Vision: Computing and Authentication Practices in Global Oil and Gas Fields

Mary Rose Martinez
Brown University
Providence, RI, USA
mary_rose_martinez@alumni.brown.edu

Shriram Krishnamurthi*
Brown University
Providence, RI, USA

ABSTRACT

Oil and gas fields are a critical part of our infrastructure, and vulnerable to attack by powerful adversaries. In addition, these are often difficult work environments, with constraints on space, clothing, and more. Yet there is little research on the technology practices and constraints of workers in these environments. We present what we believe is the first survey of oil- and gas-field workers located around the world. We establish the presence and status of a variety of computing devices and of the security practices that govern their use. We also determine the working conditions (such as personal protective equipment) under which these devices are used, which impacts usable security aspects like feasible forms of authentication. Our preliminary work suggests many directions for improving security in this critical sector.

ACM Reference Format:
Mary Rose Martinez and Shriram Krishnamurthi. 2021. Vision: Computing and Authentication Practices in Global Oil and Gas Fields. In *European Symposium on Usable Security 2021 (EuroUSEC '21), October 11–12, 2021, Karlsruhe, Germany.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3481357.3481524

1 INTRODUCTION

Oil and gas, a key part of the energy sector and critical infrastructure of many countries, is a significant security concern [8]. Its core end-products, like petroleum, are also parts of many other supply-chains: lubricants ("Vaseline" is petroleum jelly), plastics, preservatives, artificial limbs, flame-retardant clothing, and more. Furthermore, oil and gas is necessarily extracted in low-population areas and transported long distances, creating many opportunities for attacks.

The oil and gas industry has become increasingly driven by both information technology (IT) and operational technology (OT). The very components that make IT susceptible to cyberattack (e.g., software, data, connectivity, etc.) are now found in industrial control systems (ICS) and process control networks in the OT environment, thereby vastly increasing a company's attack surface. Of additional concern are the potentially grave repercussions of an OT cyber incident. Unlike an IT cyber incident, an incident in the field or a manufacturing plant has physical consequences that pose a risk to human life, safety and/or the environment.

In 2019, industrial cybersecurity company Dragos [10] said that the industry "remains at high risk for a destructive loss of life cyber-attack due to its political and economic impact and highly volatile processes." Malware, ransomware, and other attacks on petrochemical plants and pipelines make the news with some regularity. According to the 2018 Symantec Internet Security Threat Report, ICS vulnerabilities increased 29% from 2016 to 2017 [17]. Furthermore, the Dragos Threat Perspective also assessed that "state-associated actors will increasingly target oil and gas and related industries to further political, economic, and national security goals." This suggests threat actors who are well-funded and well-staffed, with more resources at their disposal than the average cyber criminal.

In this paper, we initiate study of the work environment of oil and gas personnel. Here, it is important to distinguish the three main sectors of the industry: upstream, midstream, and downstream. The *upstream* sector is focused on finding oil and gas reservoirs, and drilling wells in those reservoirs to extract crude oil and natural gas. Transportation from reservoirs and storage make up the *midstream* sector. The *downstream* sector refines and processes oil and gas into fuels and other materials. (That is, the product flows from "up" to "down".)

The contribution of this paper is to *study oil and gas field workers in the upstream sector*. We focus on them for three reasons. First, they work in locations with great potential for harm. Second, they often have the most unconventional work environments of people in this area. Finally, while they share some similarities to other "front line" workers (e.g., medical personnel), their physical location, bandwidth, etc. create unique challenges. In particular, we try to understand the *computer device use* while performing their job:

- What are the everyday computing practices of upstream oil and gas field workers?
- What ambient factors impact cybersecurity in the oil and gas field?
- Are there any usability challenges?

2 BACKGROUND ON OIL AND GAS

We assume the reader may benefit from a brief primer on the contemporary oil and gas industry. We also introduce some terminology useful in the rest of the paper.

2.1 The Use of Digital Technology

While the cyclical nature of the oil and gas industry is the norm, major shifts have occurred starting from the downturn in 2014 [15].

