Technical Report

UCAM-CL-TR-754
ISSN 1476-2986

Number 754

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Understanding scam victims: seven principles for systems security

Frank Stajano, Paul Wilson

August 2009

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

http://www.cl.cam.ac.uk/

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

http://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

Updated and abridged peer-reviewed version at:
F. Stajano, P. Wilson. "Understanding scam victims: seven principles for system security", Communications of the ACM 54(3), 2011.

Understanding scam victims: seven principles for systems security

Frank Stajano[1] and Paul Wilson[2]

[1]University of Cambridge Computer Laboratory
http://www.cl.cam.ac.uk/users/fms27/

[2]The Real Hustle
http://www.bbc.co.uk/realhustle/meetthehustlers/paulwilson.shtml

Abstract

The success of many attacks on computer systems can be traced back to the security engineers not understanding the psychology of the system users they meant to protect. We examine a variety of scams and "short cons" that were investigated, documented and recreated for the BBC TV programme *The Real Hustle* and we extract from them some general principles about the recurring behavioural patterns of victims that hustlers have learnt to exploit.

We argue that an understanding of these inherent "human factors" vulnerabilities, and the necessity to take them into account during design rather than naïvely shifting the blame onto the "gullible users", is a fundamental paradigm shift for the security engineer which, if adopted, will lead to stronger and more resilient systems security.

1 Introduction and motivation

Experience shows that real-world systems remain vulnerable to attack even though they are protected by a variety of technical security safeguards. Stronger security can only be achieved through an understanding of the failure modes [3]. In many instances, though, the weakest point in the system's defences is the human element and the attack is made possible by the fact that the security engineers only thought about *their* way of protecting the system, not about how real users would react to maliciously crafted stimuli.

We need to understand how users behave and what traits of their behaviour make them vulnerable, and then design systems security around that. How can we gain this knowledge? The message of this paper is that hustlers and con artists know a lot more about the psychology of their victims than security engineers typically do; and therefore that the latter might learn useful lessons from the former.

The bulk of the paper consists of two sections. In section 2 we examine a variety of scams, as researched and recreated for the TV documentary series *The Real Hustle*. In section 3 we distill some general principles of human behaviour that explain why those scams worked and we show how they also apply to broader settings, focusing in particular on attacks on *systems* (of which humans are an element) rather than just on short cons on individuals.

Our thesis is that an awareness of the aspects of human psychology exploited by con artists will not only help members of the public avoid those particular scams but will also help security engineers build more robust systems.

2 Scam scenarios

The following scams, inspired by real-world frauds carried out by con artists, were all demonstrated by Alex Conran, Paul Wilson (coauthor of this paper) and Jess Clement in the British TV documentary series *The Real Hustle*, originally broadcast on BBC Three. Conran and Wilson, who describe themselves in the

Revision 38 of 2009-08-28 19:47:27 +0100 (Fri, 28 Aug 2009).
Earlier drafts presented orally at SHB 2009, Boston, MA, USA (2009-06-11) and at WEIS 2009, London, UK (2009-06-25).

show respectively as a "confidence trickster" and a "scam artist", researched the scams most commonly carried out in Britain and then replicated them on unsuspecting victims, with the cooperation of "sexy swindler" Clement, while filming the action with hidden cameras. As announced at the start of every episode of the TV show, the victims were later debriefed, given their money back and asked for their consent to publish the footage in order to warn other members of the public and prevent them from falling for the same scams.

In the lingo of this peculiar "trade", the target or victim of the scam is known as the **mark**, the perpetrator is known as the **operator** (though we sometimes just say the **hustler**) and any accomplices of the hustlers that pretend to be regular customers are known as **shills**.

Since 2006 the trio have so far produced seven "seasons" of *The Real Hustle*. Each season features 8–12 episodes; each episode lasts just under half an hour and usually demonstrates 4–5 scams[1]. Out of those several hundred documented scams we are now going to highlight and discuss a few ones that we consider particularly significant for the insights they offer into how the con artists exploit and manipulate the psychology of their victims.

2.1 Monte (S1-E1)

This classic scam has many variations on the same basic principle: three cards (S4-E8), three leather discs (S1-E1), three shells and a pea (S2-E4)... The basic game, as described and demonstrated to the mark, involves an operator who manipulates the three items (say they're cards), one of which (say the queen of hearts) wins while the other two lose. The operator shows the player the cards, turns them over face down and moves them around on the table, in full view of the player. The player must follow the moves and, when the operator stops, he must put money on the card he believes to be the winning one. The operator pays out an equal amount if the player guessed correctly or he pockets the player's money otherwise.

Technically, at the core of the scam is a sleight-of-hand trick the operator can do, whereby he appears to place the winning card in a certain position while instead he is sending it elsewhere. One might therefore imagine the basic scam to consist of performing a few "demo runs" where the mark is allowed to guess correctly, then have him bet with real money and at that point send the winning card in an unexpected position.

What this so-called "game" really is, instead, is something quite different, namely a cleverly structured piece of street theatre designed to attract passers-by and hook them into the action. The sleight-of-hand element is actually the least important since it is the way the marks are manipulated, rather than the props, that brings in the money. It's all about the crowd of onlookers and players (all shills) betting in a frenzy and irresistibly sucking the mark into wanting a part of the action. One shill makes a quick and tidy profit by betting and winning, "proving" to the mark that the game is not rigged. Another shill loses money on an "easy" shuffle where the mark clearly sees that he, instead, had guessed correctly, which makes him feel "more clever" than that other player. In S1-E1, one shill (Jess, the cute girl) even gives the mark some money and asks him to bet (and win) on her behalf. Once the mark starts to bet (and of course lose) his own money, the shills find ways to keep him going for more, for example by pretending to cheat the operator to help the mark: one time (in S1-E1), Paul the shill swaps the position of two leather discs while Alex the operator pretends to cough and look the other way; another time (in S4-E8) Alex the shill bends a corner of the supposedly winning card; a third time (in S2-E4), Jess the shill adds a smear of lipstick to the supposedly winning shell. All these tactics have the common objective of making the mark feel that this is his one chance to recover his losses and win everything back with a tidy profit. Of course in all cases the operator knows about the trick and eventually the card with the hidden identification sign, on which the mark happily bets lots of money, turns out to be a losing one. While all this is going on, as a side activity other accomplices may also pickpocket the mark and

[1] A list of episodes of the documentary series, mostly accurate although occasionally incomplete, can be found at `http://en.wikipedia.org/wiki/List_of_The_Real_Hustle_episodes`. In this paper we identify each scam by a code like **S3-E4** (meaning Series 3, episode 4) and its title within the episode. There are no DVD editions of the series at the time of writing but a few highlights from the show can be found on Youtube.

any onlookers while their attention is riveted to the game. When the hustlers feel they have extracted as much money as possible from the mark, they will suddenly close the game by having a shill pretend to have seen the police (S1-E1). Even more subtly, the operator can suddenly pretend to notice the altered card and angrily accuse the mark of cheating, and refuse to continue playing with him (S2-E4).

The Monte is an excellent example that nothing is what it seems, even if the marks think they know what to expect. Many people claim to be able to beat the game, purely because they understand the mechanics of the "hype" move used to switch cards during play. But a little knowledge can be a dangerous thing. The second author of this paper has watched many mobs work the Monte and it's impossible to tell whether an experienced operator made the switch or not. More importantly, even if the cards, discs, or shells were marked in some way, there is absolutely no way for a legitimate player to secure a win: should a mark consistently bet on the correct position, then other players, actually shills, would over-bet him, "forcing" the operator to take the larger bet. This frustrates the mark who will often increase his bet to avoid being topped. Then the mob will move into the "bent-corner" strategy: one of the shills bends the corner of the money card while the operator is apparently distracted. The cards are mixed but now the mark thinks he has an unbeatable advantage. This is a very strong play: marks have been seen to drop thousands of dollars only to find that the bent card is actually a loser. While mixing the cards, it is possible for a skilled operator to switch the cards and to switch the bend from one card to another.

