On the use of security and privacy technology as a plot device

Joan Feigenbaum and Brad Rosen

Yale University, New Haven CT, 06520-8285 USA
E-mail: {joan.feigenbaum, brad.rosen}@yale.edu

Abstract. We believe that the handling of information security in fiction is, in general, neither technically realistic nor dramatically interesting. Furthermore, we believe that technically realistic treatment of information security *could* be an effective plot device. We provide examples (and one counterexample) from well regarded television shows to support our beliefs. We conclude with a short fictional work of our own creation that attempts to use information security in a technically realistic and dramatically interesting manner.

1 Introduction

In answer to the question "how is information security handled in fiction?," we are tempted to say that there doesn't seem to be much information security in fiction. Intelligence and law-enforcement protagonists generally seem to be able to break into computer systems almost effortlessly whenever they need to in order to catch villains, and their break-ins generally don't leave any tracks or have any negative consequences. Ironically, the one thing that fictional good guys sometimes have a hard time doing is something that real-world intelligence and law-enforcement agencies do pretty well, namely locate sources of incoming phone calls and messages.

There are some notable exceptions to this general state of affairs – fictional episodes in which the technical difficulty of achieving information security is apparent and in which attempts to circumvent security measures either succeed or fail in realistic and dramatically effective ways. It is our thesis that such prolonged and nuanced treatment of information-security challenges can be a great plot device and that it is underutilized by novelists and screenwriters.

2 Talk summary

Break-ins are easy and have no consequences. To support our claim that information security is often treated unrealistically in fiction, we showed three clips from well regarded TV shows. In each, a white-hat hacker manages to break into an ostensibly well defended enterprise database in less than one minute while his colleagues or friends stand around making small talk. The three targets were

a CIA personnel database [1], a Mossad personnel database [2], and a phone-company operations database [3]. In none of these episodes did the hacker suffer any consequences for his blatantly illegal act; nor did the organization that was broken into demonstrate any awareness of the break-in.

Tracing phone calls is hard. The *trace race* [4] is a police-procedural trope in which the police try to determine a calling number or to locate a (criminal) caller. They need the caller to stay on the line for a certain amount of time. The amount of time needed varies. Even if the person talking to the criminal is told to "keep him talking," and the criminal obliges by blabbing on forever, it never seems to work. Sometimes, the criminal seems to know exactly when to hang up in order to defeat a trace.

To illustrate this trope, we showed two clips from a **Law and Order: SVU** episode in which the detectives spend more than an hour (of elapsed time, not screen time, obviously) trying to locate a cell-phone caller [5].

In fact, tracing a calling number was nontrivial when "telephone switches" were actually mechanical racks of switches. Now, however, telephone switches are software systems. One can go to a console during a call, enter the number, and get the other number(s) on the call. Phones can also be located; phone companies locate them all the time, and so do police departments.

A counterexample: pacemaker hacking. One compelling exception to the weak treatment of information security in fiction is the pacemaker attack on Vice President Waldron in **Homeland** [6]. Responding to a terrorist's threat to kill his beloved Carrie Mathison, protagonist Nicholas Brody breaks into Waldron's office and finds the serial number of the pacemaker. Armed with the serial number, an unnamed, apparently highly skilled hacker (in the employ of the terrorist who has threatened to kill Carrie) gains wireless access to Waldron's pacemaker and kills him.

One of the reasons this attack is so utterly gripping is that it goes on for almost six minutes of screen time; viewers are not misled into thinking that even a skilled hacker could pull it off in a matter of seconds or that even a successful attack would kill the victim instantaneously. In the talk, we were able to show just three short cuts from the 6-minute scene.

The scene is technically realistic. Wireless-networked, implanted medical devices *are* insecure, and patients are at risk [7, 8].

A story idea: car hacking. Just as wireless access to implanted medical devices is a real threat, so is wireless access to *electronic control units* of automobiles [9]. Our talk concluded with the question of whether a good espionage story could be based on the idea of a "black operative" who uses car hacking to disguise an assassination as an accident. We solicited plot suggestions from the audience and received many good ones (unsurprisingly, given that this was a Cambridge workshop audience); they can be found in the transcript that appears in this volume.

After the workshop, we wrote a story that features both car hacking and intelligence operatives. It can be found in the appendix.

