Friction in Arenas of Repair: Hacking, Security Research, and Mobile Phone Infrastructure

Matthias Korn
Institute for Information Systems
University of Siegen, Germany
matthias.korn@uni-siegen.de

Susann Wagenknecht
Department of Social Sciences
University of Siegen, Germany
susann.wagenknecht@uni-siegen.de

ABSTRACT

This paper studies how communication infrastructure is explored, examined, and evaluated by self-identifying 'security researchers' at hacking conventions. We analyze mobile phone 'security research' as a case of negotiating infrastructural repair. 'Security research' seeks to re-negotiate with industry actors what 'security' actually means, which technological 'insecurities' need mending, which bugs, mistakes, and risks should be repaired. These negotiations are tense and contested because the relations between 'security research' and industry reach across utterly different identities and commitments, spanning an *arena* of repair. To investigate how 'security research' situates itself in this arena, we analyze presentations about hacking mobile telephony that have been given at events organized by the Chaos Computer Club between 2000 and 2015. With the help of qualitative coding techniques, we examine the identities and commitments involved in 'security research,' the agendas that 'security research' pursues, and the ways in which it addresses and relates to industry actors. We interpret our findings in terms of *friction*, highlighting how a social arena of mobile phone repair is constituted through difference, rather than despite it.

Author Keywords

public infrastructure; maintenance and repair; hacking; social arena; friction; mobile phone networks; GSM; IT security.

ACM Classification Keywords

K.4.2 [**Computers and Society**]: Social Issues; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—Unauthorized access (e.g., hacking); C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—Wireless communication.

INTRODUCTION

There is a strong cultural image of hacking: Hackers destroy, they hack things apart. In parts, hackers are nursing this image, and many of hacking's practices seem to align with the image of destruction. Hackers recklessly 'crash' and 'open' proprietary systems, they crudely reverse engineer them, unabashedly re-purpose them, and exploit their weaknesses. But, as we will show, there is a strand of hacking that self-identifies as 'security research,' taking pride in reporting bugs and mending 'security weaknesses,' claiming industry's acknowledgement and negotiating its cooperation.

In this paper, we consider 'security research' as an ambivalent form of repair work. On the one hand, 'security research' seeks to help maintain the functionality of communication infrastructure. On the other hand, 'security research' entertains a complicated relationship to industry when it trespasses the boundaries of proprietary knowledge and challenges industry's technological expertise. 'Security research' seeks to renegotiate with industry actors what 'security' actually means, which technological 'insecurities' need mending, which bugs, mistakes, and risks should be repaired. These negotiations are tense and contested. For this reason, the relations between 'security research' and industry challenge existing narratives of repair and maintenance as modest and humble occupations [18, 23], as backstage activities that are sometimes about nostalgia [47], sometimes about (environmental) sustainability [26], often about making do with 'old' technologies [12], and making ends meet [28].

The relations that 'security research' entertains to industry reach across different social worlds, across utterly different identities and commitments—spanning a social arena of repair that concerns the evaluation and removal of security risks in complex communication infrastructure. How does 'security research' situate itself in this arena? Through which narratives and arguments does it negotiate repair? To answer these questions, we analyze a sample of 26 presentations on the 'security weaknesses' in mobile telephony. These presentations have been part of the official program of events organized by the Chaos Computer Club (CCC), Europe's largest hacker association, between 2000 and 2015. With the help of qualitative coding techniques, we examine which identities and commitments are involved in 'security research,' which agendas 'security research' pursues, and how it addresses and relates to industry actors. We will interpret our findings in terms of friction, highlighting how a social arena of mobile phone repair is constituted through difference, rather than despite it.

With this paper, we contribute a study of 'security research,' a form of hacking barely investigated so far. We use our case study to examine how repair-worthiness is contested and how a social arena of repair can be knit when repair work

is distributed among diverse actors, some of which possess the privilege to repair while others do not. In examining this asymmetry, we emphasize how repair practices may resort to transgression and friction—notions with which we hope to complement existing research upon practices of repair and maintenance.

RELATED WORK

This paper builds upon CSCW's long-standing efforts to study not only people's use of single artifacts or systems but their relations to complex, comprehensive infrastructures [12, 29, 31, 33, 35, 54]. We conceive of infrastructures broadly, as the socio-technical pre-conditions for action. Infrastructures comprise the Heideggerian tool at hand as well as large computer systems, networks, and power supply. They also comprise conventions, taken-for granted paradigms, ingrained habits, and the social structures that shape our everyday lives without us paying too much attention to them [7, 40]. Infrastructures are experienced as invisible; they are acted 'through' rather than 'upon' [42].

To achieve this kind of invisibility, infrastructures need to function smoothly and reliably. Infrastructural reliability is a constant concern for those who provide infrastructures and are responsible for their operation. Infrastructures require continuous maintenance. Once infrastructures are built, they need to be managed, re-built, adjusted, repaired, updated, enlarged, partially torn down, or else they are decaying—a process that needs to be managed, too [8, 12]. In fact, infrastructures are a process rather than a thing [42].

Within CSCW and beyond, a range of ethnographic studies emerged that examine practices of infrastructure maintenance and repair [18, 24, 26, 27, 28, 43, 47, 52], highlighting the nitty-gritty of sustained and careful efforts to keep technologies performing 'as they should.' Practices of repair and maintenance restore a 'functioning order' in technological systems, re-installing (and transforming) technical functionality as well as social order [25]. Yet, despite their stake in creating order, repair and maintenance workers must not be stylized into compliant servants. In fact, corporate maintenance workers have been shown to be an unruly group, cultivating an "aggressiveness" toward higher levels of corporate hierarchy and "contempt" for production workers ([16]: 104).

In making the repair of 'old,' not the design of 'new' technologies their point of departure, studies of repair practices adopt a distinct epistemic paradigm—"broken world thinking," a thinking that proceeds from the insight that "the world is always breaking; it's in its nature to break" ([25]: 221). But precisely *where* the world breaks, and where the worst faults run, is a matter of perspective and negotiation. In fact, acts of repairing and maintaining frame, often implicitly, what exactly is in need of repair and worthy of maintenance. To repair an object means casting it as weak, dysfunctional, or decaying, declaring it a failure, damage, or risk [12]. In this perspective, repair and maintenance are part of the tacit, quotidian negotiations that determine a technology's value [24].

Studying maintenance and repair means visiting the 'backstage' of technologies in action—a multi-layered global space that stretches from the Global South to highly industrialized nations, a space where engineers but also maintenance workers, self-employed repair shop owners, hobbyists, makers, fixers, and, as we will show, hackers do their work. Maintenance work and repair are typically described as the continuous, ordinary, sometimes banal, and frequently concealed activities that ensure "quietly, humbly, and all the time" that needed technologies are ready-to-hand ([25]: 223; also [21]: 2). However, when we examine what hackers call 'security research,' we approach maintenance and repair from a different angle. 'Security research' relies upon publicizing *extra-ordinary* IT vulnerabilities, bringing hitherto unrecognized 'security risks' to the fore, and, often, positioning itself boldly in opposition to and/or ahead of corporate and government actors. In this sense, 'security research' presents us with different aspects of maintenance and repair.

Hackers and hacking practices are receiving increasing attention in CSCW [20, 32, 36, 38]. Hacking has been studied as ingenious techniques [4] of subversive thrust [37], critical of industry-produced goods, corporately-owned infrastructures, and proprietary knowledge. Furthermore, hacking has been characterized as illicit and transgressive, typically circumventing, violating, or attempting to change existing rules, conventions, and laws [53]. Crucial for the way in which hackers present themselves and legitimate their practices are the notions of 'openness' and 'freedom of information' [2, 13, 14]. Hackers advocate for 'open' access to technological knowledge and infrastructures, casting hacking as an opening of 'closed' systems and a vehicle of technological as well as societal emancipation. Yet much of hacking research in CSCW and HCI has, while sympathetic, remained wary of narratives of emancipatory power that hacking practices tend to convey and the kind of social change they may effect. In fact, hacking practices require and create privilege, establishing new socio-technical boundaries between inclusion and exclusion [1, 47, 48].

Hackers typically entertain if not tense then ambivalent relations to industry and government [5, 49, 53]. Conflicted relations between actors from different social domains have been studied in CSCW, e.g., in the context of "adversarial collaboration" [11, 17] or civic engagement for public infrastructure maintenance [22]. Examining how hacking, self-identified as 'security research,' tackles mobile phone systems, we seek to draw attention to the fact how infrastructures are repaired and maintained not through collaboration alone, but through adversarial struggles as well.