Knowledge of this ruse will protect anyone familiar with it; but the idea that one can beat the game at all reveals a key misunderstanding—it is not a game in the first place! Monte mobs *never* pay out to the marks—they keep all the money moving between the shills and the operator. The marks are only allowed to place a bet if it's already a loser. Having studied Monte all over the world we can say it's nothing short of a polite way to mug people. In New York the second author witnessed a mob separate a woman from her suspicious husband by inviting her to step up as two shills blocked the man, keeping him at the back of the crowd. By the time the husband managed to get his wife's attention, she had lost every penny. In London in 2009, Monte mobs are everywhere, playing with black rubber discs and surrounded by shills who all look strangely related to the operator. It seems so obvious but people continue to fall under the spell of this powerful little scam. Thanks to the success of *The Real Hustle* it's becoming harder for Wilson to observe these games now: whenever the mob spots him, he finds himself being blocked and gently moved to the back.

2.2 Lottery scam (S1-E2)

Jess identifies a young and wealthy mark in a café and descends on him with her charms. Once the mark believes he's making an impression on the pretty girl, Alex turns up, posing as a Bulgarian builder who knows Jess. He has a lottery ticket which has won a prize of £2,800 but he can't cash it because the winner must show some ID and he, as an illegal alien, fears he will be deported if he shows his. So he asks Jess to cash it in for him: in fact, he'll let her keep all the winnings if she just gives him £1,000 cash. Alex leaves temporarily and, while he is away, Jess phones the National Lottery helpline to check whether (or rather to prove to the mark that) it's actually a winning ticket. It turns out that not only it is but, thanks to the "bonus number", it has actually won not just a couple of thousand but over a *hundred thousand* pounds! And Alex doesn't know! Poor Jess doesn't have the thousand pounds cash that Alex wants in exchange for the winning ticket, but perhaps her new friend the mark is interested in a piece of the action? They'd pay Alex the thousand pounds he asked for and pocket the huge difference! Yes, the mark is quite willing to side with Jess in defrauding Alex. Jess and the mark each pay Alex one half of what he asked for and he gives them the winning ticket. Jess is happy for the mark to cash the ticket and give her her share of the money later because it's actually a worthless fake that Paul made earlier on his inkjet printer after the winning numbers had been announced on TV.

When filming items for *The Real Hustle*, time must be compressed; but in real life this is a type of scam that is usually played over several days or even weeks, with the hustlers adding layers of proof at each meeting to make sure the mark is firmly hooked and ready to pop before the money changes hands.

2.3 Ring reward rip-off (S1-E4)

Jess buys a cheap ring from a market stall for £5. She then goes to a pub and turns on the charm to befriend the barman (the mark). Pretty soon she's on first name terms with him. She makes it obvious she's very rich: showing off to her friend (a shill), she makes sure the mark overhears that she just received this amazing £3,500 diamond ring for her birthday. Then she leaves.

Paul and Alex arrive at the pub, posing as two regular blokes having a pint. Then Jess phones the pub, very worried, calling her friend the barman by name, saying she lost that very precious ring. Could he check if it's there somewhere? The mark checks: luckily, a customer (Paul) has found the ring! However, instead of handing it over, Paul asks what's in it for him: he wants a reward. The barman gets back to the phone and Jess, very relieved to hear that the ring is there, says she'll give £200 to the person who found it. But the barman goes back to Paul and says the reward is only £20. That's when the hustlers know they've got him: he's trying to make some profit for himself. Paul haggles a bit and eventually returns the ring to the barman for £50. The mark is all too happy to give Paul that money from the till (borrowing money that isn't even his!), expecting to get much more from Jess. But Jess, of course, never calls back.

At the end of the show there is also a brief interview with a convicted criminal, shown only as a silhouette to make him unrecognizable, who describes this hustle as one that really works: he once made a £2,000 profit with it.

2.4 Van dragging (S2-E1)

The hustlers post a sign on the door of a warehouse saying that the door is broken and that delivery people should call the specified telephone number (actually Jess's mobile) instead of attempting to ring the door's buzzer. A real delivery van comes along; the delivery man reads the sign and phones Jess, who is hiding nearby. She sends in Alex and Paul, with a trolley and suitably dressed as warehouse workmen, to collect the delivery: they act annoyed and claim that they're waiting for a locksmith to fix the door. The delivery man hands over the load, which happens to be £10,000 worth of widescreen TVs. As soon as the delivery driver is gone, Jess comes along with the hustlers' van; they load the boxes in their van and disappear.

2.5 Home alone (S2-E1)

Jess somehow gains entry into a house she knows will be empty that afternoon. In the driveway she parks a car for which she placed a "want to sell" ad, at a bargain price, in the classified section of the local paper. A prospective buyer arrives at the house and she lets him in, leaving her mobile phone off the hook so her accomplices know what's going on. She brings the mark back in the house and collects the money. Then Paul and Alex storm into the house, pretending to be policemen who need to arrest well-known fraudster Jess for stealing the car. Paul, as a fake policeman, intimidates the buyer (mark) into staying there in the kitchen without moving while he checks his story, alleging that he might be guilty too: it's illegal to buy anything you know or suspect to be stolen! While the scared mark stays put for fear of being arrested, the three hustlers drive off with their car and his money.

2.5.1 Jewellery shop scam (S1-E1)

The core idea of *home alone* is largely isomorphic to that of the *jewellery shop scam* in which Jess attempts to buy an expensive necklace but is then "arrested" by Alex and Paul who expose her as a well-known fraudster, notorious for paying with counterfeit cash. The "cops" take the "fraudster" to the police station and collect in an evidence bag the "counterfeit" (actually genuine) cash and, crucially, the necklace, which of course "will be returned". The jeweller is extremely grateful that the cops saved her from the evil fraudster. As Jess is taken away in handcuffs, the upset jeweller spits out a venomous "Bitch! You could have cost me my job, you know that?".

2.6 Valet steal (S2-E3)

Alex sneaks into a car park, dressed up in a fluorescent jacket and posing as a car park attendant, as soon as the real attendant leaves for a temporary break. A mark arrives with a luxury car; Alex collects the keys and parks it. As soon as the mark is out of sight, Alex drives away with the car. That would already be pretty good value for just a few minutes' "work", but that's not all—the car has a sat-nav in the glove box, and the sat-nav has a "home address" pre-programmed into it. There's even a copy of the home keys. All Alex has to do is drive to the mark's home (in the mark's car, knowing he's not in) and empty it.

2.7 Gadget scam (S4-E3)

The hustlers sell a homemade electronic device supposed to recharge Oyster cards[2] to a value of £50. Actually, the plastic box contains little more than a battery—all that's needed to turn on a couple of LEDs when the power switch is flicked. Paul convinces the marks to buy the device for £200 by pretending to top up their Oyster card to £50 with it and letting them try it in a nearby store. In fact he just uses sleight of hand to switch the mark's card with one that already had £50 on it.

Fake devices of this kind have been around for a long time. Count Lustig, one of history's most famous con artists[3], made a fortune selling a "money making machine" to his clients. The machine could manufacture $100 bills but took almost 24 hours to do so. For this reason the Count wanted to sell the device and was offered huge sums by greedy marks. The machine would successfully print one or two $100 dollar bills but would then do nothing. By this time, Victor Lustig had a two day head start.

2.8 Counterfeit pen con (S4-E4)

Alex visits a pub posing as a police officer. His story is that there are many people in the area who are passing off counterfeit money, so the local police want to protect the local shops by supplying them with a special detector pen. He demonstrates to the barman (his mark) how the detector pen writes in green on the special paper of a genuine note but in grey on a fake note or on standard paper. He gives the mark a pen, advising him to use it before accepting any notes into the till.

After this setup phase, Jess goes in and, with her usual feminine charm, exchanges three (counterfeit) £20 notes for six £10 notes. The barman carefully checks her three twenties with the pen and finds them ok, but doesn't realize that Alex actually gave him an ordinary green marker that writes in green ink on *any* piece of paper, whether genuine or counterfeit.

This ingenious scam was carried out all over Europe and is of special interest to anyone working in security. The counterfeit detector pen became an established and, for a while, successful way to test currency. The businesses that used the pen came to rely on it and to place a great deal of trust in it. While counterfeiters struggled to find ways to beat the pen, this scam allowed enterprising hustlers to distribute phony cash with greater ease than before. The security system was compromised by being completely replaced. The thinking is brilliant: if the counterfeit note can't defeat the pen, let's just replace the pen. The sense of protection provided by the genuine pen is transferred onto the fake pen and the rest is almost too easy.