References

1. *Royals and Loyals*, **NCIS**, Season 8, Episode 4, Oct. 12, 2010.
2. *Berlin*, **NCIS**, Season 10, Episode 21, Apr. 23, 2013.
3. *Let's Get to Scooping*, **How to Get Away With Murder**, Season 1, Episode 4, Oct. 16, 2014.
4. `http://tvtropes.org/pmwiki/pmwiki.php/Main/PhoneTraceRace`.
5. *911*, **Law and Order SVU**, Season 7, Episode 3, Oct. 4, 2005.
6. *Broken Hearts*, **Homeland**, Season 2, Episode 10, Dec. 2, 2012.
7. Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W. H.: Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In: 29^{th} Symposium on Security and Privacy, pp. 129–142, IEEE, Piscataway (2008)
8. Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., Maisel, W. H.: Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices. In: 28^{th} SIGCHI Conference on Human Factors in Computing Systems, pp. 917–926, ACM Press, New York (2010)
9. Valasek, C., Miller, C.: A Survey of Remote Automotive Attack Surfaces, `http://illmatics.com/remote%20attack%20surfaces.pdf`, 2014.

Drive Me Crazy

Friday, June 19, 2015, early evening. David's apartment

Arriving home after another humdrum day at work, David hung his windbreaker on a peg in the hall, left his shoes directly under it, and flopped onto the bed. It was hard to believe there were so many allegedly smart people who enjoyed these god-awful boring tech jobs. They must have no idea what kind of adventures the internet offered.

After 10 minutes of staring at the ceiling, he gave in and went to the closet to retrieve the photo from the dress-shirt pocket. It had been almost a week since he'd looked at this photo of Ari and himself on the crowded beach in Tel Aviv. Progress, perhaps. But he still thought about Ari constantly and still longed for him. He'd never loved anyone so intensely, before or since. More to the point, he'd never found anyone else nearly as interesting. It was hard to believe he ever would.

They'd met by chance at the Apple Store in New York's Grand Central Station. Ari was on vacation, and David was working for a hapless start-up in Silicon Alley, long since defunct. By the time Ari was scheduled to return to Israel, David had quit his boring job, packed the few of his belongings that he needed, and sold or discarded the rest. For the next 18 months, he was happy. Increasingly worried, yeah, as it gradually dawned on him what a lunatic Ari

was, but he'd mostly been happy. There were always more technical challenges, more financial rewards, and more great sex.

He put the photo back into the pocket of the dress shirt. He'd been told to erase all remnants of his life with Ari, but he figured that no one would expect him to value an old-fashioned snapshot – or anything else that wasn't just bits. So he'd kept only this one, pocket-sized print. Still, it was an addiction at this point, not a source of real pleasure. He knew that he needed to move on.

He turned on the evening news and opened the refrigerator, thinking about what to have for dinner. He'd not yet decided what to cook when he heard the news from Vienna.

"The Iran-deal negotiations were thrown into chaos today in Vienna by a fatal car crash. Iranian Deputy Foreign Minister Abbas Araghchi was en route to a meeting with representatives of all of the P5-plus-one nations when the chauffeured sedan, a 2014 Chrysler 300, in which he was travelling turned suddenly into oncoming traffic. The crash killed Araghchi, his driver, and the driver of one of the three other cars involved. Four other people were injured, two of them seriously."

David closed the refrigerator and listened intently to the rest of the news report. Of course, the most anti-western members of the Iranian delegation were accusing the other parties to the negotiation of tampering with the car. Of course, the other parties were saying that they wanted nothing more than to conclude the deal successfully at this point and that, moreover, the car, which had been in fine working order the day before, had been in a locked garage under both armed guard and video surveillance all night. Of course, it was evident that no one had tampered with the car. Perhaps the Iranian chauffeur was the one who wanted to blow up the negotiations, even at the expense of his own life.

This was Ari's handiwork. David knew it as soon as he heard the phrases "Iran-deal negotiations" and "fatal car crash" in the same news story. Ari had perfected car hacking years ago and had been waiting for an opportunity to use it. At the time he'd demoed his car-hacking skills in the parking lot, he'd told David that there didn't seem to be any suitable targets. Ari was ambitious and amoral, but he wasn't bloodthirsty. He wouldn't cause a fatal crash just to show he could do it; there had to be something important at stake.

David turned off the TV and called his CIA handler. He wasn't without ambition himself.

Saturday, June 20, 2015, mid-afternoon. Mitchell Park, Palo Alto

Joe Dunant stared at David across the picnic table. He was extremely unhappy about the crazy story that he'd just heard, but he stayed calm. He'd dealt with erratic assets before – even seriously neurotic ones – and managed to get some good stuff out of them, at least for a while. David had never flaked out on him before, but Joe would cope with flakiness if it was the price to pay for David's technical expertise and first-hand knowledge of the global hacker underworld.

"Let's go over this again, ok?" Joe said. "First of all, how is this supposed to work exactly?"

David knew better than to take that question literally. He gave Joe a quizzical look.