THEORETICAL FRAMING

Developing upon Jackson's notion of "repair worlds" [28], we conceive of 'security research' as creating an *arena* of repair, a discursive space that cuts across the social worlds of hacking and industry—a battle field that is, nonetheless, held together by a shared concern for repair.

We suggest to analyze 'security research' in terms of social worlds/arena theory, a framework developed by Anselm Strauss, Adele Clarke, and many others [44, 45, 9, 10]. Social worlds are shared discursive spaces, its members mutually responsive to one another and bound by shared identities and

commitments to collective action. As such, social worlds are meant to describe "the principal affiliative mechanism through which people organize social life" ([9]: 131). In this perspective, then, societies are composed of a multitude of social worlds that are dynamically intersecting and cross-cutting one another. Social worlds are always becoming; they have to be thought of as contingent processes. Social worlds are highly fluid, their patterns of commitment shifting and their boundaries constantly pushed in one way or another. As a concept, social worlds are not confined to a particular scale. Rather, the social worlds concept can be projected on varying scales, and each social world can be considered the sub-world of another.

Both action and discourse are constitutive of social worlds. Social worlds continuously negotiate their values. Within social worlds, "there has to emerge a collective definition that certain activities are worth doing, and 'we' are doing them... 'Worth doing' easily gets translated into deserves doing, and for some issues, should be done, must be done" ([45]: 174, 175). Social worlds come with their own performance standards ([45]: 180). Social worlds also undertake efforts of "theorizing," aiming to provide "justifications about the worth of its existence" and offering "legitimating conceptualizations" ([45]: 177). Once legitimacy, standards, and measures of worth are established (and continuously re-established), representatives of social worlds will typically try to establish their claims to worthiness in larger arenas ([9]: 132).

An arena "is composed of *multiple* worlds organized around issues of mutual concern and commitment to action" ([10]: 113, emph. add.). Arenas are the space where boundaries between social worlds are established and maintained ([9]: 133). In arenas, "issues are debated, negotiated, fought out, forced and manipulated by representatives" of different social worlds ([44]: 124). Thus, the concept of arena is tied to the empirical question: "Who cares, and what do they want to do about it?" ([9]: 133). Answering this question should unveil the ambiguous character of arenas: On the one hand, arenas associate members from different social worlds, making them recognize one another because of their mutual concern for action—they all feel that something needs to be done (or prevented). Yet on the other hand, they may crucially differ in their perspective on what exactly needs to be done, what it means to 'do' it, how it needs to be done, by whom, why, and to whose benefit. Participants in social arenas may try to form an agreement, negotiating a joint way of handling things. But they need not reach a genuine consensus, a shared perspective about what is at stake. To account for cooperation without consensus and across social worlds, Star and Griesemer [41] have famously suggested the concept of boundary objects, objects that 'translate' the concerns of one social world to the concerns of another.

Relations between different social worlds are complex, often implicitly tense. To maintain their integrity as distinct social sphere vis-à-vis other worlds, social worlds typically presume their members' commitment to the conviction "that 'what we are doing' is not just as legitimate but even more legitimate" than what members of other social worlds are doing ([45]: 175). When a social world "cannot be so easily distinguished by audiences which matter, then it will claim a legitimately different status by underlining and arguing for differences between its own ideas/activities/technologies and those of others," engaging in "distancing maneuvers" to create a distinct identity ([45]: 176). However, distancing maneuvers are just one side of the coin that is traded in social arenas. Social arenas emerge between different worlds because of a *mutual* concern. So, despite all distancing efforts, for a social arena to exist, its participants need to establish (and constantly re-establish) a concern for action that can be—in one way or another—shared by members of different social worlds.

We mobilize social worlds/arena theory to describe hacking–industry relations as an *arena of repair*. We do so not only to emphasize the fault lines that demarcate the world of hacking from the world of industry. We also emphasize the fact that many self-declared 'security researchers' are committed, to varying degrees, to both the world of hacking *as well as* the worlds of entrepreneurship and academia. Their identities are hybrid (cf. [3]). With our case, we examine how 'security researchers' seek to frame issues of mutual concern to both hackers and industry, trying to establish an arena in which corporate practices acknowledge and respond to hackers' measures of worth.

We will further borrow the notion of "friction" [50] from anthropologist Anna Tsing. With friction, we characterize how arenas, despite the lack of shared common ground, can produce effective action. With friction, Tsing describes "the awkward, unequal, unstable, and creative qualities of interconnection across difference" ([50]: 4). Through friction, Tsing argues, connections across difference are forged: "A wheel turns because of its encounter with the surface of the road; spinning in the air it goes nowhere. Rubbing two sticks together produces heat and light; one stick alone is just a stick. As a metaphorical image, friction reminds us that heterogeneous and unequal encounters can lead to new arrangements of culture and power" ([50]: 5). We adopt Tsing's notion of friction to convey our observation that infrastructural repair is entangled in tense interactions between different social worlds. We will argue that ongoing friction between social worlds is what can provide the necessary grip for the repair of infrastructural 'security weaknesses' to take place.

CASE AND METHOD

We examine 'security research' on mobile telephone networks as a case of negotiating infrastructural repair. Mobile telephone networks are global, interconnected infrastructures comprising diverse elements such as, e.g., mobile phones, cellular networks, and backbone networks; their respective hard- and software components; and, centrally, protocols and standards for their interoperation (e.g., GSM and LTE or SS7 and SIGTRAN in backbone networks). Moreover, mobile phone networks not only involve corporate operators and billions of users. They also rely on standardization and government bodies to provide legal frameworks, policies, protocol specifications, and standards for mobile telephony. GSM, the Global System for Mobile Communications, is the most widely deployed mobile telephony standard to date. GSM is used for personal and commercial communication (e.g., mobile banking)

and for purposes such as machine-to-machine communication in manufacturing and automation (e.g., home automation).

We are interested in characterizing what 'security research' actually is and which relations it seeks to entertain to industry actors. 'Security research' comprises a range of exploratory practices that, highly dependent upon technical skill, identify 'security problems' in existing technologies. Insofar as 'security research' serves the value of security, striving to 'secure' technology against breakdowns or attacks, 'security research' has an interest in reporting 'security problems' to industry actors. In the case of proprietary technologies, only industry actors can ultimately remove—i.e., repair—identified 'security problems.' With 'industry' we refer to those organizations that govern, build, deploy, and operate mobile telephony infrastructures—phone and equipment manufacturers, network operators etc.

We chose to study 'security research' by analyzing presentations of hacking and 'security research' activities concerning mobile telephony at events organized by the German Chaos Computer Club (CCC). The CCC, founded in 1986, is today's largest hacker association in Europe. In its online mission statement, the CCC describes itself as a community that seeks to promote freedom of information, discusses the impact of technology on individual and collective levels, and educates the public about it.[1] To do so, the CCC organizes, among other things, two major event series: The annual Chaos Communications Congress[2] and the CCC's summer camp,[3] which takes place every four years. While the summer camp is a relatively small gathering, the convention is a large event. It takes place in Hamburg or Berlin at the end of each year; and it had more than 12,000 reported attendees in 2015.[4]

Our data

Since the social arena of infrastructural repair is not a physical place we could visit, we decided to examine some of the material traces that actors leave behind when they navigate the discursive space an arena constitutes. Hence, the data we analyze consists in materials that document presentations held at the Chaos Communications Congress and the summer camp. For practical reasons, we limit ourselves to presentations given between 2000 and 2015. For each presentation, at least an abstract was available for us to analyze. For most presentations, we were able to extend our analysis to short presenter biographies (bios) and the slide decks used during the talk. All materials are authored and provided by the presenters before, during or after their talk and collected at a publicly accessible online schedule.[5] We complemented these materials with video or audio recordings of presentations, which are available for most talks, but chose not to make them part of our analysis. We chose to remove personal information for presentation purposes. But because all our materials are publicly available online, we are not able to provide complete anonymization.

We selected presentations that explicitly addressed the identification of 'security problems' in mobile telephony. We sampled our material in two rounds. First, we consulted title and abstract of all talks between 2000 and 2015 to identify those related to mobile telephony and its associated technologies. We identified 46 presentations in this sampling round. From these 46, we then selected only those presentations that take issue with the 'security' of mobile telephony. This second round of sampling yielded 28 presentations, of which we further eliminated two during first rounds of coding—one had an art background, engaging playfully with privacy issues around mobile telephony; the second one was about the politics of censorship.

