THE ETHNOGRAPHY OF A DIGITAL OBJECT

An Example from Computer Security

Sylvain Besençon, David Bozzini

Keywords: *cybersecurity, vulnerability disclosure, digital ethnography, ethnographic location, encryption, controversy*

What happens when Eve[1] finds a "bug" compromising the security of a particular software? She can sell it on the black market to criminal organizations or to vulnerability brokers who are building cyber arsenals for law enforcement agencies. But Eve can also decide to report the security bug – or the "vuln", for vulnerability – to the company or the team who developed the software for them to fix it as soon as possible. This happens several times per day in the global field of information security (infosec) and is called vulnerability disclosure and management. These sensitive processes engage various actors negotiating multiple aspects of what is perceived as a crisis whose proportions can vary from the distress of a handful of hyper-specialized experts to a full-blown scandal involving major companies of the digital economy.

Our current research project looks at these particular kinds of processes to explore a relevant part of the mundane fabric of computer security.[2] We aim to analyze the negotiation of practical norms and relationships of power between a wide range of experts involved in these processes. To do so, we decided to track vulnerabilities from the moment of their public disclosure and to account for their management until a fix is provided. However, we quickly had to acknowledge that the disclosures can happen behind closed doors at first and are often a disjointed and lengthy process that takes place simultaneously in different locations and for various durations. Similarly, vulnerability management processes are often obfuscated and can also be lengthy and scattered. This assessment led us to reconsider the nature of our empirical research and in particular the types of processes we are able to follow.

What follows is a reflection on the nature of our ethnography of computer security practices, taking a particular disclosure as a case in point to outline some preliminary thoughts on the conceptualization of our objects. Considering the scope of this piece, we limited our

[1] Alice, Bob and Eve are fictional characters widely populating the argumentations of computer security experts.

[2] This research project is funded under the SNSF scheme "Digital Lives". The project description can be found in the SNSF p3 database: http://p3.snf.ch/project-183223 (accessed January 21, 2020).

DOI 10.36950/tsantsa.2020.025.15

description to the way a particular process of vulnerability disclosure and management unfolded without delving into the details of the actual controversies it caused.[3]

The trajectory of a vulnerability named EFAIL

EFAIL is the name given to a series of vulnerabilities that affect two end-to-end email encryption protocols: OpenPGP and S/MIME.[4] We did not choose this example because it is representative of a usual disclosure and management of computer vulnerabilities – it is not. We chose it rather because the disclosure and management of EFAIL forced us to question the location, the temporality and the limitations of our ethnography, but also helped us to reconsider the nature of the vulnerabilities and the processes in which they are entangled. We summarize the EFAIL trajectory after public disclosure with the following four ethnographic vignettes.

The messed up public disclosure. For a few days in May 2018, most of the attention of the IT security crowd seemed to be devoted to a declaration on Twitter: on May 13, 2018, at 11pm (in Germany), Sebastian Schinzel tweeted that his team had found a series of critical vulnerabilities in email encryption protocols against which there were no reliable fixes available.[5] The tweet announced that the full details would be made public two days later. The tweet also provided a link to a blog post of the Electronic Frontier Foundation (EFF) with some provisional mitigation measures.[6] Following this announcement and even though the full details were not yet available, many people started to debate and speculate about the issues. These discussions happened in several digital spaces, mostly on Twitter, but also on forums and mailing lists. The day after the announcement, details about the vulnerability leaked,[7] leading to a chaotic situation that forced the EFAIL researchers to expedite the official disclosure of the full paper. Several articles in newspapers, websites and blogs were published immediately after, hyping even more the controversial issues about the nature of the vulnerabilities and how they were disclosed. Debates relating to the disclosure, the vulnerabilities, the threat to users (including journalists and activists) and the protocol itself raged for nearly two weeks on several online platforms before fading away. These debates, however, were only the tip of the iceberg, since a whole series of private disclosures took place away from the spotlight and well before Schinzel's tweet: more than thirty vendors were contacted (Ptacek 2018) and given deadlines to react before the public disclosure of the vulnerability.

