Chapter 6: Case Studies in Risk for UAS

This chapter illustrates the material presented in Chapters 4 and 5 using case studies. These cases are drawn from news reporting, with sources provided.

Student learning objectives. After reading this chapter, students should be able to do the following:
— Apply pragmatic risk analysis to operational decisions;
— Understand the benefits of studying the history of how things go wrong; and
— Appreciate the integration of security and intelligence.

Case 1: When the Enemy Hacks Your Data Stream

On February 23, 2016, Israeli authorities arrested a Palestinian on suspicion of hacking into Israeli drones.[43] Details of the case are meager, but it appears that Majd Ouida, 22 at the time of his arrest, had managed to breach protections and obtain access to Israeli surveillance data from the drones from 2011 to 2014.[44] Alternatively, he may simply have just collected the transmissions using appropriate antennas and processing technology; they are broadcast, after all. As David Axe pointed out, "what's really impressive is the fact that Israeli authorities caught him allegedly doing so. That's because there's no straightforward way to know whether someone has intercepted your drone video."[45]

The question that bubbles up to the top is: "how did the Israelis know that their data was being collected by unauthorized people?" This is a classic confidentiality detection problem. When secrets have been stolen in physical form, at least the physical artifact is missing. But when a copy is surreptitiously made, or a conversation is overheard, how can you detect that your secrecy has been compromised? Think back to the example of the competitor's pricing strategy in Chapter 5. If someone snuck into the building and took a photo of the strategy, how would the competitor know that their secrecy had been violated? If no detection capabilities were in place, such a theft might remain undetected indefinitely.

There are ways to detect violation of confidentiality, but most of them must be engineered into an enterprise before the compromise occurs. These include both technical and procedural solutions. Identifying the potential for secrecy compromise is an important first step. This scenario is where attack/defend exercises are valuable. Challenging a red team to figure out how to access the information collected by a sensor will reveal interesting weaknesses and opportunities to engineer solutions. Questions to consider:

- ❑What are the tactical implications for the adversary having access to your surveillance data?
- ❑What are the strategic implications of the adversary having access to your surveillance data?
- ❑How would you design an attack/defend exercise to focus on confidentiality compromise?

[43] Gross, Judah Ari et al. (2016) Israel charges Islamic Jihad hacker for spying on IDF drones. Times of Israel, 23 March 2016. Available online at https://www.timesofisrael.com/israel-charges-islamic-jihad-hacker-for-spying-on-idf-drones/
[44] Ben-Yishai, Ron. (2016) IDF's cyber defense easily breached. Ynet News, 23 March 2016. Available online at https://www.ynetnews.com/articles/0,7340,L-4782445,00.html
[45] Axe, David. (2016) How Islamic Jihad Hacked Israel's Drones. The Daily Beast, 25 March 2016. Available online at https://www.thedailybeast.com/how-islamic-jihad-hacked-israels-drones

- ❑How would understanding the intelligence efforts of an adversary help you to understand which weaknesses to focus on?
- ❑What surveillance efforts are available in discovering the compromise of secrets?
- ❑What are the costs and benefits of implementing cryptography for broadcasts from drones?
- ❑Could you use this known compromise as a way of inserting misleading information into the adversary's decision processes?

Case 2: When Your Drone Goes Missing

Unmanned Aerial Systems (UAS) are, by nature, unmanned. This implies the control of the system, such as navigation, is comprised of some combination of remote control and autonomous pre-programmed decision. In the event of loss of remote connectivity, the UAS is typically provided with a set of pre-programmed safe landing sites that conform to its mission profile.

When a UAS is sent into hostile territory, one foreseeable risk is the adversary may attempt to shoot it down. Another foreseeable risk is capturing the UAS, either in whole or in part.