Our final set of materials thus consists of 26 presentations. Of these, 24 are in English language and 2 are in German. There are 15 presentations that are single-authored; 11 presentations have two authors. There are 23 different authors in the set. Authorship, as far as we can determine, is exclusively male and international, with presenters coming, e.g., from Germany, France, Luxembourg, the United States, and South Korea. The author with the most presentations has 7 single- or co-authored presentations.

In the following analysis we refer to presentations by their number #1 to #26, and denote the source material accordingly as either 'bio,' 'abstract' or 'slides' (see Table 1). When referring to individual authors of co-authored presentations we reference them by adding '_1' for first and '_2' for second author. Hence, material quoted from the bio of the second author of our last presentation would be referenced as #26bio_2.

Coding process

To analyze our material, we adopted grounded theory techniques [46, 15]. We combined open and, in parts, axial coding strategies with theoretical considerations and hypotheses based on pre-existing knowledge of the phenomenon. For example, based on our hypothesis that 'security research' is situated in a social arena, we coded for a range of commitments that presenters hold (under the code [*commitment*]). We deliberately formulated theory-led codes only on a rather coarse-grained level, such as to guide our attention to specific issues but not presume a specific coding result.

We have conducted several iterative rounds of coding, administering three basic steps:

1. We conducted a round of loose coding first. This coding was mostly open, but we also probed theory-guided codes. As a result of this round of coding, we formulated a short, tentative code book with rather coarse-grained categories. Codes such as [*intention*], [*possibility*], and [*problematic*] were, e.g., part of the code book we developed for coding abstracts.

2. With this code book, we coded the material again, in at least one iteration.

[1] See http://www.ccc.de/satzung

[2] See http://events.ccc.de/congress/

[3] See, e.g., http://events.ccc.de/camp/2015/

[4] Both authors of this paper have long, if inconsistently, followed the CCC and observed the world of 'white hat' hacking with sympathy. They both have been at the CCC's annual convention several times; one of them has given a presentation about how hacking is perceived in academic research at the event in 2015. Both are, however, not acquainted in any way with the presenters whose materials they examine.

[5] See, e.g., https://events.ccc.de/congress/2015/Fahrplan/

set coded for	**I** multiple commitments	**II** agenda setting	**III** industry relations
materials referenced as for co-authors	bios + individual slides #<id>bio or #<id>slides #<id>bio_1 or _2	abstracts #<id>abstract –	slide decks #<id>slides –
important codes	[*commitment*] [*hacking*] [*company*] [*academia*] [*security research*]	[*intention*] [*possibility*] [*attack*] [*attackability*]	[*relations*] [*requests*] [*contacting*] [*response*]

Table 1. We used different source materials in three sets of analysis.

3. To further examine what we coded in step 2 and to develop a more detailed understanding of our coarse-grained codes, we devised more fine-grained codes. In developing these, we had a preference for in-vivo-codes. For example, we clustered what we coded as [*possibility*] in presentation abstracts with codes such as [*you-can*] and [*attacker-can*].

All three steps were accompanied by memo writing to formulate tentative ideas for categories and their relationships to one another. Both authors were engaged in coding and memoing, and frequently reported interim results to one another over the course of the analysis for detailed feedback. This enabled us to develop analytic narratives around thematic clusters.

Following these steps, we consecutively analyzed three sets of materials (see Table 1): We coded bios and 'about me' sections of slide decks for presenters' commitments (I); we coded abstracts for agenda setting activities (II); and we coded slide decks to focus attention on relations between 'security research' and industry (III).

I. ANALYZING BIOS: MULTIPLE COMMITMENTS

As a first step of analysis, we coded our sample of 26 convention presentations for [*commitment*], a category reflecting our decision to adopt the social worlds/arenas approach as theoretical framework. Through commitments actors position themselves in and around social worlds. In social arenas, commitments to different social worlds co-exist, intertwine, and clash. When coding for [*commitment*], we thus specifically paid attention to the ways in which presenters describe themselves, what they call their interests and skills, and which affiliations they use to provide their audience with an image of 'who they are' and why they feel they have the authority to speak at the convention.

We coded presenters' bios as well as cover slides, closing slides, and 'about me' slides from their slide decks. We checked whether presenters use corporate email addresses or corporate design elements. Some people give several different talks over the years and appear multiple times in our sample. We have decided not to aggregate the data we have about them into one, but to treat each of their appearances as the enactment of a distinct identity. In this sense, we have been examining 37 'identities' or identity enactments. For these 37 identity enactments, bios are available for 22 and slide decks for 34. Either bio or 'about me' section are available for each. However, 4 presenters provide only nick names and 8 presenters prefer to provide very little information about themselves. One bio, e.g., runs: "*Uhm, I don't have one lying around right now*" (#1bio, complete bio, translated from German).

Commitments to hacking, companies, and academia

Analyzing the enactments of identity that our material offered, we found multiple commitments that presenters pursue to varying degrees—sometimes just mentioning an affiliation in passing, sometimes presenting themselves as representative of a company or academic institution, as, e.g., in:

"*Hacking (for) the club [the CCC] since 1997 [..] [He] is a longtime member of the CCC and one of the founders of the [German city] CCC group and known for his presentation of [hacker game show] together with [other person] on various hacker events over the last 10 years. He is currently working as a sysadmin for an IT-security consulting company and specializes in security, perl and the game of go.*" (#24bio_1)

"*[He] is a cryptographer and hardware hacker. Towards more security in everyday devices like phones and credit cards, [he] raises public awareness about the wide-spread use of weak cryptography and advises companies ready to improve from there. [..] [His] academic research deals with privacy protection, while his white hat hacking projects focus on cryptographic hardware.*" (#9bio_2)

As these two examples illustrate, presenters describe themselves in terms of their CCC membership and their engagement with hacking communities. But they also portray themselves as IT specialists and academic researchers. For this reason, we devised the codes [*hacking*], [*company*], and [*academia*]—categories that have proven robust in the sense that each of them was coded several times across various identity enactments.

We found commitments to [*hacking*] articulated in presenters' self-descriptions as hackers—as, e.g., in "*You make it, I break it!*" (#6bio, complete bio) or in mentions of interest in hacking techniques, involvement with the CCC and/or other hacking collectives, events, initiatives etc.

Many presenters mention some affiliation with a [*company*]. Most presenters with [*company*] affiliation are either self-employed, employed by or managing IT security firms, or mention that they follow some occupation in the IT sector more generally (e.g., working as system administrator). Only

two presenters describe themselves as employed in a different realm, one of them being being employed by a major network operator, and the other one working for a leading software company: "*teh* [sic!] *enemy*," i.e., Microsoft (#3bio_2). Following our material, we refer to network operators and major software companies, along with phone manufacturers, as 'industry.' In our material, 'industry' is typically cast as the contrasting 'other' or 'not us'—a framing, notably, that is not applied to IT security firms.

Many presenters emphasize a commitment to [*academia*]. While some presenters indicate academic commitments only by providing a university email address, most explicitly self-describe as university researchers or students, as, e.g., in:

"*coder, hacker, security researcher, PhD student*" (#12slides_1)

"*I'm currently studying computer science at [university] and like to play with things :D*" (#12bio_2, complete bio)

"*[He] is a Ph.D. candidate in System Security Laboratory from [university]. He received his M.S. and B.S. in electrical engineering from [university]. He has broad interests in system security. He is mainly working on cellular network system and mobile device security.*" (#26bio_2, complete bio)

Commitments to 'security research'

We developed the code [*security research*] to characterize a commitment to the systematic analysis of 'security problems' in communication technology. 'Security research' is not invoked as an academic term, nor is it necessarily a genuinely academic practice. Rather, self-descriptions as 'security researcher' are invoked independently of commitments to academic research. They are not denoting a specific position within IT security companies either, although commitments to [*security research*] often coincide with [*company*] commitments:

"*[He] is a cryptographer and security researcher. He likes to test security assumptions in proprietary systems and typically breaks them.*" (#13bio_1, complete bio)

"*Security Researcher & Entrepreneur [..] Founder of [company] and Senior Security Consultant for [security research team]. [He] has proven expertise in network security. He founded and led technical teams in several security companies [..] as well as security research teams [..] He has written and translated security books, including some of the earliest references in the field of computer security, and has been giving speeches on network security since 1995 (RSA, COMDEX, Interop, HITB Dubai, Hack.lu).*" (#5bio)

A strong majority of identity enactments in our sample rely on self-descriptions as 'security researcher,' as performing 'security research,' or convey an interest in 'security.' We are, however, conscious of the fact that not all presenters explicitly self-describe as 'security researchers' or mention an interest in 'security.' Nevertheless, we decided to use the term 'security researcher' to refer to all presenters in our sample. We believe this decision well-justified because all presentations in our sample deal with the systematic discovery of 'security problems.'

