COMS30038 — SECURITY BEHAVIOURS

SOCIAL ENGINEERING: PRETEXTS & OSINT

*Matthew Edwards**

---

1 THE VALUE OF THE PRETEXT

In 2009, hackers linked to the Chinese state intelligence arm managed to get members of the Dalai Lama's office to download malware attached to an email. The malware in turn captured credentials and other information about the Tibetan spiritual leader and government-in-exile, allowing the hackers and their employers a close look at a number of classified documents. They accomplished this by attaching the software to an email that purported to come from colleagues in the Tibetan movement [1, 2] – people the recipients thought they could trust.

In 2019, hackers linked to the Chinese state intelligence arm managed to get members of the Dalai Lama's office to download malware distributed through WhatApp messages. The malware collected message and contact history and reported it back to the hackers and their employers. They accomplished this by pretending to be friendly Amnesty International members—people the office of the spiritual leader and government-in-exile thought they could trust—investigating protests and sharing a news link [3].

One thing we can observe from these attacks is that, while the technical portion of the attacks has changed, the social engineering involved in delivering the malware has altered very little. In both cases, here, the delivery mechanism was a seemingly-innocuous communication from an identity the recipient had little reason to mistrust. Very little of the sort of persuasion we talked about in the previous lecture was necessary, because the *pretext* for the communication—who this person seems to be, and the reason for their sending the message—did the majority of the work.

The pretext is a critical element of most social engineering. It is often the case that the information the social engineer is seeking to extract is available, but only handed out to certain people, identified by official or unofficial policies. The same can be said for many cases where the social engineer is trying to cause something to happen, like a password reset.

*matthew.john.edwards@bristol.ac.uk

Many of the Authority Principle examples discussed in the previous lecture made use of a pretext that the social engineer was someone in a position of authority: a doctor giving a nurse instructions, a senior executive telling employees to change an account number. This is because impersonation—an critical part of most social engineering pretexts—is also one of the best ways to leverage people's natural inclination to obey authority figures. However, there are many other uses of pretexts beyond those exploiting obedience. Consider, for example, Kevin Mitnick's long-time habit of pretending to be a telephone engineer in order to extract access codes and configuration details [4, p. x] – it would rarely be the case that a telephone engineer is in a position of authority over the person Mitnick was talking to, but a telephone engineer might have a justifiable *need to know* such information, leading to its disclosure to a sufficiently-convincing voice.

As is demonstrated in this week's reading [4, p. 15-29], often a social engineering attack will be carried out in stages, each of which might require a unique pretext. The first enquiry might come from a member of the public, the second from an employee at another branch, and the final pretext might be that the social engineer pretends to be their target victim themselves, trying to update their account. In each case, the main criterion for a pretext is that it should be chosen carefully to correspond to the target and the goal – after all, there is no point being able to pull off a flawless impression of a telephone engineer if you are ringing a bank in search of an account number. There are however a few key guiding principles for crafting an effective pretext [5, p. 114]:

1. **Research pays off**. The more research you have previously invested into understanding your target, the more likely it is you will be able to craft a successful pretext. If your target is an organisation, this might mean knowing which departments and offices exist which the victim of the call will know *about* as legitimate insiders, but which are sufficiently disconnected that they are unlikely to notice flaws in the impersonation. If the target is an individual, good research will turn up details about their interests, connections and disposition. These details can then be used to craft a pretext that exploits the Liking principle to win you a favourable reception. For example, identifying that a CEO regularly makes donations to a charity for a particular cause could suggest that you'll get a fair hearing on the pretext of being a fundraiser from the same or a similar charity.

2. **Seem the part**. During a Downing Street briefing on the recent pandemic, Deputy CMO Jenny Harries was asked a question about the Test & Trace programme – how were members of the public meant to know if someone ringing them was a genuine Test & Trace employee rather than a scammer? Harries' answer was that the genuine employees would sound professional – and by implication, the scammers would not. This is dangerously wrong. While low-effort scam campaigns do

exist, targeting only the most gullible, genuine social engineers are very capable of 'sounding professional' by imitating the appropriate dialect and mannerisms. In fact, an important part of a pretext is using subtle hints to give any number of other impressions. For example, wearing a hat or t-shirt with a company logo gives a strong impression that you are an employee – even though anyone could extract the logo from the company website and have it printed out, or attached to their email signature. Effort invested into these small details is useful for lowering a target's guard and selling the pretext.

