No Room at the Inn?
Analysing Hotel Room Poaching

Richard Clayton
Computer Laboratory, University of Cambridge,
JJ Thomson Ave., Cambridge, CB3 0FD, UK.
richard.clayton@cl.cam.ac.uk

Abstract

The organisers of many conferences arrange for blocks of rooms at appropriate hotels to be reserved for conference attendees, and they may contract to provide given levels of occupancy. Room poaching occurs when third parties approach attendees and persuade them to book through them. This activity is fraudulent when the third party misrepresents their relationship with the conference or fails to honour their obligations and leaves attendees with nowhere to stay. This paper presents a first-hand account of a room poaching incident at a 2015 academic conference and sets this in the context of the wider room poaching issue, analysing the issue from legal and economic viewpoints. Simple countermeasures are suggested that could reduce the incidence of the problem, particularly in the academic context.

1 Introduction

Academic papers about cybercrime seldom include first-hand accounts of an incident. This paper is an exception in that it starts by recounting how I was taken in by a hotel room poaching organisation. It then considers the accounts of other victims before setting room poaching in a wider context, analysing the legal position and providing an economic analysis of the activity. Simple countermeasures that could reduce the incidence of room poaching are then discussed.

A key contribution of this paper is, I believe, providing a detailed account of what happened to me, because this is the modern equivalent of telling 'war stories' around a camp fire. Disseminating knowledge about how scams are operated (so that others may recognise when they are at risk) remains an important barrier to their continued success.

Room poaching is perhaps not a true 'cybercrime' but a 'cyber-enabled' crime: a fraud which is simpler to do in the Internet age because it is now much easier to find potential victims and much simpler and cheaper to scale activities across many different countries.

Indeed, as will be explained, room poaching can be profitable without committing any crime at all. Other cybercrimes may evolve to looking much more like 'sharp business practice' than criminal acts, and hence it is useful to study this particular activity (which is already at an extreme of this scale) and see how poorly it is being dealt with.

2 My personal experience with EHS Housing

In Spring 2015 I was honoured to be invited to give a keynote talk at ESORICS, a well-established European academic security conference; the 20th running of which was to be held in September 2015 in Vienna, Austria. As is the convention in such matters I was expecting the ESORICS organisers to cover my travel and accommodation expenses.

On Thursday 23 July I was rung at work by a person who identified themselves as being from a company called "EHS Housing". They were aware that I was attending ESORICS and asked if I had booked my hotel yet ?

When I said I had not yet made any arrangements, they told me that hotel rooms in Vienna were in short supply and it was urgent I make a booking very promptly. They immediately emailed me (from `ehshousing.com`) a link to their booking website and stayed on the phone to talk me through filling in all of the details – including the process of using my mouse to produce a graphic that looks very vaguely like my signature.

My travel plans for September had been fluid and I had been awaiting an agenda that told me exactly which day I would be speaking. So, at EHS's suggestion, I booked the hotel from Saturday to Friday because they told me I could cancel any extra days at a later time. They took a deposit of 25% of the room fee from my credit card, with the remainder payable four weeks before my stay.

On the following Monday I (and everyone else who had registered for the conference) received an email from the ESORICS organisers.

> *It came to our attention that there have been spam calls or e-mails concerning the ESORICS Conference. The company EHS (Exhibitors Housing Services) has called or e-mailed attendees of ESORICS 2015. They claim to work for SBA Research/the conference organization and ask for credit card details to finalize the booking of accommodation (see e-mail below).*
>
> *Please do not give away any information or credit card details if you receive such a call or e-mail. This company is not working for SBA Research or any other company involved in the organization of ESORICS.*

Of particular concern was the suggestion:

> *In case you gave away your credit card details, please block your credit card immediately.*

I immediately contacted *Motel One Hauptbahnhof* where EHS had purported to make me a booking the previous Thursday and they told me that there was no booking in my name. I also asked the ESORICS organisers (who of course speak fluent German) to contact *Motel One* and they confirmed that no reservation had been made. We also established that there was no shortage of rooms in Vienna and that the organisers were planning to organise my accommodation, but had yet to start this task.