"OK, not *exactly*," Joe admitted. "In high-level terms, what the hell do you think he did?"

"He exploited what's known in the computer-security world as a 'remote automotive attack surface' to get control of the car. Cars, as you probably know, are full of computers these days. For just about every essential function (steering, acceleration, braking, and so on), there's an ECU. Stands for 'electronic control unit.' There are ECUs for inessential functions, too – power windows, for example."

This was one of the great things about David, Joe thought. Unlike almost all of the genius geeks he'd run since jumping on the cyber-espionage bandwagon, David really knew how to explain things. Joe had learned a huge amount from him about what kinds of attacks were feasible, what kinds of damage they could do, and what might be done to prevent them. Of course, Joe still didn't know *how* people got computers to do all of this scary stuff, but he really didn't need to; he wasn't in the business of writing code. He listened carefully as David went on with his explanation of car hacking.

"The ECUs are connected by an internal network. A group of related components that need to coordinate with each other is usually connected by a 'bus,' which a very simple kind of data network. So far, so good; having an internal bus connect the doors and the dome light so that the light goes on when someone opens the door to get in makes perfect sense and needn't cause insecurity. But there are problems. For example, these separate buses are 'bridged' so that different groups of components can communicate."

"Why?," Joe asked. "That sounds like a bad idea. It also sounds like something that would make the whole network more complicated and more expensive to build."

"Good," David said. "You're right that cost is a factor. I'll get to that. As far as bridging goes, it turns out to be necessary in some important cases. The ECU that controls the door locks, for example, has to receive messages from at least two other ECUs that are usually on different buses. The powertrain-control module has a sensor that determines a car's speed. It broadcasts the speed on the car's internal network. If you've ever gotten onto the highway and suddenly your doors auto-locked, it was because the ECU that controls the door locks got the message that you'd gone above the speed for auto-lock. But the same ECU also needs to get messages from the crash-detection ECUs that control the airbags ... so when a crash is detected, the doors are unlocked and survivors can get out – or be pulled out."

"Got it," Joe said. "But all this is still going on inside the car. How does someone hack in from the outside?"

"Just about every car has components that have to communicate with the outside world. Think of OnStar, for example. GM aggressively advertises the fact that OnStar can track cars and make emergency phone calls. Even in cars that are not supposed to be communicating with the outside world while their

owners are driving around, dealers and mechanics want wireless access to do diagnostics – they need to replace an ECU if they determine that it's faulty."

Joe was getting used to the idea of car hacking as a way to kill someone. He wondered whether the agency had ever used it. But he was still having trouble swallowing David's theory that Ari had hacked into this car at this time.

"David, wouldn't someone need to know a lot about a particular make and model of car in order to break into it? You said that Ari was seriously into car hacking years before you hooked up with him. How would he know what kind of car an Iranian diplomat would be in in 2015? How would he even know there would be negotiations with Iran in 2015?"

David smiled. "Good. Again. You asked about the cost of designing and developing automotive networks. You're absolutely right that, if every car manufacturer had to start from scratch for every model of car, it would be too expensive. Not to mention too time-consuming. But there are a lot of industry standards, notably CAN buses and OBD-II ports that ..."

"OK, stop." Joe was reaching his limit on the amount of new technical information he could absorb in one sitting. "Since you mentioned 'standards,' I'm assuming your point is that, once a super hacker like Ari figures out how to hack into one kind of car, it's not that hard for him to hack into other kinds."

"Right. Besides, at this point, there are some good survey papers about vulnerabilities in popular makes and models. All he'd need is for someone in Vienna to tell him what the Iranian was being driven around in; that kind of information is for sale everywhere. Then he could find most of the technical information he needs in one of the papers."

These survey papers raised another red flag. "Wait a minute. If this information is widely available, then why do you think Ari did this? Couldn't lots of skilled hackers have pulled off this attack on Araghchi's car?"

David shook his head. "No, not really. The deep magic here is bridging between buses."

Joe listened with rapt attention. Most assets have verbal tells – expressions with which they build up to something that shows why their intel is valuable. David's was "the deep magic here is ..."

"Any hacker worth his salt can figure out how to get onto one of the less privileged buses in a standard, modern automobile without having physical access to the car. It's not all that different from hacking into any supposedly private network that's connected to the internet. Bridging from a less privileged bus to a more privileged one is much harder. A few academic researchers have done it, but their papers don't say exactly how they did it. No one can just read up on how to bridge to an ECU that will steer a car into oncoming traffic. It takes many months of work to figure out how to do that, and Ari put in those months of work."

"You're sure of that?," Joe asked.

