Comments on Gridsure Authentication

This document is an edited version of notes taken to provide feedback to Gridsure after an approximately two hour meeting on Friday 8th February 2008, and based on past presentation material on the scheme seen in mid 2007.

Please note that these comments are *selective* feedback on particular issues I found with the Gridsure scheme, which can aid other analysts in continuing this work. This document is not intended to be a fully representative or balanced appraisal of the scheme.

Mike Bond, 27th March 2008

Weber's Report

I dispute the worth of Professor Weber's analysis[1]. Whilst his mathematical calculations in themselves I'm sure are flawless, there are a number of tacit assumptions made that undermine its meaningfulness, mainly about the psychology of choice of patterns. Weber first selects a set of "likely to be chosen" shapes, including lines, ticks and boxes. On what basis is it argued that users are likely to pick these shapes? Intuitively we might want to believe that squares, lines, ticks are all common, but it psychology results often defy intuition and need to be properly researched. Secondly, Weber assumes that all alignments of common shapes are equally likely to be chosen, for example that a four digit line running from left to right could start from the second column as well as the first. Beyond this, the combinatorics clearly say nothing about the relative likelihood of different patterns actually being chosen. So if we were to accept his assertion that there are 11,640 common patterns on the grid, it still is of huge significance that some of these patterns are more common than others. So the results of this report rely on psychology assumptions that Weber has not justified, and totally ignores the wider issue of relative probabilities of different shapes.

My suspicion is that the practical entropy of Gridsure patterns will be at least as low as that for PINs (way less than 10,000 combinations because PINs involving dates and years (e.g. 1984) are probably more common). Now, for PINs this can easily be rectified by issuing initial PINs rather than encouraging cardholders to choose their own. The advantages of Gridsure are eroded if the user cannot select his or her own pattern, and the results of the usability study conducted by Sasse are no longer applicable in this scenario.

Resistance of Challenge/Response to Pattern Recovery

During the meeting Gridsure stated that (according to Consult Hyperion), three "engineered grids" were required to determine a PIN with certainty. Below follows

[1] "GrIDsure – The mathematics of Patterns & Sequences", provided to me by Gridsure on 11/06/07

excerpts from my original analysis of June 2007, which Gridsure does not seem to have taken note of. Consider the following two engineered grids:

Challenge A	**Challenge B**
12345	11111
12345	22222
12345	33333
12345	44444
12345	55555

If a user is challenged with the following two patterns, then the pair of response codes together will leak the X and Y coordinates of each digit in the pattern. Clearly then a maximum of two challenge grids are required, not three as suggested by Consult Hyperion. Challenges A & B can have their digits permuted randomly, so long as the same transformation is applied to both A & B. The human eye will then not be able to detect the presence of a pattern. Furthermore, digits can be doubled up, so that pairs are used interchangeably. For example, the challenge grid A would become as follows:

Challenge A	**Challenge A (doubled up)**
12345	12895
12345	67345
12345	12890
12345	17345
12345	67345

Here the pairs are as follows: 1&6, 2&7, 3&8, 4&9, 5&0. The grid already appears much more random to the human eye, and remains just as usable for the attack; and this is before even the permutation step is undertaken.

Even better results could be achieved by using specially designed challenge grids based on empirical analysis of the common shapes and patterns chosen. The grid could be specially designed to make it as likely as possible that the pattern can be determined with a single challenge. For example, supposing we knew that straight lines either horizontally or vertically were 100 times more likely to be used than any other, then consider the following challenge grid.

Challenge C
12345
34567
56789
78901
32609

All possible length 4 horizontal and vertical straight lines are then uniquely coded:

1234, 3456, 5678, 7890, 3260	(horizontal, starting left most)
2345, 4567, 6789, 8901, 2609	(horizontal, leftmost + 1)
1357, 2468, 3579, 4680, 5791	(vertical, topmost)
3573, 4682, 5796, 6800, 7919	(vertical, topmost + 1)

This is just an example. With some care and attention, a very efficient single challenge grid aimed at exposing the most common shapes could be created.