*Partially supported by the US National Science Foundation. Author thanks Tiago Guerreiro for citations.

EuroUSEC '21, October 11–12, 2021, Karlsruhe, Germany

ACM ISBN 978-1-4503-8423-0/21/10…$15.00
https://doi.org/10.1145/3481357.3481524

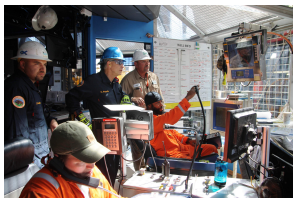

Figure 1: Typical onshore (left) and offshore (right) upstream workplaces. Images are, respectively, from Felix Adamo / *Bakersfield Californian* [1] (used with permission) and US Bureau of Safety and Environmental Enforcement [5] (public domain).

Its rapid and protracted nature caused companies to focus on operational efficiency as oil shifted from over $100/barrel to under $65/barrel, and then under $40/barrel. Shifts in both energy generation and emission reduction are further forcing technology changes [6, 9], a major part of which is the adoption of the Industrial IoT.

2.2 The Nature of Upstream Workplaces

Readers may have certain clichéd mental images of the nature of an upstream oil and gas field. In fact, the upstream workplace may take many forms, shown visually in fig. 1.

An onshore hydraulic fracturing spread typically includes a data van where field engineers and other company personnel monitor and manage the operation. Data vans range in size similar to a recreational vehicle (RV) and provide an office-like environment in the field. They have air conditioning, control noise levels, and protect personnel and computing equipment from the elements. There are desks for 3–4 people with space for laptops and peripherals such as monitors, keyboards, and computer mice. Some of the computer peripherals are connected to rack-mounted personal computers (RMPCs) stored in a small cabinet along with networking gear to support a local area network on the job site. For more remote locations without cellular coverage, connectivity is typically achieved using a satellite dish installed on the exterior of the van. There may also be a small seating area for guests who can observe a job using overhead monitors that are connected to the RMPCs.

Offshore oil and gas fields, on the other hand, are in far-flung and harsher environments, some located in ultra-deepwater where drilling occurs in depths greater than 1,500 meters. Their remoteness means they lack cellular connectivity, and may have much more drastic connectivity issues (section 2.3). Compared to land operations, offshore platforms also have significantly less space and accommodations for personnel to operate computing equipment.

Unlike in many corporate workplaces, in many upstream sites, there are many companies with shared governance. Typically, there is an *operator* who owns the asset (e.g., Shell, Chevron, ExxonMobil); one or more *service companies* that provide different services (e.g. Halliburton, Schlumberger, Baker Hughes); and a *rig owner*. There can actually be several (5–6) service companies on a particular site.

2.3 Bandwidth

In this paper we will see a persistent use of USB devices, which may surprise some readers, given their known security threats. These have a strong justification in this industry.

Oil and gas fields generate a significant volume of data. Fiber optics monitor a well's pressure, temperature, and the flow of fluids as oil and gas. Nuclear magnetic resonance and pulsed-neutron technology provide insight into rock formations, such as its lithology and mineralogy, to find oil and gas reservoirs. Sensors and processors are used downhole from where tens of thousands of data points every second are transmitted to drilling engineers who analyze the data to increase drilling precision in, if possible, near-real time.

In 2017, an offshore platform generated 1-2 terabytes of data daily while a typical satellite connection provides a transfer rate of 64 Kbps to 2 Mbps [12]. The amount of data generated in an oil or gas field continues to increase with the utilization of the Industrial IoT. Sensors are used in a variety of surface operations from monitoring of storage tank levels to, in combination with analytics and machine learning, preventive and predictive maintenance of equipment.

Owing to this wide variety of data transmission needs, a correspondingly wide range of devices is used. Some respondents use USB drives; others even continue to use USB sticks. Either way, the the volume of data relative to available bandwidth in effect demands physical data carriage.