"Yeah, I'm sure. He did a demo for me in a parking lot. I was the driver."

Much as he wished he could dismiss it, Joe knew he had to take this bizarre story to his superiors and the rest of his team. If he ignored it, and it proved to

be true, his relationship with David would be seriously damaged. Not to mention that Ari may strike again if the negotiations continued.

He flicked the ON-OFF switch on a device that looked like a USB stick but was actually an audio recorder. He would need to give the more technically oriented members of his team a fleshed out version of David's theory, and he didn't trust himself to render it accurately. This device could be shredded after he played the recording for his colleagues.

"Once more. What do you think he did?"

"He probably took over the car's built in telematics system, which is connected to the internet. Then ..."

"Wait. Telematics? What's that?"

"It's a catch-all term for the many ways in which cars collect data, process it, and send the results to various Big Brothers using wireless communication. Insurance companies use the data to reward good drivers and penalize bad ones. Car manufacturers use the data to keep track of how well various features are working – airbags, for instance. Dealers can keep track of when routine maintenance is performed and remind the owners if it's overdue. The most straightforward kind of telematics is simply vehicle tracking. If a car is stolen, and the thief doesn't disable the telematics system, the police should have an easy time catching him."

"OK, go on."

"Then he probably used the bridge to the parking system. Advanced models like this one have ECUs that let the car park itself; they're awesome in really tight spots in which drivers can't see well enough to maneuver in and out but sensors can. The parking ECU can turn the wheels as much as it needs to. It's not supposed to do anything when the car is driving at high speeds, but it's easy enough to bypass that by flooding the CAN bus with traffic. And then *WHAM*, your steering wheel is jerking hard to the left or right, and you're flying into oncoming traffic. And in the split second before you're splattered across the dash, the code is busy erasing itself so there's no trace."

Joe wasn't sure whether that would make sense to his colleagues and figured it wouldn't hurt to ask for some clarification.

"So what's 'flooding' exactly, and how does it make the wheels turn when they're not supposed to?"

David answered patiently. They went on like this for a little while longer and then parted. Joe said he would be in touch soon.

Sunday, June 21, 2015, mid-morning. David's apartment

Usually, he slept well after meeting with Joe but not last night. He could tell during the meeting yesterday that Joe didn't believe that Ari was trying to blow up the Iran deal.

Maybe that made sense. Joe knew that Ari was a brilliant and unscrupulous cyber criminal, but he didn't know him personally. All of the attacks by Ari that Joe knew about were motivated by profit or technical challenge or both. The idea that Ari would attack "the enemies of Israel" probably sounded ridiculous to Joe.

During the year and a half that they were together, David had delighted in the profit and technical challenge. It felt like a dream come true for a while: the best sex he'd ever had, the most interesting work he'd ever done, and more money than he knew what to do with. Plus Ari knew an amazing number of smart and crazy black hats from all over the world; David's "professional" network was expanding by the day.

And life wasn't all work. They talked about everything, including politics. Including Israel's "right to exist." David didn't know what to make of Ari's embattled, aggressive world view when he first heard it. He'd read about the rightward drift in Israeli society and in the American Jewish organizations that considered themselves "pro-Israel," but he'd never actually talked to anyone who believed that stuff. At first, he chose to ignore it – to concentrate on everything he loved about Ari. As time went on, it didn't sound so weird to him; they were living in Israel, and lots of people held similar views, including many whom he agreed with about everything else. He kept reminding himself that nobody was perfect and that his life with Ari really was closer than he'd ever been to the life he'd always dreamed about.

But dreams don't actually come true, do they? As time went on, he couldn't ignore the fact that much of what they were doing was not only illegal but dangerous. And that Ari could be reckless. In the middle of their second year together, recklessness caught up with them. Or at least it caught up with David.

They'd been part of a massive banking scam that Ari had spearheaded. It was not the first time that Ari had had a brilliant idea, enough enthusiasm and charisma to enlist a lot of people, but not quite enough devotion to make sure that those people had all of the information they needed to cover their tracks. This time, David was one of the ones who got caught. End of dream.

That was when he met Joe Dunant. He'd been an emotional basket case at the time, but even then he'd had a hint that Joe was a no-bullshit guy. And a decent one. The US Treasury department had orchestrated the sting, and Joe had been read in very early. He'd arranged to meet with David shortly after he was arrested, rather than leaving him to grow increasingly terrified and disoriented in jail as time went by. And Joe had been completely straight about what he wanted: David's unqualified cooperation with the CIA and the rest of the US intelligence community in exchange for extradition to the US and a good job in Silicon Valley. Joe would be his handler; he'd be an "asset" with intimate knowledge of the cyber underworld. He'd known that he had no cards to play and had accepted the deal very quickly. But making the deal with Joe had been less disgusting than making it with someone else would have been.