Yet, when we use the term to speak of a social world of 'security research' in contrast to the social world of 'industry,' we realize that 'security research' is a hybrid social world, a world that itself intertwines different commitments. In fact, most social worlds reveal, if only studied closely enough, some degree of hybridity and diversity. Whether or not to consider a discursive space a social world or an arena is an analytic decision [9]. Since we are interested in studying how 'security'-concerned presentations at a hacking convention address the manufacturers and operators of communication infrastructure, we chose to conceive of the discursive space we study as an arena of repair in which the social world of 'security research' addresses the world of 'industry.'

II. ANALYZING ABSTRACTS: AGENDA SETTING

To get a detailed understanding of what presenters seek to achieve and how they argue their case, we analyzed presentation abstracts. After a first round of open coding, we developed the code [*intentions*]. When coding for [*intentions*], we noticed that all 26 abstracts analyzed are written in a language that, in large parts, is reminiscent of scientific intentions. According to the abstracts, the presentations intend to 'introduce,' 'investigate,' 'analyze,' 'explore,' 'provide an overview,' 'explain,' 'discuss,' and 'conclude' with 'results.' An exception, here, are single abstracts that exclusively foreground the [*fun*] of mobile phone hacking, e.g.:

"*Listen to satellites and decoding is fun. We show how you can do it with a Software Defined Radio and some spare time. And we show what interesting stuff you can expect to find.*" (#24abstract).

Striking in this quote is the repeated use of the verb 'show,' another characteristic of most abstracts. Our code [*show*] is by far the most frequent category in labeling intentions, its predominant sub-code being [*show-how*]. The talks intend to 'show how' its authors hacked the technologies at hand, and how listeners can do so as well. The codes [*show-that* or *demonstrate*] typically occur in connection with 'attacks' or 'attack scenarios': "*...we will show new attacks based on mobile paging that can ultimately disrupt mobile telecommunication or even worse*" (#19abstract); and: "*We also introduce and demonstrate new attack scenarios...*" (#21abstract).

We noticed that in our material to demonstrate actual attacks or viable attack scenarios is considered proof of a 'security weakness.' To fix such weaknesses, many of the talks make suggestions or evaluate existing attempts of risk mitigation. If mentioned in the abstracts, we coded such occurrences as [*recommendation*]. Recommendations are directed to two different addressees—to users and to corporate actors, e.g.: "*This talk will explain... what you can (and can't) do against being located...*" (#4abstract); and: "*... some good and bad attempts to enhance the security of M2M systems will be presented*" (#16abstract).

Furthermore, some abstracts offer remarks not just on the immediate intentions of the talk, but its [*motivation*]:

"*Prepare to change the way you look at your cell phone, forever.*" (#9abstract)

"*Defense knowledge has not scaled at the same speed as attack capabilities. This talk intends to revert this imbalance.*" (#18abstract)

"*It's time to bring the decades of TCP/IP security research into the GSM world... [GSM] stacks never have received the scrutiny of thousands of hackers and attack tools like the TCP/IP protocol suite on the Internet. It's about time we change that.*" (#7abstract)

As passages such as these suggest, the motivation of presentations is framed as a matter of knowledge dissemination (cf. [2]). The talks promise 'changing' listeners' perspectives, educating them about their cell phones, 'reverting imbalances' in knowledge and capability, or addressing a lack of scrutiny. Through knowledge dissemination, the talks seek to address perceived epistemic mismatches—knowledge asymmetries between network 'attack' and 'defense,' between industry and users, as well as between different technologies (e.g., between open protocol internet technologies and proprietary mobile phone technologies).

'Attacks are possible'

Early on in our analysis, we were struck by the frequency of expressions such as: "*We explain how it is possible...*" (#23abstract), "*It becomes possible to tell...*" (#14abstract); and: "*... show you some possibilities how to...*" (#3abstract). We hence started to code for [*possibility*]. For the abstracts analyzed, we soon began to distinguish between [*technological possibility*], [*the possibility of attack*], and [*human capacities*]. Technological possibility describes system features ("*The SIM-firmware can be updated over the air.*" #17abstract). The possibility of attack is highlighted repeatedly ("*We show our results and the kind of attacks that are possible with our bugs.*" #12abstract). Interestingly, human capacities are usually ascribed to a set of distinct subjects, and we therefore coded such occurrences as [*you-can*], [*attacker-can*], [*anyone-can*], [*researcher-can*], and [*hacker-can*]. While the first two codes were applied frequently, the last three occurred no more than twice.

The distinction between [*you-can*] and [*attacker-can*] is a moral one: [*You-can*] retrace what the authors of the talk have done, protect yourself against security breaches, or circumvent technical limitations such as defending "*your right to talk voice over-ip where ever and whenever you want to*" (#3abstract). What [*you-can*] is framed in a way that does not appear morally dubious; it is not tied, at least not explicitly and not immediately, to the performance of 'attacks' that would affect other users. In contrast, an [*attacker-can*] "*perform caller spoofing and denial of service attacks*" (#26abstract)—acts that are acknowledged to have undesirable consequences for other users.

Many talks seek to increase the technical possibilities that their listeners have by presenting specific software tools ([*tool release*]). While some talks present [*tools for enhanced use*] (e.g., "*tools that block or alert users to many common attacks*," #21abstract), most tools presented are [*tools for analysis*]. The abstracts mention, e.g., "*tools to measure the level of vulnerability of networks*" (#18abstract) or a "*graphical mapping tool*" (#14abstract). Such tools help explore systems. What is done with the insights that these analyses deliver, however, can go either way. Most abstracts suggest that technical insights can be used to formulate recommendations for technological improvements, but these insights can be used to exploit technical weaknesses as well:

"*With the help of this program we want to analyse the anti voice-over-ip filters implemented by different cellular providers and show you some possibilities how to circumvent them efficiently.*" (#3abstract)

Since another expression with striking frequency is 'attack,' we also coded for [*attack*]. We coded for [*attack as spectacle*] and [*attack as fun*], if only with one occurrence each: "*...machine-to-machine (M2M) communication is often poorly secured and some day, shit will hit the fan!*" (#16abstract); and: "*Attacking the SS7 network is fun...*" (#5abstract).

However, the material soon led us to distinguish between [*unattributed attacks*] and [*claimed attacks*] (or hypothetical 'attack scenarios'), which are claimed by the authors themselves. [*Claimed attacks*] are typically attacks performed to identify, analyze, and prove attack possibilities and to alert users and industry: "*26C3's rainbow table attack on GSM's A5/1 encryption convinced many users that GSM calls should be considered unprotected*" (#13abstract; the rainbow table hack itself is presented in #9abstract). In contrast to [*claimed attacks*], [*unattributed attacks*] are not attributed to specific actors—they just have 'happened' and are referred to as events that need to be 'blocked' and 'defended against': "*Modern phones include all components necessary to block—or at least make visible—a large range of attacks...*" (#21abstract). [*Unattributed attacks*] are typically invoked to illustrate industry failure.

Here, again, we observe moral ambiguity. Whereas [*claimed attacks*] explore 'security weaknesses,' helping to address knowledge lags and asymmetries between hackers and industry, [*unattributed attacks*] are potentially harmful. It is their undesirable consequences that 'security research' seeks to prevent.

Problems, their causes, and their solutions

Coding for [*problematic*], we found that all abstracts except for three take issue with a 'security problem' in one way or another—a problem that invariably translates as the continuous threat of 'attacks' (i.e., [*attackability*]). Problematic, hence, is the fact that 'attacks' against mobile phone technologies have been carried out or that they could be carried out in the future. To explore this issue, we coded for [*consequences*] and [*causes*] of [*attackability*].