2.9 Cash machine con (S4-E5)

The hustlers build a rudimentary stand-alone ATM, roughly the size of an old-style public telephone box, and deploy it on a busy street. The box has the front of a real ATM but its insides are replaced by... Jess, who manually operates a laptop PC that drives the display of the fake cash machine. When a mark introduces his card, Jess grabs it and swipes it on her PC, acquiring the magstripe data. Between that and the PIN, which the mark enters on the ATM's keypad, the hustlers have all they need to produce a cloned

[2] The Oyster card is the prepaid contactless smart card used in the London Underground.

[3] In 1925, Lustig famously managed to "sell" the Eiffel tower to a scrap metal dealer.

card[4] and raid the victim's account. Meanwhile, the display says that there is a problem and this ATM cannot dispense cash at the moment. The card is returned to the mark, who is none the wiser. In just a couple of hours, the hustlers manage to bag the details of 25 cards.

Real-world versions of such machines are far simpler but, for the TV show, the con was deliberately taken to extremes, partly also for entertainment value. Interestingly, as a testimony to people's candid naïveté, while the box was being built on the street, with the door open and Jess being handed a coffee by one of the crew, a queue of people had formed to use the machine. Despite all the equipment that was yet to be hidden for the shoot and the box that was yet to be marked up, people were blindly trying to use the fake machine! Once the rig was working, people used the machine and, when it failed, they simply went to the next ATM down the street. The most disturbing aspect of the show as eventually broadcast was the "expert advice" given to the public: without the approval of the writers, the producers approached someone for the interview who said that people should always call their bank after using a fake or adapted ATM. Since the whole point of this scam is to trap card details and PIN numbers *without* alerting the victim, this advice was plainly useless.

2.10 Recruitment scam (S4-E5)

The hustlers set up a fake recruitment agency and, as part of the sign-on procedure, they collect all of the applicants' personal details, including mother's maiden name, date of birth, bank account details, passport number, even PIN (by asking them to protect their data with a 4-digit code—many people memorize only one PIN and use it for everything). With this loot, the hustlers are free to engage in identity theft on everyone who came for interview.

This was set up to mimic the many online sites that fraudulently collect user data. On the day this scam was shot, one of the marks flatly refused to fill in anything that could be used to compromise her: she worked with the Met Police to help victims of fraud. But the producer did not include her in the final edit, ignoring the author's protests. Despite many public campaigns to teach people about protecting their personal data, it is surprisingly easy to obtain, from most people, anything one would need to steal their identity. It's like shooting fish in a barrel.

2.11 Shop phone call scam (S4-E7)

Jess targets a small shop. With a pretext phone call she finds out when the manager is going to be away, then she goes into the shop posing as a delivery person with a parcel for him. She asks the shop assistant to call the boss for her and then speaks with him directly to see if he wants to take the parcel (yes, he does) so she agrees to leave it there. Apparently he also agrees to have his assistant pay the £60 cash-on-delivery fee, taking the money from the till. But this second part was just staged by Jess: the boss had hung up after saying he wanted the parcel, and the bit about the £60 charge was merely Jess talking into a disconnected handset. So the shop assistant pays Jess £60 believing that this had been authorized by the boss.

This exact scam was pulled on a friend's butcher shop. A more modern variant uses a VOIP service that lets you send text messages and specifying (i.e. faking) the caller's number. The text arrives with that number and is interpreted by the phone as an existing number in the user's address book. So, when Mary receives a text from her husband Harry telling her that he's going into a meeting with his boss and that he forgot to tell her that she should give the keys to the mechanic when he comes to pick up the car, Mary sees the message as coming from `HARRY` and trusts it completely.

[4] Only the magstripe is cloned, not the chip found on newer cards; but a cloned magstripe card can still be profitably used in foreign countries that don't require Chip and PIN, or in machines that fall back to magstripe when Chip and PIN appears not to work [4].

2.12 Exchange rate rip-off (S4-E9)

In Ibiza (Spain), a popular holiday destination for British tourists, Alex pretends to be selling maps to holidaymakers. Once he reels in two marks, Alex asks them if they're British because he has some UK currency he wants to get rid of: he's willing to sell them £500 for €200—an amazingly good deal since, at the time the show was filmed, £500 would have been worth about €700, not €200. Paul approaches the trio pretending to be another tourist also interested in the deal. Paul really wants to go for it but only has €100, so he asks the marks if they want to join in and split. They do.

Alex, however, pretends he doesn't want to be seen handling that much money in the street, so they perform the exchange inside Paul's straw hat. But when Paul and the marks split the British pounds, they find that, except for the first and last note, they're all very obviously fakes. How is that possible? They did have a quick look at them while they were being exchanged and they looked genuine... All three of them feel ripped off and devastated but Paul, who is also pretending to be a victim, convinces them that going to the police would be a bad idea in this case because there is probably an organized crime gang behind this hustle and they risk retaliation from the gang if Alex the scam artist ends up in jail.

As with the *Monte* (section 2.1), although the cleverness of the scam is in the setup and in the way the hustlers manipulate the psychology of the victims, at the core of the scam there is a sleight-of-hand trick: at the crucial moment, Paul switches the wad of genuine notes supplied by Alex with the bundle of fakes he already had in his hat all along.

This scam was observed in Madrid, where it was being pulled on tourists by crooked lottery vendors. In a previous working version of the reconstruction for the TV show, Alex handed Paul the cash, which Paul counted for the benefit of the marks before switching it with a spot of sleight of hand. But the camera simply couldn't see the switch and it was very hard to follow. So Paul came up with the hat switch which turned out to be easier to follow, easier to do and much more convincing.

The final part of this scam, cooling out the mark, is as important as the switch—see the classic 1952 paper by Goffman [9]. By telling the marks about the dangers of reporting to the police, the shill manipulates them into walking away. To make sure this works, the hustlers try not to take too much—not enough to force the marks into action. A similar tactic is often used when stealing money from credit cards: a smart operation hits thousands of cards for a few dollars[5] instead of one card for thousands of dollars.

3 Lessons and principles learnt

Teaching a useful lesson to viewers is the explicit objective of the TV show, as stated in the opening title: by exposing how the scams work, it is hoped that viewers can avoid being ripped off by the same scams.

Can we do more? In what follows we extrapolate some general lessons from the instructive examples we just described. Each of the following sections discusses a typical human behavioural pattern. The associated "principle" summarizes how con artists exploit that pattern as a vulnerability that enables specific classes of attacks.

Real-world hustlers have proved to be excellent psychologists: they identified those patterns and those principles before anyone else. We argue that now is the time for the good guys to catch up with them in understanding the victims. Those behavioural patterns are not merely opportunities for individual short cons but inherent security weaknesses of "the human element" present in any complex system. A thorough understanding of these issues is therefore essential for the security engineer.

3.1 The Distraction principle

While you are distracted by what retains your interest, hustlers can do anything to you and you won't notice.

[5] As the amount stolen from each card gets smaller and smaller, it first goes below the threshold at which the mark takes action; but eventually it may even go below the threshold at which the mark *notices*.

The young lady who falls prey to the *recruitment scam* (section 2.10) is so engrossed in her task of accurately compiling her personal details form in order to maximize her chances of finding a job that she totally fails even to suspect that the whole agency might be fake.

Distraction is at the heart of innumerable fraud scenarios; it is also a fundamental ingredient of most magic performances[6], as interestingly discussed by Macknik et al. [13] who argue that studying magicians may help neuroscientists understand more about how to manipulate attention and awareness[7].

There is a theory amongst conjurors that the idea of being "one ahead" is the cornerstone of magic and that everything else is merely a variation of it. When an illusionist is using identical twins, he is one ahead; when he employs a secret device, he is one ahead; if he palms something or executes sleight of hand—in all these cases he is one (or more) steps ahead of the audience in some way. Cons and scams work similarly: much like conjuring tricks, the operator must somehow be ahead of his mark; but, in all such performances, including conjuring and confidence games, the Distraction principle is what ensures the success of the one-ahead strategy. It is referred to in the conjuring fraternity as *misdirection*; but this is, in fact, a misnomer: a better term would be **direction**. The audience will always follow what is most interesting and what seems to be the most important action. If they no longer focus their attention on just that, the illusion is lost. This is exactly how the Distraction principle works in all confidence games: the mark is directed away from the scam and towards that which they desire.