3. **Use the truth**. You will be least able to convincingly sell a pretext for which you have no real-world experience. A social engineer who has no technical expertise might be able to pass as a technician to someone similarly inexpert, but will quickly come unstuck if challenged by a real technician. Conversely, one of the best methods of appearing credible is to make use of the truth. Using parts of your real background as part of the pretext can be an excellent method—you already know the material in depth, and should be able project confidence in how you handle queries from your target. This doesn't mean using your real identity, but if you have prior experience as a junior developer, a sales rep, a journalist, or any other appropriate role, then making use of that background in your pretext will lead to a more convincing deception.

4. **Keep it simple**. When crafting a lie, there is sometimes an impulse to make it a byzantine web of creation – the character you invent becomes a full-blown alter-ego, with their own hopes and dreams, a rich network of family and friends, and a complex backstory reaching back to primary school. In some exceptional circumstances this might be appropriate, but for most social engineering purposes, it is not only unnecessary, but actively harmful. Firstly, this background of lies is something that you will have to remember, sometimes on the spot, and the richer and more detailed your construction the greater the probability that you will forget something. Lies are for various reasons more difficult to recall than the truth, and if social engineering is carried out in-person or on the phone, conversation partners can grow suspicious if you find it difficult to remember critical elements of your own life[1]. Secondly, elaborate preparations can become worthless if your needs change during the con. Perhaps, in response to something your target has just said, it would be advantageous if your character was also from Birmingham, or has a caravan in Wales, or a daughter living in London. A rigid prepared structure would then become an obstacle. A good pretext is flexible, and a simple, straightforward premise makes for the best starting-point.

[1] Of course, having to invent these details on the spot can lead to similar suspicious pauses. The best approach is to have a vague outline – a few prepared names and places you can make use of – which helps you through but doesn't constrict you.

5. **Appear spontaneous**. While in many cases a social engineer knows the stages they want a conversation to work through—they may have an outline of the questions they want to ask and even how they want to ask them—there is little more likely to raise the suspicion of the target than giving them the impression you're reading a script[2]. The character in the pretext should not be flipping through a set of prepared responses that they robotically repeat, they need to respond like a real person would in their role. As mentioned in the previous week's notes, social engineering should be considered a form of *improv*, combining thinking-on-your-feet with staying in character.

Remember: the techniques we're discussing can be *criminal* if applied to deceptively extract protected personal information. Attempting to practice these techniques on organisations like your bank could lead to you being prosecuted.

2 OPEN-SOURCE INTELLIGENCE

As mentioned, good intelligence on your target is important for successfully carrying out a social engineering attack. There are various ways you could gather intelligence on a target organisation. If you know someone who works there, or has worked there, or at least visited before, you could ask them about what they know about the people, procedures, layout, etc. – this would be human intelligence, HUMINT. Alternatively, if you've already carried out a technical attack against the organisation, and are able to monitor their internal communications, you could learn a lot of what you need from these messages, a practice known as signals intelligence, or SIGINT. It is commonly the case, however, that the social engineer has no special access to begin with, and only has access to information openly available to the public. This open-source intelligence, or OSINT, may not sound like much on the face of it, but can be surprisingly powerful.

For example, in 2015 the United States Air Force destroyed an Islamic State bomb factory. They had identified the location of the factory from a social media post made by an Islamic State propagandist a mere 22 hours earlier – the images included in his post had revealed enough of the structure of the building's roof that the airmen were able to use satellite mapping imagery[3] to locate the building [6]. In another, privately-led investigation by the investigative journalist site Bellingcat, the Russian commander responsible for the downing of flight MH17 was identified using a series of investigations into a phone number and some public vehicle registration data [7].

As you might appreciate, if public information can locate jihadist bomb factories and unmask undercover Russian commanders, it can definitely suf-

[2]There is perhaps one exception, when you're impersonating someone whom the target would expect to be reading a script. For example, if you impersonate a call centre employee carrying out a telephone-based survey.

[3]Which is also available to any internet user, courtesy of Google Maps.

fice for gathering information on ordinary businesses and their employees. There are a great variety of resources and techniques that can be exploited for this purpose, but their application is perhaps best described by example.

Let's imagine I am a social engineer, a criminal sleuth somewhere between a private investigator and a hacker-for-hire, who has been hired by a competitor of Example Corp. to dig up details of Example Corp.'s upcoming business deals and financial status. The problem is I know nothing about Example Corp. other than their name – not a strong position to be in for socially engineering those financial details out of the company.