We identified three perceived major [*consequences*] of 'security problems': privacy breaches, fraud, and system breakdown. Our material, hence, frames 'security' predominantly as the capacity to protect users' privacy, users' economic interests, and reliability. 'Security problems' have, as analyzed abstracts suggest, manifold [*causes*] such as lack of user authentication or lack of encryption. Yet many of the abstracts analyzed maintain that the lack of such security features is, essentially, caused by [*industry negligence*]:

"*Vendors often don't take into account that a device might get compromised...*" (#16abstract)

"*The network operators, however, have not woken up to the threat yet*" (#13abstract)

"*Many networks are still reluctant to implement appropriate protection measures in legacy systems. But even those who add mitigations often fail to fully capture attacks...*" (#20abstract)

We note that what we labeled [*industry negligence*] can be subsumed under [*lack of scrutiny*]—a code we initially developed for the statement that hacking communities have not yet sufficiently explored mobile phone technology, a claim that abstracts repeatedly make. [*Lack of scrutiny*], thus, is attributed both to industry as well as to hackers. What, according to our material, has long kept hackers from 'scrutinizing' mobile phone technologies is the 'closed' character of proprietary technologies, which is considered a deeper [*cause*] of 'security weaknesses':

"*The largest weaknesses of mobile network[s] are well hidden from users... Of the large interconnect perimeters, only SS7 has received proper scrutiny from the research community thus far*" (#25abstract)

"*Recently, location tracking in major smartphones caused quite a stir. Closed systems make discovering such unwanted behavior more difficult*" (#17abstract)

To solve identified 'weaknesses,' abstracts are addressing industry actors, mostly indirectly, with security [*expectations*]: "*Mobile networks should protect users on several fronts: Calls need to be encrypted, customer data protected, and SIM cards shielded from malware*" (#20abstract). Some abstracts offer an [*appraisal*] of industry's efforts to fix known 'security weaknesses'—i.e., acknowledging and/or evaluating the changes that industry made to existing technologies:

"*The main question of our study is to determine how this insecurity [in SS7] is mitigated by network operator's action to prevent compromise on both network exposure of infrastructure and privacy compromise of subscribers*" (#23abstract).

"*The operating systems... are getting hardened by vendors as can be seen in the case of Apple's iOS—the current release uses data execution prevention and code signing. In contrast, the GSM stack running on the baseband processor is neglected*" (#10abstract)

Whether or not industry actors react to their 'research findings' is closely observed among 'security researchers.' Some abstracts voice their disappointment at a perceived lack of reaction to demonstrations of [*attackability*], e.g., calling upon listeners to "*upgrade from complaining to self-defense*" and promising that the talk "*releas[es] tools that block or alert users to many common attacks*" (#21abstract). 'Scrutiny' is, thus, what the abstracts suggest in order to solve the problem of [*attackability*]—calling upon fellow hackers to research 'security' issues, carefully appraising industry reactions, and enabling users to 'scrutinize' their cell phones themselves.

III. ANALYZING SLIDE DECKS: INDUSTRY RELATIONS

To further pursue this focus on hacker–industry relations, we expanded our analysis and coded for [*relations*] in the slide decks available for most presentations (21 out of 26). We found that presenters address [*relations*] to industry typically toward the end of their talks. [*Contacting*] industry with specific security [*requests*] is presented as result of 'security research,' receiving industry [*responses*] its reward. However, we noted that the actual 'research,' the phase of experimental exploration before results are presented and publicized, is commonly performed in a way that keeps 'security research' separate from industry and does not—should not—interfere noticeably with industry's network operation.

Through open coding we formulated the category [*non-interference*] to characterize the demands for care and caution that presenters attach to the descriptions of their work: "*Don't interfere with operator's network*" (#12slides). And when, e.g., the presenters of one talk consider the advantages and disadvantages of several methods to perform a 'fuzzing attack,' they point out that one "*[c]ould send [messages] over the air... [but:] Telco gets to watch you fuzz. [And:] You might (make that WILL) crash Telco's equipment*" (#6slides). This is why the presenters prefer a method the execution of which is barely noticeable by network operators: "*Telco (mostly) doesn't know its happening*" (#6slides). Once 'security research' has been able to obtain what it considers valuable results, industry actors may be contacted with specific security [*requests*].

Formulating requests, contacting industry

Based on our analysis of abstracts, we coded the slide decks for [*requests*] addressed at industry. Several presentations are explicitly requesting industry to make technological changes, but they do so to varying degrees of vigor, demanding that:

- mobile phone technology "*must be overhauled*" (#9slides) and securing them "*requires actions*" (#15slides),
- industry actors "*must upgrade*" (#15slides), "*must support*" (#20slides), "*need to consider*" (#16slides), "*should provide*" (#16slides), "*should remove*" (#22slides),
- upgrading encryption "*should be a mandatory security patch*" (#9slides), and
- certain messages "*should be filtered*" (#22slides).

We identified a number of explicit [*recommendations*] for industry to modify and update existing systems. Such suggestions are typically presented as tables or lists of possible 'counter measures' or 'mitigation measures' (e.g., entitled "*wish lists*" in #13slides, #15slides, and #18slides). Some of the talks analyzed assign each suggestion a "*responsible entity*" (#26slides).

When we coded our material for efforts to contact industry ([*contacting*]), we found mention of two ways in which 'security research' tries to approach industry—through informal notification via email and through the more formal, standardized 'Vulnerability Notes' via platforms such as those provided

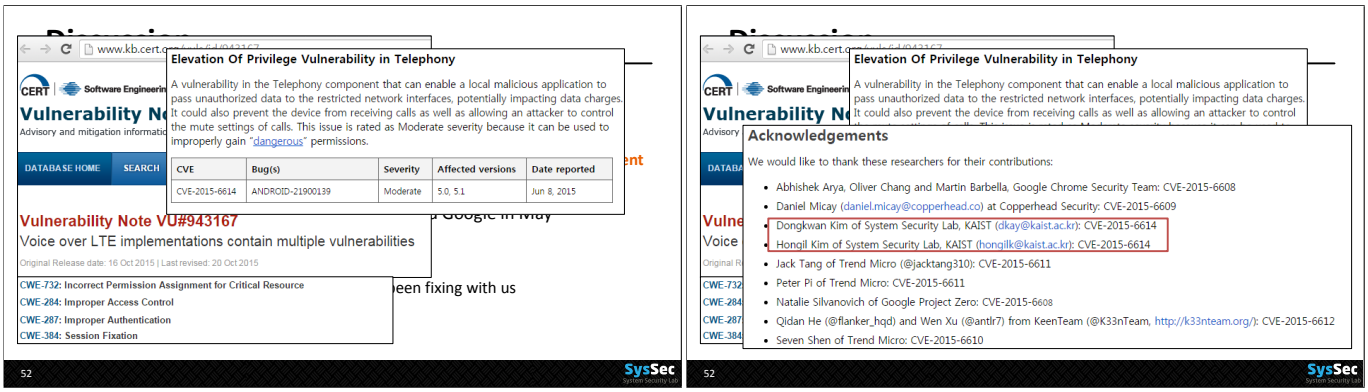

Figure 1. Two slides in which presenters notice they are prominently acknowledged in an official Vulnerability Note (right) based on vulnerabilities they reported through the platform earlier (left) (#26slides). *Source:* Hongil Kim and Dongkwan Kim, System Security Lab, KAIST (with permission).

by computer emergency response teams or CERTs (see Figure 1):[6]

"*We reported vulnerabilities to US/KR CERTs, and Google in May*" (#26slides)

"*Notifying Vendors [..] Sony Ericsson: email was #fail, but I ran into one of them at a con #win [..] Motorola: security@motorola.com does not really work that well [..] LG [and] Micromax: Haven't found a security contact*" (#12slides)

Observing industry responses

We coded mentions of industry reactions to 'security research' disclosures as industry [*response*], two facets of which we highlight in the following—[*acknowledgement*] and [*response-through fix*]. We coded [*acknowledgement*] in cases in which industry actors are perceived by presenters to have recognized their efforts to determine a 'security problem.' One form of recognition is direct contact. In fact, several presenters in our material report 'being contacted,' e.g.: "*Samsung: [We] [g]ot contacted in Jan 2011 after initial presentation*" (#12slides), "*Vendor outreach by Microsoft*" (#10slides), and "*HTC told us the bug in TouchFLO is fixed*" (#6slides).

A particular form of public [*acknowledgement*] for 'security researchers' is to be recognized on platforms such as CERT. By prominently displaying their Vulnerability Note on the slides, presenters take pride in their recognition on CERT (see Figure 1): "*We reported vulnerabilities to US/KR CERTs, and Google in May [..] Google replied 'moderate severity'*" (#26slides). The presenters also mention on the same slide: "*All two U.S. operators ACK'ed, but no follow-ups*" (#26slides), using internet jargon 'ACK' for 'acknowledge.'