At this point I contacted my credit card company to dispute the transaction and was told that if it was all completely fraudulent then I would get a refund, albeit we could

not know that this was the case until I went to Vienna in September! In the meantime I was advised to ask EHS Housing for my money back. They also suggested that I make a particular point of checking future statements for any unexpected charges.

I then had a long email correspondence with EHS. Since my travel plans were now decided, we explored a shorter booking period, but they wanted to charge me considerably more than the rate I could get on the hotel website. Eventually, after I had insisted that I wanted to cancel, they converted the 25% deposit I had paid on 23 July into a 25% cancellation fee because, they informed me, their terms and conditions permitted them to do this, and they drew my attention to their website where these terms and conditions were documented.

I did not hear from them further.

After the date of the conference I was contacted by my credit card company who wished to know if I wanted to pursue my claim – which I did. EHS Housing then disputed the charge-back, providing in evidence the invoice generated from my interaction with their website – including the approximation to my signature! They also said that they were not affiliated with ESORICS and claimed that they had never represented otherwise.

I produced a detailed account of my side of the story in which I repeated that EHS Housing had misrepresented themselves. However, since this was hard to prove, my account stressed the failure of EHS Housing to book a room at a time when they claimed that there was a shortage. I also drew attention to their failure to provide me with any paperwork at the time of the transaction (a requirement of European Union law). For whatever reason, EHS Housing did not contest my claim any further and my credit card company refunded me £122.84.

Careful checking of all my subsequent credit card statements has not revealed any unexpected transactions.

3 Further incidents involving EHS Housing

An online search for "EHS Housing" throws up a number of hits for "Educational Housing Services" which provides student accommodation in New York, but "Exhibitor Housing Services", the company I dealt with, does appear on the first page of results – their website says that they "provide Housing Services for 120 City Wide Conventions in 79 destinations across USA, Canada, Europe, & Middle East" and that "EHS Housing Services processes over 120,000 hotel reservations annually".

On the second page of search results is a link to `scambook.com`[1] whose summary is that there have been 46 complaints recorded against EHS Housing since May 30 2013 (33 months). The average reported loss, according to `scambook.com`, is 850 USD.

I examined this data carefully. There are in fact 44 reports (two are duplicates) and 14 of these are generic reports, mainly by conference and exhibition organisers which state that EHS Housing has approached their attendees falsely claiming to be associated with their event. Some of these include loss estimates, in one case 20 000 USD, but these do

[1] `http://www.scambook.com/company/view/129876/EHS-Exhibitors-Housing-Services`

not look especially accurate, so in the table below I have only considered the loss amounts (many of which were exact to the dollar, and hence plausible) from the 30, first-hand, victim reports:

loss in USD	occurrence
0	12
150 to 499	5
500 to 999	8
1000 to 2000	0
2000 to 4000	4
12000	1

There were various reasons for people not losing money. Seven of them saw through the scam at an early stage and they did not provide any credit card details. Four more realised within a few minutes that there was a problem and blocked the payment or cancelled their card. In the one final case the credit card company flagged the transaction as potentially fraudulent and the person had by then realised that there was a scam occurring.

For those who did lose money, (ignoring the 12 000 USD outlier) the mean loss was 1074 USD and the median loss was 555 USD.

The reason for ignoring the outlier, and for considering both the mean and median values is because of the way in which atypical, or high variations in, loss figures can cause the impact of a fraud to be misunderstood. Florêncio and Herley explore this issue in detail in their 2011 WEIS paper [4]. It should of course be noted that only a subset of people will make a report on `scambook.com` and there is no reason to believe that their losses are typical – however it is the only substantial dataset that is publicly available and it corresponds reasonably well to the price of hotel rooms and the typical length of stay at events. The reported losses are, I believe, either 100% of the cost of the room or, where only a 'cancellation fee' has been incurred, 25% of the cost.

3.1 Variations on a fraudulent theme

The various accounts on `scambook.com` shed further light on how the company operates. Contact is always made by telephone and the claim is made of a connection with the event organisers. If no room has yet been booked then there is said to be a shortage of rooms – if a room has been booked then a better price can allegedly be obtained.