Distraction is used in all cases that involve sleight of hand—including the special "throw" found in all variants of the *Monte* (section 2.1), the hat trick in the *exchange rate rip-off* (section 2.12) and so forth. At a higher level, the Monte also reuses this same principle when the accomplices of the operator pick the pockets of the marks whose attention is riveted to the game. Indeed, most pickpocketing scenarios rely on some form of distraction: from the relatively straightforward, such as "accidentally" bumping into the mark so as to disguise the light touch of the hustler's hand in their pocket (S2-E6, untitled), to the purposefully elaborate such as the *mustard dip* (S1-E1) in which the hustlers first covertly squirt some mustard on the mark's coat to have an excuse to "clean him out" shortly afterwards. Perhaps the simplest example of a distraction steal is the *window tap* (S1-E2): one hustler in the street taps on a café window, signalling to some mark inside that she would like to know the time. As the mark shows her watch, her bag is taken from under her chair by a second hustler inside the café.

In the *bogus agency scam* (S1-E2) the hustlers pose as talent scouts and extract money from marks who hope to become rock stars: the marks are too excited at the thought of their first recording contract to worry about the legitimacy of the agency that is offering it to them. In the similar *rock band steal* (S4-E7), the hustlers invite a young rock band to come and perform in front of a VIP audience; they then steal all of the band's expensive musical instruments while the young hopefuls are too excited about their upcoming performance to worry about what's happening. (Many such scams should also be classed under the Need and Greed principle of section 3.6.)

The very presence of a "sexy swindler" in the team of hustlers is a tribute to the Distraction principle: although we tend to protect ourselves by initially regarding strangers with some suspicion, the natural defenses of the male mark are softened, if not defeated, by the charm of the attractive female who smiles at him. The implicit hope, skillfully fuelled by Jess, that something exciting might happen later with the pretty blonde is enough to throw caution to the wind. The mark focuses on what he really wants, not on generic and boring security advice he got in the past. This too is related to the cited Need and Greed principle (q.v.), since sex is such a fundamental human drive.

In the wider context of security engineering, the well-known tension between security and usability could be usefully revisited in light of the Distraction principle. It's not that the users are too lazy to follow the prescribed practice on how to operate the security mechanisms, but rather that their interest is principally focused on the task, much more important to them, of accessing the resource that the security mechanisms protect. The users just see what they're interested in (whether they can conveniently access the resource) and are totally blind to the fact that those annoying security mechanisms were put there

[6] Unsurprising if we accept to see magic performances are a kind of "benign fraud" for entertainment purposes.

[7] An interesting parallel with our suggestion of studying con artists to understand more about human-related system vulnerabilities.

to protect them from obscure hypothetical attacks. Smart crooks will exploit this mismatch to their advantage, knowing that a lock that is inconvenient to use is one that users often leave open.

For example, the system administrators of the university department of the first author recently imposed a draconian policy of disabling remote access for any users whose `ssh` configuration specified `from=⋆` as opposed to something more specific such as `from=myhomemachine.myprovider.com`. Anecdotal evidence, from discussions with students and colleagues, showed widespread discontent at this annoying restriction, especially from users who had been locked out of remote access by, e.g., their provider unexpectedly changing their dynamically assigned address or by their not being able to access their files from a location they hadn't previously thought of listing in their configuration file. Countermeasures from users included specifying very generic access patterns such as `from=⋆.com,⋆.net,⋆.edu,⋆.uk` or even `from=⋆.⋆`, which totally defeated the system administrators' original purpose and turned the issue from a fight between the lab members and the outside attackers to a fight between the lab members and the system administrators who are in theory paid to protect them.

Another example of the Distraction principle in action in the context of information security is found in that most widespread of computer frauds, the so-called 419 or Nigerian scam, of which anyone with an email address typically receives several instances per week. There are many variations but the vanilla version is that the hustler, posing as a Nigerian government officer with access to tens of millions of dollars of dodgy money, wants the mark to help him transfer the money out of the country in exchange for a slice of it, and of course everything must be kept very secret. Once the mark accepts the deal, the hustler demands some advance money to cover expenses. New unexpected expenses come up again and again, always with the promise that the money is just about to be transferred. This scam demonstrates several of our principles, including Need and Greed (section 3.6) and particularly Dishonesty (section 3.4), but also relies on Distraction insofar as the mark is kept focused solely on the huge amount of money he is supposed to receive. The convincers used to extract the necessary fees also keep the mark on track and believing that the transaction is completely genuine.

For those who might take a patronizing attitude towards the gullibility of those unsophisticated 419 victims, Abagnale[8] shows how the Distraction principle works equally well on CTOs, CIOs and other sophisticated three-letter officers. He tells of his 1999 visit to the offices of a company that was frantically preparing for Y2K: everywhere, programmers were busy fixing code to avert the millennium bug. He asked the executives how they found these programmers [2].

> "Oh, these guys from India," they said. "They're really sharp. And they're cheap." [...] Their thinking was, these guys know computers and they're inexpensive, as were a lot of other off-shore firms from India, Russia, and Taiwan that were fixing Y2K problems. But [...] I knew that any dishonest programmer could easily implant a so-called "backdoor" [...]

When people are focused on what they want to do (which is most of the time), the task they care about distracts them from the task of protecting themselves. Security engineers who don't understand this principle have already lost their battle.

3.2 The Social Compliance principle

Society trains people not to question authority. Hustlers exploit this "suspension of suspiciousness" to make you do what they want.

The barman in the *counterfeit pen con* (section 2.8) happily accepts the fake pen (to all intents and purposes a Trojan horse) that is offered by Alex posing as a police officer. The car buyer in *home alone* (section 2.5) quietly submits to the menacing orders from fake police officer Paul for fear of being mistaken for a willing accomplice to the alleged crime. The jeweller in the *jewellery shop scam* (section 2.5.1) gratefully hands over both necklace and cash when fake police officer Alex says they're needed as

[8] Frank Abagnale is the former con artist and convicted fraudster, now security consultant, played by Leonardo Di Caprio in the Hollywood blockbuster *Catch me if you can*.

evidence, and she naturally believes him when he says they'll be returned later. And other episodes in the series show more scams based on impersonating police officers than we have space to list.

The second author recalls his impression of the victim's "deer in headlights" reaction in *home alone*: while observing this particular mark, he quickly noticed that the subject was extremely easy to manipulate and very open to suggestion. The sudden change in circumstances, his respect for authority and, most importantly, his desire to "sort things out" and get away gave the author a very powerful influence over him. Despite his protests and complaints, it was clear he could be made to do *anything* in order to get out of this situation. In the end Wilson ordered him to stay in his seat until further notice: "if not, I'm going to arrest you!". Wilson then walked outside, jumped into the car and drove off. The mark sat in the chair for over 20 minutes.

But the social compliance principle has of course much wider applicability than just the impersonation of police officers: in the *valet steal* (section 2.6), Alex only needs a fluorescent jacket and a convincing attitude to become a car park attendant and drive away with the mark's expensive car. Similar situations include the *fake waiter scam* (S2-E8), where Alex pretended to take food orders from customers and walked away with the credit cards of his marks; and the *bogus workmen scam* (S2-E8), where the hustlers entered a house by posing as workmen from the water board and then Paul robbed the place while Alex distracted the houseowner.

More subtly, in the *shop phone call scam* (section 2.11), Jess exploits the hierarchical relationship between the shop assistant and his boss: she makes the boss say over the phone that he wants the parcel and thus she convinces the shop assistant to hand over money from the till by pretending that the boss said that as well.

Mitnick[9] wrote a fascinating book [16] on social engineering, with special emphasis on the practice of doing so over the telephone. In a particularly cheeky anecdote he impersonates a law enforcement officer to nothing less than a law enforcement agengy! He describes how, piece by piece, he builds up credibility and therefore trust merely by exhibiting knowledge of the lingo, of the procedures and of the right phone numbers. He is successful in having the local state police clerk consult the central National Crime Information Center database for him and deliver confidential information about any offenses on file for a named target. His insightful observation is that the police and the military, far from being a riskier and harder target for this sort of scam, are instead inherently more vulnerable to it:

> People in law enforcement, like people in the military, have ingrained in them from the first day in the academy a respect for rank. As long as the social engineer is posing as a sergeant or lieutenant—a higher rank than the person he's talking to—the victim will be governed by that well-learned lesson that says you don't question people who are in a position of authority over you. Rank, in other words, has its privileges, in particular the privilege of not being challenged by people of lower rank.

It has been observed that impersonating policemen, customs officers and other figures of authority is a particularly naughty crime against society because society (or perhaps government) *needs* people to submit to the authority of policemen. The TV show authors themselves, in the editorial comments preceding the *customs seize scam* (S1-E3), note that, for this reason, the penalty against this crime is particularly high.