The very first thing, of course, will be to use one of the most powerful OSINT tools in the world, and put that name into a search engine. This immediately brings up a number of results, including news articles and PR pieces in business magazines, the company's Twitter and LinkedIn accounts, and a number of other hits – all of which will have to be queued up, because the first thing I will be investigating in detail is the very top result: the company's public-facing website.

Example Corp.'s website immediately tells me a lot about them. Some of this is relatively uninteresting – their corporate vision, the awards they have won, their basic elevator pitch for investors. However, a few things of use can be immediately be added to my file: the company's address is on their website, which tells me where I'll need to go if I'm going to infiltrate them in-person. There's also a contact email address, which I might be able to use for initial queries under a pseudonym, and links to the Twitter and LinkedIn accounts I found earlier – always good to have confirmation. Looking a bit closer, the web design company that built their website for them has included their name in the footer of the frontpage. This gives me my first business connection, and I can make a note to investigate that company further – they might have access to Example Corp.'s systems, or they could be a good identity to assume as part of a pretext. Looking around other pages on the site identifies some other business partners, including National Corp., a big company likely to have many sub-offices and branches who don't talk to each other. Example Corp. likely have a specific contact within National Corp., which isn't listed, but it's possible that someone else within National Corp. would find some reason to call Example Corp. for information – another potential pretext. All the business partners get noted down, but National Corp. and the web designers are top of the list so far.

Usefully for my investigation, on a different page Example Corp. also mention some of their investors. Not much information is given, but a name is all I'll need. Investors might be expected to have some information on how their money was spent – and if I can get private information from them about Example Corp., that's a route that avoids the sort of direct contact where my target might be alerted if I mess up. Another very useful page is 'Meet the Team', which has the faces, names and organisational titles of several of the most important people in Example Corp. – all prime targets for investigation, both as potential leaks who might be targeted for the information I'm after,

or as people who could be impersonated or referenced in a conversation with more junior staff. I can start drawing up an organisational chart. One final link on the site is useful to me: 'Join Us' reveals that Example Corp. currently have an opening for a Software Engineer. This opens up a great opportunity – not for me to become a software engineer, but for me to get a risk-free pretext for engaging someone from the company in conversation, and in particular a conversation where it's not at all strange that I would be pumping them for lots of information about how Example Corp. works. This is an open invitation – all I need to do is send in a fake CV with the right experience and credentials, and top it off with a convincing cover letter. A piece of cake for a professional social engineer.

There is nothing else visibly linked from the organisation's website, but that doesn't mean we're done with it. First of all, it's worth checking the domain registration data using `whois` on `example.com`. This used to be a good source of technical contact information, but organisations have mostly caught on to this, and `example.com`'s record is now pretty typical: "REDACTED FOR PRIVACY" is the value in most of the fields – all we get is the date the domain was registered. Reading the site's information in our browser console doesn't tell us much more – the existence of a `wp_content` folder serving some of the CSS and Javascript tells us the site is based on Wordpress, and there are a number of `plugins` in use. If we were interested in a technical attack, we could check a vulnerability database (or an underground market) to see if there are any known exploits for these plugins.

More fruitfully, we can try some Google Dorks for the website. These are patterns we can use to pick up all the links the search engine has indexed from the site, and in particular to find things like documents which may have been accidentally made available. For example, a search for `site:example.com *.pdf` turns up a report from last year on a previous Example Corp. project – this isn't currently linked to from anywhere on `example.com`, but it's still hosted on their server. There isn't anything particularly sensitive inside, but the report reveals some other business connections of Example Corp., including some international corporations. Examining the document metadata reveals a few things about the author, including the version of Microsoft Word for MacOS they were using when they wrote it – another detail that might be useful for a technical attack.

So, from the website alone I have an address, contact details, a few leads on convincing pretexts, a number of external partners to probe, some public details about recent projects, some technical details, and a fledgling organisational chart which identifies critical people within Example Corp..

Now let's see what's in the official record. Companies House[4] is a publicly-accessible government database which tracks companies, who must all file annual financial statements, including details of the responsible officers for the company. A search for Example Corp. quickly retrieves their record. The

[4] `https//companieshouse.gov.uk`

overview just tells us some things we already knew about the business sector, address, and that they're up-to-date on their filings, but it does reveal the date of incorporation, which we didn't have before, and which predates their domain registration. Looking at the officers associated with the company gives us much richer information – 7 names are listed, along with their role in the organisation, the date they were appointed to it, their month and year of birth, and their *correspondence address*. Some of the people listed were also on the company website, but some of them weren't mentioned, so we can expand our organisation chart.