So the standard mode of the gridsure system clearly is not strongly resistant to chosen challenges (such as might be deployed in a phishing attack). What then is the information leakage from response to a randomised grid challenge?

In a random challenge grid filled with digits 1 through 10, evenly distributed, we can expect every challenge to reduce (on average) the range of possible squares for each element of the pattern by a factor of 10 – namely a leak of 3.3 bits of information per digit responded to, or a total of 13.3 bits for a 4 digit response.

A fully random 4 digit pattern will have 25*24*23*22 combinations, equal to 18.2 bits of information (assuming non-repetition of the same square in pattern).

Clearly after two challenges, up to 26.6 bits of information have been revealed in the response, yet the maximal entropy of a pattern is 18.2 bits. Given the typical entropy of a pattern will be much lower, due some common patterns being much more appealing than others, it is likely that knowledge of both challenge grid and response from a single challenge will yield enough information to determine the pattern fully in a significant proportion of cases, and two challenge/response pairs will suffice in most cases. Thus if an eavesdropper is able to observe the challenge and response (e.g. with a mobile phone camera or fixed CCTV camera in a shop) or via screen capture in the case of malicious software on a PC, the pattern will quickly leak.

Though this analysis is far from complete, my opinion so far is that if the challenge can be seen, Gridsure is no more secure than a PIN, and possibly less so for the reasons described in other sections of this document.

Shoulder Surfing

The analysis of resistance to shoulder-surfing based on experiments with Children was inadequate. The learning curve and dynamics of teaching shoulder surfing are not known. Consider pick-pocketing – a criminal skill which requires some considerable level of practice to get good at. Yet we know it still can be done. Likewise shoulder surfers could specifically learn to determine patterns in a better way, probably with reference to common patterns. What we don't know is whether this is easy or difficult to learn, and it would be unwise to assume either. Note also that because the user always has to respond freshly with a different number to the challenge grid, the user will not be able to type the response number so quickly, and potentially not whilst also shielding it with their hand. This sort of protection is only likely to come into play upon repeated entry of the PIN. So one cannot assume that the response PIN is as well protected in the case of Gridsure (indeed it is proposed for accessibility purposes that certain respondents might read their response code aloud).

Compromised Terminals

The major current threat for PIN recovery in Point-of-Sale environment is not shoulder surfing (where Gridsure provides limited resistance), nor hidden cameras (where Gridsure resistance is even less as entire challenge and entry can be recorded for later review), but *compromised terminals*. This is where the Point-of-Sale terminal is sabotaged in order to record PIN and account details. The Gridsure scheme is no more resistant than PIN against sabotaged terminal, as the sabotaged terminal can record entire challenge and response (or indeed submit an engineered grid and then translate the response code from this grid to the response code for the grid received from the central server).

Multiple Entry Attempts

When the correct pattern cannot be determined with certainty (probability 1) from a challenge and response pair, it must be borne in mind that if there were several candidate patterns that could not be distinguished from one another, the user trying to authenticate will get (for example) three attempts to respond correctly. This means that if a challenge/response pair yields three possible patterns, then the attacker will still be able to respond correctly with certainty.

Side Channel Leakage of PIN

From early experimentation during the meeting, considering disjoint patterns or patterns with a change in direction (e.g. the tick), such as the following examples:

12345	12345
12345	1234**5**
12345	**1**2**3**45
12345	1**2**345

I noted that I hesitated during entry of the response code as I negotiated the gap or the change in direction of the sequence. If the time intervals between keypresses were monitored as well as the key presses themselves, this could yield extra "sidechannel" information about the nature of the pattern entered, which could help resolve between different possible combinations. Such timing attacks (and other sidechannels which act as windows on the mental processes of the secret holder) should be considered.

Writing down the Pattern

Some people are unable to remember PINs. It is conjectured that Gridsure patterns are easier to remember than PINs, though no evidence has been offered to this effect (I do note some of Sasse's references are broadly in support of this thesis however). Those who are unable to remember PINs often write them down, with the advice that they disguise their PIN, for instance as the area code of a telephone number. This means that if their wallet is stolen, the criminal will have to search carefully to try and recover the disguised copy of the PIN, and even then may not be successful. To accommodate those who do not wish to use Gridsure (but who are not sufficiently disabled as to actively reject its use e.g. some people use "chip & signature" cards

instead of chip&PIN), how might they record their correct Gridsure pattern in such a way that it can be easily concealed? This issue is unresolved, and as stated in the meeting, one should plan for a scheme to be resilient against disinterested, reticent and even sometimes totally self-destructive behaviour from users.