In many cases the scam came to light because the event organisers reported that others were being contacted – if so, the loss was generally the failure to refund the 25% up-front deposit. In other cases the hotel made contact to ask why people had two bookings ? In some cases there was no booking made or it was made (to obtain a reference number) and then fairly promptly cancelled. If this was not detected then EHS Housing would ring again, say that a technical error had caused the original booking to be lost, and an attempt would then be made to get more money to make a booking somewhere else.

The contact details for those that EHS Housing contacted were often found on the web (for scientific conferences several victims were, like myself, specially invited speakers) or

they would ring a company that was apparently going to exhibit at a trade show and ask to speak to the person organising the attendance. A regular feature of the accounts was someone who was contacted being concerned enough to ask the event organisers to clarify the relationship with EHS Housing (or even just to ask if there was a shortage of rooms) resulting in the organisers doing a general mailing that prevented further victimisation (and set existing victims onto the path of disputing the charges that were made).

There are, it should be noted, a number of other websites that hold complaints about EHS Housing, but none has as many reports as `scambook.com`. Searches also find a number of instances of the warnings posted by event organisers about the company.

Besides EHS Housing there appear to be many other companies operating in similar ways,[2] and in particular Exhibitors Housing Management (EHM) has accumulated 25 complaints to the Better Business Bureau (they are not accredited by the BBB and score an F on their A to F scale). The BBB also has a page on EHS Housing (who they also score at F) and they have 39 complaints. However, the BBB appears to have mixed up Exhibitors Housing Services (the company this paper is discussing) with Exhibition Housing Services and a number of the warnings sent out by event organisers have also used the "Exhibition" name and this confusion means that I think it is unsafe to include the BBB data in my analysis. It is beyond the scope of this paper to establish which company each of the BBB reports refers to, but for the avoidance of doubt I have no reason to believe that Exhibition Housing Services operates in anything other than a completely honest manner.

None of the methods used by the room poachers to inveigle their victims are in any way unusual and they correspond well with the persuasion techniques used by sales people that Cialdini described in 1985 [1]. In particular 'Scarcity' can be seen in the alleged shortage of hotel rooms. More recently, Stajano and Wilson analysed a number of scams [7] and several of their principles are present here: 'Social Compliance' is in play when the poachers claim to be associated with the event, 'Time' is related equivalent to Cialdini's 'Scarcity' but emphasises the need to act quickly and where the poachers offer a better price for an already booked room then 'Need and Greed' is being exploited.

4 A wider analysis of room poaching

Thus far I have been describing frauds from the point of view of the individuals that have been contacted by the fraudsters – but this type of activity has been named 'room poaching' because the fraud also affects event organisers. It is common for organisers to arrange for blocks of rooms to be made available for delegates to book in appropriate hotels. The hotels will generally provide special pricing for the sleeping rooms – or for conference space hire – in exchange for contractual guarantees of occupancy levels. When third parties 'poach' attendees away then there is a risk that the room block will not be filled and the event organiser may face financial penalties.

The US convention trade body CIC (the Convention Industry Council) has been concerned about what they call "attrition" from room blocks for some time. In 2004 they published

[2] The website for "Coverings 16: the global tile and stone experience" lists 46 company names: `http://www.coverings.com/Content/Housing-Warning/6_79/`

a report [2] that identified the main issues at that time as being reduced travel after '9/11' (so that fewer people came to events) along with a rise in attendees making their own booking using Internet travel websites. Although there was a brief mention of room poaching (which the report calls "guest room pirates") the main focus of the report was on techniques for encouraging attendees to book rooms within the official blocks.

However, room poaching is now CIC's main concern. In 2014 they set up an expert working group under their APEX (Accepted Practices Exchange) initiative. Their 4-page report *"Best Practices for Poaching and Piracy Prevention and Responses"* sets out the basics of room poaching and then provides an extensive check-list of measures that can be used to address it [3]. Their approach is to list how each of the check-list items addresses the five specific harms they have identified:

- Selling fictitious reservations and credit card fraud.
- Misrepresentation resulting in bookings outside the room block.
- Trademark infringement.
- Unauthorised access, use and selling of data.
- Obtaining (hotel room) inventory through misrepresentation or omission.