3 SURVEY METHODOLOGY

We ran an anonymous, online survey on computing and authentication processes. The full survey and related materials, as well as interviews with select participants, are on arXiv [14]. All respondents were volunteers and not compensated. To protect respondents, an application was submitted to Brown's Institutional Review Board (IRB). The respondents were deemed to be Key Informants rather than Human Subjects, and hence not requiring IRB approval. Nevertheless, we have applied all standard and reasonable safeguards in collecting, retaining, and presenting data.

Recruitment. Using the first author's professional contacts, emails were sent to the CISOs of several upstream oil and gas companies to solicit participation from their field personnel. The email also contained a link to the online survey.

The list of oil and gas companies included some of the largest operators and oilfield services companies in the world, most of whom are on the Fortune 500. The invited operators included both international oil companies and independents, in order to obtain a global perspective. Hence, the representation of field personnel activity and processes spans the various stages and job types of the upstream oil and gas lifecycle, from drilling to production.

Procedure. The online survey was run from early July 2020 to the end of the month. Invited CISOs were left free to decide whether

to distribute the survey within their respective companies. We have no evidence that employees were pressured to respond; had they been, we may have received many more responses. At one company's request, the first author attended global meetings with its OT representatives to provide context and brief them on the study's intent. Some companies forwarded the survey directly. One major company made an internal copy of it and shared the results; this may have resulted in some redaction, making our findings an undercount. The survey was conducted anonymously, and study respondents were not compensated for their time or input.

In addition to demographic information, the survey consisted of three sets of questions. The first set centered around the computing equipment used, if any. Secondly, questions were asked regarding security practices while using computing equipment. Finally, there were questions geared towards understanding the impact of ambient factors in field operations. Free-response boxes were included throughout the survey for optional further elaboration.

Our survey is necessarily limited in scope. First, we were unable to ask particularly sensitive questions, due to companies wanting to protect information about vulnerabilities. Second, the survey needed to be brief: upstream workers often alternate between high-intensity work on-site followed by periods of relaxation off-site. This makes their time precious, and did not give us the luxury of asking about all the security practices of potential interest. Indeed, we worked extensively to limit our survey size to persuade the CISOs to share it. Finally, we were unfortunate to run into COVID-19, which has shrunk the workforce in this sector and has created significantly greater pressure and job anxiety for those who remain employed. Our design had to account for these realities.

Respondents. A total of 91 people participated in the survey, summarized in fig. 2. Although the demographic questions were optional, only 9% of the respondents declined to answer. Of the 84 respondents, seventy-nine (94%) of the respondents were male and five (6%) were female. In terms of age distribution, most were between 25 and 54 years old, with an even split among the 25–34, 35–44, and 45–54 age ranges.

In terms of education level, in 2017, the RAND Corporation projected that more than 60% of jobs from 2014 through 2024 in the upstream sector will require postsecondary education, a number higher than that of the midstream and downstream segments [4]. In comparison, the majority of respondents had a bachelor (4-year) degree or higher; 33% of this group also obtained a graduate degree. Only five people (6%) did not have any additional training or education beyond a high school diploma or secondary education. This indicates that the surveyed group represents more of the educated upstream workforce than average.

Respondents were also asked about their number of years of experience in the oil and gas field. The responses reflected a wide range of experience levels, from 0–5 years of experience to one respondent having over 40 years of experience. Most people had between 0 and 25 years of experience.

The geographies represented in the survey spanned the globe and provided relatively good coverage. Multiple responses were allowed in this question since it is not uncommon for oil and gas field workers to work in more than one location. The regions most indicated were North America (26%), the Middle East (23%), Europe (21%), and Asia (20%), with one person having worked across all four regions. There were also five respondents from Oceania and three from Africa. Other than lower participation from Africa, the geographical distribution is representative of the oil and gas regions around the world reported in the 2019 Oil & Gas Employment Outlook Guide [2].