More importantly, the correspondence addresses are valuable new information. A couple of people just gave Example Corp.'s office address, but several gave other addresses they could be reached at. Helpfully, Companies House makes it easy to see all records associated with each individual here, so we can actually retrieve several addresses for those officers that have filed as part of other companies. Plugging these addresses into Google Maps quickly lets us assess what we're turning up. A few addresses in London seem to just be offices some of the high-level employees work out of, but several of the addresses turn out to be homes. For example, we can see that Joe Bloggs, listed as an IT Consultant for Example Corp., lives in a quiet suburb in Cheshire – we can even use StreetView to take a look at his house. If he has a driveway, we have a pretty good chance of being able to figure out what his car looks like, which would help us find it in the car park near the office.

Before we get sidetracked, though, let's not forget the primary purpose of Companies House – to record various filings about the company. These are all available for download as PDFs, and contain useful additional information as part of a timeline of Example Corp.'s history – from the first filing, through various changes of addresses for both the company and its officers, including also various legal reorganisations. We can see who the original founders of the company were, and identify those who have resigned, who replaced them, and how shares in the company have been allocated. Some time spent reconstructing these pieces could identify fault-lines in the organisation's internal politics – people who are likely to mistrust one another. It's also worth noting that some of the documents available for download are signed by the current Director – useful if we need to forge his signature on an official document or some sort of approval.

So, we now have a better internal picture of Example Corp., with a timeline we can complement by tracking their mentions in the news and various PR releases – this gives us a solid sense of what's going on in the company and who the key players are. We also have the names and home addresses of several of their key staff. One option we have now is to stage a break-in at one of their homes while it's empty – malware installed on their personal devices has a good chance of making it onto their corporate network, and even if it doesn't we're likely to be able to make use of it for surveillance purposes – watching 'over their shoulder' as they check work emails from home. If all else fails, we could even gamble on critical information being stored locally and

unencrypted, and just steal their personal devices and see if the information my employer wants is on there. But it's not clear that it is, and daylight robbery is a risky business, so let's stick to reconnaissance for the moment.

One thing we can do with an individual's address is look it up in the electoral register[5]. Access to the full register is restricted, but the open register is fairly accessible, and there are a number of companies that provide online access to it, such as 192.com. A free search is enough to turn up the names of the people that live with Joe – in this case just his wife Jane. The names of family members can be valuable for various ploys, from dropping in to casual conversation with other staff to give the impression we're close friends of Joe's, to phonecalls to get Joe away from his desk[6], to outright threats.

Given Joe's status in the company – a founder also listed as an IT consultant – he likely has a lot of access to the sort of information we want, so he's worth continuing to investigate. Searches combining his full name with that of the company turn up a variety of hits. Surprisingly, he's not on Twitter, but he is on Facebook, unearthing a lot of detail about his personal life, friends, interests and other connections. We can also turn up a number of videos of Joe on Youtube, including full-length interviews he's given about Example Corp. – enough footage to train some open-source voice imitation software to a level capable of impersonating Joe over the phone, even when speaking to someone who knows him [8]. Similarly, we find a few samples of his writing, important if we want to send an email "from" Joe to another employee and have it seem authentic – though if we take that route we'd be best off gathering a sample email from him directly by contacting him under a pseudonym with some innocent enquiry.

We could continue down this rabbithole almost indefinitely. For example, if we're focusing on Joe, then it makes sense to investigate Jane as well. A search for both their names reveals that Jane is employed as a secretary for her husband in a private corporation of Joe Bloggs Limited, with its own filing history – an interesting financial arrangement. We could also start to dig through Jane's social media presence, find out the organisations she's a part of – where do they shop? If Jane's part of a reading group, when does it meet? At some point a line needs to be drawn, and we need to return and follow up other leads closer to our original goal, like the other employees whose home addresses we have unearthed, or the recent business partners of Example Corp. we flagged for investigation.

