Building Attacker Personas in Practice — a Digital Banking Example

Caroline Moeckel
Royal Holloway, University of London
Egham Hill, Egham TW20 0EX, UK
caroline.moeckel.2012@live.rhul.ac.uk

In this short paper, a framework for building attacker personas based on a 10-step process model borrowed from user-centred design is proposed and applied to digital banking. In line with conventional personas, attacker personas are archetypical attackers to a system and ideally characterise the full threat landscape to a system. Benefits of attacker personas are currently seen in the context of generic security awareness programmes, usage by security experts alongside other threat modelling techniques and to 'make threats real' for non-experts in an organisation. However, attacker personas are by no means a mature method in information security—the largest drawback is currently a lack of their integration into threat modelling and the wider security management environment. The research report presented here covers the chosen methodology including data sources as well as the seven attacker personas proposed for digital banking systems. This work is primarily viewed as a basis for discussion to help foster methodological advancement for building better attacker personas in the future. Current limitations as well as potential future research directions are therefore given in the last part of this paper to promote discussion and collaboration with others in academia and industry.

Personas/attacker personas. Information security. Digital banking. User-/adversary-centred design.

1. INTRODUCTION

Over the last decade, personas (representations of a range of archetypical users of a product or system), have become commonplace across offices in the UK, Europe and the rest of the world. While mostly found in 'digital' environments such as start-ups, external or in-house agencies as well as digital marketing departments, persona posters can also be found with support teams or in technical areas.

Interestingly, the situation could not look more different for their security counterparts. Attacker personas, representing a range of archetypical attackers to a given system, have not found widespread uptake in information security or matured significantly as a method to date. However, it is not that there has been no interest in academia or commercial settings. Steele and Jia (2008) directly transferred personas as a user-centred design approach into the security space by proposing 'anti-personas' to embody the behaviour of attackers. The term 'attacker personas' was then further developed in Atzeni (2011) with their report on developing and using attacker personas in a project setting. In his key work on threat modelling (a methodology providing structured approaches to identifying threats in information security), Shostack (2014) also included an example set of attacker personas. There are several assumed reasons for why attacker personas have not gained significant interest from many security professionals to date. It could be that attacker personas are not perceived as useful or effective. This view is supported by the fact that the value of attacker-centric threat modelling (basing threat identification and risk management processes on intelligence featuring attackers primarily) is not well understood currently in information security (Shostack, 2014, p.40). It may also simply be down to a lack of skills or time to build meaningful attacker personas in an organisation.

The aim of this short paper is to provide an accessible and replicable approach to building attacker personas. The intention here is twofold. Firstly, it is intended that the detailed representation of attacker persona examples will help bring the method closer to practitioners. Secondly, it is also hoped that works like this one will help facilitate the dialogue between subject matter experts (both in academia and industry) to discuss further intersections between human-computer interaction (HCI) and security. Digital banking is used as a focus for the attacker personas—this example is expected to be relevant and easy to relate to for a wide audience. The next section will present the chosen methodology, followed by a presentation of results and brief discussion and conclusion.

2. METHODOLOGY

The requirements for an underlying framework for building the attacker personas in this work were as follows. An approach with relatively high levels of formality and guidance to ensure potential replicability, adaption and extension of the method (by the author and potentially others at a later point) was desired. Furthermore, the absence of mature methods for attacker personas specifically meant that a user persona creation method from user-centred design was selected and adaptions to account for attacker personas had to be made.

Based on this rationale, an adapted version of the process model proposed by Nielsen in her works (2007 and 2013) has been used in this research. Nielsen's framework is especially compelling as it provides a relatively formal, sequential approach to persona building. It also incorporates learnings from many key works in persona research (such as e.g. Bødker, 1997; Cooper, 1999, 2007; Grudin and Pruitt, 2002; Adlin and Pruitt, 2010).

While this framework provides useful guidance and structure to the attacker personas building process, a varying level of adaption and flexibility to each step has been employed to make sure the method remains relevant for attacker personas. It is also expected that further adaptions in methodology will be required in the future as this particular project progresses and attacker personas as a method mature further.

