Pers Ubiquit Comput (2010) 14:227–236
DOI 10.1007/s00779-009-0257-0

ORIGINAL ARTICLE

Designing for social interaction with mundane technologies: issues of security and trust

Sara Bury · Johnathan Ishmael · Nicholas J. P. Race · Paul Smith

Received: 10 October 2008 / Accepted: 2 July 2009 / Published online: 16 January 2010

Abstract This paper documents some of the socio-technical issues involved in developing security measures for wireless mesh networks (WMNs) that are deployed as part of a community network. We are interested in discovering whether (and exactly how) everyday social interaction over the network is affected by security issues, and any consequent design implications. We adopt an interdisciplinary methodological approach to requirements, treating a community as an 'organization' and implementing an approach, OCTAVE, originally designed to uncover security elements for organizations. Using a focus group technique we chart some of the assets and security concerns of the community, concerns that need to be addressed in order for WMNs, or indeed any network, to become a truly 'mundane technology'.

1 Introduction: mundane technologies and wireless mesh networks

What is a mundane technology? Some might argue that there are no mundane technologies merely mundane *uses*, suggesting, for example, that technologies such as the scalpel or the MRI scanner whilst mundane within medical settings are likely to be regarded as fairly unusual, if not illegal, elsewhere. Others might point to devices such as the mobile phone, or word processing applications that have a wide, almost universal availability and familiarity and whose appearance is largely taken for granted and unremarkable to suggest that there are such things as mundane *technologies*. Still others, such as Petersen [23], adopt a different position, talking about 'mundane cyborg practice' and suggesting that as the Internet and the home computer have become a mundane technology the concept of mundane cyborg practice helps explain cyborg relations as they unfold in everyday life. We want to sidestep this debate by considering something that all positions effectively embrace: the idea that somehow technologies *become* mundane, and that they become mundane through everyday use. While all designers might wish that their technologies are universally desired and adopted, technologies are not born mundane but rather become so through processes whereby, to put it simply, the technology is adapted to and by the user, processes such as 'domestication' and 'innofusion' [14, 15, 24]); and the user adapts to the technology, effectively 'becoming a user' [6]. Our overall, and longstanding research interest, is in exactly how and in what ways technology gets used and adapted; in identifying the important global properties that shape adoption and use; in looking at issues of reliability (issues of trust and experience); explicitness (the tension between trust and privacy); and coordinating and reconciling information needs and resources. Such processes are inevitably, irremediably linked to the social production of trust, whereby a technology becomes a trusted technology and its use and effects predictable and trustable—what Sacks (1992) would call 'at home in the world'. Some basic sense of security that others are not accessing and using or misusing your technology without your permission is an obvious and central feature of the production of trust. So,

S. Bury (✉) · J. Ishmael · N. J. P. Race · P. Smith
Computing Department, Lancaster University, Lancaster, UK
e-mail: s.bury@comp.lancs.ac.uk

J. Ishmael
e-mail: ishmael@comp.lancs.ac.uk

N. J. P. Race
e-mail: race@comp.lancs.ac.uk

P. Smith
e-mail: p.smith@comp.lancs.ac.uk

while this paper is focused on a specific technology (WMNs), deployed in a specific location, it also has a wider and more ambitious concern—a concern with electronic networks in general and specifically with understanding the process of becoming 'mundane', suggesting that this process is inextricably linked to related concerns of security and trust.

Why do networks matter? Specifically why do they matter for security, trust and the process of becoming mundane? The sociologist Castells [9] identifies the network as *"the social structure characteristic of the Information Age, … It permeates most societies in the world, in various cultural and institutional manifestations, ..shifting to the cultural realm, we see the emergence of a similar pattern of networking, flexibility, and ephemeral symbolic communication, in a culture organized primarily around an integrated system of electronic media, obviously including the Internet"* [10]. With particular reference to wireless networks, Mackenzie [21] argues, *"wireless networks persistently associate themselves into the centre of media change. Their connectivity, intermittent, unstable and uneven as it often is, lodges in many of the overlaps, overflows and outgrowths badged as convergence, mobile media, and pervasive or ubiquitous computing. …. It might not be going too far to say that wireless networks are the very substrate of network media convergence today. … Because of their pre-positional power to connect subjects and actions, wireless networks act conjunctively, they conjoin circumstances, events, persons and things"*. Now neither we, nor the good villagers of Wray, necessarily need any sociologist to tell us of the importance of networks. What is interesting is Castells' argument about the emergent social forms of time and space that characterize the network society, specifically 'timeless time' and the 'space of flows' [19]. 'Timeless time' refers to the compression and de-sequencing of time whilst the 'space of flows' refers to the use of technology to organize social activities without the necessity of geographical proximity, of being in the same place at the same time. So, whilst previously the good villagers of Wray could only have their houses burgled and their possessions stolen at particular and obvious times of day and by someone who actually had to come to their house in order to do the deed and could therefore implement some rather obvious, and trusted security measures; electronic networks now create the possibility of them being robbed, electronically burgled, at any time of the day and from almost anywhere on the planet. Security and trust in this circumstance become rather complex.