	N	%
Gender		
Female	5	6
Male	79	94
Age		
18–24	2	2
25–34	24	29
35–44	23	28
45–54	24	29
55–64	10	12
Education		
High school diploma / secondary education	5	4
Trade / technical / vocational training	3	54
Associate / 2-year degree	3	33
Bachelor's / 4-year degree	44	6
Graduate / 6-year degree or higher	27	4
	N	%
Years of Oil & Gas Field Experience		
0– 5	15	18
6– 10	19	23
11– 15	14	17
16–20	16	19
21–25	10	12
26–30	3	4
31–35	3	4
36–40	2	2
40+	1	1
Work Location (multiple responses allowed)		
Africa	3	3
Asia	17	20
Central America	1	1
Europe	18	21
Middle East	20	23
North America	23	26
Oceania	5	6

Figure 2: Respondent Demographics.

Sampling Threats. Of course, several factors conspire to skew the respondent sample. Naturally, this is only a small fraction of the total number of people employed in this area. Second, they are in a kind of position where they might be reached by a CISO and respond. Most of all, the survey was conducted at the height of the COVID-19 pandemic, at a time when layoffs and job uncertainties were high globally, but especially so in the oil and gas industries, which had seen demand worldwide plummet. Some of these factors may explain the higher education level of our respondents. Nevertheless, despite these factors, we do not (based on the expert

knowledge of an author) find the responses to the survey especially outside the bounds of expectation.

4 SURVEY FINDINGS

The overwhelming majority of respondents (96%) use at least one computing device at a job site. Only five respondents answered "none" to the question "What computing device(s) do you use for work at a job site?". (Note that some of the questions allow multiple answers, so participation may appear to exceed 100%.)

4.1 Computing Equipment

Twenty percent of survey respondents use computing devices that are fixed (e.g. installed inside a field trailer, mounted on equipment, etc.). The rest use mobile computers such as laptops and tablets, some in addition to fixed computing devices. Of the mobile computing users, 90% use machines that are assigned to them while 22% share a computer with others. A mouse and keyboard are the most commonly used peripheral equipment in the field (85% use a mouse, 59% use a keyboard). 15% also indicated the use of a pen or stylus.

In terms of external USB devices, 53% of respondents use USB storage. Of those, 68% use one provided by the company and 45% use a personal one.

Respondents were evenly split on whether the comfort of the work environment affected their use of a computer. Some common challenges, especially for offshore or remote locations, were space restrictions, limited connectivity, and lack of privacy. On the other hand, a respondent reported, "*At the worksite, the computing device is usually used in a data van, which has the requisite air conditioning and seating space.*" Yet another reported "*There is a standard office environment on [a] job site.*"

4.2 Security Practices

User IDs and passwords remain the prevalent method of logging onto computers used in the field with 86% of the computer users. The next most prevalent was badge scans at 18%. Biometrics were rare: 6% use fingerprints while 4% use facial recognition. Another 4% use some other methods. 18% used more than one method.

For survey respondents who use a shared computer, a little over two-thirds use individually assigned user IDs and passwords, while 31% use a shared user ID and password.

When asked what they *preferred*, support for passwords reduced to 58%, with 38% preferring fingerprints and 23% facial recognition. Support for badge-scans was nearly twice its current use, at 31% badge scans. 2% also suggested other methods. Some readers may find some of these numbers surprising: e.g., why would so few be in favor of biometrics and so many still in favor of passwords? We believe the use of protective equipment may have a major impact, and discuss this in section 4.3.

There were a wide range of frequencies with which respondents were forced to change passwords. The most frequent by far—for 70%—was, perhaps surprisingly, every 2–3 months. The next most frequent was yearly (9%), every 4–6 months and never (each 6%), and some (one person) as frequently as every week. Some also reported more detailed policies, such as not having to change them unless there was a problem ("*all accounts are changed after a failed phishing exercise or proof of compromise*"). Also, for some respondents the frequency depended on whether or not multi-factor authentication was used: "*[Passwords are changed] yearly provided you have MFA enabled, 3 months for non-MFA accounts.*" Respondents also made distinctions between field computers, corporate computers on the job site, and control systems.