The crucial psychological insight here is that it is very hard for a stranger to force the mark to behave in the desired way (why should the mark do what a random stranger asks him to?) but it is much easier for a hustler to do so by letting the mark behave according to an already-established pattern, namely that of obeying a recognized authority[10].

The extent to which a person is willing to put aside any other considerations in order to comply with requests from an authority was eloquently demonstrated by the famous Milgram [15] experiment[11].

[9] Kevin Mitnick was at one point the most wanted computer criminal in the United States. After a conviction and a prison stint he now works as a security consultant and author.

[10] Regardless of the fact that the recognition was incorrect.

[11] Experimental subjects were ordered to administer electric shocks of increasing strength to other subjects (actually accom-

In computing, the most egregious example of the Social Compliance principle at work is probably phishing—the practice of setting up a web site that replicates the appearance of a bank's site and directing customers to it in order to steal their online banking credentials. Your bank tells you to do something (under penalty of revoking your access) and you do it. It's hard to fault non-technical users on this one, especially in the minority of cases where the phishing email actually bears the name of *their* bank. Note also the conflicting interests at stake—for example between a bank's security department instructing its customers never to follow links in email messages and the marketing department of the same bank sending them clickable email advertisements for new financial products—and the double jeopardy in which they place the user.

The lesson for the security architect is that training users always to obey commands from certain people (as "system administrators" of all flavours, including government authorities, like to be able to do), can be a double-edged sword. Although people are generally pretty good at recognizing people they already know (by face, by voice, by shared memories. . .), they are not very good at all at authenticating strangers[12], whether over a network, over the phone or even in person. And incentives and liabilities must be coherently aligned with the overall system goals. If users are expected to perform extra checks rather than subserviently submitting to orders, then social protocols must change to make this acceptable; if, on the contrary, users are expected to obey authority unquestioningly, those who exercise the authority must offer safeguards to relieve users of liability and compensate them if they fall prey to attacks that exploit the Social Compliance principle. The fight against phishing and all other forms of social engineering can never be won unless this principle is understood and taken on board.

3.3 The Herd principle

Even suspicious marks will let their guard down when everyone next to them appears to share the same risks. Safety in numbers? Not if they're all conspiring against you.

A good example of this principle is seen in the first scam we described, the *Monte* (section 2.1), where most of the participants pretend to be random players or onlookers but are in fact shills. The whole game is set up to give the mark confidence and make him think: "Yes, the game looks dodgy, but other people *are* winning money" as well as: "Yes, the game looks hard, but *I did* guess where the winning disc was, even if the guy who played actually lost". As we said, in the Monte the shills are at least as important as the sleight-of-hand trick.

Any other con that uses shills is also a valid application of the Herd principle. The *exchange rate rip-off* (section 2.12), for example, has Paul "losing" as much money as the marks, which crucially makes them feel less bad about it ("it wasn't our fault for not spotting the scam, really: look, even this other poor guy fell for it, there was nothing we could have done"). And, during the initial phase, even though they might not have accepted the slightly dodgy deal in the first place, the fact that Paul was so eager to go for it made them feel better about accepting it themselves. Other cons that illustrate the same point include the *hardware hustle* (S2-E7) in which Paul and Alex run a computer store and persuade members of the public to leave their laptop with them for a cheap, or even free, memory upgrade. At a crucial moment, Jess walks in, pretending to be another customer, showing obvious satisfaction at being able to pick up her upgraded computer: she is the **convincer** who subliminally persuades the mark that everything is OK. There is also the *mock auction* (S2-E5) where the hustlers rent a hall for the day and offer incredible bargains on goods whose retail boxes are slightly damaged. The pace of the auction is very rapid and all the good deals go to the hustlers' numerous shills, who have been explicitly instructed to bid for anything on offer. The few marks are implicitly pressured into buying something too, as quickly as possible so as not to lose out to the shills (cfr. also the Time principle of section 3.7), but they feel confident and safe because so many other people around them are doing the same and look happy with the bargains they got.

plices who did not in fact receive the shocks) when those made mistakes. Subjects complied to a frightening extent, even continuing to administer shocks up to the maximum of 450 V after the pretend victims screamed and fainted.

[12] In this context, "authenticating a stranger" can be taken as meaning "establishing whether a stranger belongs or not to a designated class" such as policeman, water company employee, clerk from XYZ Bank and so forth.

Moving from street scams to information security, this last scenario leads us directly to online auctions, where a variety of frauds are possible if bidders are in cahoots with the auctioneer [20]. The first and most successful online auction site, eBay, pioneered a reputation system in which bidders and auctioneers rate each other at the conclusion of each sale and the history of feedback messages of each participant is available to others who might use it to decide whether to deal with that person or not. Clearly, such a system is vulnerable to fraudsters boosting their reputation by clocking up positive feedback through transactions with shills[13].

In the context of online communities and social networks, multiple aliases created by the same person in order to give the impression that many other people share a given opinion are indicated as **sockpuppets**. In the context of political elections, the practice of introducing fake identities to simulate grassroots support for a candidate, party or idea is known as **astroturfing**[14]. In the context of reputation systems in peer-to-peer networks, as opposed to reputation systems in human communities, multiple entities controlled by the same attacker are known as **Sybils**[15] [7]. The variety of terms that have been created for different contexts testifies to the wide applicability of the Herd principle to all sorts of multi-user systems.

3.4 The Dishonesty principle

Anything illegal you do will be used against you by the fraudster, making it harder for you to seek help once you realize you've been had.

A prime example of this principle is the *gadget scam* (section 2.7). The marks have bought a machine that is supposed to recharge their Oyster card. If it worked, it would clearly be illegal—a fraud against the subway company. Therefore, once they discover it doesn't work, they can't go to the police (or Trading Standards, or whoever) and complain about the seller, because they'd be asked questions about what they intended to do with the device.

An entertaining example that uses something shameful rather than illegal is described in the movie *Lock, Stock and Two Smoking Barrels*: the character called Tom suggests selling anal vibrators via classified ads in the back of gay magazines. Customers are supposed to mail their cheques to a company with an innocent name, "Bobbie's bits". The hustlers cash the cheque and send back a refund, saying they couldn't get hold of enough stock from America. However, the refund cheque comes from a company named "Arse Tickler's Faggots Fan Club", ensuring that few if any marks will go to the embarrassment of cashing it. Interestingly, in this case nothing of what the hustlers are doing is actually fraudulent from a legal standpoint!

In the *Monte* (section 2.1), the shills encourage the mark to cheat the operator and even help him do it. Then, having fleeced the mark, the operator pretends to notice the mark's attempt at cheating and uses it as a reason for closing the game without giving him a chance to argue.

The Dishonesty principle also applies to all cases of hustlers selling stolen (or purported-to-be-stolen) goods. The message is "It's illegal, that's why you're getting such a good deal", which discourages the marks from complaining to the authorities once they discover they've been had. In the *black money blag* (S1-E4), the hustlers spray-paint some pieces of paper and sell them off at a car boot sale as "cancelled banknotes"[16], together with a miraculous gadget and a liquid that is supposed to wash off the black ink. At the end of the show, a real-world victim is interviewed who admits (anonymously) to losing £20,000 to this scam; police told him that it happens all the time but that few victims report it (the latter being evidence of the Dishonesty principle at work—victims would be exposing their own attempt at fraud if they reported the scam).

[13] Where the countermeasure of the online auction house is to validate new membership applications by requesting a credit card number, the fraudster only has to buy a few hundred numbers from the appropriate gang of hackers, at a modest expense.

[14] The etymology is a pun on "grassroot": "astroturf" is a brand of artificial grass.

[15] Here the etymology goes back not to the Greek prophetess but to (the pseudonym of) a psychiatric patient suffering from multiple personality disorder.

[16] The story goes that the Royal Mint occasionally prints too much money and then has to burn the excess. To prevent theft on the way from the mint to the incinerator, the money is "cancelled" by covering it in insoluble black ink. But the hustler claims to have a "solution" (pun intended, in the hustler's own sales pitch).