This happened in December 2011, when Iran captured and displayed, to great propaganda fanfare, a surveillance drone operated by the U.S. The drone, a Lockheed Martin RQ-170 Sentinel, had been operating over Afghanistan near the Iranian border. The Iranians claimed that they captured the RQ-170 through cyber warfare means. They later claimed that that they were able to decode all the stored data from the RQ-170 sensor systems. Various claims have been made by both the US and Iran on how the capture was made and under what circumstances. These claims include GPS spoofing, cyber intrusion into the control system, and physical damage. The US demanded the return of the RQ-170. Iran countered those demands by alleging that Iranian airspace had been violated and that international laws had been violated. By 2016, Iran claimed to have reversed engineered the design of the RQ-170 and created their own version. The event remained in the news for several years.[46]

Questions remain; did the drone fail or was it intentionally brought down? One possibility is the RQ-170 failed in flight and crash landed in an area where Iranians recovered it before friendly forces could. The question of what caused the failure is somewhat tangential. Did the system simply die? Were navigation systems were compromised? Was there some sort of physical damage to the aircraft?

[46] Sources for this material include the following:
Wikipedia. (2018) Iran–U.S. RQ-170 incident. Available online at https://en.wikipedia.org/wiki/Iran–U.S._RQ-170_incident. Last edit date when accessed 1 July 2018.
Peterson, Scott. (2011) Downed US drone: How Iran caught the 'beast'. Christian Science Monitory, 9 December 2011. Available online at https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast
Cenciotti, David. (2016) Iran unveils new UCAV modeled on captured U.S. RQ-170 stealth drone. The Aviationist, 2 October 2016. Available online at https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modeled-on-captured-u-s-rq-170-stealth-drone/
Opall-Rome, Barbara. (2018) Israel Air Force says seized Iranian drone is a knockoff of US Sentinel. Defense News, 12 February 2018. Available online at https://www.defensenews.com/global/mideast-africa/2018/02/12/israel-air-force-says-seized-iranian-drone-is-a-knockoff-of-us-sentinel/

An obvious question that arises is, "why was there no self-destruct capability embedded?" After all, if you expect to fly near or over hostile territory, then there must be a remote risk of capture. Refer to history for risk analysis; The U-2 piloted by Francis Gary Powers, shot down by the Soviet Union in 1960. The U-2 had the hallmarks of stealth (extreme altitude) and risk was considered low. But even so, it was shot down.[47] An auto-destruct system could have been triggered remotely when it was determined that the system was not in friendly control. Alternatively, a destruct mechanism could be logically triggered by lack of signaling, an extended period without authorized contact could be used as a triggering event for auto-destruct.[48]

Since no system is perfect, alternatives to such a capability for self-destruction should be considered as well. In this line of analysis, more questions come to mind. "What security controls were in place to detect the compromise of the sensitive data and equipment?" and "when detected, what reactions were engineered into the system to reduce the risk of data and equipment being exposed?" For example, a localized destruct capability (explosive, acid, etc.) could be built into the protective casing of the systems. The detect mechanism could be integrated into the casing itself through various means, the easiest being as an elemental part of the casing. If the casing were to be opened, the integrity of the case would be destroyed, triggering the reaction. In this case, the result would be the destruction of data and/or equipment. A real-life example of this type of integrated detection/reaction capability can be seen in any museum. Fine grids of wire are integrated into casings, which, when parted, cause an electrical circuit to be broken, which triggers an alarm.[49]

Questions to ponder:

- ❑ How could a table top exercise have helped in discovering this risk?
- ❑ What information would you need about adversary capabilities to understand the level of risk? How could you obtain that information?
- ❑ When should you include minimal risk, but high impact problems, in your engineering analysis?
- ❑ How did the capture of this UAS impact the risk to friendly forces?
- ❑ How did the capture and analysis of the UAS alter the balance of power in the near and far term? Consider allies of Iran while pondering this question.