[3] Several files documenting EFAIL can be found on our online data repository: https://cva.unifr.ch/content/trajectory-vulnerability-named-efail/essay (accessed January 21, 2020).

[4] See https://efail.de/ (accessed January 21, 2020) for more details. An encryption protocol consists of a text document that specifies the specs and instructions to encrypt and decrypt a given file. OpenPGP and S/MIME are the two main encryption protocols that are used for emails.

[5] https://twitter.com/seecurity/status/995906576170053633 (accessed January 21, 2020).

[6] https://www.eff.org/deeplinks/2018/05/attention-pgp-users-new-vulnerabilities-require-you-take-action-now (accessed January 21, 2020).

[7] For some details regarding the leak see Ptacek (2018).

The IETF OpenPGP working group mailing list. The Internet Engineering Task Force (IETF) is the organization responsible for the standardization of many internet protocols including OpenPGP and S/MIME.[8] There was no immediate reaction after the public disclosure of EFAIL, but on June 30, 2018, an email called "AEAD mode chunk size" was sent to the mailing list[9] and provided some technical thoughts about how to mitigate one specific issue of EFAIL. An asynchronous conversation started – mostly on a highly technical level – which happened only through emails involving many actors worldwide. In other words, the EFAIL vulnerability management took place in this forum. This process lasted till May 2019 and resulted in the release of a new version of a part of the protocol which was later implemented in many software programs and libraries.[10]

During that time, many other topics were discussed on this mailing list but interestingly, there were only very few explicit references to EFAIL. Instead, the vulnerabilities were dissociated into a series of technical issues to be remediated separately, sometimes by different people. It is also interesting to note that the tempo of what was done and exchanged through the IETF mailing list was not impacted by other manifestations of the vulnerability in the infosec community, like the Usenix presentation that took place in August 2018. The discussion happened predominantly amongst engineers and developers committed to finding a consensual solution to be implemented in various compatible yet competing products.

The academic presentation at Usenix conference. On August 16, 2018, in the Grand Ballroom VII–X of the Marriott Waterfront hotel in Baltimore, USA, Damian Poddebniak, on behalf of the EFAIL team, presented the EFAIL attack in front of an academic audience at the Usenix Security Symposium.[11] Poddebniak deciphered the technicalities of the flaws they uncovered on the encryption protocols. In this particular case, the EFAIL vulnerabilities were assembled for an academic audience as an object of study in computer science: a paper presenting a formal explanation of a new cryptographic technique that the researchers called "malleability gadgets" (Poddebniak et al. 2018). In this sense, EFAIL was presented at Usenix as an example of a novel class of attacks on cryptographic protocols and was accordingly received and valued very well according to the researchers. As Schinzel himself told us, the Usenix paper had to be "translated" into a more digestible format for developers and users (personal interview in Leipzig, 27.12.2018). One example of such a translation was presented by himself at the Chaos Communication Congress.

[8] IETF standards are published as "Requests for comment" (RFC) and are freely accessible to anyone on the IETF website. Each protocol is the responsibility of a working group composed of volunteers dedicated to defining and maintaining the standard during the trimestral 5-day IETF meetings or on the mailing list which is freely available online to anyone. For example, the specs for the OpenPGP protocol is the RFC4880: https://tools.ietf.org/html/rfc4880 (accessed January 21, 2020); and the mailing list can be found here: https://www.ietf.org/mailman/listinfo/openpgp/ (accessed January 21, 2020).

[9] https://mailarchive.ietf.org/arch/msg/openpgp/t79iRZ80KHuVTEyVVLAoCLl4Rwc (accessed January 21, 2020).

[10] In computer development, a library is a collection of resources used by software.

[11] We did not attend this conference, but the paper, the video and the slides are available online: https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak (accessed January 21, 2020). We also discussed this talk with the researchers.