Cons such as the *lottery scam* (section 2.2) can only work thanks to the mark's dishonesty: if he doesn't have a little larceny, or the requisite ego to feel superior to Alex's immigrant character, then it is very difficult for the hustlers to ignite the mark's greed. There's a certain look every mark gets when they really bite into the hook. They realize they apparently stand to make a lot of money, or get an amazing bargain, and they immediately try to hide their excitement. Some hide their feelings better than others but that moment when the scam "gets them" is always the same. The second author of this paper studied con games since he was a kid, but found that executing them requires a much deeper understanding. The lesson from taking down this mark was that people accept their own ideas and thoughts more readily than ideas presented to them by others. Through scams like this one, we understand how hustlers can lead a mark to a conclusion. This is why many con artists patiently groom their marks before slowly building a con around them.

In information security, the Dishonesty principle is a core component of the 419 or Nigerian fraud we mentioned in section 3.1: once the mark realizes it was a scam, going to the police is not an attractive option because what the mark intended to do as part of this deal (essentially money laundering) was in itself illegal and punishable. Several victims have gone bankrupt and some have even committed suicide, seeing no way out of that tunnel.

The security engineer needs to be aware of the Dishonesty principle. A number of attacks on the system will go unreported because the victims don't want to confess to their "evil" part in the process. When a corporate user falls prey to a Trojan horse program that purported to offer, say, free access to porn, he will have strong incentives *not* to cooperate with the forensic investigations of his system administrators to avoid the associated stigma, even if the incident affected the security of the whole corporate network. Executives for whom righteousness is not as important as the security of their enterprise might consider reflecting such priorities in the corporate security policy—e.g. guaranteeing discretion and immunity from "internal prosecution" for victims who cooperate with the forensic investigation.

3.5 The Deception principle

Things and people are not what they seem. Hustlers know how to manipulate you to make you believe that they are.

The device in the *cash machine con* (section 2.9) attracts marks who are not in any way suspicious of inserting their card, and typing their PIN, into the fake ATM. When Alex wears a fluorescent jacket in the *valet steal* (section 2.6), he is by default assumed to be the car park attendant. And, whenever Jess approaches a mark with her gorgeous cleavage and flirty smile, as in the *lottery scam* (section 2.2), in the *ring reward rip-off* (section 2.3) and on countless other occasions, she is immediately seen as a lovely girl rather than a hustler. Indeed, practically *all* scams exploit this principle, insofar as all scams are forms of deception.

A variation of the *valet steal* (section 2.6) that the trio performed in Las Vegas (*valet distraction*, S5-E2) demonstrates how a hustler who really understands his victim can reassure him and mount a counterattack even when the mark is suspicious about the very scam that is about to be pulled off. Paul's mark, in a luxurious Cadillac Escalade, refused to let him park his car because he'd been ripped off before. Paul complimented him on his car and told him to park it up front so he could keep an eye on it for him. This secured his trust while flattering his ego—Las Vegas valets only park the very best cars in front of the house. As soon as he was parked, Paul asked him to leave the keys. He didn't think twice, handed in his keys and walked smiling into the restaurant. Paul then drove the car straight out—easy to do since it was parked "up front".

This illustrates something important. Many people feel that they are wise to certain scams or take steps to protect their property; but, often, these steps don't go far enough. A con artist can easily answer people's concerns or provide all sorts of proof to put minds at ease. In order to protect oneself, it's essential to remove all possibility of compromise. There's no point parking your own car if you then give the valet your keys. Despite this, the mark felt more secure when, in actual fact, he had made the hustler's job easier.

The first author recently witnessed a similar kind of double-cross in a hilariously ingenious 419 email that purported to originate from a fraud-fighting force in Nigeria: they said they had apprehended a number of 419 fraudsters and wanted to return a share of the stolen money to each of the people listed on the fraudsters' computers. They therefore asked for the recipients' details so that they could send them a $4.5 million flat-fee compensation[17]. Undoubtedly, even some true 419 victims who should know better will fall prey to this scam!

Scams such as *van dragging* (section 2.4) take advantage of people's expectations. So long as the hustlers fit the scenario and act within the framework of a given situation, the mark never wakes up and simply goes through the normal motions. The same happens with a spoofed web site: if the victim is familiar with the original site, they will continue without stopping to question the situation unless something unexpected occurs. Indeed, in the computing domain, the most widespread application of the Deception principle is probably phishing, already mentioned in section 3.2 under the Social Compliance principle.

Much of systems security boils down to "allowing certain principals to perform certain actions on the system while disallowing anyone else from doing them"; as such, it relies implicitly on some form of *authentication*—recognizing which principals should be authorized and which ones shouldn't. The lesson for the security engineer is that the security of the whole system often relies on *the users* also performing some authentication, and that they may be deceived too, in ways that are qualitatively different from those in which computer systems can be deceived. In online banking, for example, the role of verifier is not just for the web site (which clearly must authenticate its customers): to some extent, the customers themselves should also authenticate the web site before entering their credentials, otherwise they might be phished. However it is not enough just to make it "technically possible"[18]: it must also be humanly doable by non-techies. How many banking customers check (or even understand the meaning of) the `https` padlock?[19]

The message for the security engineer can be summarized in the following bullet points:

- Identify the cases where the security of your system depends on an authentication task (of known people, of unknown people or of "objects", including cash machines and web sites) performed by humans.

- Understand and acknowledge that users are very good at recognizing known people but easily deceived when asked to "authenticate", in the widest sense of the word, "objects" or unknown people.

- Wherever possible, design the system to be robust in the face of incorrect "authentication" by users.

- When it is necessary to rely on authentication by users, don't make it merely technically possible for a committed geek but rather design the mechanism in a way that actually works for an ordinary human verifier.

Norman [17] introduced the concept of a *forcing function*: a design feature that prevents any user behaviour other than the correct one—for example a power button that, when pushed to the "on" position, mechanically prevents the insertion of a peripheral that should only be plugged in when the power is disconnected. This may be useful to ensure that the human actually performs the required verification. However a good security design will also ensure that this forcing function doesn't get in the way of usability, otherwise the user will be driven to ingenious ways of bypassing the security mechanisms, as we already discussed in section 3.1.

[17] Even more than in traditional 419s, the crooks are also exploiting the Need and Greed and the Dishonesty principles: the recipient typically *didn't* lose $4.5 million to Nigerian scammers, but won't mind claiming that amount back as compensation.

[18] For example with `https`—even ignoring the problems of PKI and assuming that everything is properly implemented.

[19] One might even be tempted to ask: "how many security officers do?", seeing how many banks complicate this already difficult recognition task for their customers by *not* hosting their own online banking web site at their own regular `bankname.com` domain.

We emphasize again that systems security is not limited to *computer* systems: in all the frauds involving the impersonation of police officers (section 3.2), for example, the high-level "system" being attacked is the infrastructure of society and what is needed is more robust protocols for ordinary people to take the correct decision on whether or not to grant these strangers in uniform the trust and authority they request[20].

3.6 The Need and Greed principle

Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you.

We originally called this simply the Greed principle but we changed the name after realizing that it would be quite improper to characterize all of a victim's strong desires as morally despicable. Loewenstein [12] appropriately speaks of

> *visceral factors* such as the cravings associated with drug addiction, drive states (e.g., hunger, thirst, and sexual desire), moods and emotions, and physical pain.

We say "need and greed" to refer to this whole spectrum of human needs and desires: all the stuff you really want, regardless of why.

In the 419 scam (already discussed in section 3.1), what matters most is not necessarily the mark's greed but his or her personal situation: if the mark is on the verge of bankruptcy, needs a medical operation or is otherwise in dire straits, the offer of a solution is very hard to question. In such cases the mark is not greedy, just depressed and hopeful. If someone prays every day for an answer, an email from a Nigerian Prince might seem like the solution.

The obvious inclusion of sexual desire as a fundamental human need justifies, through this principle, the presence of a "sexy swindler" in most of the scams enacted by the trio. As we observed in section 3.1, there is often a connection between the Need and Greed principle and the Distraction principle.

Having said that, it is still true that in some cases "greed" is an accurate description for this behaviour. In the *ring reward rip-off* (section 2.3), the hustlers know the mark is hooked as soon as he offers them a reward lower than that promised by Jess over the phone. They know he wants to make a (dishonest) profit out of it, so they know how to pace and lead him. As we said in section 3.4 about the mark in the *lottery scam* (section 2.2), if the barman of the *ring reward rip-off* is too honest, this scam simply won't work: he could just tell Paul to negotiate the reward with Jess directly. Scams like this one have been around for centuries: one party offers the mark a large and attractive sum of money if they can secure some object from a second party. The mark is quickly led to believe that the object can be bought for a lower price but the situation demands that the mark must pay for the object with his own money in order to make a sizable profit when he or she sells it to the first party.