Given the support that remains for passwords, it is interesting to see responses to how often they thought passwords *should* be changed. To researchers, the revised NIST recommendations [11] to not demand frequent changes are probably well-known, based on the rationale that frequent changes lead to weaker passwords [3]. Yet the most chosen response was still every 2–3 months (35%), followed by 4–6 months (22%), then monthly (14%), and annually (12%), with 2% choosing even weekly and daily. Of course, not all respondents were fans of password changes: one commented that they should be changed only when passwords are "*exposed*", another only "*when necessary*", and yet another, "*Changing passwords across devices & applications is time consuming and tedious. This should be engineered out.*"

One of our interests is in creating better authentication mechanisms for field workers. Several factors play into this: the ease with which passwords can be stolen in cramped spaces (which can lead to misattribution, masking attacks, etc.), the likelihood that passwords shared between individuals are likely to be of much lower quality than those kept private, and the interest of respondents in biometrics. We are therefore curious about the potential to use other authentication methods (even if not as a primary method, then at least as a second factor).

4.3 Personal Protective Equipment

While biometrics are attractive, field personnel do not work in white-collar office space. Safety is paramount in the oil and gas industry and specific personal protective equipment (PPE) is required in field operations. Most field personnel wear coveralls, steel-toed shoes, and hard hats. Additional PPE may be required depending on the type of operation being conducted, a person's job function, and the environment. For instance, gloves are typically used when managing heavy equipment, ear plugs protect against high noise levels generated by pumps and other machinery, and respirators prevent fume inhalation when handling chemicals. Any and all of these can interfere with one or more forms of biometric authentication.

This survey was conducted while COVID-19 was well in progress. Our goal was to get "steady state" information that was not overly biased by temporary factors. We were concerned that simply wording the survey to indicate that would not be sufficient, since some respondents might not read the instructions carefully, thereby skewing our results. We therefore added explicit questions about PPE during COVID-19 to appear first, followed by the steady-state question, to make clearer the context when they reached the general question about PPE.

Both questions we posed to respondents asked "which personal protective equipment (PPE) do you use that **INTERFERES** with your use of the computer" (boldface and caps in the original questionnaire). The survey had check-boxes for *all* the PPE commonly used in the field, even if it is a priori unclear how some of them—e.g.,

steel-toed shoes—might interfere with computer use. (Full details are in the arXiv version.)

In both situations, slightly over half indicate that PPE does not interfere with computer use. Of the remaining respondents, outside COVID, gloves are the greatest obstruction (64%), followed by safety glasses (24%), masks (19%), coveralls (14%), and hard-hats (14%), and a few others. Some of the hindrances may not be obvious:

- "*A hard hat sometimes 'slips', although this may be corrected with proper wearing of the hard hat.*" This is especially likely to occur when leaning over terminals for short-term use.
- "*Ear protection needs to be removed when viewing video 'guides' and 'reference materials'.*"

Under COVID-19, the biggest differences were masks (which went up to 68% of those reporting interference) and respirators (10%, as opposed to nobody outside COVID). Since these are predictable differences, it suggests that our survey strategy reasonably distinguishes between COVID-19 and "steady state" information.

A small number of respondents may nevertheless have listed all the PPE they *use* (especially the one who checked all the boxes), not only that which interferes. We have not, for instance, been able to determine how steel-toed shoes can be problematic. However, the reasons may be subtle: e.g., respondents noted that safety goggles can get smudged or scratched, making it hard to perceive fine-grained details.

Some of these issues, such as slipping hard-hats, seem to be general computer use issues (and may be better corrected by, e.g., raising the machine). Others, like ear plugs, may be relevant to the design of authentication systems (e.g., audio-based authentication). It is especially important to consider combinations of PPE: for workers wearing heavy protective gloves, it can be particularly cumbersome to remove ear plugs.

5 DISCUSSION

While oil and natural gas can be expected to play a role in the global energy mix, market economics are demanding a marked change in operating practices to reduce cost. Operators and oilfield services companies alike are leveraging digital technology in field operations to increase efficiency and lower operating costs. Digital technology is further used for real-time monitoring and remote operations, allowing jobs to be executed by fewer personnel onsite (in industry parlance, "de-manning of the rig"). With fewer field hands, the remaining onsite personnel use technology and software to feed data to remote operating centers and manage field systems. For instance, physical checks of fluid levels in a tank are replaced by liquid level sensors monitored by a computer. This study confirms the prevalent use of computing in oil and gas field operations with 96% of respondents confirming that they use at least one computing device. The results of the study also underscore the importance of system design for improved usability and security.