That was a year ago. This "asset" business had gone pretty smoothly for the first year. Nothing Joe had asked him to do was particularly interesting, but none of it was particularly hard either. And Joe was an ok guy to have a cappuccino with from time to time.

This time was different. Joe hadn't asked. David had come to him with the best intel he'd ever received, and Joe didn't know what to make of it.

Sunday, June 21, 2015, mid-afternoon. David's apartment

David was desperate for something to happen. Joe hadn't called to report on his team's reaction. Did that mean that they were still considering it or that Joe was just being polite when he'd said that they would?

He'd resisted the temptation to search for evidence to support his theory. He wanted to know whether anyone had indeed purchased information recently about chauffeured sedans in Vienna, but he knew that such a search was bound to leave some breadcrumbs. Let Joe's CIA colleagues leave those breadcrumbs if they really needed the evidence.

He started reading his work email, figuring that he might find something to focus on. He opened the BBC World Service radio player in a browser window. It was more effective as background noise than music.

Just ten minutes later, he got the confirmation that he needed.

"Confusion and accusations continue to dominate the Iran-deal negotiations. Today in Geneva, the American Undersecretary of State Wendy Sherman failed to show up for a meeting with similarly high-placed members of the Iranian and other P5-plus-one delegations. A US State Department spokeswoman said that the Undersecretary's car had stalled out en route to the meeting, that she had tried to phone the meeting participants to explain that she would be late, but that the car was in a large cell-phone dead zone. Later, it was discovered that the driver had followed an incorrect route delivered by the car's GPS device."

"Coming hard on the heels of the fatal accident that killed Iranian negotiator Araghchi, this further disruption threatens to derail the negotiations entirely. Nonetheless, the leaders of Iran and the P5-plus-one nations have issued statements saying that they intend to press on and to meet the June 30 deadline if at all possible. 'We've come so far in these negotiations,' said US President Obama. 'We can't let a bizarre but innocent mishap stop us when we're so close to a deal that would benefit all of the parties.' "

David reached for the secure phone. "Joe, it's me. Did you hear about Wendy Sherman's car?"

"Yes, we got the call about 15 minutes ago. I was just going to call you. Is it on the news already?"

"I heard it on the BBC World Service. Do you want to meet?"

"6:00 in Foothills Park."

Sunday, June 21, 2015, 6 p.m. Foothills Park, Palo Alto

Joe had gotten right down to business. The agency had tipped Sherman's people in Geneva that a car hacker might have killed Araghchi in Vienna and advised them to disable external wireless access to Sherman's car.

David was one step ahead of him. "Ari could get access to that car's system through Bluetooth, even if the cellular network was disabled. They probably left Bluetooth on for hands-free calling, and that's enough. All it takes is a little patience and a brute-force attack to find the PIN. With a directional antenna, you don't even have to be that close if you start brute forcing a day in advance."

Joe had heard something similar from the geeks on his team. As usual, he didn't understand the technical details, but he got the general idea: Someone with Ari's skills and connections could hack into a car network with a Bluetooth connection. The purpose of this meeting was to verify that David had the same story as Joe's colleagues. David would have learned this stuff from Ari; it made his theory that Ari was the culprit very believable.

"So how did he fool the GPS system?," Joe asked, continuing the verification exercise.

"I doubt he needed to mess with the custom hardware that processes the GPS coordinates. The *maps* used by GPS systems are just regular data displayed by easily compromised software. The GPS screen in that car probably showed the right coordinates, but the map was fake, and it led them into the dead zone."

So far so good. Joe had one more question.

"The breakdown?"

"If he could spoof the dead-zone coordinates, he could also take the engine out. There are specific diagnostic messages used to control individual cylinders in the engine, but flooding the engine ECU can shut them all down."

David stopped walking. "Joe, listen to me." Joe stopped and turned around to face his companion. "The BBC said that the negotiations are continuing. Is that right?"

"Yes. They'd probably all have cut and run if Sherman had been driven off a cliff, but what happened today wasn't quite a show stopper."

"You have to stop him. Someone else is going to get killed. Maybe many more people. You saw what happened on Friday."

Joe nodded. Now wasn't the time to explain that his agency's primary concern was the successful completion of this Iran deal on which the Obama administration had staked so much. More casualties would only be problematic because they'd mean the end of negotiation.

"We're working on a plan to disconnect him from the internet."

"You need to mount a DDoS attack. It stands for 'Distributed Denial of Service.' Hit the internet connections through which he's contacting these cars with so much data from so many sources that they can't send anything. I'm sure your people know how to DDoS someone."