2.1 10-Step Attacker Persona Building Process

This section presents the initial 10-step process model proposed for the attacker persona building process, closely based on Nielsen (2007, 2013), but tailored to attackers instead of users. The ten proposed process steps for building attacker personas are presented below:

(i) data collection: finding the attackers;
(ii) building a hypothesis of initial attacker types (hacker taxonomy): identifying differences between attackers;
(iii) verification: adding information relevant to attacker types to accept/reject hypothesis;
(iv) finding patterns: define number of attacker personas and structure of persona set;
(v) constructing the attacker personas: detailed description, e.g. name, photo, biography, characteristics and capabilities;
(vi) definition of attacker motive: preparation of the situation the attacker persona is in;
(vii) validation and buy-in: obtaining acceptance of attacker personas from stakeholders;
(viii) dissemination of knowledge: sharing the attacker personas in the organisation;
(ix) creating scenarios: writing the narrative;
(x) on-going development: review and adjust.

2.2 Data Sources

One of the issues around attacker persona creation is the data they are based on. Without substantial grounding in data on real-life attackers and attacks, attacker personas can become unrealistic, irrelevant and hard to relate to. As Grudin and Pruitt (2002) state in their discourse on engagement through personas, "links between personas and the supporting data should be explicit and salient". Attackers, while they can be considered users to systems (albeit malicious ones), naturally differ significantly from users when it comes to their preparedness to collaborate. After all, they are mostly cybercriminals trying to 'stay under the radar'. This makes collecting primary data at scale difficult, e.g. through interviews or surveys (examples exist, like the Hacker Profiling Project in Chiesa, 2009).

To get around this difficulty, secondary data sources were chosen to inform the presented attacker personas. Over 200 freely available documents containing information about digital banking fraud cases and the attackers involved from three data sets (BCS, 2014; CCCD, 2018; FBI, 2018) were chosen. Where indicated, individual sources were added to expand certain factors and character traits and to help build scenario narratives (see table 1).

A multitude of attacker properties were identified in the data: personal characteristics, group dynamics and social ties, geographical factors as well as usual modus operandi and targets. For persona creation, factors such as age and gender, motivations, resources (funding, equipment and skills), potential insider knowledge, preferred means of attack or modus operandi, functions or position in their group are certainly interesting. Other relevant factors, mentioned less frequently, were for example entry path into criminality, notes on their 'moral code', plans for the future or information on their family or life circumstances.

Table 1: *Overview of data sources and purposes*

Data Sources	**Usage for attacker personas**		
	Main purpose	*Persona profile*	*Persona narrative*
FBI (2018)	*Initial profiling; narrative story*	***x***	***x***
BCS (2014)	*Initial profiling; narrative story*	***x***	***x***
CCCD (2018)	*Initial profiling; narrative story*	***x***	***x***
Additional Reports on cybercrime	*Focus on character traits and story lines*		***x***
Materials related to attacker categories (e.g. blogs, interviews)	*Focus on character traits and story lines also provides direct quotes or statements*		***x***

3. RESULTS: THE ATTACKER PERSONAS

Following the 10-step process using the data sources identified in 2., seven distinct attacker personas specific to digital banking were produced and are shown in figure 1 to the right. Figure 2 below shows an exemplar attacker persona from the set.

Based on the persona types used for user personas in Cooper (2007, pp.104), this attacker persona set makes use of three different types of personas: primary attacker personas, secondary personas and supplemental personas. While all of these represent realistic attacker portraits from the data (Goodwin, 2009, p.275), primary personas form the focus for security design. Designing mitigations against threats posed by them should protect against most of attacks to the system. While secondary attacker personas still pose significant threats to the system, this is usually covered by protecting against primary personas. Supplementary attacker personas do not usually pose a significant threat and are also covered under the security design against primary personas — they will help stakeholders to gain a full picture of the range of attackers encountered.

