# Archetypal Users—Personae non Gratae (PnGs) Case Study

Nancy R. Mead

Forrest Shull

Krishnamurthy Vemuru, University of Virginia

Ole Villadsen, Carnegie Mellon University

**April 2021**

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.



This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

## Archetypal Users—Personae non Gratae (PnGs) Case Study

### Background

Personae non Gratae (PnGs) represent archetypal users who behave in unwanted, possibly nefarious ways. However, like ordinary personas, PnGs have specific goals that they wish to achieve and specific actions that they may take to achieve their goals. Modeling PnGs can therefore help us to think about the ways in which a system might be vulnerable to abuse and use this information to specify appropriate mitigating requirements.

The PnG approach makes threat modeling more tractable by asking users to focus on attackers, their motivations, and abilities. Once this step is completed, users are asked to brainstorm ideas about targets and likely attack mechanisms that the attackers would deploy. The theory behind this approach is that if engineers can understand what capabilities an attacker may have and what types of mechanisms, they may use to compromise a system, the engineers will gain a better understanding of targets or weaknesses within their own systems and the degree to which they can be compromised. Some critics of this approach argue that a PnG can often take users down the wrong path. For example, for a system related to national security, users might reason that the system may be the target of a sophisticated attack from another nation-state. This conclusion, however, overlooks the fact that a nation-state might compromise a system first through a much simpler entry point and then ratchet up operations from there.

We provide examples of two PnGs in Figure 1. These PnGs were constructed manually for training purposes and target the domain of Electro-Cardio Converters. Each PnG includes an image of the persona, his or her name, a description, the assumed role (e.g., Mechanical Engineer), and a moniker (e.g., Bitter and revengeful). Furthermore, it includes a set of relevant goals and skills, and a set of misuse cases that describe specific ways in which the PnG intends to attack the system [Opdahl 2009]. From this, we can construct a threat model that includes the actor (i.e., the PnG) and the attack mechanism and target specified in the misuse cases. Attack intent is provided in the general description.

A different set of examples is provided in the Example Solution section.