The presentation at the Chaos Communication Congress. The Chaos Communication Congress (CCC) has taken place every year since 1984 and is a major rendezvous for all geeks and technology enthusiasts in Europe. On December 28, 2018, at 8.50 pm, Sebastian Schinzel took the stage wearing a tee-shirt with the logo of EFAIL. Notably different from the Usenix paper, this 1-hour presentation was neither too formal nor too specialized and in addition to the technical details, it also gave room to broader considerations such as the pervasive lack of privacy that affects emails and took the opportunity to address the misadventures of the EFAIL disclosure process. Hence, among other things, this talk was an opportunity to underline some lessons Schinzel had learned from the disclosure and a way for him to bring the controversy that erupted after his initial tweet to an end: first, Schinzel explained that his experience in reaching developers and giving them more than 200 days to fix the issues before publicly disclosing the vulnerabilities had proved counterproductive. As a consequence, he went on to declare that henceforth he would stick to the rule of 90-days before disclosing his future research publicly.[12] The second lesson Schinzel shared was about the warning he had initially tweeted. He found that people did not understand his intentions and added that he would probably never again release a warning statement prior to the publication of the vulnerability itself.

The simultaneous lives of a vulnerability

These vignettes show that the EFAIL vulnerabilities took many forms at different times: like a proton in a high energy physics experiment, the impact of disclosure created different simultaneous strains transforming what the researchers discovered into various instances of EFAIL:[13] it instantly morphed into an urgent threat for journalists and activists, a communication fiasco severely criticized, another reason to abandon OpenPGP adding to a two-decade old polemics about the standard, a series of technical issues to define and to fix separately, a series of remedies to negotiate and assess, an academic paper defining a new type of attacks on cryptography, and a myriad of discourses about what should constitute respectful and ethical vulnerability management as well as a CVE number, a logo and a domain name (efail.de).[14] As in any ethnographic research, we were not able to follow every step and discussion related to EFAIL that took place behind the scenes. Perhaps nobody could grasp the complete processes, not even the EFAIL researchers themselves.

Our ethnographic experience did not give us enough time to reflect analytically on what EFAIL was: we assumed we had to keep up with a unitary object that had created a crisis for a significant number of people all over the world including those who were trying to solve

[12] An arbitrary period fixed on the software development cycle that is widely respected by computer security researchers to allow developers to find a remedy to a vulnerability before disclosing their research publicly.

[13] In computer science and in particular in programming, an instance is an object of a class with particular variables assigned to it. By extension here, an EFAIL instance is a technical object with particular characteristics (or a version) that belongs to what Schinzel and his team named EFAIL in May 2018.

[14] CVE stands for Common Vulnerability and Exposure, the most widely used register which references the major vulnerabilities publicly disclosed.

it. EFAIL kept popping up in different locations, adding new sets of actors to the debates or new events to our EFAIL timeline. We decided to work on this article to engage with the unease we felt when we tried to define our ethnography in terms of locations and events. Eventually, we came to the conclusion that EFAIL was not one object we were tracking but several instances of what the public and messy disclosure sparked off.

In this paper, we mention four ethnographic vignettes that correspond to four discrete instances of EFAIL. Each of these public manifestations of EFAIL led to discussions about what EFAIL was, using different discursive registers and coalescing different participants and audiences together. However, these instances remained closely related to the EFAIL vulnerabilities discovered by Schinzel and his team. Hence, each vignette represents one particular instance of EFAIL, rather than a period or a location of ethnographic documentation.[15] Each instance is indeed coterminous with the audiences, the practices and the significations it has coalesced, letting us consider EFAIL as a boundary-object characterized by a high interpretative flexibility (Star and Griesemer 1989). In other words, the EFAIL vulnerabilities acted in the world to materialize themselves through different, but sometimes intersecting, instances.[16] The last part of this article reviews the spatial and temporal dimension of the process of vulnerability disclosure and management.