Interestingly, the APEX report lists the stakeholders as industry organisations, event organisers, hotels, and destination marketing organisations (the last group being associated with all the hotels and other tourist attractions in any particular city or region). The event attendees, the people who are directly defrauded, are not listed as stakeholders and there is no advice aimed directly at them – merely recommendations that other stakeholders educate them.

4.1 What is the legal position?

When room poachers misrepresent facts to drum up business then they commit fraud. Common misrepresentations are their relationship with an event, an alleged shortage of hotel rooms, or the price that they can obtain. It is also, fairly obviously, fraudulent to take money for a service and then fail to provide it.

Where there has been misuse of trademarks, or claims to be officially associated with an event then the approach generally taken (and recommended in the APEX report) is to issue cease-and-desist letters and to report the incident to the Better Business Bureau (hence the F scores remarked upon earlier).

The APEX report also recommends making complaints to law enforcement agencies. However, no criminal prosecutions of room poachers seem to be occurring – probably because of the relatively low monetary value per incident, a failure to detect a pattern in the activity, and of course the difficulty of proving a case where key aspects of the fraud occur in unrecorded telephone conversations. There is also the usual barrier of multiple jurisdictions – albeit the majority of the fraud appears to occur within the USA but agencies from many different states may be involved.

Although 'cease-and-desist' letters are regularly issued there has been just one civil court case concerning room poaching, back in 2008. The American Society of Association Executives (ASAE), which is an association for those running associations, went to Federal Court to sue Complete Event Planning, Inc. (CEP) of Henderson, Nevada. The claim was that CEP had used ASAE's logo without permission and misrepresented themselves as authorised to arrange hotel rooms for ASAE conference attendees. This was settled out of court with CEP agreeing not to continue these practices not only for ASAE itself, but for all events organised by associations whose employees are members of ASAE.

So far as the individuals caught up in room poaching are concerned then they have numerous protections. In the UK, and doubtless many other jurisdictions, the credit card company can be held jointly liable with the merchant so that legal action can be taken against either party. However, the most likely way for a consumer to proceed (in any jurisdiction) is to just ask the credit card company to nullify the transaction in some manner. As already noted above, this was an effective tactic in many of the incidents reported on `scambook.com`.

However, as I found out myself, the credit card company may not be prepared to deem the transaction to be fraudulent until the room poacher has failed to provide a room. It is also clear, from reading the various accounts of the fraud, that when the room poacher produced a 'signed' (with a mouse) document many individuals believed that they had no further recourse. I did not give up at this point because I was always prepared to admit that I had tried to enter into a contract, but my position was that EHS Housing had reneged on their side of the bargain.

Europeans will doubtless be wondering about the applicability of the EU Directive on Consumer Rights (2011/83/EU) which replaces (and indeed repeats) many of the provisions of the Distance Selling Directive (97/7/EC). Hotel rooms are one of the classes of goods for which there is no right to cancel, however the general provisions of the Directive apply and it is still necessary to provide clear information about the contract and details of the payments. In my case these documents existed (because they were supplied as evidence when I raised a dispute), but since they were not sent to me, as they should have been, at a much earlier stage then technically the purported contract was void.

4.2 Economic considerations

Alongside their Best Practice document the APEX working group also produced a 'white paper' that summarises the issues around room poaching. They surveyed 622 meeting professionals finding that 73.1% had encountered room poaching (although there is presumably some selection bias here because they do not give a figure for those who failed to answer the survey).

The survey indicated that the biggest impact was disrupting the meeting planning process, closely followed by an effect on attendee satisfaction. Monetary issues, such as legal fees, or unexpectedly low rates of room take-up, affected fewer survey respondents than those who reported that there had been a negative impact on their brands.

