Ethics Case Study:
Alleged In-Flight Hacking

Paul R Phillips

2018–03–11

Articles

Stout, David. ”Feds Probe Security Expert Who Claims to Have Hacked Numerous Flights.” Time, 18 May 2015. Accessed 11 Mar. 2018.

Moyer, Justin W. ”Hacker Chris Roberts told FBI he took control of United plane, FBI claims.” The Washington Post, 18 May 2015. Accessed 11 Mar. 2018.

”White Hat Hacker.” Technopedia. .

Shahani, Aarti. ”FBI Probes Hacker's Claim He Took Over Plane's Engine Controls.” NPR, 19 May 2015. Accessed 11 Mar. 2018.

”Is It Possible For Passengers to Hack Commercial Aircraft?.” WIRED, edited by Kim Zetter, 26 May 2015. Accessed 11 Mar. 2018.

Krehel, Ondrej, and Darin Andersen. ”At what point do white hat hackers cross the ethical line?.” Network World, 14 Aug. 2015. Accessed 11 Mar. 2018.

Introduction

Hacking has become an important component to developing security systems for technology. It is easy to associate the word hacking with individuals who seek to steal, manipulate, and exploit information. In reality, there are individuals who hack as a profession in order to help test security systems. Techopedia defines a white hat hacker as a computer security specialist who breaks into protected systems and networks to test and asses its capability. These specialists use the same methods offenders would use (i.e. black hat hackers) in order to mimic potential attacks. There are ongoing arguments on the topic of where to draw the line on what is considered ethically acceptable for these specialists and what is not (Krehel and Andersen, August 2014). One side of the argument of what is considered ethical can be derived from human intention; that is, if an individual did not cause harm or steal information, then his or her course of action should be treated as ethically acceptable. Although, question is raised to this logic with the case of an individual by the name of Chris Roberts who was caught hacking into an active Boeing 737 during flight (Krehel and Andersen, August 2014).

Case

The issue was first publicized when Chris Roberts, employee on One World Labs, which is a security intelligence firm in Denver, tweeted about playing with United Airlines planes in-flight entertainment and crew-alerting system on April 15, 2015. Upon his landing federal agents had been waiting for his arrival. He was questioned, and a portion of his equipment was seized. Chris Roberts told the FBI during his investigation that he has compromised commercial flights during 15 to 20 occasions from 2011 to 2014 by hacking in-flight entertainment systems (Moyer, May 2015). Essentially Roberts was able to allegedly access the plane system via ethernet by popping off the cover to an electronic box located below each passengers seat (NPR, May 2015). Once he connected his laptop to this box he was able to gain access to the entertainment system, then find his way to the navigation system. During one occasion Roberts was allegedly able to access a planes navigation system and caused the craft to veer sideways briefly mid-flight. The FBI obtained a search warrant after Roberts mentioned these capabilities. FBI Special Agent Mark Hurley wrote in his warrant application, He stated that he thereby caused on of the airplane engines to climb resulting in a lateral or sideways movement of the plane during one of these flights (Moyer, May 2015). Roberts response to the FBI investigation was tweeted, Over last 5 years my only interest has been to improve aircraft security. Given the current situation Ive been advised against saying much (Moyer, May 2015). Though this investigation has gained widespread attention, there are doubts publicized on whether this procedure is actually possible to begin with.

Public Analysis

During a discussion between Renee Montagne (NPR Host) and Aarti Shahani (NPR technology reporter), Shahani mentions that law enforcement officials have told NPR

> there is no credible information suggesting that he in fact did this (NPR, May 2015).

Other private security researchers agree to this statement along with an individual who consults cybersecurity for a large airline (NPR, May 2015). This individual mentioned that that in-flight entertainment is typically segmented from the control networks for motion (NPR, May 2015). Another individual interviewed by NPR pointed out that software has to constantly be patched, therefore if a patch was never performed to segment this software from other systems it may be possible to access. During an interview between WIRED and David Soucie, a former investigator with the Federal Aviation Authority, Soucie mentions this scenario could only occur if the planes autopilot is not engaged. Planes are designed to maintain balance with respect to thrusts projecting from plane engines (Anderson, May 2015). Soucie mentions during his interview while autopilot is engaged:

> you can shut one engine down and keep the other at full throttle and it wont flip the plane over or fly sideways (Anderson, May 2015).

Essentially if the autopilot feature is engaged during flight and a sudden increase in thrust were to occur in one of the planes engines, the plane would simply correct itself to stay on course. Soucie also mentioned that if the autopilot were disengaged, then a thrust could cause one of the wings to dip (Anderson, May 2015). Soucie further commented

> You would really have to change the throttle, where the passengers would really notice it, to pull it off course (Anderson, May 2015).

Reviewer Analysis

Although there is controversy over the possibility of Roberts being able to accomplish his claims, this case still raises some ethical concerns. If Roberts did in fact hack into planes during flight there are issues that lie with how he conducted his methods and what he was capable of doing with the access he allegedly gained. Initially United Airlines did not consent to having their systems evaluated by Chris Roberts. There was not a nondisclosure agreement created between Roberts and United Airlines for this work. In fact, if he indeed took control of the plane without such consent Roberts could face plane hi-jacking charges. Also, he allegedly performed his methods in an unsafe work environment. There were other civilians on this plane, who also did not consent their involvement in his experiments. These actions are an invasion of privacy on multiple levels. His actions, though did not seem to be harmful, could place him in a position which could have jeopardized not only his life, but the life of every person on that plane. Hacking is an important profession with respect to improving security, there must be limitations to what is considered acceptable white hat hacking.