Computer Hardware and Software. Despite the widespread use of mobile devices, 56% of respondents still reported using an external keyboard and 80% still use a mouse. The widespread use of peripheral equipment indicates that laptop touchpads and keyboards are not easy to use in the field, likely due to the required use of gloves—which respondents consistently reported as interfering with computer use. Weather conditions may also be a factor (e.g., lack of finger dexterity in extreme cold; sweaty hands in extreme heat), especially for computers on fixed equipment that are subject to the elements. The need for additional peripheral equipment may also exacerbate already existing space constraints, especially in offshore operations.

Operations managers should consider the increased use of badges, or touchscreens with suitable gloves. The user interface of software programs could likewise be improved: e.g., using button selections instead of dropdown menus, reducing the need to type information with a keyboard, and providing support for voice commands and responses (though this can be problematic in some field locations due to ambient noise levels).

Data Transmission. Half of survey respondents also reported the use of USB storage devices. With 45% of the USBs used in the survey being personal devices, USBs pose an even more serious risk to field operations. Even where connectivity is available, it comes with burdens: "*Limited internet connectivity offshore means sharing a small, cramped room with other individuals to perform duties that require connectivity and internet access.*" Our preliminary study did not investigate practices in place to guard such devices; this is clearly an area for future work.

Authentication. The study shows a difference between current and preferred authentication methods. Given the generally perceived cumbersomeness of passwords, we were surprised that respondents wanted passwords at all, and wanted them changed frequently (and in some cases, more frequently than they are now). Survey comments indicated the use of individual accounts for corporate devices but shared accounts for field computers. This may explain the continued preference for passwords, but in reality necessitates better identity and access management. The preference for passwords may also be because individuals are comfortable with using logon credentials as the customary method, or that there is skepticism around the use and storage of their biometric information. (Biometrics like facial recognition may also interact poorly with PPE, beard growth, etc.) Again, future work must provide more insight into this topic.

6 RELATED WORK

We are aware of no comparable work on field practices in this sector. There is other work in security for oil and gas. Some of it is constructive in nature: e.g., a cryptographic protocol for SCADA communications that is designed around the low bandwidths available in critical infrastructure [19]. There are also investigative studies, including ones cited above, that analyze attacks. However, we are not aware of ones that focus directly on the people who actually work in upstream sites. In terms of authentication and PPE, systems like ZEBRA [13] may be useful. NIST guidelines for public safety usable security also cover some PPE-related issues [7]. Another rich source of information is research on situationally-induced impairments and disabilities, which our domain corresponds to [16, 18].

7 FUTURE WORK

There are many directions for future work:

- Sample a bigger population and in more depth.

- Better understand the security mindset of these employees (e.g., do they view USB storage as a threat?).
- Investigate secure data transfer for these environments.
- Do on-site work; this is difficult because, even if access to a rig were granted, the safety training alone is prohibitive (e.g., it includes water survival in case of a helicopter crash).

Nevertheless, ultimately, a deep understanding of the impact of PPE and other ambient factors should result in innovation in both hardware and software design, as well as novel authentication practices, which seem essential in these constrained domains.

REFERENCES

[1] INSIDE FRACKING: Chevron offers rare look at controversial practice. *The Bakersfield Californian* (July 2015). https://www.bakersfield.com/news/inside-fracking-chevron-offers-rare-look-at-controversial-practice/article_bf5f4865-0b98-592a-905c-63a8e007c2d5.html, retrieved 2021-08-01.

[2] 2019 oil & gas employment outlook guide. Tech. rep., OilAndGasJobSearch.com, 2019. https://energyoutlookguide.com/wp-content/uploads/2019/07/oil_and_gas_outlook_guide_2019.pdf, retrieved 2021-02-25.

[3] NIST special publication 800-63: Digital identity guidelines: Frequently asked questions, July 2020. https://pages.nist.gov/800-63-FAQ/#q-b05, retrieved 2021-02-25.