This paper is concerned with developing some understanding of the security and trust issues that both afford and constrain people's everyday or mundane social interactions over the Web. The setting we are interested in is a rural community using a wireless mesh network (or WMNs) to provide access to the Web. The Web is, of course, a prime example of a 'mundane technology' as a seemingly quite unremarkable, simple technology that has been 'made at home' in people's lives, has become 'ordinary', perhaps even 'invisible'—at least in the sense that people rarely consider, or give more than a passing thought to, the technologies that ensure access. For some, however, and particularly for designers, this very 'invisibility' means that issues of security and trust need to be made far more transparent that people need to be aware of the vulnerabilities of the technology they routinely use and designers need to be aware of users' security concerns, not least because of the impact such issues have on people's trust and very sense of community. It is in this sense, and with this focus on security that we are interested in WMN as a technology that both provides an account of, and makes us account for, our actions; in the kinds of visibility that technology enforces despite its 'embeddedness' and 'invisibility'; and in the importance of the relationship between ordinary technologies and notions of space and place, particularly the notion of 'community'.

Wireless Mesh Networks are being increasingly used to provide affordable network connectivity to communities where wired deployment strategies are impossible or unreasonably expensive—for example, in rural areas. Such communities rely on WMNs to bridge what is sometimes referred to as the 'digital divide', the separation between those with high quality Internet access and those without, and they are proving to be particularly valuable to individuals, community activities and local businesses [4]. Unfortunately, computer networks are frequently being exploited by recreational and professional attackers that can affect their utility for legitimate use, especially in the more unusual networking scenarios presented in community WMNs. In response to the general threat a number of counter measures have been developed, including intrusion prevention systems such as network firewalls, and intrusion detection systems that aim to detect anomalous behaviour caused by attacks; unfortunately these technical responses are not directly applicable in a community WMN.

This paper documents and seeks to understand some of the socio-technical issues involved with developing security measures for WMNs that are deployed in and as part of a community network. These communities may have very different approaches to network management and operation when compared to the understood norm in computer network security, alongside the obvious technical complications. By emphasising the socio-technical we suggest that security provision extends beyond a narrow technical emphasis to include the perceptions, knowledge and fears of users. This information may well impact on the success or failure of security policies and the eventual use and

usefulness of the network, especially in the community environment ie, the extent to which it becomes a 'mundane technology'. Our interest is then in gaining some understanding of 'domestication' as a precursor to design, in order that technologies may be created that might encourage the process of domestication that might facilitate the process of 'becoming mundane'. At the heart of this argument is the notion that whilst the process of domestication and its key elements have been well described [24], fundamental to this process is some notion of trust, some belief in the security of the network being utilized.

However, getting some analytical purchase on exactly how a community feels about security, what their fears and (mis)perceptions might be, and translating them into security policies and protocols is far from easy, and perhaps relies on skills and practices not obviously associated with security experts or even computer scientists. In this project therefore, we deliberately adopt an interdisciplinary approach, and this paper presents our efforts to understand whether the formalization of an OCTAVE [2] style process, a user-driven and asset-centric process, to identify an appropriate security strategy in a community WMN is both possible and useful.

2 Problems of security in wireless mesh networks

Wireless mesh networks create a networking infrastructure using a combination of wireless networking technologies and ad-hoc routing protocols. They are effectively self-managing networks in which a set of nodes in the network act as routers that route traffic directly or via multi-hop paths, typically to the Internet. The system is dynamic in that it is able to adapt to nodes entering and exiting the network, perhaps as a result of a node failure or poor wireless connectivity, resulting in a flexible, easy to operate network, highly suited to situations such as communities where time for network management is at a minimum.