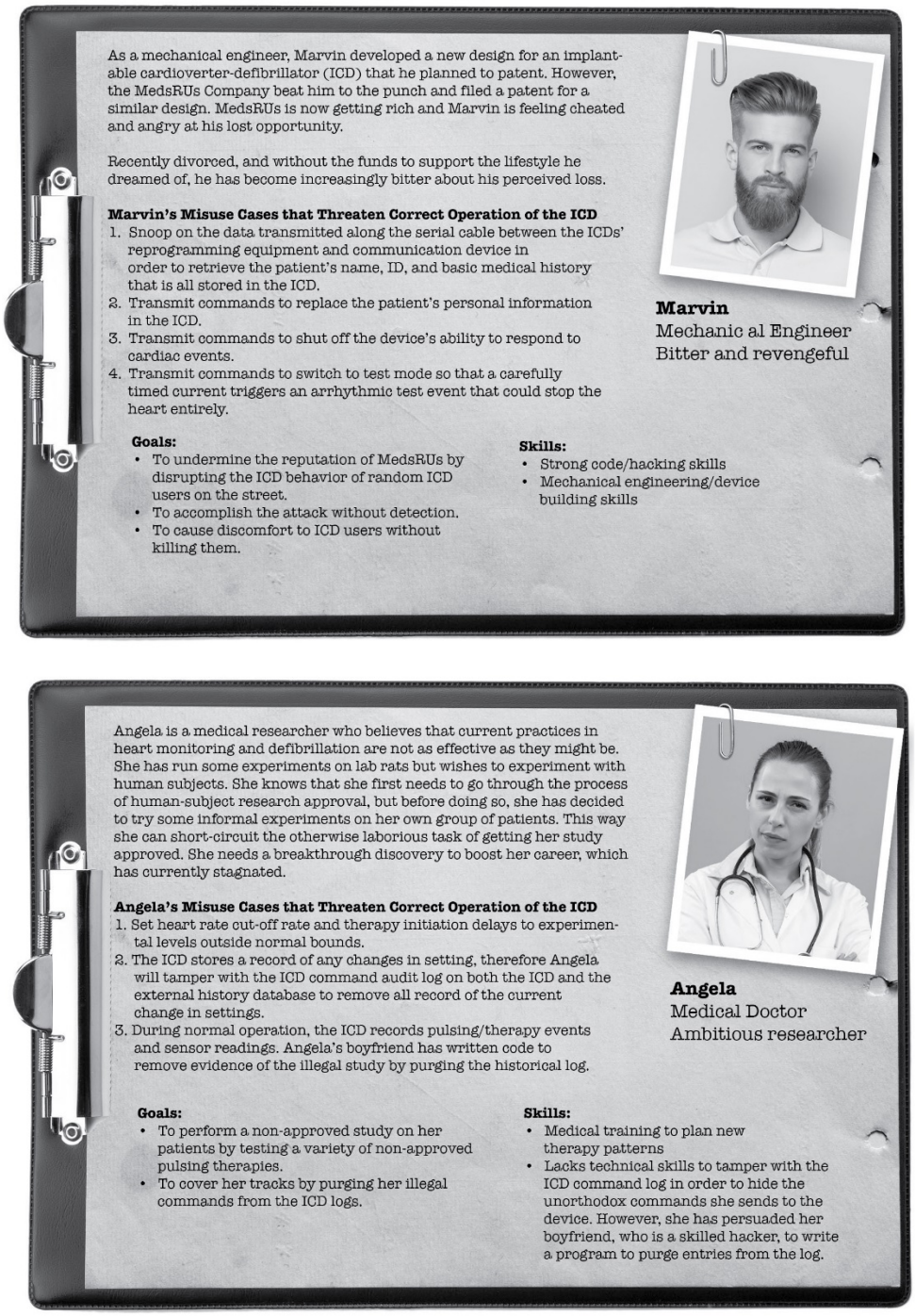


*Figure 1: Two Personae Non Gratae*

We asked students in two introductory information security courses, one undergraduate and the other graduate, to work in teams of three to four people to construct PnGs for one of two systems [Shull 2016b]. Here we focus on one of these systems, which utilized unmanned aerial vehicles (UAVs) to perform a rescue mission. The drones could carry payloads such as emergency supplies and were capable of autonomous operation if communication with the base station was lost. Each scenario was described in a two-page document that represented very early ideas for

each of the projects. Goals, major constraints, and high-level designs were provided, but not the lower-level implementation decisions.

We used crowdsourcing in conjunction with PnG to enhance the results. Mead describes the crowdsourcing part of the study [Mead 2017].

## Case Study Overview

A persona provides a realistic and engaging representation of a specific user group. It is typically depicted through a representative image and a personal description that portrays something about the psyche, background, emotions and attitudes, and personal traits of the fictitious person [Putnam 2012, Nielsen 2013]. The task of creating a persona usually involves surveying and inter-viewing users, identifying optimal ways for slicing users into categories, collecting data to demonstrate that the proposed slices create distinguishable user groups, discovering patterns with-in the user groups, constructing personas for each group, and then creating scenarios describing how the persona might interact with the system under development. A project will typically have about five to eight personas.

## Student Instructions

Complete the PnG example you have been given, until you have a complete profile including the PnG description, goals, skills and misuse cases. Discuss the likelihood of the misuse cases and prioritize them accordingly.

## Instructor notes

The instructor could introduce PnG exercises to the students gradually. For example, after explaining the method and giving the students some examples, you could start by giving the students the PnG description, Goals, and Skills, and ask the students to construct the misuse cases, and discuss how likely they are. For a more advanced exercise, the students could be given only the PnG description, and asked to identify the likely Goals, Skills, and Misuse Cases, and then discuss the likelihood and prioritize accordingly. This is best done as a team exercise as there is an element of brainstorming, and different students are likely to have differing ideas of priority. These could either be homework or classroom exercises, but they are not likely to occupy significant parts of a semester.