"So they tell me," Joe said. "We're probably going to need your input during the next two days. Stand by."

Tuesday, June 23, 2015, early afternoon. L'Acajou Bakery and Cafe, South of Market, San Francisco

Joe and Mary Lawson, his opposite number in MI6, were finishing lunch at Mary's favorite spot in SoMa. Once again, Joe marvelled at how the Brits had placed Mary in the city, surrounded by cutting-edge start ups and great food and coffee, while Joe's own fine country had placed him in Sunnyvale, a mature, boring suburb, near a bunch of mature, boring, incumbent tech companies.

Nonetheless, it was Joe's agency, his asset, and his connections at the National Security Agency who were going to salvage the Iran talks. This was a once-in-a-decade career booster – assuming everyone up the chain in Langley

gave him credit for it. Time for him and Mary to go over the crucial points of their joint op. They couldn't have that conversation in L'Acajou. Joe asked for the check, and soon they were strolling on 9^{th} toward Mission.

"Well, Dunant," said Mary. "I admit that I was pretty skeptical when you sprung this on me yesterday morning." They walked on, Mary looking straight ahead and Joe looking at her. "Skeptical! Hell, I was bloody incredulous."

"Yeah, I was incredulous, too, when it was sprung on me. But the intel is solid, and the op is pure cyber. There's really nothing to lose."

"And a lot to gain," said Mary. "Look, we can't assume that 'pure cyber' means non-lethal. We could wind up DDoS'ing a control system ..."

"Oh come on," Joe interrupted. "You're not talking to a fresh recruit, Lawson. Of course there are risks. There always are. But this is probably the least risky op we'll ever run together."

Mary smiled, nodded, and turned toward Joe. She'd felt obliged to say that they needed to be cautious and acknowledge the risks. But, truth be told, she loved the idea of this multinational DDoS attack, and she was amped up.

"Right then. You're sure this lone wolf we're targeting could actually have hacked into both cars? And, more to the point, that he would want to?"

"Yes and yes. Our asset is his ex-boyfriend."

Mary raised her eyebrows, having just heard for the first time that there was a gay angle here. For that matter, she was hearing for the first time that there was a sex and romance angle at all. Oh well. Not worth interrupting Dunant's story – all sources of good intel were fair game, and ex-lovers of all orientations were the most tried and true of sources.

"Our target hates the idea of a deal with Iran that would bring the Iranians into the 'international community,' whatever the fuck that is. He's not for a pre-emptive strike on Iran ..."

Mary snorted. "Nice of him, that. Especially since Israelis who are in favor of a pre-emptive strike usually mean a pre-emptive strike by the US, with the UK to follow."

Joe didn't need a lesson in geopolitics any more than he needed a lesson in cyber-physical risks. "As I was saying, the target just wants Israel, Saudi Arabia, and all of their allies to be in a permanent cold war with Iran. A deal that ends that cold war would 'upset the balance of power in the region.' So, yeah, he wants to blow up the negotiations."

They turned left on Mission. No one was following them. Hell, no one had noticed them. They blended perfectly into the neighborhood.

"More interestingly, he's studied car hacking seriously for years. The attacks used against Araghchi and Sherman are well documented in the open literature at this point, but he had them years ago, well before they were published."

"He knew them, or he did them?," Mary asked. Just as Joe had asked David. It was a crucial question.

"Did them. Our asset left no doubt about that."

"OK, Dunant. I'm not going to press you for those details."

Joe was happy to be working with a professional. Mary knew that she and her agency would benefit if this op worked and that Joe had done her a favor by bringing her into it. She didn't expect Joe to tell her everything about his asset, who had probably been up to his eyeballs in illegal activity during his affair with the target.

Joe continued. "I do want you to know how we got the target's IP address. Actually, his IPs, plural. He's not the type to use just one." Indeed, Mary needed this information. The IPs were the cyberspace addresses of the machines they'd be attacking, and those machines would be crippled for quite some time. They needed to aim carefully.

"One of the most useful things we've gotten from this asset is the fact that the target is a regular in the Gaybros Internet Relay Chat room, especially on Tech Thursdays. We've been chatting with him every week for a year now. Lots of different guys on our end; we don't want him to get too interested in any of them. But they're interesting enough to keep him chatting."

Stopped at a crowded intersection, they had to change the subject while waiting for the walk signal. A minute and a half on real-estate prices – currently the least remarkable topic of overheard conversation in San Francisco.