In comparison to other network types (e.g., the wired Internet and cellular networks), WMNs are particularly vulnerable to attacks due both to the number of available attack vectors, and the severe consequences of attacks that may take place. The attack space is particularly large, in addition to conventional attacks which apply to both wired (e.g., Internet Worms) and wireless (e.g., jamming) networks, they can also suffer from attacks to the network control traffic (e.g., forwarding infrastructure) because of the ease of physical access. This makes it relatively straightforward to capture, clone or tamper with wireless hops and orchestrate an attack. This suggests there is a set of challenging technical problems to address with regard to security on WMNs. However, in a community network scenario the users probably do not possess the knowledge required to consider and address these challenges. They may also have very different conceptions of what a security threat might be or what kind of response might be appropriate. Furthermore, considering security will likely require a greater degree of network administration, perhaps making a WMN less self-managing. These are all predominantly *social* concerns, perhaps even mundane issues, and potentially far more difficult to identify and address than technical concerns. It is evident therefore that to address the problems of security in community WMNs we need to adopt a socio-technical approach.

We have seen little research that has concerned itself with some of the important socio-technical issues involved in determining security requirements in community settings. It is in this sense that this research requires some interdisciplinary sensitivities, not least in a concern with exactly how certain basic questions might be posed to users: what are users afraid of?, what do they value that's worth protecting?, how much do they want to be involved?, how automated do they want the process to be?, etc. and what weight we need to attach to their answers. As Agre [1] argues; *"The design of community networks can support positive values in this complicated world, but only so long as the designers understand what they are getting into."* We would like to have some greater awareness of exactly what kind of security issues we are getting into. What we are aiming at in this project is then an awareness of and sensitivity towards a range of user concerns that may in turn impinge on and inform approaches to the security of the network. Like Dourish et al. [11, 12] then, we also stress the ways in which security issues and perceptions are inevitably embedded in complex social and cultural contexts. The particular context we wish to explicate is that of communal life.

3 WMN in the community: communities, technology and design

The WMN, and the community, we are interested in is Wray, a small, relatively remote village in the north of Lancashire, where the community felt strongly that the lack of broadband availability (a consequence of their remoteness) in their village was jeopardising local businesses, education and impacting on other aspects of community life. It has a population of less than 500 and has a single post office and general store, two pubs, a café, a parish church, a school, a village hall and a single main street.

In early 2004, a Lancaster University-led project into wireless mesh networking provided the community with access to broadband—their remote location meant that their only option for Internet access had been a slow (often unreliable) dial-up service. The University built a WMN

within the village to investigate the resilience and capabilities of the technology, offering Internet access to residents in their homes and at public locations around the village. For our purposes, it appeared a thriving, interesting and (for research purposes) convenient community.

The WMN is deployed in Wray as a 'community' network. Undoubtedly the word 'community' is a feelgood word, for as Bauman [5] argues: *"It feels good: whatever the word 'community' may mean, it is good 'to have a community', 'to be in a community'"*. However, it is evidently the case that social, economic and technological changes have altered the nature, importance and influence of 'community' Wellman [30, 31], so exactly what the expectations are for a community network is open to some debate.

Technology allows for the use and maintenance of any dispersed social network, so 'community' may have little to do with the individual's geographical location, but become instead an achieved social construct of mutual ties, orientations and obligations. But technology alone has no obvious relationship with any sense of community and can evidently either reinforce or fragment community and community life, depending on the interaction between technologies (and their affordances) and particular communities (and their dynamics). Our interest in affordances and dynamics is, in this particular case, shaped by a concern for security. As Mynatt et al. [22] note, the essential features of community are to do with boundaries, relationships and change—values and emphases that correspond fairly well with a range of security concerns. For example, the boundaries of community are not just spatial but also relational, social, technological, institutional, etc. Indeed, fundamental to this notion of 'community' is the notion of 'place' that Harrison and Dourish [17] define as "*a space which is invested with understandings of behavioural appropriateness, cultural expectations, and so forth*." This therefore incorporates some notion of 'membership' (and of awareness of membership) of inclusion and exclusion. But this is not to reinvent Parsonian or Durkheimian notions of the 'moral order', nor is it to simply suggest that 'community' is merely constituted in opposition to 'outsiders'—though this division can be important. Instead we are trying to point to various subtleties in a community's own understandings of the notion; of the multifarious ways in which 'community' is based on meaningful and multi-layered relationships that are significant and persistent for members. These relations become a mutual source of orientation and definition of appropriate and inappropriate behaviours and values. In this way the 'community' establishes expectations and responsibilities, these might be said to be the 'mundane features' of everyday communal life, indeed they are, as Hobbes argued, what make communal life possible at all, avoiding a life that is 'solitary poor, nasty, brutish and short'. These mundane features will include notions of reciprocity and commitment as well as shared values and practices; values and practices that may well include adhering to a range of basic security protocols and practices. In the everyday world this might include simple maxims such as remembering to lock doors and close windows, or not to take sweets from strangers; on the Internet it might include injunctions to close down applications, to protect passwords and not to open attachments from 'strangers'—and from neighbours whose approach to security might be very different and occasionally less than desirable.