## Example Solution

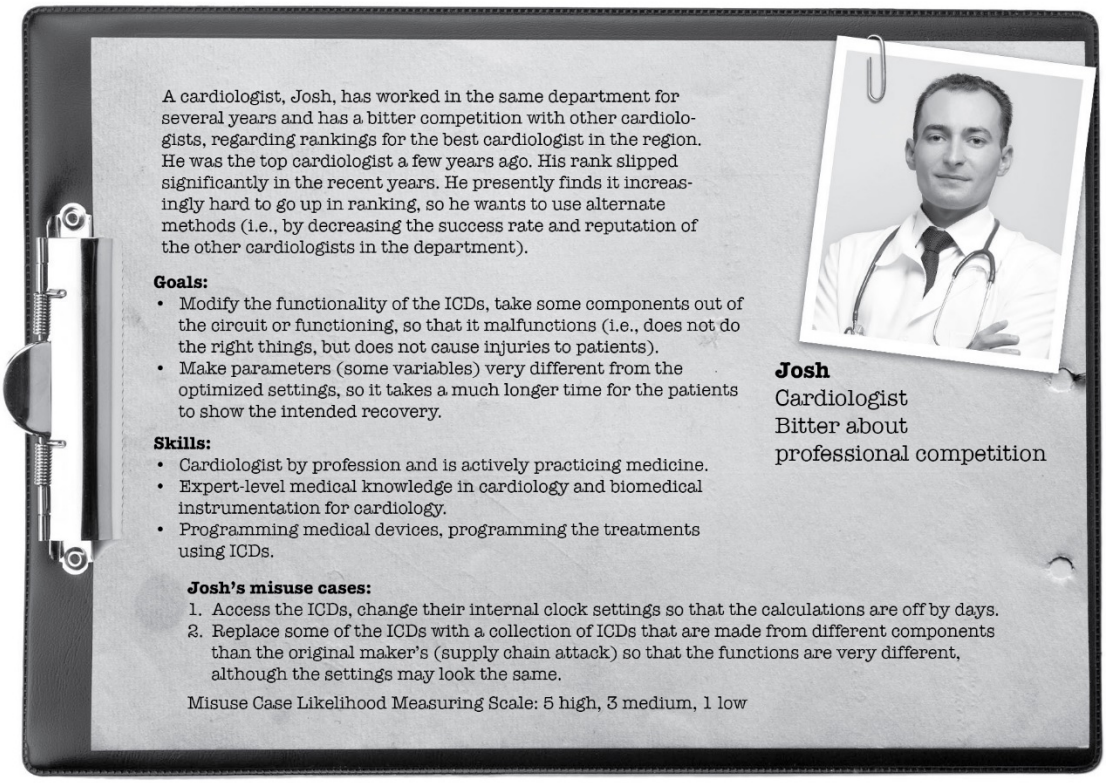


*Figure 2: PnG Competing Cardiologist*

### Misuse Cases

The PnG profile in Figure 9 lists the following Misuse Cases:

1. Access the ICDs, change their internal clock settings so that the calculations are off by days.
2. Replace one of the ICDs with a collection of ICDs that are made from different components than the original maker's (supply chain attack) so that the functions are very different, although the settings may look the same.

### Misuse Case Discussion: Case 1

How likely is this case?

Let us take a look at the function block diagram of a typical implantable cardioverter-defibrillator (ICD):