Case 3: When Pilots Are Targeted for Assassination

In 2016, it was widely reported that the Islamic State had compiled and published a list of US drone pilots, including home addresses and photographs. The list was posted online with an accompanying message urging followers to attack the pilots by any means available.[50]

---

[47] Historian, US Department of State. (n.d.) U-2 Overflights and the Capture of Francis Gary Powers, 1960. Office of the Historian of the U.S. Department of State. Available online at https://history.state.gov/milestones/1953-1960/u2-incident

[48] Hsu, Jeremy. (2017) Self-Destructing Gadgets Made Not So Mission Impossible. IEEE Spectrum, 9 February 2017. Available online at https://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/selfdestructing-gadgets-made-not-so-mission-impossible

[49] Anderson, Ross. (2008) Chapter 16: Physical Tamper Resistance. Security Engineering (2nd edition). Available online at https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c16.pdf

[50] Gadher, Dipesh and Toby Harden. (2016) Islamic State hackers publish hit list of US drone pilots. The Australian, 2 May 2016. Available online at https://www.theaustralian.com.au/news/world/islamic-state-hackers-publish-hit-list-of-us-drone-pilots/

Clearly, the knowledge that you personally are a specific target differs from the usual warfare rules of engagement. , where a person in a uniform is a general target while on the battlefield. This type of tactic has occurred at least once previously, in the case of the USS Vincennes shoot-down of an Iranian civilian airliner.[51]

Questions to consider:

- ❑ What types of security controls *could* be put in place to protect the identity of drone pilots?
- ❑ What types of security controls *should* be put in place to protect that data?
- ❑ How would those security controls increase the complexity of UAS operations?
- ❑ What are the risk trade-offs?

Case 4: When Commercial Drones Spy Domestically

In 2017, stories began to emerge alleging that a commercial drone manufactured by DJI, Inc, a Chinese company, was collecting data about U.S. infrastructure and sending it back to China.**[52]**,**[53]**,**[54]** The stories stemmed from a memo that was issued in August 2017 from the Los Angeles office of U.S. Immigrations and Customs Enforcement. The memo stated that the office assessed, "with moderate confidence that Chinese-based company DJI Science and Technology is providing U.S. critical infrastructure and law enforcement data to the Chinese government" and "with high confidence the company is selectively targeting government and privately owned entities within these sectors to expand its ability to collect and exploit sensitive U.S. data."**[55]** The memo, originally classified as Law Enforcement Sensitive, was leaked.**[56]**

It is not optimal to use equipment that surreptitiously collect data about your facilities and locale. This has been a repeated theme through the years. For example, a Popular Mechanics article from 1997 recounted the story of a camera placed inside a Xerox copying machine.**[57]** Another interesting story related to

[51] Bernstein, Leonard and Richard A. Serrano. (1989) Bomb Blows Up Van Driven by Wife of Vincennes Captain; She Escapes. LA Times, 11 March1989. Available online at http://articles.latimes.com/1989-03-11/news/mn-792_1_pipe-bomb
[52] Newman, Lily Hay. (2017) THE ARMY GROUNDS ITS DJI DRONES OVER SECURITY CONCERNS. Wired Magazine, 7 August 2017. Available online at https://www.wired.com/story/army-dji-drone-ban/
[53] Mozur, Paul. (2017) Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say. New York Times, 29 November 2017. Available online at https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html
[54] Corfield, Gareth. (2018) Yes, drone biz DJI's Go 4 app does phone home to China – sort of. The Register, 25 Apr. 2018. Available at https://www.theregister.co.uk/2018/04/25/dji_data_security_audit/
[55] U.S. Immigration and Customs Enforcement (2017) Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government. ICE-IL-17-0019, 9 August 2017. Available online at https://info.publicintelligence.net/ICE-DJI-China.pdf
[56] Smith, Ms. (2017) Leaked DHS memo accuses drone maker DJI of spying for China. CSO Magazine, 3 December 2017. Available online at https://www.csoonline.com/article/3239726/security/leaked-dhs-memo-accuses-drone-maker-dji-of-spying-for-china.html
[57] Stover, Dan. (1997) Spies in the Xerox machine: how an engineer helped the CIA snoop on Soviet diplomats. Popular Science, 1 January 1997. Available online at https://electricalstrategies.com/about/in-the-news/spies-in-the-xerox-machine/

Acoustic Kitty: a cat that was operated on to embed listening electronics inside its body for espionage purposes.[58],[59]

Questions to be considered:

- ❑ How do you know if you can trust your equipment?
- ❑ Assume your equipment is in perfect working order. How would one detect clandestine operations?
- ❑ How would you craft a security policy regarding equipment probing?
- ❑ What types of operational risks does this type of activity pose, and how can one engineer countermeasures to mitigate it?
- ❑ How would one use an attack/defend exercise to test for these activities?
- ❑ What would an adversary gain from this type of intelligence activity?
- ❑ What risk did DJI expose China to when they implemented these measurements into their equipment? Consider all the elements of national power; Diplomatic, Information, Military, and Economic (DIME).
- ❑ What could one gain from discovering and exploiting this intelligence capability without exposing one's knowledge to the adversary?

Case 5: The Drone That Steals Your Wi-Fi Password

Security researchers have discovered substantial activity of small UASs, including spying, data theft, and other nefarious acts. The "Wireless Aerial Surveillance Platform, or WASP, … is equipped with an HD camera, a cigarette-pack sized on-board Linux computer packed with network-hacking tools including the BackTrack testing toolset and a custom-built 340-million-word dictionary for brute-force guessing of passwords, and eleven antennae." As one researcher, describing his invention, said "This is like Black Hat's Greatest Hits. And it flies."[60] As a rare spot of good news, other researchers have developed detection capabilities for this type of activity, "someone using only a laptop and an object that flickers can detect if someone is using a drone to spy on them."[61] Meanwhile, UASs are getting smaller and are being implemented in swarms.

These are both security and intelligence issues. The confidentiality issues are paramount; having secrets stolen electronically or using video is a significant problem. The next level of threat to be concerned about is the infiltration of bad data, misleading data, meaconing signals, and jamming signals into SOP.
Questions to ponder:

- ❑ What types of intelligence could help detect whether data integrity is being attacked?

[58] Hillman, Jennifer. (2008) What the CIA Learned from Get Smart. Wired Magazine, 19 June 2008. Available online at https://www.wired.com/2008/06/pl-print-19/

[59] National Security Archives. (n.d.) Memorandum for: [deleted], Subject: [deleted] Views on Trained Cats [deleted] for [deleted] Use, March 1967, 2 pp. Available online at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB54/

[60] Greenberg, Andy. (2011) Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones. Forbes, 28 July 2011. Available online at https://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/

[61] Charlaff, Joe. (2018) Spies in the Sky: Israeli researchers develop a counter-surveillance drone system. The Jerusalem Report, 6 August 2018. Available online at https://aabgu.org/wp-content/uploads/2018/07/JRep-August-6-38-39-Joe-drones.pdf

- ❑ What level of surveillance is required to detect unauthorized UASs operating near or in your sensitive areas?
- ❑ What level of operational security training for personnel is required to reduce the potential impact of these types of attacks?
- ❑ How can these threats be included in attack/defend scenarios?

Concluding Thoughts

These five cases are real world examples. Unfortunately, the enemy always gets a vote. Keeping up with developments and news from the security and intelligence communities can be time intensive. A management best practice; divvy up the work. Have team members research diverse sources and report back on interesting developments. Make learning about advances an important part of team activities. Learn from your peers. Participate in professional networks. Go to conferences and listen to the experts. There is too much to know for any one person, so you need to develop your personal team as well as participate in a professional team.

References

Anderson, Ross. (2008) Chapter 16: Physical Tamper Resistance. Security Engineering (2nd edition). Available online at https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c16.pdf

Axe, David. (2016) How Islamic Jihad Hacked Israel's Drones. The Daily Beast, 25 March 2016. Available online at https://www.thedailybeast.com/how-islamic-jihad-hacked-israels-drones

Ben-Yishai, Ron. (2016) IDF's cyber defense easily breached. Ynet News, 23 March 2016. Available online at https://www.ynetnews.com/articles/0,7340,L-4782445,00.html

Bernstein, Leonard and Richard A. Serrano. (1989) Bomb Blows Up Van Driven by Wife of Vincennes Captain; She Escapes. LA Times, 11 March1989. Available online at http://articles.latimes.com/1989-03-11/news/mn-792_1_pipe-bomb