4 Methodological issues in understanding security

Friedman et al. [16] in 'Users Conceptions of Web Security' suggest we need to help users construct more accurate understandings of security. Such understandings can take various forms but they both point to the fragility of users understandings and appreciation of security, documenting both how users mistakenly understand and evaluate security. In large part this is because as Edwards et al. [13] argue, and our own focus group studies confirm, for most users, security is simply not a paramount, sometimes not even a conscious, goal, often being merely incidental to the particular task at hand (see also [7]). However, the obvious solution of automating security faces profound technical and social factors that diminish the acceptance and efficacy of automated end-user security solutions. Failure to correctly identify stakeholders and stakeholder values; to identify and meet users' needs are at the heart of many of the problems of 'usable security' and initiated our interest in forms of stakeholder analysis using an established focus group method and the eventual design and deployment of technology probes.

While it seems essential that measures are taken to determine the most probable and damaging attacks for a particular network, in order to make best use of the limited monetary, time and computing resources that are available in a community WMN context, determining exactly how to proceed appropriately in a community, as opposed to a more easily understood business, context is complex. How can we best proceed to understand security in a community WMN? And importantly, how can we understand it in a way that is useful and informative to design considerations?

One approach to this involves identifying the most vulnerable 'assets' associated with an organization (those that, if exploited, would have the highest impact, and also those that have the highest probability of being attacked) and the vulnerabilities associated with them.

Within business settings there exists the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method [2] to determine an enterprise's critical assets and the technical vulnerabilities associated with them.

The motivation for adopting an OCTAVE-like approach in a community context is compelling. The method defines a set of principles; for example, the process of determining a security strategy should be led by the organization itself—an attractive proposition in our context because of the probable lack of funding for expensive security consultancy. Assets form the basis on which a security strategy is developed—given the largely non-technical user-base in Wray, who may have an idea of what they want to protect, but not how to achieve it, defining assets is an approachable starting point that could be built upon by more a more technically adept subset of the community. A process like OCTAVE brings to the fore security trade-offs, which will have an important role in forming a security strategy in this context—consider the 'how do I want to be involved?' question. However, determining how best a community could go about this process, potentially by itself, raises a number of important and interesting methodological issues.

The original OCTAVE method is intended for use in large corporate, military, and governmental organizations. Based upon the OCTAVE principles further methods can be developed for use in different contexts. One such method is OCTAVE-S, specifically created for use in businesses with less than 100 employees. The process is carried out by much smaller groups of people, knowledgeable about the network they are assessing. Meetings are held to create asset-based threat profiles, which involves identifying what exists on the network that is valuable, and ranking their value according to perceived necessity and importance. The second step is to identify vulnerabilities in the networking infrastructure that could affect the assets that have been identified as most critical. The last step is to take the information from steps one and two and identify specific risks that combine the vulnerabilities and assets, and from that develop security strategies to mitigate potential problems.

But can a process such as OCTAVE-S be easily transposed to a community WMN context? In what ways, and to what extent, is a community like a business or an organization? Or a business like a community? Understanding some of the relevant differences and similarities between a business and a community forms part of the bedrock of modern sociological analysis as reflected in Tonnies' [29] seminal work on *Gemeinschaft* and *Gesellschaft*. The detail of this debate need not concern us: basically a business is an organization that is planned, rational and purposeful in pursuit of a restricted range of goals associated with the development, production and sale of a particular product or service. A community is an organization or group of some kind that shares, to a greater or lesser extent, particular values, resources and beliefs. Our interest and our analysis is concerned with whether subtle differences in motivation, expectation and involvement come to be reflected in security concerns—in ideas about assets that need to be protected or threats that might be identified. While assets such as those in an enterprise setting obviously exist, the set of assets to protect in a community WMN context may be quite different. However, there is no overwhelming theoretical or methodological reason why a community cannot be treated like an organization and there are obvious advantages of comprehensiveness and generalizability to be gained from adopting a structured approach like OCTAVE, particularly when combined with other qualitative approaches to security requirements, since their combination permits us to explore some of the subtleties of determining security issues.