It is also clear from the large number of trade conferences that mention room poaching on their websites that meeting planners consider this an important issue – however, it is

rare to find generic warnings on academic conference websites (for example there is no mention anywhere on the `usenix.org` website), only specific warnings when a particular conference has already been targeted.

Whilst monetary issues may not be front and centre for the meeting professionals it is clearly the main problem encountered by the victims. Losses will be either the cost of a room (assuming that the victim ends up paying twice but staying only once), the cost of the deposit (which the room poacher converts into a 'cancellation fee' if the victim abandons the booking), or it will be the excess cost of the room compared with what the victim might have paid (in my case EHS Housing at one point offered to book me a room at 141% of the price I could obtain for myself on the hotel website).

In principle of course the room poacher could pay a 'trade' price for a room and give up some of their margin so as to undercut the 'rack rate' which someone booking direct would pay. However, this will not be a very large amount of money because much of this margin is already available to people who book through generic Internet websites and the conference organiser will have rooms to offer at a discount already – because that is inherent in them doing a special deal with hotels to offer an official block.

So, although a room poacher could restrict themselves just to poaching and not do anything fraudulent, this is unlikely to be especially lucrative when dealing with well-informed consumers. Nevertheless, restricting their activities to selling over-priced rooms (to people who were unaware of the market rate) could be a reasonably profitable business and, provided they did not misrepresent their relationship with the event, or lie about room shortages, would not be unlawful.

One might expect to see a bigger role for the credit card companies in dealing with the fraudulent aspects of room poaching. McCoy et al. in their 2012 "Priceless" paper [5] consider the complex role of payment processing in monetizing the modern affiliate program ecosystem: that is they see how credit card company policies and the impact of charge-backs impact the behaviour of groups selling counterfeit pharmaceutical and software products.

Although I personally succeeded in my dispute – my credit card company will have deducted my payment from monies passed on to the merchant – the evidence from the accounts on `scampages.com` is that complaining to the credit card company is not an approach that most victims take, at least not successfully. It may well be that the existence of an agreement, and the mouse-generated signature (which others mention) persuades some victims that they cannot succeed in a claim. This is unfortunate, because until victims complain at scale the credit card companies will not raise the charges that the room poachers pay, or consider terminating their relationship.

5 Countermeasures to room poaching

As has already been mentioned, the APEX report has a multi-page checklist of countermeasures to room poaching and doubtless these are all valuable. The interested reader can find the detail in the report: but the general approaches are education of all concerned; ensuring that relevant intellectual property (logos &c for the event) is controlled;

working to keep blocks of rooms out of the hands of the room poachers; and monitoring discrepancies between registration and room bookings.

What is entirely apparent from the first hand accounts on `scambook.com` is that the most effective countermeasure in practice is for those who are approached by room poachers to report this to the event organisers in a timely manner and for the event organisers to immediately send a warning to all of the potential attendees. The APEX report does not, in my view, stress this sufficiently because they do not really consider special advice to potential victims (rather than a general view that they should be "educated"). Clearly proactive messaging at the earliest possible stage, stressing the value of passing on any reports of attempted poaching, will decrease the likelihood of anyone being taken in and by encouraging reports to the organisers it will allow them to send further, and very specific, warnings as may be necessary.

Although the APEX report cautions that lists of (potential) attendees should be kept securely, it seems fairly clear that the room poachers are mainly using the public websites for the events to identify potential victims. Hence, for academic conferences it is clearly going to be important to communicate the risks (and the intended room booking process) to keynote speakers at a very early stage – certainly before their names are made public. Additionally, when papers are accepted, telling the authors of the risks of room poaching (and the value of reporting any occurrence) needs to have taken place before the list of acceptances is published.

6 Discussion and conclusion

This paper has considered fraudulent activity around 'room poaching', giving a first-hand account of one incident and analysing 30 other reports of loss involving the same company. The mean loss was just over 1000 USD with the median loss being about half that.