In another instance, a group of presenters found public [*acknowledgement*] in a press statement issued by GSMA, an organization representing the interests of mobile phone operators. The presenters quote parts of the press statement on their slides:

"*[W]e strongly suspect the team developing the intercept approach has underestimated its practical complexity. A hacker would need a radio receiver system and the signal processing software necessary to process the raw radio data.*" (industry press statement by GSMA, quoted in #9slides)

Although they are not mentioned by name, presenters interpret the press statement as recognizing the relevance of their work. When they comment upon the press statement, they frame the critique that the statement makes ('*underestimated its practical complexity*') and the requirements that it poses ('*would need...*') as a challenge: While the press statement argues that hacking attempts are improbable, presenters are eager to show that they are, in fact, not. To demonstrate the 'attackability' of the system, they outline a series of steps to master this challenge and report how they actually carried them out in a subsequent talk.

'Security research' does not always receive direct [*acknowledgement*] by industry. In several of the talks we analyzed, however, we found presenters noting instances of [*response-through fix*]: These are software 'updates,' 'patches' or 'fixes' that presenters interpret as an indirect industry response to the 'security problems' they found—as, e.g., in "*Android CRC1 also fixes our WAP push DoS bug*" (#6slides) or listing industry's measures taken as "*Response [to a] Finding*" (#20slides).

A distinct form of [*response-through fix*] is [*response-in collaboration*], which we found mentioned only infrequently. Here, presenters report to have been collaborating with industry to remove a specific 'security problem': "*Working with Apple to get 1st issue in Infineon stack fixed, update for TMSI bug out soon*" (#10slides); and "*Only two among three KR operators have been fixing with us*" (#26slides). A sense of pride and a sense of disappointment accompanies these passages as 'security researchers' finally find themselves recognized as partners by some industry actors, but not by others.

A few of the talks we analyzed mention following up on industry [*responses*], efforts we coded as [*appraisal*], e.g.: "*HTC told us the bug in TouchFLO is fixed [..] Haven't found a way to download/install it :(*" (#6slides); "*Industry reacted swiftly but not thoroughly*" (#20slides); and: "*iPhone OS 3.0.1 [..] ONLY fixes our CommCenter bug :)*" (#6slides). We found that appraising industry reactions can be associated with the

[6] CERTs are organizations that handle computer security incidents. CERTs "provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security" ([39]: 73).

Figure 2. "*Security research is successful if vulnerabilities get removed*" is the title of a slide in which presenters posit their understanding of the relationship between security researchers and industry (#20slides). *Source:* Karsten Nohl and Luca Melette, Security Research Labs (with permission).

motif of 'holding industry accountable,' which we found articulated, e.g., in: "*Keeping network operators honest... Tracking mobile network [security] evolution online*" (#20slides).

Industry [*responses*] are important because only industry, as the proprietor of mobile phone technology, is in a position to improve its security sustainably. Without industry cooperation, 'security research' cannot be effective. In fact, from the perspective of one presentation, 'security research' and industry may have to fit together like two parts of a puzzle for 'security research' to be "successful" (#20slides, see Figure 2). 'Security research,' hence, has to find ways to enlist industry efforts in its puzzle game—provoking, pushing, criticizing, perhaps threatening and attacking, but also appraising industry.

DISCUSSION

In this paper, we study 'security research' about mobile telephony as a case of repair. As infrastructure, mobile telephony has evolved into a crucial element of the conveniently at-hand substrate of much of our everyday lives. Yet, from the perspective of 'security research,' parts of mobile phone infrastructure are broken, their promised functionality, their 'security,' diminished—and thus require repair.

Repair, particularly repair of infrastructure, is typically invisible, carried out backstage, usually receiving little recognition, and not bestowing much prestige on those who carry it out [23]. Generally, repair tends to be characterized as 'humble,' seeking to conserve and restore. Repair is often improvised, and it shows. A repaired object, mended and patched, looks perhaps a little botched. Repaired, often, means old. However, our story of repair is different, shedding light upon facets of repair that typically receive little attention.

First of all, 'security research' exemplifies a form of repair that intertwines both destruction and renewal. While 'security research' demonstrates ways to break and crash a system, its demonstrations of [*attackability*] are framed as helping to 'secure' the system in the long run, pushing industry to repair a system's 'weaknesses' and update its technological standards. Here, repair is nothing that makes technology look old. Rather, repairing 'security problems' through updates renews technology and is, potentially, intertwined with cutting-edge innovation.

Second, our study of 'security research' shows that repair begins much earlier than the actual act of restoration. Repair begins with establishing what actually needs repairing and is worthy of it. Repair, in our case, begins with notions of what 'security' actually means and what it is supposed to provide. 'Security research' contributes to repair by finding, and defining, 'security problems.' What exactly is in need of repair is far from self-evident. In our study, we observe how the repair-worthiness of mobile phone infrastructure needs to be negotiated in a heterogeneous social arena. These negotiations stretch across social worlds, enmeshing the sensibilities and interests of hackers, academic researchers, IT security specialists, and industry actors.

Third, to convey its judgment of repair-worthiness to industry, 'security research' acts boldly. It conjures up a constant threat of [*attackability*], blamed largely upon [*industry negligence*]. In so doing, repair stops being a quiet, behind-the-scenes affair. In fact, our study illustrates that repair is a contested privilege. Not just anyone can repair infrastructures. Contrary to the internet, mobile phone networks do not operate upon open standards. Much of mobile phone infrastructure is owned by network operators and global software companies. Here, repair is the business of big corporate players. 'Security research' alone cannot repair what it deems worthy of it; only industry actors can. Trying to enlist industry in its cause, 'security research' mobilizes what we characterize as friction.

In-/security—negotiating what is worthy of repair

To illustrate some of the stakes in negotiating a system's 'in-/security,' we supplement our analysis with a concrete episode from our material: The official program of the 2001 Chaos Communications Congress, then in Berlin, had scheduled a presentation about IMSI-catchers, devices used for intercepting mobile phone traffic. The presentation was to be given by Gerd Kramarz von Kohout, an industry representative, invited by members of the CCC. According to the bio attached to the abstract of his talk, von Kohout was, at the time, working for a leading German network operator. Apparently without consulting von Kohout, the presentation was given the title "GSM Insecurity in Practice," a title not quite to von Kohout's liking. The presentation was audio-recorded and is still accessible online in the convention archive. Right at the beginning of his presentation, we hear von Kohout saying:

"*That the hall is now crowded is certainly due to the fact that Mr. M... didn't call the talk 'IMSI Catcher' but 'GSM Insecurity in Practice' instead. Of course, that sounds much more spectacular. Naturally, I have to defend myself against that a bit, because I work to make sure that GSM and D1 [a German GSM network at the time] are not quite as insecure. In fact, I believe we can say D1 is relatively secure.*" (#2, audio recording, translated from German)

So, is the system insecure or not? Does it need repair or not? Technological security is a widely shared concern, but it is also what drives a wedge between 'security research,' a social world with strong commitments to hacking communities, and the world of industry.

Industry values security as smoothly executed routine, as 'doing what it should do,' as commodity that can be marketed to users for profit. In contrast, hackers value security as technological perfection, as a barrier against breaches of privacy, as an intellectual challenge. After all, an ingenious hacker can find a loophole everywhere; for an ingenious hacker any technology is, prima facie, insecure. For hackers, potential insecurities, a system's [*attackability*], is what makes a technology interesting, what enables them to perform their craft. 'Security research' enmeshes hackers' interest in technological insecurity, their commitment to privacy, and the value of free knowledge dissemination with a concern for technological functioning. And when 'security research' translates hackers' interest in insecurity into users' and industry's—everybody's—concern for security and reliability, it seeks to establish itself as valuable industry collaborator.

Forging a connection, enlisting industry

Values, sensibilities, and interests are not the only divide between the worlds of 'security research' and industry. The political economy of mobile telephony creates a stark legal and economic split between them. While industry holds technological ownership, secured by intellectual property rights, 'security research' has neither legal access to the inner workings of proprietary technologies nor does it have the means to actually repair, once identified, 'security weaknesses.' For this reason, 'security research' has to enlist industry actors in an arena of repair. By publicizing 'security weaknesses,' [*contacting*] industry actors with [*requests*], creating accountability through the [*appraisal*] of industry actions, by following up on industry [*response*], and cherishing industry's [*acknowledgement*], 'security research' establishes an arena of repair—forging a dialogical connection. With 'security,' 'security research' tries to create a mutual concern, seeking to enlist industry in a shared commitment to the removal of 'security weaknesses.' In so doing, 'security research' tries to set the pace, and determine the direction, of technological change.

