007). Jenny 867-5309. Retrieved 19 March, 2012, from http://www.snopes.com/music/songs/8675309.asp

Urban Dictionary (2004). 867-5309. Retrieved 19 March, 2012, from http://www.urbandictionary.com/define.php?term=867-5309

What's My Pass? (2008). The Top 500 Worst Passwords of All Time. Retrieved 21 March, 2012, from http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

Wikipedia (2005). USS Enterprise (NCC-1701). Retrieved 19 March, 2012, from http://en.wikipedia.org/wiki/USS_Enterprise_(NCC-1701

Zwienenberg, R. (2012). The security of unlocking an Android based device, the future is near? Retrieved 19 March, 2012, from http://blog.eset.com/2012/03/13/the-security-of-unlocking-an-android-based-device-the-future-is-near