Cenciotti, David. (2016) Iran unveils new UCAV modeled on captured U.S. RQ-170 stealth drone. The Aviationist, 2 October 2016. Available online at https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modeled-on-captured-u-s-rq-170-stealth-drone/

Charlaff, Joe. (2018) Spies in the Sky: Israeli researchers develop a counter-surveillance drone system. The Jerusalem Report, 6 August 2018. Available online at https://aabgu.org/wp-content/uploads/2018/07/JRep-August-6-38-39-Joe-drones.pdf

Corfield, Gareth. (2018) Yes, drone biz DJI's Go 4 app does phone home to China – sort of. The Register, 25 Apr. 2018. Available at https://www.theregister.co.uk/2018/04/25/dji_data_security_audit/

Gadher, Dipesh and Toby Harden. (2016) Islamic State hackers publish hit list of US drone pilots. The Australian, 2 May 2016. Available online at https://www.theaustralian.com.au/news/world/islamic-state-hackers-publish-hit-list-of-us-drone-pilots/

Greenberg, Andy. (2011) Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones. Forbes, 28 July 2011. Available online at https://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/

Gross, Judah Ari et al. (2016) Israel charges Islamic Jihad hacker for spying on IDF drones. Times of Israel, 23 March 2016. Available online at https://www.timesofisrael.com/israel-charges-islamic-jihad-hacker-for-spying-on-idf-drones/

Hillman, Jennifer. (2008) What the CIA Learned from Get Smart. Wired Magazine, 19 June 2008. Available online at https://www.wired.com/2008/06/pl-print-19/

Historian, US Department of State. (n.d.) U-2 Overflights and the Capture of Francis Gary Powers, 1960. Office of the Historian of the U.S. Department of State. Available online at https://history.state.gov/milestones/1953-1960/u2-incident

Hsu, Jeremy. (2017) Self-Destructing Gadgets Made Not So Mission Impossible. IEEE Spectrum, 9 February 2017. Available online at https://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/selfdestructing-gadgets-made-not-so-mission-impossible

Mozur, Paul. (2017) Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say. New York Times, 29 November 2017. Available online at https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html

National Security Archives. (n.d.) Memorandum for: [deleted], Subject: [deleted] Views on Trained Cats [deleted] for [deleted] Use, March 1967, 2 pp. Available online at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB54/

Newman, Lily Hay. (2017) THE ARMY GROUNDS ITS DJI DRONES OVER SECURITY CONCERNS. Wired Magazine, 7 August 2017. Available online at https://www.wired.com/story/army-dji-drone-ban/

Opall-Rome, Barbara. (2018) Israel Air Force says seized Iranian drone is a knockoff of US Sentinel. Defense News, 12 February 2018. Available online at https://www.defensenews.com/global/mideast-africa/2018/02/12/israel-air-force-says-seized-iranian-drone-is-a-knockoff-of-us-sentinel/

Peterson, Scott. (2011) Downed US drone: How Iran caught the ‘beast’. Christian Science Monitory, 9 December 2011. Available online at https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast

Smith, Ms. (2017) Leaked DHS memo accuses drone maker DJI of spying for China. CSO Magazine, 3 December 2017. Available online at https://www.csoonline.com/article/3239726/security/leaked-dhs-memo-accuses-drone-maker-dji-of-spying-for-china.html

Stover, Dan. (1997) Spies in the Xerox machine: how an engineer helped the CIA snoop on Soviet diplomats. Popular Science, 1 January 1997. Available online at https://electricalstrategies.com/about/in-the-news/spies-in-the-xerox-machine/

U.S. Immigration and Customs Enforcement (2017) Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government. ICE-IL-17-0019, 9 August 2017. Available online at https://info.publicintelligence.net/ICE-DJI-China.pdf

Wikipedia. (2018) Iran–U.S. RQ-170 incident. Available online at https://en.wikipedia.org/wiki/Iran–U.S._RQ-170_incident. Last edit date when accessed 1 July 2018.