The example above took us from knowing nothing but a company's name to knowing not only a lot about it as a company but also the home addresses, family members, and personal history of one of its senior members, with a lot of leverage to manipulate or impersonate him. If you are wondering whether this works in real life, I caution you: Example Corp. is a *real* example – I actually carried out all the steps I describe above on a randomly-selected

[5] https://www.gov.uk/contact-electoral-registration-office

[6] e.g., "I'm a nurse at X hospital, we've just admitted Jane – she's had a fall. She's okay, but she told us to call you to come pick her up..."

small company, and described the results faithfully (albeit anonymously). Not only is this very achievable, it doesn't even take very long – I spent far more time writing up these notes about the reconnaissance than it took to achieve.

More importantly, the above only touches on some of the most easily-accessible resources. We didn't even get into investigating phone numbers[7], email addresses[8] or image metadata[9]. We haven't looked at enumerating the lower-level employees via LinkedIn[10], and we haven't touched more illicit sources such as searching data breach dumps and carding collections. All of these methods could be used to be used to quickly extend our dossier of data about Example Corp. and the people who work there, including a lot of information they may not realise is available to the public.

3 OPTIONAL EXERCISES

These are suggestions for students who are particularly interested in the topics of social engineering and intelligence-gathering. They are not assessed in any way. You don't need to complete the below to do well on the course.

3.1 *In Practice*

As mentioned in the main body, deceptively eliciting information can be illegal, and you should not attempt it unless you have an explicit agreement in place with the target (e.g., as an employee of a penetration testing company). There is however nothing to stop you researching companies or individuals using public data sources, and seeing what you can find out. If you want, use some of the tools and methods I've discussed to investigate a small-to-medium-sized company – ideally one to which you have no existing connection. Map out the company's history, and see what you can learn about the current employees purely from passive, public sources.

3.2 *Further Reading*

In addition to Mitnick's book [4], Hadnagy's "Social Engineering: The Art of Human Hacking" [5] is a decent read on the practical end of social engineering, though you should try to find a recent edition if you can, as any book about the Internet dates quickly. For OSINT, there are a variety of resources already linked, but for practical instruction one of the best resources is Bellingcat's free online set of guides, available at `https://www.bellingcat.com/category/resources/how-tos/` – they cover everything from Bitcoin and Tiktok to tracking planes and locusts, with many guides even talking you through writing Python scripts to help with the analysis.

[7] `https://github.com/sundowndev/PhoneInfoga`
[8] `https://hunter.io/`
[9] `https://exiftool.org/`
[10] `https://github.com/leapsecurity/InSpy`

REFERENCES

References

[1] IANS, "Cyber-spies used social sites to trick Dalai Lama's office: US expert," *Thaindian News*, 2009, accessed 2020-08-24. [Online]. Available: https://www.social-engineer.org/wiki/archives/Spies/Spies-DalaiLama.html

[2] R. J. Deibert, R. Rohozinski, A. Manchanda, N. Villeneuve, and G. M. F. Walton, "Tracking Ghostnet: Investigating a cyber espionage network," Munk Centre for International Studies, University of Toronto, Tech. Rep., 2009.

[3] T. Brewster, "Androids and iPhones hacked with just one WhatsApp click — and Tibetans are under assault," *Forbes*, 2019, accessed 2020-08-24. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2019/09/24/whatsapp-fakes-hack-tibetan-iphones-and-androids-to-steal-facebook-data-and-more/

[4] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, 2003.

[5] C. Hadnagy, *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, 2010.

[6] B. Everstine, "Carlisle: Air Force intel uses ISIS 'moron's' social media posts to target airstrikes," *Air Force Times*, 2015, accessed 2020-09-14. [Online]. Available: https://www.airforcetimes.com/news/your-air-force/2015/06/04/carlisle-air-force-intel-uses-isis-moron-s-social-media-posts-to-target-airstrikes/

[7] M. Rakuszitzky, D. Romein, R. Dobrokhotov, A. Toler, and K. Anders, "MH17- Russian GRU commander 'Orion' identified as Oleg Ivannikov," *Bellingcat*, 2018, accessed 2020-09-14. [Online]. Available: https://www.bellingcat.com/news/uk-and-europe/2018/05/25/mh17-russian-gru-commander-orion-identified-oleg-ivannikov/

[8] Y. Jia, Y. Zhang, R. Weiss, Q. Wang, J. Shen, F. Ren, P. Nguyen, R. Pang, I. L. Moreno, Y. Wu *et al.*, "Transfer learning from speaker verification to multispeaker text-to-speech synthesis," in *Advances in Neural Information Processing Systems*, 2018, pp. 4480–4490.