The location and temporality of computer vulnerabilities

It is easy to realize that an ethnography of vulnerability disclosure and management is spatially fragmented. It necessarily takes place in multiple locations as the EFAIL case exemplifies. In addition, the tracking of computer vulnerability involves various types of ethnographic locations: nowadays, conference venues, as well as digital platforms such as Twitter or a mailing list have become usual sites or locations of ethnographic interest. However, we remained uncomfortable when thinking about our ethnography in terms of field-sites. We could easily mention that our ethnography is multi-sited and consists of following specific things (Marcus 1995) but this was not helping us to account for our ethnographic approach and the nature of the processes and the object we were following, until we stopped thinking about our objects and our ethnographic approach in terms of spatial dimensions.[17]

Like Emily Martin (1997: 146) before us about the ethnography of science, we came to the conclusion that our ethnography was not primarily spatial and that the spatial distribution of vulnerability disclosure and management is equally not a primarily relevant dimen-

[15] Moreover, in the case of the first vignette we can easily define several instances of EFAIL caught in various intersecting controversies. For the sake of clarity, we decided, nevertheless, to follow a conventional ethnographic description, wrapping up a multiplicity of issues and arenas in one unitary event we called "public disclosure".

[16] In addition, EFAIL illustrates well how disclosures can sometimes give rise to indeterminacy about the management of vulnerabilities. Hence, the actors, the places, the infrastructure of remedies, etc. often cannot be defined beforehand (in research project applications for instance).

[17] Concomitantly, we reminded ourselves of the seminal text of Gupta and Ferguson (1997) and acknowledged that spatiality was indeed still an implicit and crucial dimension in our understanding of our own ethnographic labor.

sion of the processes we are observing.[18] What is primarily relevant to account for these processes is of course the dynamic assemblage of people, ideas and practices around a known vulnerability or, as we argue more specifically, a series of discrete but interconnected instances of it.

In our experience, the difficulty we had in thinking in spatial terms about our object and our ethnography, helped us to eventually identify the multiplicity of EFAIL instances. In other words, the four vignettes we defined firstly as sites of ethnography were revealed to be more importantly four instances of what we were observing. We contend that this heterogeneity is by no means specific to digital objects.

EFAIL also cannot be apprehended by a single temporal unit such as an event in the sense proposed by Bensa and Fassin (2002). If the EFAIL disclosure is itself undeniably a noticeable event planned as such by the researcher,[19] it is important to note that the disclosure is not a unique point in time: the researchers disclosed their findings to a significant number of concerned persons before deciding to name and tweet EFAIL. Subsequently, the disclosure event also encompassed a version of EFAIL on a website (efail.de) and on a blog post written by an EFF staff member. In addition, we argued that Schinzel's tweet sparked various strands of debates and actions at different times: almost immediately for some and over the course of the year for others. Instances of EFAIL were presented during important events such as conferences in which the meanings of the vulnerability were again reframed.

All things considered, it not so easy to determine when EFAIL started and when it ended when we acknowledge the existence of various instances composed of different meanings, audiences and practices. Accordingly, we could not determine a beginning, a climax and an end to EFAIL without reducing its complexity. Therefore, the linear model of a vulnerability lifecycle commonly depicted by computer scientists (Frei et al. 2008) or the attempt to conceptualize disclosure and vulnerability management as an event – or even a series of sub-events – run the risk of over-simplification in coalescing various and simultaneous processes and controversies in one linear workflow and one unique timeframe.

Moreover, it appears obvious that we cannot limit our understanding of vulnerability disclosure and management to the discussions taking place at events such as conferences or during a Twitterstorm. It is indeed necessary to look beyond the rhetoric of crisis that characterizes these events to consider the quite un-eventful and asynchronous deliberations of a one-year conversation over the IETF mailing-list and contemplate the routinized work of protocol maintenance: a continuous effort to keep up with the never-ending flows of famous and less known vulnerabilities.