To characterize the relations between 'security research' and industry, one of the slide decks we analyzed uses the imagery of puzzle pieces (#20slides, see Figure 2). Puzzle pieces are different from one another, but they are equally important. They fit together—the knob of 'security research' reaching into industry's territory—but remain distinct. The imagery also suggests that the core concern of 'security research' ('removing vulnerabilities') constitutes a higher cause above and beyond particular interests. In this vein, the imagery seeks to override the antagonisms that exist between hackers and industry, antagonisms against the backdrop of which enlisting industry might appear difficult, if not implausible or, perhaps, insincere.

Western hacking communities tend to nourish anti-corporatist sensibilities [5, 49, 53]. Time and again, authors of the materials we analyzed distance themselves from industry, ironizing their industry employment (working for "*teh enemy*" in #3bio_2) or criticizing [*industry negligence*]. [*Industry negligence*], together with industry's exclusive property rights, is seen as one of the main [*causes*] for [*attackability*]. Many of the presentations feature software tools that, so presenters argue, can make their listeners independent of [*industry negligence*]. The tools can help listeners to 'secure' the technologies that they use on their own, positioning themselves provocatively ahead of industry's state of the art. For 'security research' to enlist industry, thus, comes with the awkwardness of having to work with someone you frown upon, of patronizingly offering help and minaciously requesting cooperation at the same time.

Working with friction

'Security research' distances itself from industry, building its own knowledge base and maintaining an avant-garde status that allows to harshly criticize [*industry negligence*]. But to get a grip upon industry's actions, 'security research' creates an arena of repair and tries to enlist industry in removing 'security vulnerabilities.' We suggest to understand this dialectic of push and grip through the notion of friction.

Building upon Tsing's notion of friction [50], we understand friction as a quality of encounters across difference—whereby precisely difference plays a productive role, triggering actions that change the status quo (cf. [50]: 206, 246). In social arenas, where social worlds meet, friction does not just arise from the worlds' differences in commitment and sentiment. Rather, we argue, friction is selectively *enacted*.

'Security research' enacts friction to provoke the world of industry into action. Enactments of friction articulate itself in the chafing and grinding, scrunching and gnashing that this arena produces. 'Security research' publicly criticizes industry in a combative language of 'attack' and 'defense,' threatening and taunting industry by demonstrating the [*attackability*] of its technology. In this vein, 'security research' is continuously putting a spoke into industry's wheels, trying to shape a trajectory of technological change.

Elaborating upon friction in the context of collaboration, Tsing argues that "[o]ne of the best places to look for this kind of friction is in the formation of collaborative objects, which draw groups into common projects at the same time as they allow them to maintain separate agendas" ([50]: 246). Tsing [51] is aware that her account of friction in collaborations is similar to Star and Griesemer's account of boundary objects [41]. Boundary objects have been invoked in studies of repair [6], and we suggest that the construction of 'security problems,' along with the issuing of detailed 'wish lists' of technological upgrades, can be characterized as an effort to craft boundary objects that help translating the concerns of 'security research' into industry action.

Still, we suggest to emphasize friction rather than translation because we want to highlight that, in our case, translation efforts are a continuous struggle: Industry actors are reluctant to acknowledge the 'security problems' that 'security research' formulates, reluctant to acknowledge actors who are

publicly nagging and exposing them. 'Security research,' in turn, makes use of critique and provocation to address the political economy of mobile phone infrastructure, an economic configuration that leaves 'security research,' in its own perception, little leeway. Therefore, instead of explaining how 'security research' and industry find a way to cooperate *despite difference*, we suggest to understand the back and forth between them as productive *through difference*.

Depending upon point of view, friction may appear undesirable and illegitimate. If politics are evaluated in terms of their conduciveness to consensus and convergence, mobilizing friction does not seem to be the right thing to do. Yet with a political lens that values difference, contestation, and struggle, friction becomes 'good' politics. Mouffe [34] argues that political theory should recognize dissensus and confrontation as productive elements of democracy. According to her, pluralist democracies should strive to transform hostile conflicts between enemies into constructive controversy (cf. [19]). In this view, which Mouffe calls 'agonistic' rather than 'antagonistic,' mobilizing friction gains legitimacy (cf. [30]).

CONCLUSION

In this paper, we have studied mobile phone hacking as a case of negotiating infrastructural repair. To do so, we have analyzed materials that document the presentation of 'security research' at hacking conventions that the Chaos Computer Club (CCC) organized over the course of several years. We situate 'security research' in an arena of repair, where the worlds of hacking and industry meet and where measures of worth—what is worthy of repair? what not?—are negotiated. We argue that 'security research,' itself characterized by hybrid and sometimes ambivalent commitments, relates to industry through friction, trying to push industry to increase the 'security' of mobile phone infrastructure. In so doing, we highlight the productive potential of difference and friction in maintaining infrastructures and negotiating their future. While we acknowledge existing research on adversarial collaboration, we would like to encourage the field of CSCW to do more research in this direction.

We realize that our study is limited in scope. More research is needed to elucidate, e.g., how industry actors handle 'security research,' how 'responsible disclosure' of 'security problems' is facilitated by online platforms such as those provided by CERT, and how users perceive hacking–industry relations as they are confronted with 'security problems' as well as software updates, recalls, warnings, and a broad offer of IT security products to 'defend themselves.'

ACKNOWLEDGEMENTS

Both authors contributed equally to this research and are listed in alphabetic order. Parts of this research have been funded by the German Research Foundation (DFG) via the Collaborative Research Center 1187: Media of Cooperation at the University of Siegen.

REFERENCES

1. Morgan G. Ames, Jeffrey Bardzell, Shaowen Bardzell, Silvia Lindtner, David A. Mellis, and Daniela K. Rosner. 2014. Making cultures: empowerment, participation, and democracy—or not?. In *Proceedings of the Extended Abstracts of the 32nd Annual ACM Conference on Human Factors in Computing Systems (CHI EA '14)*. ACM, New York, NY, USA, 1087–1092.
2. Nicolas Auray. 2000. *Politique de l'informatique et de l'information: les pionniers de la nouvelle frontière électronique*. Ph.D. Dissertation. Paris, EHESS.
3. Nicolas Auray and Danielle Kaminsky. 2007. The professionalisation paths of hackers in IT security: The sociology of a divided identity. In *Annales Des Télécommunications*, Vol. 62. Springer, 1312–1326.
4. Jeffrey Bardzell, Shaowen Bardzell, and Austin Toombs. 2014. Now that's definitely a proper hack: self-made tools in hackerspaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 473–476.
5. Colin J. Bennett. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press, Cambridge.
6. Matthias Betz. 2010. The Secret Life of Machines – Boundary Objects in Maintenance, Repair and Overhaul. In *Proceedings of Pervasive 2010*. Springer-Verlag, Berlin Heidelberg, 174–191.
7. Geoffrey C. Bowker and Susan Leigh Star. 1999. *Sorting Things Out: Classification and its Consequences*. MIT Press, Cambridge MA and London.
8. Stewart Brand. 1997 [1994]. *How Buildings Learn. What happens after they're built*. Phoenix Illustrated, London.
9. Adele E. Clarke. 1991. Social Worlds/Arenas Theory as Organizational Theory. In *Social Organization and Social Process. Essays in Honor of Anselm Strauss*, David R. Miles (Ed.). Aldine de Gruyter, New York, 119–158.
10. Adele E. Clarke and Susan Leigh Star. 2008. The Social Worlds Framework: A Theory/Methods Package. In *The Handbook of Science and Technology Studies*, Edward J. Hackett, Olga Amsterdamska, Michael Lynch, and Judy Wajcman (Eds.). MIT Press, Cambridge MA and London, 113–137.
11. Andrew L. Cohen, Debra Cash, and Michael J. Muller. 2000. Designing to Support Adversarial Collaboration. In *Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work (CSCW '00)*. ACM, New York, NY, USA, 31–39. DOI: http://dx.doi.org/10.1145/358916.358948
12. Marisa Leavitt Cohn. 2016. Convivial Decay: Entangled Lifetimes in a Geriatric Infrastructure. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM, New York, NY, USA, 1511–1523. DOI: http://dx.doi.org/10.1145/2818048.2820077
13. Gabriella Coleman. 2013. *Coding Freedom. The Ethics and Aesthetics of Hacking*. Princeton University Press, Princeton and Oxford.