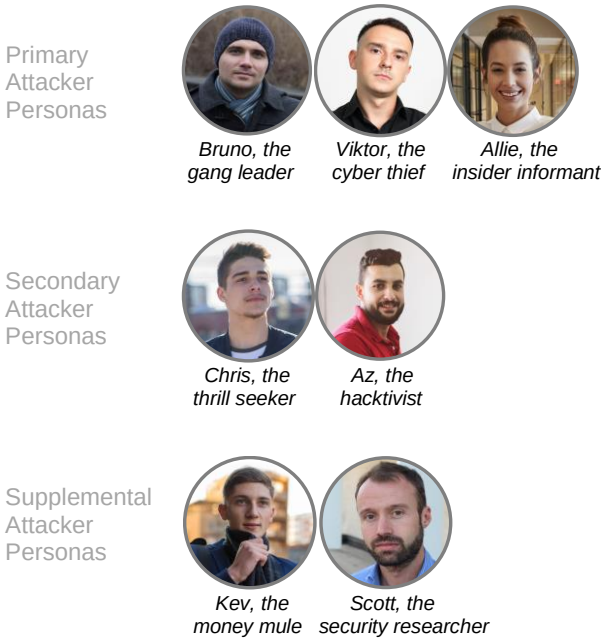

Figure 1: *Attacker personas for digital banking (photographs sourced from Getty, 2018)*