Therefore, we contend that EFAIL can be more accurately understood as an assemblage of instances that emerge, develop and intersect in various locations and at different times. In this sense, EFAIL indicates that a computer vulnerability can be conceptualized in similar

[18] To be sure, we are not saying that the instances of a vulnerability or the parts of the disclosure and management processes are nowhere to be found and immaterial. On the contrary, they can be instead located in a countless number of sites and their materiality is of course undeniable.

[19] See for instance, Jan Wildeboer's answer to Schinzel's tweet on May 13, 2018: "Why the drama? Why not simply release the details now instead of Hollywood style 'come back tomorrow for more!'" (https://twitter.com/jwildeboer/status/995919421901361152, accessed January 21, 2020).

terms as what Zigon defines as a global situation: an assemblage of manifestations diffused across different global scales and in which persons and objects get caught up in various capacities, intensities and conditions (2015: 502). In that perspective, tracking vulnerabilities allows us to partially witness how the global field of information security is constantly (re) constituted in various transitory but also recursive collectives forming around particular issues that they contribute to shaping discursively and in practice.

References

Bensa Alban, Fassin Eric. 2002. «Les sciences sociales face à l'événement». *Terrain* 38: 5–20.

Frei Stefan, Tellenbach Bernhard, Plattner Bernhard. 2008. "0-Day Patch – Exposing Vendors' (In)security Performance". *Black Hat Europe*, London. https://www.blackhat.com/presentations/bh-europe-08/Frei/Whitepaper/bh-eu-08-frei-WP.pdf, accessed January 21, 2020.

Gupta Akhil, Ferguson James (eds.). 1997. *Anthropological Locations*. Oakland: University of California Press.

Marcus George E. 1995. "Ethnography in/of the World System: The Emergence of Multi-sited Ethnography". *Annual Review of Anthropology* 24: 95–117.

Martin Emily. 1997. "Anthropology and the Cultural Study of Science: From Citadels to String Figures", in Gupta Akhil, Ferguson James (eds.). *Anthropological Locations*. Oakland: University of California Press: 131–146.

Ptacek Thomas H. 2018. "A Unified Timeline of Efail PGP Disclosure Events". Online: https://flaked.sockpuppet.org/a-unified-timeline/, accessed January 21, 2020.

Poddebniak Damian, Dresen Christian, Müller Jens, Ising Fabian, Schinzel Sebastian, Friedberger Simon, Somorovsky Juraj, Schwenk Jörg. 2018. "Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels". *27th USENIX Security Symposium*. https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak, accessed January 21, 2020.

Star Susan Leigh, Griesemer James R. 1989. "Institutional Ecology, Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39." *Social Studies of Science* 19(3): 387–420.

Zigon Jarrett. 2015. "What is a Situation? An Assemblic Ethnography of the Drug War". *Cultural Anthropology* 30(3): 501–524.

Authors

Sylvain Besençon is a PhD candidate in Social Anthropology at the University of Fribourg where he is preparing a dissertation on the making and unmaking of online communication security with a focus on the standardization and maintenance work related to cryptographic protocols. He is interested in the Free and Open Source Software (FOSS) movement and in hacker cultures. He holds a MA degree in Anthropology from the University of Neuchâtel and has been researching on community-based tourism in Peru as well as on activism, art and migration in the USA and South Africa.

sylvain.besencon@unifr.ch
University of Fribourg
Department of Social Sciences
Boulevard de Pérolles 90
CH-1700 Fribourg

David Bozzini is Professor of Anthropology at the University of Fribourg since 2017. He received his PhD in Anthropology from the University of Neuchâtel in 2011. He has been researching on surveillance, insecurity, social movements and hacktivism in Eritrea, Europe and North America. His current research projects investigate the social fabric of computer security and in particular vulnerability disclosure and bug bounties.

david.bozzini@unifr.ch
University of Fribourg
Department of Social Sciences
Boulevard de Pérolles 90
CH-1700 Fribourg