14. Gabriella Coleman and Alex Golub. 2008. Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory* 8, 3 (2008), 255–277.
15. Juliet M. Corbin and Anselm Strauss. 1990. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology* 13, 1 (1990), 3–21.
16. Michel Crozier. 1964. *The Bureaucratic Phenomenon*. University of Chicago Press, Chicago.
17. Aldo de Moor and Hans Weigand. 2006. Effective Communication in Virtual Adversarial Collaborative Communities. *The Journal of Community Informatics* 2, 2 (2006). http://www.ci-journal.net/index.php/ciej/article/view/271
18. Jérôme Denis and David Pontille. 2015. Material Ordering and the Care of Things. *Science, Technology, and Human Values* 40, 3 (2015), 338–367.
19. Carl DiSalvo. 2012. *Adversarial Design*. MIT Press, Cambridge MA and London.
20. Sarah Fox, Rachel Rose Ulgado, and Daniela K. Rosner. 2015. Hacking Culture, Not Devices: Access and Recognition in Feminist Hackersaces. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. ACM, New York, NY, USA, 56–68.
21. Stephen Graham and Nigel Thrift. 2007. Out of Order. Understanding Repair and Maintenance. *Theory, Culture & Society* 24, 3 (2007), 1–25.
22. Mike Harding, Bran Knowles, Nigel Davies, and Mark Rouncefield. 2015. HCI, Civic Engagement & Trust. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2833–2842. DOI: http://dx.doi.org/10.1145/2702123.2702255
23. Christopher R. Henke. 2000. The Mechanics of Workplace Order: Toward a Sociology of Repair. *Berkeley Journal of Sociology* 44 (2000), 55–81.
24. Lara Houston, Steven J. Jackson, Daniela K. Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in Repair. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1403–1414. DOI: http://dx.doi.org/10.1145/2858036.2858470
25. Steven J. Jackson. 2014. Rethinking Repair. In *Media Technologies. Essays on Communication, Materiality, and Society*, Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot (Eds.). MIT Press, Cambridge MA and London, 221–240.
26. Steven J. Jackson, Syed Ishtiaque Ahmed, and Md. Rashidujjaman Rifat. 2014. Learning, Innovation, and Sustainability Among Mobile Phone Repairers in Dhaka, Bangladesh. In *Proceedings of the 2014 Conference on Designing Interactive Systems (DIS '14)*. ACM, New York, NY, USA, 905–914. DOI: http://dx.doi.org/10.1145/2598510.2598576
27. Steven J. Jackson and Laewoo Kang. 2014. Breakdown, obsolescence and reuse: HCI and the art of repair. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 449–458.
28. Steven J. Jackson, Alex Pompe, and Gabriel Krieshok. 2012. Repair Worlds: Maintenance, Repair, and ICT for Development in Rural Namibia. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW '12)*. ACM, New York, NY, USA, 107–116. DOI: http://dx.doi.org/10.1145/2145204.2145224
29. Helena Karasti, Karen S. Baker, and Florence Millerand. 2010. Infrastructure Time: Long-term Matters in Collaborative Development. *Computer Supported Cooperative Work* 19, 3-4 (2010), 377–415.
30. Matthias Korn and Amy Voida. 2015. Creating Friction: Infrastructuring Civic Engagement in Everyday Life. In *Proceedings of the 5th Decennial Aarhus Conference: Critical Alternatives (AA '15)*. ACM, New York, NY, USA, 145–156. DOI: http://dx.doi.org/10.7146/aahcc.v1i1.21198
31. Charlotte P. Lee, Paul Dourish, and Gloria Mark. 2006. The Human Infrastructure of Cyberinfrastructure. In *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work (CSCW '06)*. ACM, New York, NY, USA, 483–492.
32. Silvia Lindtner, Garnet D. Hertz, and Paul Dourish. 2014. Emerging sites of HCI innovation: hackerspaces, hardware startups & incubators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 439–448.
33. Scott D. Mainwaring, Michele F. Chang, and Ken Anderson. 2004. Infrastructures and Their Discontents: Implications for Ubicomp. In *Proceedings of the 6th International Conference on Ubiquitous Computing (Ubicomp '04)*. Springer, Berlin, 418–432.
34. Chantal Mouffe. 2013. *Agonistics. Thinking the World Politically*. Verso, London and New York.
35. David Ribes and Charlotte P. Lee. 2010. Sociotechnical Studies of Cyberinfrastructure and e-Research: Current Themes and Future Trajectories. *Computer Supported Cooperative Work* 19, 3-4 (2010), 231–244.
36. David Roedl, Shaowen Bardzell, and Jeffrey Bardzell. 2015. Sustainable Making? Balancing Optimism and Criticism in HCI Discourse. *ACM Trans. Comput.-Hum. Interact.* 22, 3, Article 15 (June 2015), 27 pages. DOI: http://dx.doi.org/10.1145/2699742
37. Daniela K. Rosner and Jonathan Bean. 2009. Learning from IKEA hacking: I'm not one to decoupage a tabletop and call it a day. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 419–422.

38. Daniela K. Rosner, Silvia Lindtner, Ingrid Erickson, Laura Forlano, Steven J. Jackson, and Beth Kolko. 2014. Making Cultures: Building Things & Building Communities. In *Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW Companion '14)*. ACM, New York, NY, USA, 113–116.

39. Robert W. Shirey. 2007. *Internet Security Glossary, Version 2*. RFC 4949. IETF. 1–365 pages. https://tools.ietf.org/html/rfc4949

40. Susan Leigh Star and Geoffrey C. Bowker. 2006. How to infrastructure. In *Handbook of New Media*, Leah A. Lievrouw and Sonia Livingstone (Eds.). Sage, Thousand Oaks, 230–245.

41. Susan Leigh Star and James R. Griesemer. 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 (1989), 387–420.

42. Susan Leigh Star and Karen Ruhleder. 1996. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research* 7, 1 (1996), 111–134.

43. Stephanie B. Steinhardt. 2016. Breaking Down While Building Up: Design and Decline in Emerging Infrastructures. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2198–2208. DOI: http://dx.doi.org/10.1145/2858036.2858420

44. Anselm Strauss. 1978. A Social World Perspective. *Studies in Symbolic Interaction* 1 (1978), 119–128.

45. Anselm Strauss. 1982. Social Worlds and Legitimation Processes. *Studies in Symbolic Interaction* 4 (1982), 171–190.

46. Anselm Strauss. 1987. *Qualitative Analysis for Social Scientists*. Cambridge University Press, Cambridge.

47. Yuling Sun, Silvia Lindtner, Xianghua Ding, Tun Lu, and Ning Gu. 2015. Reliving the Past & Making a Harmonious Society Today: A Study of Elderly Electronic Hackers in China. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. ACM, New York, NY, USA, 44–55.

48. Joshua G. Tanenbaum, Amanda M. Williams, Audrey Desjardins, and Karen Tanenbaum. 2013. Democratizing Technology: Pleasure, Utility and Expressiveness in DIY and Maker Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 2603–2612.

49. Paul Taylor. 1999. *Hackers. Crime in the Digital Sublime*. Routledge, London.

50. Anna L. Tsing. 2005. *Friction. An Ethnography of Global Connection*. Princeton University Press, Princeton and Oxford.

51. Anna L. Tsing. 2012. Frictions. In *The Wiley-Blackwell Encyclopedia of Globalization*, George Ritzer (Ed.). Blackwell, West Sussex, 707–709.

52. Kami Vaniea and Yasmeen Rashidi. 2016. Tales of Software Updates: The Process of Updating Software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3215–3226. DOI: http://dx.doi.org/10.1145/2858036.2858303

53. Susann Wagenknecht and Matthias Korn. 2016. Hacking As Transgressive Infrastructuring: Mobile Phone Networks and the German Chaos Computer Club. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM, New York, NY, USA, 1104–1117. DOI: http://dx.doi.org/10.1145/2818048.2820027

54. Richmond Y. Wong and Steven J. Jackson. 2015. Wireless Visions: Infrastructure, Imagination, and US Spectrum Policy. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. ACM, New York, NY, USA, 105–115.