"Anyway, he uses Tor to connect to Gaybros IRC, and he's careful enough to use the version with stronger crypto. But a year is more than enough time for our NSA friends to crack a specific instance of even the stronger version, and we've given them all of the traffic we've collected. There are four IPs with high-bandwidth connections that he uses regularly. It stands to reason that he's using them for these car hacks."

Mary was impressed. Millions of people use Tor to connect anonymously with chat rooms and other online services; Tor protects the users' IPs with encryption, and even the NSA cannot break that encryption quickly or at scale. If Joe's asset had showed up when the first car hack was performed on Araghchi and said "That's my ex's work. Go find him on Gaybros IRC on Thursday," they'd have been out of luck. But Joe and his people had been tracking this target for a year, ever since they were tipped by their asset that the guy was bound to strike at some point and that he'd do so anonymously and in cyberspace. So they'd patiently collected the data that the NSA needed to deanonymize a specific user. Now that the strike had occurred, they were ready to strike back.

"It's a go, then, as far as I'm concerned. I assume you've got to clear it all the way up?"

"Yeah," Joe said. "I'm working on getting that done by noon on Thursday. How long do you need?"

"Thursday should work for me, too. I don't think I'm going to have to go all the way up. High-tech, no bloodshed, work with the cousins, ..., this is exactly what we're supposed to be doing these days."

"Let's touch base on Thursday afternoon, then."

Mary nodded. "In the meantime, we need to get a bunch of our favorite geeks on stand-by, ready for activation. I'm assuming we're going to hit this target from everywhere on the planet that's home to a lot of black hats."

"Good assumption." Joe had been about to explain that part of his thinking, but Mary was already there. "Our Mossad friends will know that your agency and mine are involved. If there's DDoS traffic coming from everywhere, especially the other P5-plus-one countries, maybe they'll spread the blame around."

"France, Russia, China, US, UK, and Germany. A veritable 'permanent five plus one' club of fucked up geeks. We can spread the net even wider – include Ukraine, why not? Confuse the issue further."

"I agree," Joe said. "Talk to you Thursday."

Mary nodded and turned toward the nearby BART station. "I wouldn't worry too much about alienating Mossad," she said in parting. "They're not as paranoid about Iran as the Netanyahu government."

Few people are, Joe thought.

Thursday, June 25, 2015, 11 a.m. Secure videoconference room, Mountain View

Joe swirled the dregs of his second hit of coffee around in the styrofoam cup. He didn't mind waiting, really. It was only the second time in his 15 years with the agency that he'd met with the Director of National Intelligence and the first time he'd done so by videoconference from the Silicon Valley field office. The fact that the DNI wanted to talk to him directly could only mean good things for him and for SV station. But waiting was still a drag.

At last the station chief, Larry Stern, arrived with a late-20s guy Joe didn't know.

"Could you connect us with the DNI's office, Seth?," the chief asked.

Seth remained silent but got to work. Must be the videoconference guru.

"Hello, sir," Joe said to the division chief. "Good to see you again."

"Call me Larry, please. It's California. No one calls anyone 'sir.' Thanks, Seth. Stay by your phone in case we need help." Seth nodded and left without a word. "Ready, Joe?"

They sat facing the screen and watched the DNI's face come into focus.

"Morning, gentlemen."

Seth had turned the volume too high. Fortunately, that was something Stern didn't need a guru to fix. He pushed a button on a hand-held control. "Morning, sir," he said. Joe coughed quietly into his fist instead of chuckling.

"It's afternoon here. And there's a lot to do before close of business. So let's get down to it. This is a highly unusual operation you've proposed, Dunant. Are you sure it's our best option?"

Joe didn't hesitate. "It's our only reasonable option, sir. David knows more about Ari's m.o. than anyone else. We're as well positioned to DDoS him as it's possible to be at this point."

"I'm not asking whether you've got the best DDoS plan in place. I'm asking whether DDoS'ing Ari is the best option. Do we want to stay in the shadows on this? If we went to the President with this car-hacking story, he might be able to force the Israelis to arrest the son of a bitch."

This was a strategic question, not an operational one. Stern took over. "Taking this to the President is unlikely to work, sir. He would need time to convince the Israelis that Ari is behind these disruptions, and they would need more time

to find him and put him out of commission. We're into the last week of negotiations, and Ari's almost certainly poised to strike again. If we want to spare the next victim, we either have to neutralize Ari or temporarily suspend the negotiations; the deal won't survive a suspension."

This DNI was a great listener, with a great poker face. He turned calmly to Joe. "What do you think, Dunant?"

"I think Mr. Stern is right, sir. Besides, reading in the President and the Israelis would mean burning David, who cost us quite a bit to acquire and who's been a superb asset. I'd hate to lose him."