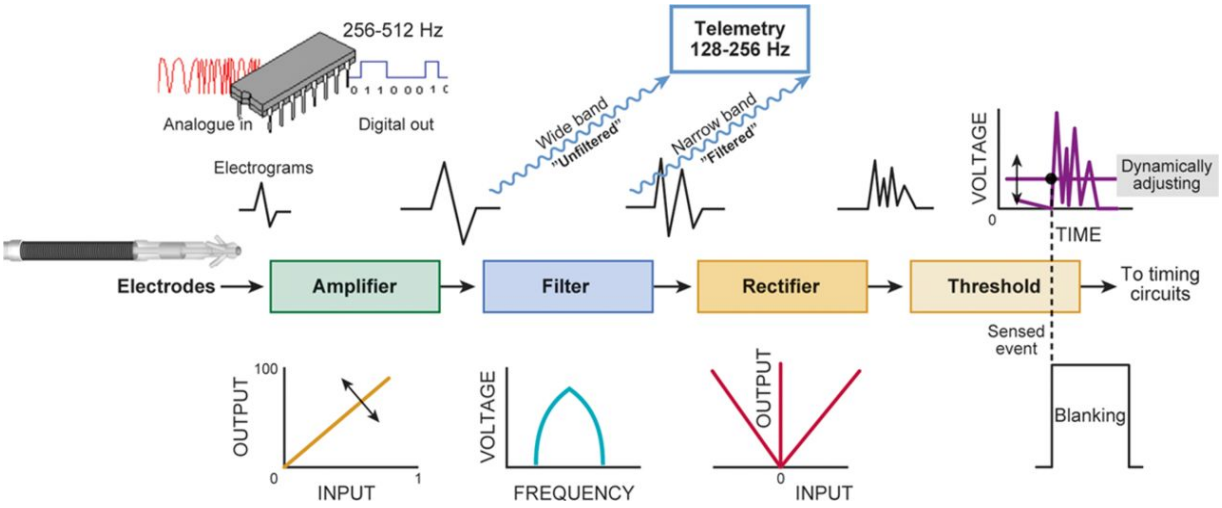


*Figure 1: Functional Block Diagram of ICD*
*(Source: [Swerdlow 2014] http://circep.ahajournals.org/content/7/6/1237.figures-only)*

Looking at the block diagram, one can imagine that the clock has a range of frequencies. By changing the frequency (i.e., making it different from what is initially set up), one should be able to modify the pulse patterns.

We can also see that there are several ways the ICD's performance can be modified from its intended operation.

Alternate modes of attack on the ICD: Change the amplifier gain, filtering parameters, rectifier parameters, change threshold.

Based on these vulnerabilities, which are not difficult to implement (if the attacker gets some time to play with the ICDs, then he could make the changes), we can easily give a high score of 4-5 for this misuse case.

What should the defender do to be prepared, and how much might it cost?

Consider some pulse shape verification algorithm or real-time pulse shape display so that the internal function of the chip can be continuously monitored to prevent a potential attack. The features are some minor changes in the programming, so it should take some time, but not too much cost if there is an internal IT team.

## Misuse Case Discussion: Case 2

How likely is this case?

The block diagram shows that the ICD has three main components. It is most likely that these three components are integrated in a single chip. If this is the case, then the chip can be replaced with a duplicate one that has similar components—but its gains, filter, and rectification circuit are designed differently, so that the pulse shape is different.

Considering that the complexity of designing a chip that performs similar function as the original one involves manufacturing of a new chip, we can assign the likelihood as 2-3.

What should the defender do to be prepared, and how much might it cost?

The physician should be advised to physically examine each ICD internally to make sure the components are not compromised. If this is not possible for the physician, then an electronics engineer can do the inspection before the device is implanted into the patient. This additional protocol should not cost extra, it only requires planning to have the electronics engineer be present at the time of installing the ICD.

For additional reading on secure ICD programming, see the review article by Biffi [Biffi 2014].