Room poaching is a 'cyber-enabled' crime in that it is only practical to operate it at scale by using the Internet to identify conferences (and to then identify keynote speakers, exhibitors, and likely attendees). There are perhaps 1000 major exhibition locations in the USA alone, and so there will be well over 50000 large exhibitions a year. If fraudsters snared just 1 person per event then we can envisage room poaching to be (to avoid overhyping this, I use the median loss of 555 dollars) a 28 million dollar a year crime. If, as discussed above, the room poachers did not misrepresent themselves and actually delivered the rooms they promised, then they might make perhaps just a 100 dollars profit per victim – so this would be a legitimate business making 5 million dollars a year. Of course this is entirely hypothetical – there are no statistics as to the number of people who are taken in by the room poachers, nor are the likely to be in the short term if victims do not complain to the credit card companies, let alone to the police.

Cybercrime is already, in a great many cases, tackled fairly ineffectively – often because investigations stall at the point where it is necessary to identify the criminals. Room poaching, that may appear to many to be 'sharp business practice' rather than outright fraud, is also being poorly dealt with, despite the perpetrators being relatively easy to identify. Let us imagine that some other cybercrimes were somehow to morph into activities that were rather less criminal, but easier to investigate and where the criminals were

easier to identify. The lesson from examining how room poaching is being tackled is that this imagined change seems unlikely to lessen the damage or cause more criminals to be caught or otherwise put out of business.

The paper has explained how room poaching affects event organisers as well as individual victims and I have explained the efforts made by meeting organisers to analyse the problem and document the countermeasures that can be taken to reduce the incidence of room poaching. Happily, it should be the case that incentives are fully aligned between event organisers and attendees – and the organisers clearly recognise that it is their reputation that is at risk as much as their money. However, as I have pointed out, the expert working group failed to consider event attendees as 'stakeholders' and they did not, in my view, especially stress the practical importance of ensuring that as many attendees as possible are aware of the issue so that if fraud is attempted it will get reported to the event organiser. The impact of the warning that can then be sent – giving precise details of identity the room poachers and the exact methods they are using – is clearly going to be far higher than generic cautions about the issue.

I have drawn attention to how room poaching has historically been an issue for trade shows and professional meetings, but I have shown that it is now becoming an issue for academic conferences. That, I suggest, gives an extra importance to studying this issue in academia.

In particular, one of the claims I made at the start of this paper is that the 'war story' it contains will assist others in not becoming victims. Rader et al. consider how non-expert computer users learn about security through stories and repeat those stories to others – albeit their concern is that the security decisions that are made are not especially good or sophisticated [6]. I hope that the security decisions made by those who have read this far will be of sufficient sophistication that they will not make the mistakes I made – although if they do, I hope that they will take heart from my success in persuading my credit card company to refund my money.

Acknowledgements

The author is funded by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific via contract number N66001-13-C-0131. This paper represents the position of the author and not that of the aforementioned agencies.

References

[1] R.B. Cialdini: Influence: Science and Practice, Fifth Edition. Pearson, 2009. (First Edition 1985).

[2] Convention Industry Council: Project Attrition. 2004. `http://www.conventionindustry.org/ResearchInfo/ProjectAttrition.aspx`

[3] Convention Industry Council: Best Practices for Piracy and Poaching Prevention and Responses, 2014. http://www.iaee.com/downloads/1456022789.57367100_bf548e85bb/Best%20Practices%20for%20Piracy%20and%20Poaching%20Prevention%20and%20Responses.pdf

[4] D. Florêncio and C. Herley: Sex, Lies and Cyber-crime Surveys, WEIS, 2011.

[5] D. McCoy, H. Dharmdasani, C. Kreibich, G.M. Voelker and S. Savage: Priceless: the role of payments in abuse-advertised goods. 2012 ACM conference on Computer and communications security (CCS '12), ACM, pp. 845–856, 2012.

[6] E. Rader, R. Wash and B. Brooks: Stories as Informal Lessons About Security. Eighth Symposium on Usable Privacy and Security (SOUPS '12), ACM, 2012.

[7] F. Stajano and P. Wilson: Understanding Scam Victims: Seven Principles for Systems Security, Communications of the ACM, 54(3), pp. 70–75, 2009.