Even the Enemy is Not the Enemy

Adam Shostack

Shostack + Associates
adam@shostack.org

Abstract. In the paper which provides the theme for this event, Sasse and colleagues make the case that the user is not the enemy. In this paper, we extend that idea and argue that in several important ways, that even "the enemy" is not the enemy. Those include the human-centric reality that most people don't see their use of computers as adversarial, that understanding enemies is harder than it seems, and that even success in thinking about enemies may not lead to the secure systems which we aspire towards.

1 Mental Models Rarely Include Enemies

Computers are tools that people use to accomplish an astonishing variety of tasks, including both work and personal goals. As they do so, they struggle with a variety of challenges such as usability, fitness for purpose, and competition for their attention. A combination of news stories, folk tales, and awareness training leads to some knowledge that bad things can happen on the internet. Those things are of varying salience during tasks, and attackers look for ways to mimic the normal flow of emails, text messages, phone calls, and other activations in ways leading to people being in a scenario which seems familiar enough so they slip (do the wrong thing) or make mistakes (execute the wrong task for the situation.)

Clinically, paranoia is defined as a pervasive pattern of distrust and suspicion of others. Most people aren't thinking about security, never mind enemies, most of the time. Even when they do, Wash has shown that their models are generally simplistic [3].

Sophisticated models of attacker behavior are rare. A sophisticated model might include awareness of attacker groups and their associated "TTPs" (tactics, techniques and procedures, or what and how they attack). These models are associated with "threat intelligence" a subset of "operational security," a subset of cybersecurity or information security. Thus a subset of a subset of a relatively small profession.

2 People Don't Consider Enemies as They Work or Live

Most people's daily lives are not consumed with enemies either in work or in life. They may identify with a sports team with *rivals*, they may use violent metaphors like crushing the competition, but declaring that we're literally going to crush the competition would be horrifying. In work, we want to help people, serve them, feed them, and the like. In life, we want to connect, build relationships and families, and have meaningful experiences. Enemies rarely make an appearance.

Once they grow beyond childhood, people don't generally self-conceptualize as soldiers, policemen, heroes or others with enemies. In fact, some people will resist actively being assigned those roles: "I'm not here to be a cop" or "I don't come to work to play soldier." Much has been written on how gender is highly correlated with perceptions of military, warrior or ninja motifs in security teams.

Of course, some people do choose to work as soldiers, police or other such roles. They are not quite 'exceptions which prove the rule,' but they are unusual.

3 Understanding Enemies is Hard

Much threat modeling advice used to start from either "think like an attacker" or "make a list of adversaries." This led to (at least) two types of mistakes: The wrong adversaries were listed (or the right ones were not), or the adversaries goals, tactics, or behaviors were misunderstood. These errors, combined with the fact that the step added little practical value, and the realization that enemies might change through a product's lifetime, led to alternative approaches to threat modeling [5] [4].

The challenge of fully understanding and predicting what an enemy will do is tremendous. Famously, the CIA failed to predict perestroika. (For a CIA-friendly rebuttal, see [2]) In an extensive interview, President Obama said the United States had underestimated the impact of tribalism in Libya [1]. If the entire US government advising the President can make that mistake, it seems unlikely that a normal user — or even a skilled defensive team at a commercial entity — will routinely get it right.

4 Securing Systems Doesn't Rely on Enemies or Understanding Them

Early work in computer security was funded by militaries and intelligence agencies, and a focus on enemies came along with that.

But other types of engineering don't center enemies or even risk. To build a bridge, we start from a span we'd like to cross, and continue with the goals for the crossing (people, cars, trains, etc.) We might consider adversaries after things like weather and earthquakes, but most bridges are not designed to resist a military assault. There are many sources of metaphor for building security,

including engineering or public health, which avoid treating the people as the enemy.

Ironically, as I was writing this paper, I got a warning from Microsoft Word[1]:

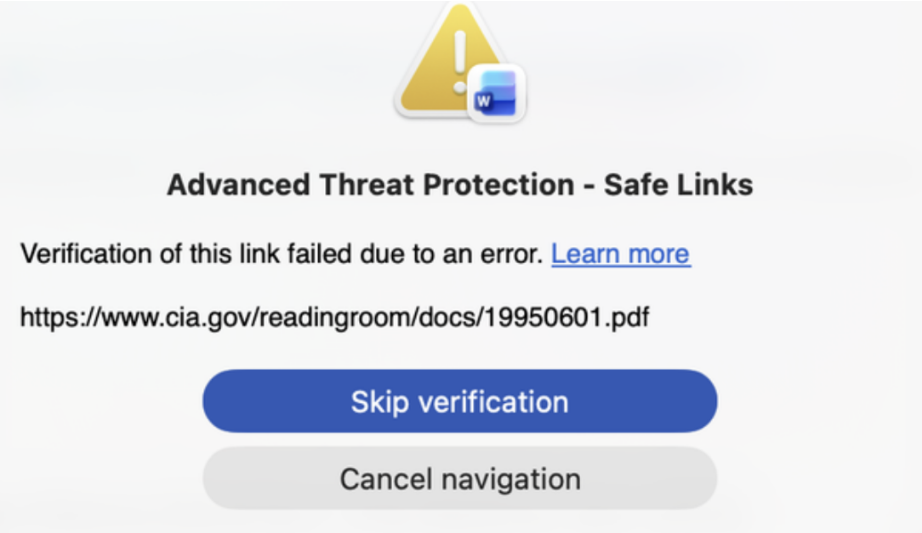

Fig. 1. Example of a figure caption.

Whatever problem triggered this interruption, the warning is inscrutable. It's the sort of error that Angella Sasse has taught us to notice and critique — and even how to do better.

5 "The enemy is my friend"

There are parties, including governments and software companies, who want you to focus on enemies. Militaries and spy agencies want you to focus on enemies because that's core to their worldview. Similarly, some large software companies enjoy talking about criminals and nation states either because they have an adversary-centered view of the world, or, more cynically, because their software has frequent security flaws and they'd like us to focus our attention elsewhere.

[1] The useless support article is here: https://support.microsoft.com/en-us/topic/what-to-do-when-you-are-blocked-from-a-site-and-believe-the-result-is-mistaken-6f41d3fd-55d3-467e-a5a4-49da4132bb9c ; even the support article is a waste, with a trailing GUID that screams "this is not a place for usable security! All are cursed who try to understand this article!"

6 Conclusion

Not treating the user as the enemy, but rather as a human being, navigating a difficult system, subject to constraints and pressures, has been not only a theme of Angela Sasse's work, but an inspiration to me and others.

It's a theme she's had to fight for, because — as she has illuminated — thinking about enemies is a pervasive mistake.

References

1. Goldberg, Jeffrey. "The Obama Doctrine." The Atlantic, Apr. 2016, www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/.
2. Lundberg, Kristen, CIA and the Fall of the Soviet Empire: The Politics of "Getting It Right" https://www.cia.gov/readingroom/docs/19950601.pdf
3. Wash, Rick. "Folk models of home computer security." Proceedings of the Sixth Symposium on Usable Privacy and Security. 2010.
4. Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.
5. Shostack, Adam. "Experiences Threat Modeling at Microsoft." MODSEC@ MoDELS 2008 (2008): 35.