Screen Scraping, and Retrieving Challenge Grids from PCs

During the meeting Gridsure discussed how the scheme could be used in an online environment (for instance integrated with 3DSecure or VBV). Whilst Gridsure clearly provides no protection against phishing here (as engineered grids can be submitted), or against man-in-the-middle, it does apparently provide protection against keyboard logging viruses/worms/trojans.

Why do viruses not commonly scrape screens to retrieve password information? The answer is because the economics are not yet aligned for it to become necessary. There are easier and better ways at current to attack which do not require this technology. Yet the technology definitely exists and is demonstrably in the hands of the crooks as it is being used to recognise the text from "CAPTCHAs" – the distorted codes or phrases that one often has to re-type when signing up for a new account at a website. These are designed to resist automation by computers, but come under regularly attack, demonstrating that the crooks have the capability to perform sophisticated image processing in order to defeat security mechanisms.

With regards to screen scraping from Flash plugins or from "Silverfish", it may be true that current deployed screen scrapers have an issue with this, but this is not the same as saying that it cannot be done. As soon as the economics yields a reason to want to scrape from Flash, it will become possible. There are no significant technical barriers to attacker code running on a compromised machine reading all the screen information it likes.

Mobile Phone Gridsure

A variety of schemes were discussed where the Gridsure grid is rendered by a mobile phone, including methods where the challenge grid arrives in encrypted form via SMS, or where a challenge grid is constructed from pertinent transaction data such as destination and sort code. All of these schemes rely on the security of the mobile phone as an independent channel, and on the underlying cryptography. None of the detail of this proposed cryptography was presented in the meeting, so one cannot say either way if it would work or not. However it seems that this cryptography (if implemented successfully) would stand alone to make a formidable authentication mechanism, and the Gridsure code itself has rather little to add – only a substitution of PIN entry into the phone with generation of response code from challenge.

Memorability of Multiple Patterns

A study is recommended into the memorability of multiple patterns, although the idea of differently "cueing" the grid with framework patterns in order to evoke memory of a particular associated pattern is indeed clever, and a clear advantage over PIN prompts. This advantage should be stressed more strongly when comparing to PIN

entry. Whether these cue frameworks could be implemented effectively on black and white screens is a matter for further research too.

Summary of Threats and Protection

Threat	**Gridsure**	**PIN**
Shoulder surfing at POS/ATM	Partially resistant. Difficulty of shoulder surfing unknown	Partially resistant. Some studies of shoulder surfing performed.
Camera at POS/ATM	Not resistant	Not resistant
Sabotaged POS/ATM	Not resistant	Not resistant
Online, keyboard logger trojan	Resistant	Not resistant. However resistance achieved easily through PIN entry using drop-down boxes.
Online, Phishing (naïve clicking on emails)	Not resistant (engineered challenge grids)	Not resistant
Online, Phishing (Installed trojan misdirects user to bad site even though correct URL typed)	Not resistant	Not resistant
Shoulder surfing at PC logon	Resistant. Economics not in favour of colleageues learning to shoulder surf grids.	Partially resistant.
Physical keyboard logger attached to keyboard cable	Resistant.	Not resistant.

Conclusions

The Gridsure authentication mechanism remains largely unproven. Studies so far are flawed or taken out of context; my own initial studies indicate further weaknesses.

Many of the attacks discussed in this document rely upon Gridsure becoming a focus of attacks – for the economics to work – as it would indeed become were it used in a Point-of-Sale environment. Gridsure could well be more suitable for deployment in enterprise scenarios. Indeed it does provide protection against certain enterprise threats such as keyboard-cable keyloggers. Only if it achieves a large market share would it become economic to develop the attack methodologies properly.

Mike Bond

11th Feb 2008
(edit 27th March)