[4] Bozick, R., Gonzalez, G. C., Ogletree, C., and Carew, D. G. Developing a skilled workforce for the oil and natural gas industry: An analysis of employers and colleges in Ohio, Pennsylvania, and West Virginia. Tech. Rep. RR-2199-NSF, Rand Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2100/RR2199/RAND_RR2199.pdf, retrieved 2021-02-25.

[5] Bureau of Safety and Environmental Enforcement. BSEE director participates in offshore inspection, July 2017. https://www.bsee.gov/newsroom/latest-news/statements-and-releases/press-releases/bsee-director-participates-in-offshore-inspection, retrieved 2021-02-25.

[6] Candina, J., González Fernández, D., Hall, S., and Verre, F. Reinventing upstream oil and gas operations after the COVID-19 crisis. Tech. rep., McKinsey, 2020. https://www.mckinsey.com/industries/oil-and-gas/our-insights/reinventing-upstream-oil-and-gas-operations-after-the-covid-19-crisis, retrieved 2021-02-25.

[7] Choong, Y.-Y., Franklin, J. M., and Greene, K. K. Usability and security considerations for public safety mobile authentication. Tech. Rep. 8080, National Institute of Standards and Technology, 2016. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8080.pdf, retrieved 2021-06-06.

[8] Cybersecurity & Infrastructure Security Agency. Critical infrastructure sectors, Oct. 2020. https://www.cisa.gov/critical-infrastructure-sectors, retrieved 2021-02-25.

[9] Dickson, D. 2021 oil and gas industry outlook. Tech. rep., Deloitte, 2020. https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/oil-and-gas-industry-outlook.html, retrieved 2021-02-25.

[10] Dragos. Global oil and gas cyber threat perspective. Tech. rep., Dragos, Aug. 2019. https://www.dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf, retrieved 2021-02-25.

[11] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Danker, N. B. L. J. M., and Theofanos, Y.-Y. C. K. K. G. M. F. Digital identity guidelines: Authentication and lifecycle management. Tech. Rep. 800-63B, National Institute of Standards and Technology, June 2017. https://pages.nist.gov/800-63-3/sp800-63b.html, retrieved 2021-02-25.

[12] Hand, A. Oil and gas at the edge. Tech. rep., Sept. 2017. https://www.automationworld.com/products/control/blog/13317745/oil-and-gas-at-the-edge, retrieved 2021-02-25.

[13] Mare, S., Molina-Markham, A., Cornelius, C., Peterson, R. A., and Kotz, D. ZEBRA: zero-effort bilateral recurring authentication. In *IEEE Symposium on Security and Privacy* (2014).

[14] Martinez, M. R., and Krishnamurthi, S. Computing and authentication practices in global oil and gas fields, 2021. arXiv:2108.02660v1.

[15] Rogoff, K. What's behind the drop in oil prices?, Mar. 2016. https://www.weforum.org/agenda/2016/03/what-s-behind-the-drop-in-oil-prices/, retrieved 2021-02-25.

[16] Sears, A., Lin, M., Jacko, J., and Xiao, Y. When computers fade… pervasive computing and situationally-induced impairments and disabilities. In *International Conference on Human-Computer Interaction* (2003).

[17] Symantec. Internet security threat report. Tech. rep., Symantec, Mar. 2018. https://www.phishingbox.com/assets/files/images/Symantec-Internet-Security-Threat-Report-2018.pdf, retrieved 2021-02-25.

[18] Wobbrock, J. O. Situationally aware mobile devices for overcoming situational impairments. In *Symposium on Engineering Interactive Computing Systems* (New York, NY, USA, 2019).

[19] Wright, A. K., Kinast, J. A., and McCarty, J. Low-latency cryptographic protection for SCADA communications. In *Applied Cryptography and Network Security, Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004, Proceedings* (2004), M. Jakobsson, M. Yung, and J. Zhou, Eds., vol. 3089 of *Lecture Notes in Computer Science*, Springer, pp. 263–277.