Obviously certain aspects, relevant to security—like a concern with boundaries, relationships and change—are common to both communities and businesses, even if the motivations behind them, the contrasting motivations of profit and sociality, may be very different. Other assets, such as privacy, trust, identity, reputation or safety may also manifest themselves very differently, and have different priorities within a community setting. For example, while businesses and communities share much the same legal framework, their orientation to issues of privacy, e-mail privacy for example, may, for very good and compelling legal reasons, be entirely different.

There are also a range of difficult practical organizational issues to be faced, determining exactly the *who*, *how*, *where* and *when* to hold the kind of meeting required by an OCTAVE-like approach to security. For example, can a group of three to five people sufficiently know the usage and organization of a network to carry out the process on behalf of everyone else? Probably not, we think.

Nevertheless, as part of a methodologically eclectic project we are currently investigating ways that an activity such as OCTAVE could be carried out in the context of the Wray village network, using, as an initial approach, the mechanism of focus groups in order to identify the assets and current security practices of the villagers. In this fashion, we hoped to test the applicability and the boundaries of the OCTAVE approach and perhaps identify areas for further development or supplementation in this particular setting. We aimed then to investigate the use of the core OCTAVE ideas and the available prior knowledge in this area, but extending it to apply in a community environment, thereby hopefully empowering community users to ensure the security of their own networks.

5 Implementing an OCTAVE method approach to community security

We embarked on an OCTAVE-S like approach by setting up a focus group meeting in the village café—a setting intended to overcome at least some of the artificiality of a focus group approach, and further enabled by the fact that we have been involved in research and development in this community for some considerable time and using a variety of techniques [28]. The focus group was facilitated by members of the project team and a number of villagers, with a variety of interests, experience and expertise (from business users of the WMN to those who only used it for leisure or family purposes), were invited to come along and discuss their use of the WMN and any security concerns they might have. In this fashion, we hoped to obtain some specific empirical data on WMN users concerns about security issues such as identity theft, privacy, and so on, reflecting people's actual, as opposed to imagined, security worries.

In a wide-ranging discussion various issues were raised. As part of an attempt to begin the process of identifying assets, the session began with coffee and cakes (another 'mundane technology') and some fairly general questions about security, safety and storage.

Focus Group Extract 1 (simplified abbreviated transcript)

P (project team)—*what sort of things do you have stored on your computers?… This is potentially private, so don't think we're forcing you to tell us. Who are you comfortable sharing those things with?. Are you particularly concerned about keeping any of those things safe?*
V1 (villager)—*Personal, family photos saved, no negatives any more, etc., work stuff - invoices, time sheets, tax, data files. .. things that are critical to keep*
P—*If someone got them who wasn't supposed to have them would that cause a problem?*
V1—*Would be bad, could be terrible for the company. Like when building a new rig, industrial espionage…. I don't have these printed out so much, use Linux, I go away a lot so I keep a regular back up at my brother's [house], if someone stole the laptop there would be a second copy somewhere else.*
V2—*Billions of photographs, backed up onto a portable hard disk. Village website, also on the community laptop, and also on the desktop and the portable storage. Backs up to Gmail, lots of accounts. ..always have access to them somewhere else, then. Bank details held in the web interface, books for the business held. Wouldn't like people going to look at my computer, but nothing especially to hide. Anyone I know can look. More bothered about phishing emails, can see lots of people being taken in. …thinking about protecting unwary people.*
V3—*Personal computer doesn't have much on I'd be worried about others seeing. Keep the village details, backs up every 3 months or so. .. There are issues with people having financial business accounts which can't be shown prior to trading, can't release the information before a certain time…Don't store passwords on the machine. Do Internet banking, want that to be safe.*
V4—*Ran a business, closed down a few years ago, still receiving information.. correspondence, personal stuff, but not confidential. .. I don't want to lose my photos, but aren't of much interest to other people.*
V5—*Photos saved… correspondence is kept. That's about all. I'm worried about phishing, how do they get your address? One of them the web browser said it was a phishing attack, the other didn't.*
V3—*You shouldn't click! ..they can install spyware on your computer by visiting the page.*
V2—*If you hover over the link in the email you can see where the link is taking you.*
V6—*Photographs, and emails, but only pictures I'd be sad to lose. I don't do anything to keep them safe, my son put some on a CD, but I'm bad about that.*
V7—*I have no work stuff on my personal computer, only on laptop that's backed up at work. .. at a personal level, don't keep passwords saved,…. Take backups, put photos on DVD every month. .. you can't lose memories, I wouldn't want to throw them away, but losing a few photos, I'm not worried about…*
V8—*Same as V7, I've worked in a business, seen people cry when their data has been lost and not backed up. I put stuff on a CD, I use the mother in-law's house as an external backup place. Purely because if you have something stolen, it's important to keep photos safe, and other things. …it's all about risk, what you conceive the risk to the data to be.*