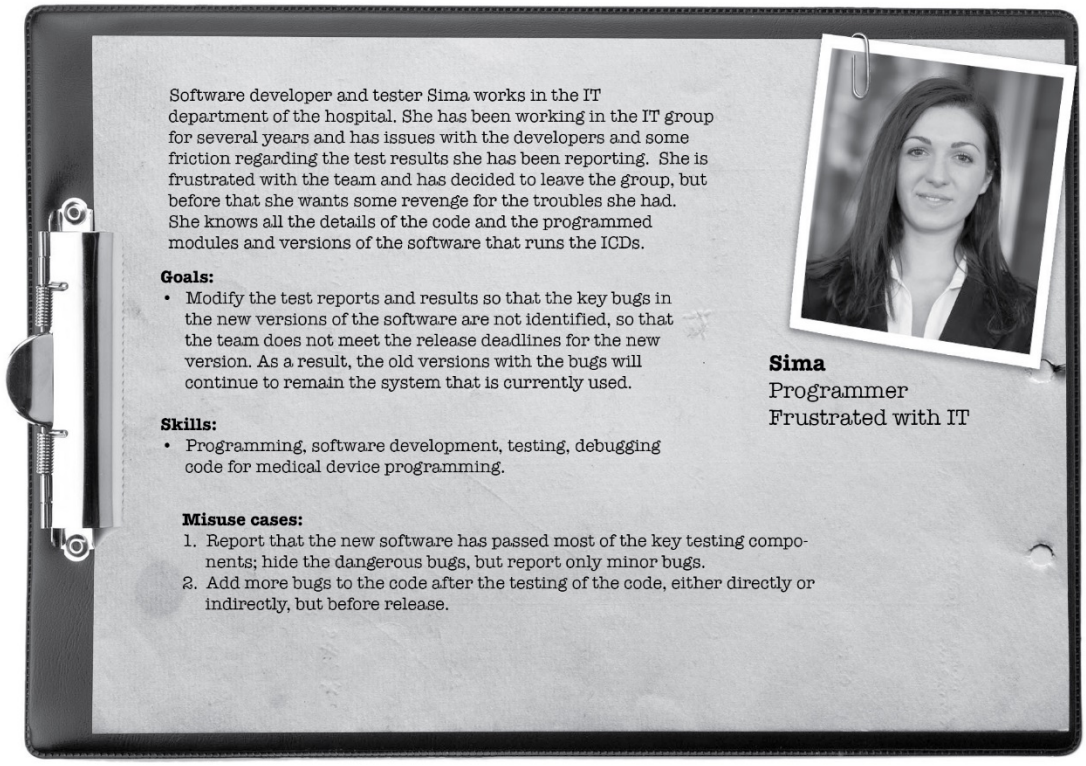


*Figure 32: PnG Software Developer and Tester*

## Misuse Cases

The PnG profile in Figure 3 lists the following Misuse Cases:

1. Report that the new software has passed most of the key testing components; hide the dangerous bugs but report only minor bugs.
2. Add more bugs to the code after the testing of the code, either directly or indirectly, but before release.

## References


Biffi, M. ICD Programming. *Indian Heart Journal*. Volume 66. S88-S100. January, 2014. DOI:10.1016/j.ihj.2013.11.007.

Mead, Nancy; Shull, Forrest; Spears, Janine; Hiebl, Stefan; Weber, Sam; & Cleland-Huang, Jane. Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling. Pages 404–409. *IEEE International Requirements Engineering Conference Proceedings*. September 2017. DOI 10.1109/RE.2017.63.

Mead, N. R., Shull, F., Vemuru, K., and Villadsen, O. "A Hybrid Threat Modeling Method." *Carnegie Mellon University Software Engineering Institute*. 2018. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf

Nielsen, L. Personas – User Focused Design. *Human-Computer Interaction Series*. Volume 15. Springer, 2013.

Opdahl, A. L. & Sindre, G. "Experimental comparison of attack trees and misuse cases for security threat identification." *Information & Software Technology*. Volume 51. Number 5. 2009. Pages 916–932. 2009.

Putnam, C.; Kolko, B. E.; & Wood, S. Communicating about users in ICTD: leveraging HCI personas. *Proceedings of the Fifth International Conference on Information and Communication Technologies (ICTD 2012)*. Atlanta, Georgia. March 2012. Pages 338–349.

Shull, F. & Mead, N. Cyber Threat Modeling: An Evaluation of Three Methods. *SEI Blog*. November 11, 2016. https://insights.sei.cmu.edu/sei_blog/2016/11/cyber-threat-modeling-an-evaluation-of-three-methods.html