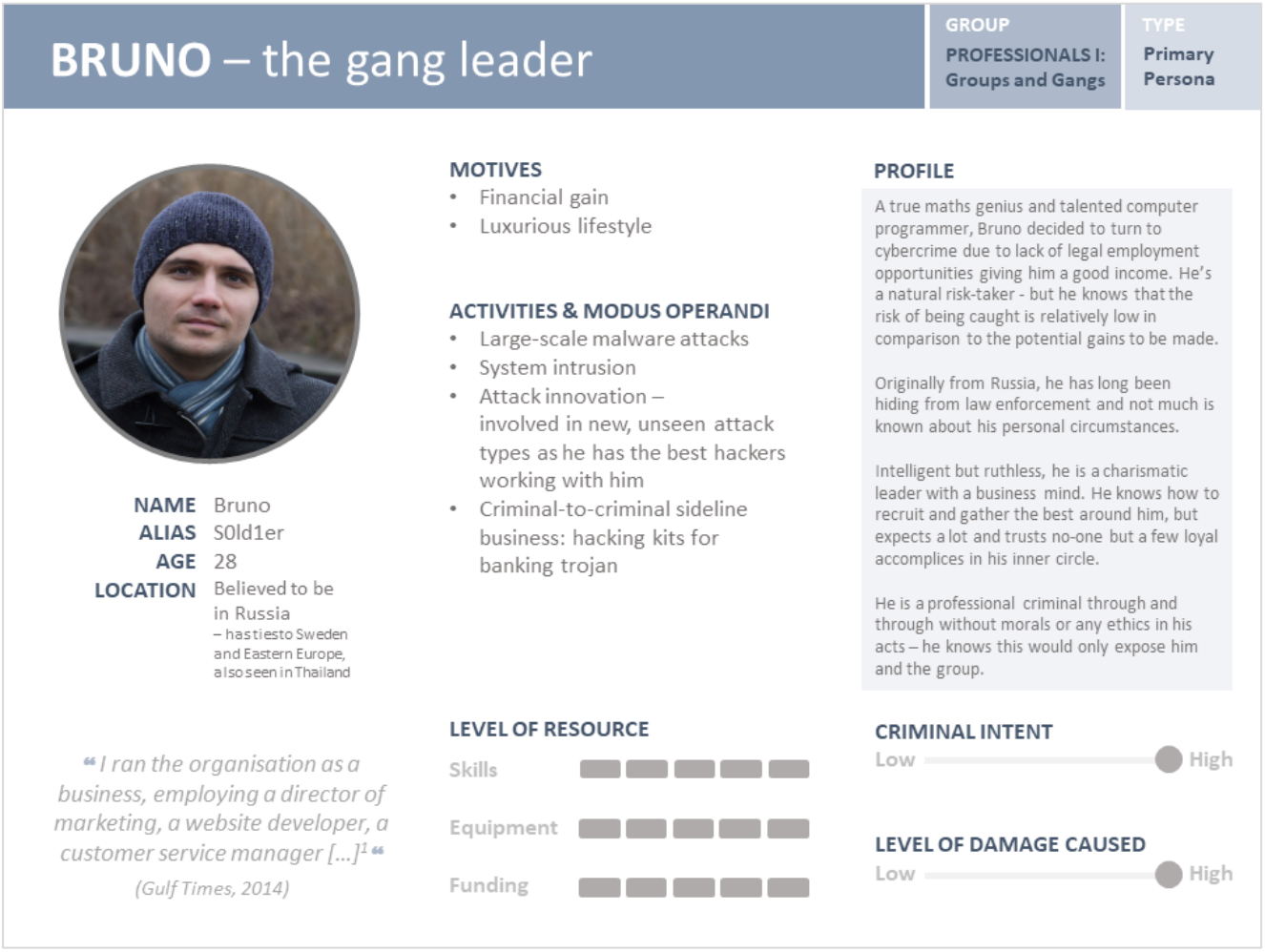

Figure 2: *Persona card for Bruno, the gang leader (photograph sourced from Getty, 2018)*

4. DISCUSSION

4.1 Putting Attacker Personas into Action

Now that the attacker persona set has been defined, it is time to make effective use of them. One element that is crucial to this and has not been covered within the limited scope of this document are scenarios. Placing the attacker personas into the context of a narrative scenario is a key part of their creation**.** For user personas, a scenario will present a concrete story about system use (Carrol, 2000). For attacker personas, they are usually about specific attacks. One attacker persona can therefore have multiple scenarios (attacks) attached to them and these would likely change over time.

Another crucial step at this point is verification of the attacker personas with the potential stakeholders to ensure they are coherent, logical and ultimately convincing and useful to them. For this study, a limited amount of informal reviews with subject matter experts in digital banking security has been completed, with more formal efforts such as group sessions and workshops still outstanding.

Once the attacker personas have been created, initial scenarios and adequate verification efforts have been completed, it is time to communicate them out to the organisation and a wider set of stakeholders**—**this phase is described in great detail as the 'birth and maturation' of a persona set in Adlin and Pruitt (2010 ch.5). Persona dissemination and communication is widely discussed in standard works (such as Cooper, 2007; Goodwin, 2009 or Adlin and Pruitt, 2010) for conventional personas and can be used as a guide for attacker personas.

At this point, the following three main use cases have been identified for attacker personas. Firstly, security experts may use attacker personas to support their daily work routines (Atzeni, 2011). It is important to understand here that, for security experts, focussing threat modelling solely on attackers is not a realistic or advisable approach (Shostack, 2014, p.34-43). However, attacker-centric approaches such as attacker personas may provide valuable support when used in conjunction with other threat modelling approaches. Secondly, "talking about human threat agents can help make the threats real" (Shostack, 2014, p.40). Using attacker personas to illustrate threats can help security teams explain risks to non-expert audiences in product development or management. This can help to build a case for more time or funding for further risk assessments or even changes to the product specification to make the product more secure before it reaches the end user. Lastly, just like user personas may help to build a customer-centric organisation by reminding employees of key users on a daily basis (for example through persona artefacts such as posters), attacker personas can form part of an overall security awareness programme. In an organisation trying to build a proactive security culture, distributing the attacker persona set may help to raise the awareness for potential attack risks every day (see Ki-Aries, 2017).

4.2 Limitations

There are two main drawbacks to this work. Firstly, verification efforts and stakeholder engagement have been limited to date, which raises questions around the validity of the presented attacker personas at this point in time. Secondly, the source materials used have several limitations**—**as they are of secondary nature and often focus on the attack only, they may lack detail regarding the attackers involved. While this has been addressed by using complementary sources (table 1), both points will require further enquiry.