In the *lottery scam*, greed is used as the convincer. First, the mark is offered what is already a pretty good deal: essentially a guaranteed £1,400 prize in exchange for a £500 cash advance. The mark is considering the offer and might even go for it, but after all he doesn't know any of the people involved so he still hesitates. Then, suddenly, his share of the prize goes up to over £50,000! If he was almost convinced then, he must be definitely convinced now! The hustlers could just as easily have offered the ticket as a £100,000 winner from the start; but by doing it in two stages they make the offer much more compelling because they have already calibrated the mark's expectation on the lower prize—so the second stage drives him off the scale.

The Need and Greed principle includes most of the cases covered under the Dishonesty principle: most marks, if they act as "occasionally dishonest", will do so not because they're inherently evil but because of a need. But the two principles do not totally overlap: one can also be needy (or greedy) without necessarily being dishonest. In the the *bogus agency scam* (S1-E2) we cited in section 3.1 when

[20] We note in passing that, in some early episodes of the show, the suggestion given after the scam was to ask the purported policeman for his badge and to call the phone number on the badge to verify. Clearly this is not the best advice, as the fraudster can make a fake badge with the phone number of an accomplice. A better suggestion, given in later episodes, is to call the police station through the number found in the phone book or some other higher-integrity channel.

discussing the Distraction principle, young hopefuls are ripped off by Paul posing as a music producer who might take them from their current lowly status of, say, truck driver, to that of glamorous rock stars—all for the modest fee required to launch their first performance.

In the editorial comments that precede the *gadget scam* (section 2.7) Paul says to the camera: "If you want to con someone, all you need to know is what they want, even if it doesn't exist!"

If the security engineer does not understand what users *really* want, and that they'll go to any lengths to get it, he won't understand what drives them and won't be able to predict their behaviour. He will always lose against a fraudster who has instead understood how he can lead his marks.

In this, as in most other fraud situations, a strong defense strategy should also include user education: in order not to become victims of scams the potential marks must learn that, as stated at the conclusion of every episode of the TV show,

> "If it sounds too good to be true, it probably is!"

3.7 The Time principle

When you are under time pressure to make an important choice, you use a different decision strategy. Hustlers steer you towards a strategy involving less reasoning.

In many good scams, such as the *ring reward rip-off* (section 2.3) and its many variations, the mark is made to believe that he or she must act quickly or lose the opportunity. The same thing happens with long cons: the build-up may take days, weeks or months but the final sting forces the mark into a corner—get the money on the table or lose everything! When caught in such a trap, it's very difficult for people to stop and assess the situation properly.

In earlier drafts of this paper we listed only six principles. From the start we had been considering the addition of time pressure as a seventh principle, but we were initially unsure whether we could plausibly class it as a behavioural pattern and therefore a systematic vulnerability of the victim, like the other six: wasn't it rather a "trick of the trade" used by the hustlers, like the special move used to switch cards in the Monte?

Reviewing the literature on decision theory eventually validated our decision to consider Time[21] as a behavioural trait of the victim, as in our other principles. In contrast with the theory of rational choice, namely that humans take their decision after seeking the optimal solution based on the available information, Simon [19] suggested that

> organisms adapt well enough to "satisfice"; they do not, in general, "optimize"

and that they may "satisfice"[22] through much simpler and quicker strategies than those needed for optimization. In different circumstances people will adopt different decision strategies, some determined by reasoned judgements and others based on quicker but fallible heuristics, as extensively studied by Kahneman and Tversky [21, 10]. Finucane et al. [8] showed that time pressure can shift decision making from a reasoned to an affect-dominated strategy. The strategy used for decision under time pressure is therefore typically based on intuitive and affective heuristics with established trigger conditions, rather than on a reasoned examination of all the possible options.

Although the hustlers may have never formally studied the psychology of decision making, they intuitively understand this shift. They know that, when forced to take a decision quickly, the mark will not think clearly and will act on impulse according to predictable patterns. So they make their marks an offer they can't refuse and make it clear to them that it's their only chance to accept it.

Evidence for the validity of the Time principle, and for the need to protect potential victims from its effects, is also implicit in the UK's Consumer Credit Act 1974, under which buyers are granted a cooling-off period of several days during which they can cancel a purchase agreement if, for example, it was signed in their home (e.g. in response to solicitation by a door-to-door sales representative) rather than at the vendor's normal business premises.

[21] More precisely: the fact that a victim will switch to a different decision strategy when under time pressure.

[22] I.e. reach a "good enough" sub-optimal solution that is sufficient to cover their needs.

From the systems viewpoint, the Time principle is particularly important: it highlights that the human element might cause the system's response to the same stimulus to be radically different depending on the urgency with which it is requested. In military contexts, for example, this is taken into account by wrapping dangerous situations that require rapid response[23] in special "human protocols"[24]. These are meant to enforce, even under time pressure, some of these step-by-step rational checks that the heuristic strategy would otherwise omit.

In the civilian world, the architect concerned with overall system security should identify the situations in which the humans in the system may suddenly be put under time pressure by an attacker and whether the resulting switch in decision strategy can open a vulnerability. This applies to anything from retail situations to stock trading and online auctions, and from admission of visitors in buildings to handling of medical emergencies. Devising a human protocol to guide the response of the potential victim towards the goal intended by the security architect may be an adequate safeguard and may also, if the protocol is properly designed, relieve the human in question from stressful responsibility.

	Episode	Scam	3.1 Distraction	3.2 Social Compliance	3.3 Herd	3.4 Dishonesty	3.5 Deception	3.6 Need and Greed	3.7 Time
2.1	S1-E1	Monte	●		●	○	○	○	○
2.2	S1-E2	Lottery scam			○	●	○	●	●
2.3	S1-E4	Ring reward rip-off				●	○	●	●
2.4	S2-E1	Van dragging	○	○			●		○
2.5	S2-E1	Home alone	○	●			○	○	
2.5.1	S1-E1	(Jewellery shop scam)	○	●			○	○	
2.6	S2-E3	Valet steal	○	●			●		○
2.7	S4-E3	Gadget scam				●	○	●	○
2.8	S4-E4	Counterfeit pen con		●			○		
2.9	S4-E5	Cash machine con	●		○		●		
2.10	S4-E5	Recruitment scam	●	●	○		●	○	
2.11	S4-E7	Shop phone call scam	○	●			○		○
2.12	S4-E9	Exchange rate rip-off	○		●		○	●	●

Table 1: A concise summary of the scams (rows) described in section 2 and of the principles (columns) described in section 3 that each scam is based on. The two symbols in the table show whether the given principle is of major (●) or minor (○) importance for the given scam.

4 Related work

While there exist a few narrative accounts of scams and frauds, from Maurer's study of the lingo and subculture of the criminal world [14], which inspired the classic movie *The Sting*, to the autobiographical works of notable former fraudsters such as Abagnale [1] or Mitnick [16], the literature still contains very little about the behavioural patterns of scam victims.

[23] Such as an armed guard challenging a stranger at a checkpoint, or an officer receiving the order to fire a ballistic missile.

[24] Blaze [5] offered an interesting analysis of a few time-honoured security protocols that are run by humans rather than by computers, although he did not describe any military ones.

The notable exception is the interesting 260-page report prepared for the Office of Fair Trading by an unnamed team of psychologists at the University of Exeter [18], released while this paper was being written. Unlike us, the Exeter authors limit their research to email and postal scams. For these, though, they base their analysis on a wealth of experimental data: interviews with victims, lexical analysis and classification of a corpus of fraudulent mailings, and even an active experiment in which they send a fake scam letter to random people who are later asked for feedback. Unlike ours, their experimental setup is scientifically rigorous and they examine enough victims for each scam to be able to draw statistically significant quantitative conclusions. On the other hand our experimental contributions are more varied: *The Real Hustle* investigated many more frauds beyond postal and email scams and therefore highlighted aspects of face-to-face interaction between hustler and mark that a study on postal fraud cannot take into account. Another difference is that their only "active" experiment (impersonating the scammers to observe the reactions of the marks) is much more cautious and subdued than ours: in the same envelope in which they sent the fake scam, they also included a "sorry for deceiving you" letter; we, instead, ran each scam to full completion before informing the marks. Interestingly, even though our approaches are in many respects very different, many of our findings are in agreement. In particular, several of the factors that the Exeter authors highlight as influential in the postal scams they examined correspond fairly accurately to four of our seven principles: Social Compliance (3.2), Herd (3.3), Need and Greed (3.6), Time (3.7). Comparing our results with theirs was instructive and stimulating. Their report is also to be praised for its commented survey of the available literature.