Seven seconds of silence, which was an eternity in a videoconference. Any longer and people start wondering whether the link has gone down.

"OK, I can see your point," the DNI said at last. "And of course there might be leaks if the President confronted Netanyahu with your theory. 'Iran Nuclear Deal Taken Down by an Israeli Car Hacker.' Jesus. The public would think we're totally crazy."

He was clearly ready to move on to the next crisis. Easy peasy, Joe thought.

"You're working with the Brits on this?," the DNI asked.

"Yes, sir." Stern and Joe said in unison.

"OK, carry on." The screen blanked as the DNI was standing up to leave his own secure conference room.

Stern used the remote to power down on their end. "He didn't mention the real reason that the President can't ask Netanyahu to shut Ari down."

Joe just raised his eyebrows and waited for Stern to continue.

"Netanyahu wouldn't do it. The Israeli right wing hates this Iran deal. They'd probably view car hacking as a brilliant way to blow the whole thing up."

Tuesday, June 30, 2015, early evening. David's apartment

The BBC presenters were droning on about sports. David spooned coffee into the stove-top espresso maker, more because he needed something to do than because he really wanted coffee. There's always a soccer game on somewhere, and people actually seem to care, don't they? David forced himself to listen, even though he truly hated sports, especially soccer. The sports news finally ended as he was pouring his first espresso.

"Negotiations between the government of Iran and the P-5-plus-one powers have concluded successfully in Vienna. President Rouhani of Iran appeared with the leaders of the P-5-plus-one at 1:37 this morning Central European summer time to announce the signing of the agreement and the beginning of a new era in relations between Iran and the west.

"BBC News with Neil Nunez."

David sipped his espresso, listening with one ear as the terms of the agreement were presented yet again – for people who were tuning into the news for the first time in over a year, he guessed. He took the coffee over to his computer, turned the volume down, and started reading his work email. He wanted to look for news of the DDoS attack in the chat rooms, but he also wanted to avoid the whole thing. Dunant would probably fill him in.

Sure enough, the secure phone rang just as he hit send on the one message that his colleagues needed to read. He wasn't planning to go to the office tomorrow, and no doubt he'd get some grief for that, but the smartest and most conscientious guys in his group would stay busy all day with the information he'd just sent them. That would be the subject of conversation when he showed up on Thursday, not why he was out sick on Wednesday.

"Hi, Joe."

"Good evening. Looks like you were right."

David closed the BBC player window and sat in silence for a few seconds.

"David? You there?"

"Yeah, I'm here."

"Let's meet. How about 2 o'clock tomorrow in Mitchell Park?"

"OK." David disconnected, sipped some more coffee, and then closed the email client. He walked to the bedroom closet, pulled the photo out of the dress-shirt pocket, and flopped onto the bed. They were even now, sort of. He could stop being angry at Ari for not protecting him well enough in the banking scam. Maybe someday he'd stop thinking about him constantly. Not any time soon.

Wednesday, July 1, 2015, mid-afternoon. Mitchell Park, Palo Alto

"You did something great, David," Joe said. "For your country and for the whole world."

"You and your black-hat network did it, Joe. All I did was betray my friend."

They finished their second walk around the quarter-mile path and sat at a picnic table. Joe had been through this kind of thing with assets before. David now knew the full implications of the deal he'd made to avoid conviction and imprisonment in Israel. He'd now seen how unhesitatingly, even eagerly, the CIA would use the intimate details about Ari that he'd given them. He may or may not be able to go on with his second-chance life in Silicon Valley; if he couldn't live with himself and carry on without attracting attention, Joe would have to treat him as a threat.

"Do you know where he is now?," David asked.

"No. Nothing from any of his known pseudonyms or locations since we attacked. No contacts with any of his known associates."

David stared at the kids playing on the lawn and their helicopter moms. What the hell was he doing here? There was nothing to live for here. Nothing in the park, in the Valley, or in the whole damned country. How much longer was he supposed to pretend that working on data-center network security most of the time and meeting with his CIA handler every once in a while was anyone's idea of a life?

"What do you want me to do now?," he asked Joe.

"Take it easy for a while. I'm sure you'll be back in touch with us before too long. Or we'll be in touch with you."

"That's it? Ari's off the grid, and you people aren't even looking for him?"

"We'll find him, David, if there's a reason to. Maybe you'll point us to him, as you did this time. Try to focus on something else now. Maybe someone else."

David snorted and looked back at the lawn. “Yeah, sure,” he said, “Someone else.” What did Dunant mean, anyway? Find another boyfriend, or give them intel on another cyber wacko? Both, maybe. It was a pretty creepy way to live.

But he didn’t walk away.