In this brief, abbreviated extract we see some of the villagers concerns about security begin to surface. These concerns focus on the security of personal information, photographs and business information. We also see that these concerns have evoked a range of personal, individual solutions in terms of back-up, storage and secrecy. Although the researchers facilitated the discussion, it is fairly obvious that within a short period of time comments and contributions are freely given and exchanged and are not just a simple product of the focus group format. The discussion then began to focus on more specific concerns about safety and about the possible malicious use of the network—either by those in the village or outsiders:

Focus Group Extract 2 (simplified abbreviated transcript)

P—*what are your concerns, safety concerns on the network? People are worried about losing things, do you have any other worries .. when using your computer on the Internet?*
V8—*I worry about identity, what you've done on the network, or how people can pretend you've done things, .. something maybe you've never done, or the worst thing you've done.… maybe if I dislike you I could make stuff up and tell people bad things about you.*
V3—*kids do this on Bebo! pretend to be other people…*
V9—…I *work with people who are scared of their teenage children on chatrooms. They get worried. In their rooms with their mates fiddling about..*
P—*You have kids who use the computer, do you have concerns?*
V7—*They are pretty sensible, MSN requires them to accept people they know. They talk to their friends, don't talk to random people. They're not using social networking sites, only communicating with people they know.*
V3—*Social networking, friends of friends are the issue, ..two clicks and it's nasty.*
V8—*Friends Reunited, someone made a site about someone else, a silly one, people thought it was true. How do they authenticate a person as themselves?.*
V2—*Someone in the village made a Bebo page, .. posted pictures of herself on the Internet. Linked to that are pictures of V3's children.*

In this extract the villagers fears about security are focused not on their possessions but on themselves and their children; about the possibilities of identity theft, of possible defamation, the problem of really knowing who one is talking to and the possible consequences of using chatrooms or social networking sites *"two clicks and its nasty"*. Finally, there was also some unprompted discussion on the specific security of the WMN:

Focus Group Extract 3 (simplified abbreviated transcript)
P—*… interested to know if there are concerns that are mesh specific?*
V7—*If I were using a wired network, would I be more secure? What access does the university have to see the data being transferred? These are the questions that occur to me. I don't worry about people accessing my computer specifically, have a wireless network in my house controlled by MAC address.*
P—*At the moment you're not sure if you're better off on the wired network or mesh network?*
V7—*Yes.*
V2—*Same as this person who thinks it's not as secure.*
V3—*It probably isn't as secure as wired, but not as insecure as the messages in windows "unsecured network connection" would imply.*
V2—*Is it any less safe using the Uni[versity]? Normal ISPs still have to record information.*
V8—*Always make sure you understand anyone could be watching your network traffic…. Mesh network is wireless, if you buy a cable from BT, that goes through to their network. they own and manage it. If you connect to Wray you won't specifically know you are connecting to Wray … in the same way as making a connection to a BT exchange.*
V3—*If you run a home network without restrictions, you have the same problems, your network could spill out into other houses.*
V8—*No disrespect, but someone could have your MAC address in seconds.*

These three short extracts give some flavour of precisely how, in the course of the focus group session, a range of fears and vulnerabilities (real or imagined) were identified. These included; mesh infrastructure spoofing; specific targeting of information stored, for reasons of industrial espionage; phishing emails and how to deal with them; breaking hard-drive data encryption; identity theft, or knowledge about usage; lack of security stopping people gaining direct access to the WMN; fear of downloading something and not realizing or knowing what it's doing. They also illustrate the interesting interplay between a purely technical view of security and a socio-technical view where users interests, fears and concerns, including their misunderstandings and misconceptions, are identified and then taken account of in the design process.

