1 | AT&T Hacker ”Weev”

1.1 | What are the ethical choices people faced? What, if any, actions would you consider unethical? Why?

Auernheimer faced a couple of choices: primarily there was a choice of how he wanted to report this information and a choice of whether or not he should actually act on the vulnerability and fetch all the emails. I think reporting the bug to Gawker rather than privately contacting AT&T was somewhat unethical as it didn't provide the company a chance to properly respond, although I can understand why he might've preferred it (AT&T could sweep it under the rug, but not if it's public). I also think actually collecting all of the emails once he was aware of the vulnerability was unethical and didn't contribute to any possible investigation of the vulnerability.

1.2 | What, if any, actions in this story do you think should be illegal? What actions are actually illegal? Specify laws that might be relevant, even if no one was caught or prosecuted.

The relevant laws are mainly identity fraud and conspiracy to access a computer without authorization. I think the act of actually using another iPad's ICC-ID to get an email should be a crime, as it is fraud. This action was actually illegal.

1.3 | What things do you think the people involved could have done to achieve their goals while staying within legal and ethical bounds?

Privately contacting AT&T once the exploit was known and then working to resolve it would have been the most legal and ethical course of action. Even better would be to create another AT&T account and test the ICC-ID authentication for that one so that nobody would have their privacy breached.

1.4 | What would you consider appropriate punishment? If relevant to your story, how does that compare to the punishments that were handed down?

I would consider a misdemeanor and maybe a short amount of jail time plus community service to be a just enough punishment - the blame is primarily on AT&T for negligence. The actual punishment was three and a half years in prison, which is substantially more severe.

1.5 | What are the technical lessons that can be learned to improve security

Ensure that authentication systems for private data are rigorous and not easily exploitable. A script should not be able to successfully fetch information.

2 | Stuxnet

2.1 | What are the ethical choices people faced? What, if any, actions would you consider unethical? Why?

Nation states like the US faced the choice of how they wanted to use viruses in wartime, and the choice to target public utilities was somewhat unethical because it had the potential to hurt innocent people and it inspired variants that caused more damage.

2.2 | What, if any, actions in this story do you think should be illegal? What actions are actually illegal? Specify laws that might be relevant, even if no one was caught or prosecuted.

Usage of computer viruses to intentionally decieve and compromise nuclear power plants should be illegal on a domestic scale, and to some extent an international one. Attacking critical resources like hospitals or power utilities is unethical and should likely be a war crime. None of these have been established as international law yet, so there aren't any relevent laws.

2.3 | What things do you think the people involved could have done to achieve their goals while staying within legal and ethical bounds?

Targeting military encampments and bases or solely nuclear utilities would've been better to an extent as it wouldn't push boundaries of warfare as much.

2.4 | What would you consider appropriate punishment? If relevant to your story, how does that compare to the punishments that were handed down?

I don't think this deserved punishment, and it did not recieve any.

2.5 | What are the technical lessons that can be learned to improve security?

Public utilities need competent cybersecurity and need to be prepared for external threats. Glue your USB ports. Minimize internet connectivity in critical portions of utilities.

3 | Reflections.

See Code of Conduct.