4.3 Future Research Directions

Based on the work conducted here, the following aspects should be considered as starting points for future research efforts. Firstly, methodological refinement and advancement for attacker persona building is required through more practical examples and experimental approaches brought forward**—**this could also provide alternative ways of addressing issues around data sources. Secondly, the question of where attacker personas fit into the overall security assessment and risk modelling ecosystem of an organisation and what value can realistically be expected from them needs to be addressed further. Lastly, approaches for stakeholder verification and collaboration specific to attacker personas need to be devised and tested in practice. This is also likely to be the next iteration for this work.

5. CONCLUSION

This paper has presented an abbreviated step-by-step process for creating an attacker persona set for digital banking systems, closely based on the 10-step process model for user personas by Nielsen. Using publicly available materials on digital banking cybercrime cases, seven attacker personas were created.

While this paper shows that detailed and convincing attacker personas for a specific purpose can be built relatively quickly using elements of user-centred design methods, a range of questions and potential further research directions have arisen from this. Just as advances in methodology and further research examples are required, organisations will also need to define how attacker personas could fit into their overall security management approach. Necessary extensions for this paper include further verification and collaboration with stakeholders as well as refining the existing attacker personas through more specific scenarios.

6. REFERENCES

Adlin, T. & Pruitt, J. (2010) The essential persona lifecycle: your guide to building and using personas. Elsevier.

Atzeni, A., Cameroni, C., Faily, S., Lyle, J. and Flechais, I. (2011) Here's Johnny: a methodology for developing attacker personas. 2011 Sixth International Conference on Availability, Reliability & Security, Vienna, 2011, pp. 722-727.

Bødker, S., & Christiansen, E. (1997) Scenarios as springboard in CSCW design. In S. S. G. Bowker, W. Turner, & L. Gasser (Eds.), Social science, technical systems and cooperative work (pp. 217–234). London. Lawrence Erlbaum.

BCS - British Computer Society (2014) Cybercrime Forensics Specialist Group Briefings. Compiled by Denis Edgar-Nevill (Canterbury Christ Church University), available via group distribution list, 2010-2014.

CCCD - Cambridge Computer Crime Database - Hutchings, A. (2018) https://www.cl.cam.ac.uk/~ah793/cccd.html (16 April 2018)

Carroll, J. M. (2000) Making Use: scenario-based design of human-computer interactions. Cambridge, Mass, MIT Press.

Chiesa, R., Ducci, S. (2009) Profiling Hackers. CRC Press, Taylor & Francis.

Cooper, A. (1999) The inmates are running the asylum. SAMS.

Cooper, A., Reimann, R., et al. (2007) About Face 3.0: The essentials of interaction design. Wiley.

FBI - Federal Bureau Investigation (2018) Cyber's Most Wanted. https://www.fbi.gov/wanted/cyber (16 April 2018)

Getty Images – iStock database (2018) Source for attacker persona images – IDs for purchased images: 82011555, 247519731, 249380561, 125323949, 125705417, 117226075, 249461806, 249461806. https://www.istockphoto.com (16 April 2018)

Goodwin, K. (2009) Designing for the digital age: how to create human-centred products and services. Wiley.

Grudin, J., & Pruitt, J. (2002) Personas, participatory design and product development: An infrastructure for engagement. PDA.

Gulf Times (2014) 80 detained in global cyber-crime takedown. http://www.gulf-times.com/story/392708/80-detained-in-global-cyber-crime-takedown (16 April 2018)

Ki-Aries, D., Faily, S. (2017) Persona-centred information security awareness. Computers & Security. Vol. 70, Sept. 2017, p.663-674. Elsevier.

Nielsen, L. (2007) 10 steps to personas. http://personas.dk/wp-content/LOWRES-Personas-english-version-oktober-200821.pdf (16 April 2018)

Nielsen, L. (2013) Personas - user focused design. Springer.

Shostack, A. (2014) Threat modelling: designing for security. John Wiley & Sons.

Steele A., Jia, X. (2008) Adversary-centred design: threat modelling using anti-scenarios, anti-use cases and anti-personas. International Conference on Information and Knowledge Engineering (IKE 2008). Las Vegas, Nevada, USA, July 14-17, 2008. CSREA Press.