While peer-reviewed studies on scams are rare, some precious insights on why victims fall for scams can be gleaned from the vast literature on decision making, starting with the cited pioneering works of Simon [19] and Tversky and Kahneman [21, 11, 10].

Insofar as sales and marketing techniques that aim to separate customers from their money can be cynically seen as quasi-scams (even though they may be technically legal), an analysis of the persuasion techniques adopted by salespeople, such as that by Cialdini [6], will also offer interesting food for thought. At least three of Cialdini's "weapons of influence" are closely related to our principles: Social Proof (Herd, 3.3), Authority (Social Compliance, 3.2) and Scarcity (Time 3.7). Another one, Liking, matches our observations about the sexually attractive swindler in the Distraction (3.1) and Need and Greed (3.6) principles.

5 Conclusions

We trust that readers will by now agree with our thesis that any systems involving people can only be made secure if system designers understand the inherent vulnerabilities of the "human factor".

Our first contribution to knowledge with this paper is the vast body of original research on successful scams and cons initially put together by Wilson and Conran for the TV show, of which in section 2 we presented a few highlights. Because that work started as a TV show rather than an academic study, it was not conducted as a controlled scientific experiment (each scam repeated many times with different victims etc etc); despite that, this write-up still offers valuable first-hand data on scams and scam victims that, although qualitative rather than quantitative, is not otherwise available in the literature.

A second contribution is our taxonomy of seven principles, each of which identifies a specific behavioural pattern that ordinary people exhibit and that hustlers have been exploiting for their scams—sometimes for centuries. The fascinating reconstructions of real-world scams performed by Paul, Alex and Jess in *The Real Hustle* were meant to educate the public so that they would avoid becoming victims by being caught off guard. In this paper we have shown that additional value is to be gained from these scenarios through the insights they give into the psychology of the scam victims. Some may argue with our choice of those particular seven items as the most representative; we even noted ourselves in the text, where appropriate, that our principles are not entirely independent of each other. Other authors have proposed different taxonomies, though with significant commonalities, as we discussed in section 4 under Related Work. Comparing the intersection and difference of these sets is in itself instructive[25]; however,

[25] For example, we appear to be the first to note the significance of exploiting the mark's dishonesty against themselves

what we feel is most important is not the particular principles but what we do with them.

This brings us to our third and perhaps most significant contribution: to look at these behavioural patterns from a more general viewpoint. These patterns are not just chances for the kind of small-scale hustles in which they were observed but are also typical vulnerabilities of the human component of any complex system.

Our message for the system security architect is that it is naïve and pointless just to lay the blame on the users and whinge that "the system I designed would be secure if only users were less gullible"; instead, the successful security designer seeking a robust solution will acknowledge the existence of these vulnerabilities as an unavoidable consequence of human nature and will actively build safeguards that prevent their exploitation.

6 Acknowledgements

We are extremely grateful to Paul's *Real Hustle* colleagues Alexis Conran (co-author and co-presenter of the show) and Jessica-Jane Clement (co-presenter), without whom the TV series would not exist.

We also thank Joe Bonneau, danah boyd [sic], Omar Choudary, Saar Drimer, Jeff Hancock, David Livingstone Smith, Stuart Wray and especially Roberto Viviani for interesting comments, reading suggestions and discussions on either previous drafts of the paper or the brief talks we gave at SHB 2009 in Boston and at WEIS 2009 in London.

References

[1] Frank W. Abagnale. *Catch Me If You Can*. Grosset & Dunlap, 1980. ISBN 0448165384.

[2] Frank W. Abagnale. *The Art of the Steal: How to Protect Yourself and Your Business from Fraud*. Broadway Books, 2001. ISBN 0-7679-0684-5.

[3] Ross Anderson. "Why Cryptosystems fail". *Communications of the ACM*, **37**(11):32–40, Nov 1994. http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf.

[4] Ross Anderson, Mike Bond and Steven J. Murdoch. "Chip and Spin". *Computer Security Journal*, **22**(2):1–6, 2006. http://www.cl.cam.ac.uk/~sjm217/papers/cl05chipandspin.pdf.

[5] Matt Blaze. "Toward a Broader View of Security Protocols". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (eds.), "Proceedings of 12th International Security Protocols Workshop, Cambridge, UK, 26–28 April 2004", vol. 3957 of *Lecture Notes in Computer Science*, pp. 106–120. Springer, 2006. ISBN 3-540-40925-4.

[6] Robert B. Cialdini. *Influence: Science and Practice*. Pearson Education, 5th ed., 2008. ISBN 9780205609994. (1st edition 1985).

[7] John R. Douceur. "The Sybil Attack". In "Proceedings of IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems", vol. 2429 of *Lecture Notes in Computer Science*, pp. 251–260. Springer-Verlag, 2002. ISBN 3-540-44179-4. http://research.microsoft.com/pubs/74220/IPTPS2002.pdf.

[8] Melissa L. Finucane, Ali Alhakami, Paul Slovic and Stephen M. Johnson. "The affect heuristic in judgments of risk and benefits". *J. Behav. Decision Making*, **13**:1–17, 2000.

[9] Erving Goffman. "On Cooling the Mark Out: Some Aspects of Adaptation to Failure". *Psychiatry*, **15**(4):451–463, 1952. http://www.tau.ac.il/~algazi/mat/Goffman--Cooling.htm.

(section 3.4).

[10] Daniel Kahneman. “Maps of Bounded Rationality”. Nobel Prize in Economics documents 2002-4, Nobel Prize Committee, Dec 2002. http://ideas.repec.org/p/ris/nobelp/2002_004.html.

[11] Daniel Kahneman and Amos Tversky. “Prospect Theory: An Analysis of Decision under Risk”. *Econometrica*, **47**(2):263–291, Mar 1979. http://ideas.repec.org/a/ecm/emetrp/v47y1979i2p263-91.html.

[12] George Loewenstein. “Out of Control: Visceral Influences on Behavior”. *Organizational Behavior and Human Decision Processes*, **65**(3):272–292, Mar 1996. http://ideas.repec.org/a/eee/jobhdp/v65y1996i3p272-292.html.

[13] Stephen L. Macknik, Mac King, James Randi, Apollo Robbins, Teller, John Thompson and Susana Martinez-Conde. “Attention and awareness in stage magic: turning tricks into research”. *Nature Reviews Neuroscience*, **9**:871–879, Nov 2008. ISSN 1471-0048. http://dx.doi.org/10.1038/nrn2473.

[14] David W. Maurer. *The Big Con: The Story of the Confidence Man*. Bobbs-Merrill, 1940.

[15] Stanley Milgram. “Behavioral study of obedience”. *Journal of Abnormal and Social Psychology*, **67**(4):371–378, 1963. http://library.nhsggc.org.uk/mediaAssets/Mental%20Health%20Partnership/Peper%202%2027th%20Nov%20Milgram_Study%20KT.pdf.

[16] Kevin D. Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002. ISBN 0-7645-4280-X.

[17] Donald A. Norman. *The Psychology of Everyday Things*. Basic Books, New York, 1988. ISBN 0-385-26774-6.

[18] University of Exeter School of Psychology. “The psychology of scams: Provoking and committing errors of judgement”. Tech. Rep. OFT1070, Office of Fair Trading, May 2009. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf. Crown Copyright.

[19] Herbert A. Simon. “Rational choice and the structure of the environment”. *Psychological Review*, **63**:129–138, Mar 1956.

[20] Frank Stajano and Ross Anderson. “The Cocaine Auction Protocol: On The Power Of Anonymous Broadcast”. In Andreas Pfitzmann (ed.), “Proceedings of IH’99, Third International Information Hiding Workshop”, vol. 1768 of *Lecture Notes in Computer Science*, pp. 434–447. Springer-Verlag, 1999. ISBN 3-540-67182-X. http://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-cocaine.pdf.

[21] Amos Tversky and Daniel Kahneman. “Judgment under Uncertainty: Heuristics and Biases”. *Science*, **185**(4157):1124–1131, Sep 1974. http://www.jstor.org/stable/pdfplus/1738360.pdf.