The focus group also enabled us to begin the OCTAVE-style process of identifying 'assets', including:

- stored photographs and work documents;
- unfettered use of the home computer;
- personal information stored on the computer;
- privacy—of browsing habits, etc.;
- personal identity and reputation—protection from theft and damage or unauthorized use;
- children—and the protection of children from various forms of exploitation or abuse;
- safety and security of the less computer literate members of the community;
- and access to the Internet with a high quality connection allowing; remote access, teleconferencing and Skype.

What is interesting from an interdisciplinary view is the way in which conventional sociological interests in community are also reflected in these readily identified security concerns and assets. It might also be argued that the concerns voiced by the villagers reflect precisely the kinds of issues that need to be dealt with in order for the technology to become 'domesticated', to be tamed, to become 'mundane'.

One obvious example is the worry about membership (who 'belongs'); since recognizable members and membership categories, allied with recognizable boundaries can be utilized as initial filters for suspicion and trust. Similarly, the allied concern with identity and representation over the WMN; how people can represent themselves and manage their 'identities' as a means for ensuring both the security of their identity and their trusted interactions with others; and managing spatial relations in order to integrate the 'real' and the 'virtual' also reflect common sociological tropes. These involve having ideas about exactly where people, who are interacting via the WMN, might be in time and space as part of the common grounds for shared, for trusted, expectations and comprehension of behaviour. Finally, an expressed desire for a security-related FAQ sheet clearly points to ongoing aspects of community development and history that the community should be able to reflect and learn from experience, to develop 'robust sociality'.

Above all, and with a few notable exceptions, our focus groups suggest that our respondents were not especially interested in security—they just wanted their machines to work. Indeed a number of them likened computer systems to their cars, they did not want to look under the bonnet and know how they worked, they did not really want to think about them at all, they just wanted them to work every time. As Kindberg et al. [18] suggest *"people bring to bear very different kinds of reasons when making judgments about technologies. Trust and security issues may play a role, but other kinds of issue may be equally or even more important, like ease of use and convenience, or social ones. These other kinds of issue may be deliberately traded off or discounted in making decisions and reasoning about technology*". Our research further illustrates how difficult people find it to talk about, represent or understand security, unless they themselves have experienced a security breach or it is the subject of a current media panic. But failing to foresee the future, and future security needs, is not a particular, reprehensible failing of our sample or our community but it does make gathering requirements and design rather more difficult, since it is not only designing for the (unknown) future but designing in the face of indifference. It does, however, contribute to what Stewart and Williams [27] call 'the design fallacy' whereby particular and unchanging values are attributed to users, users responses to technology in the form of 'domestication' [25] and 'innofusion' [14, 15] are ignored and, in consequence the system or application becomes increasingly divorced from and irrelevant to user needs. Stewart and Williams point to the importance of social learning over the lifecycle of the design and deployment of a technology, the processes of domestication and innofusion that are rarely considered in the understanding and evaluation of design. We agree and also concur with another conclusion that; "design must confront the inevitable metaphorical leap in creating a representation of 'the user' in a context of incomplete information about current users and their requirements (let alone future users who do not yet exist)." But saying things are difficult is not a reason for abandonment, however, superficially attractive that might seem, and we suggest that the eclectic methodological combinations presented here indicate our attempts to develop some sensitivity towards initial user requirements, to tap into and respond to changes in both user requirements and changing user populations.

6 Conclusion: 'Becoming Mundane'—designing for social interaction with mundane technologies

This paper, and this research, has been interested in exploring aspects of security and trust as understood by potential users as a pre-cursor to design. That is, whilst previous research on domestication has taken an existing technology and speculated as to exactly why and how it has been incorporated into everyday life this approach has attempted to use security and trust as a *predictor* of the likely acceptance, the likely domestication of a technology.

While previous research has examined the deployment and modification in use of a technology as providing insights into the process of domestication, this research has attempted to operate at a more fundamental level, to look at the potential basis of the domestication process, to examine notions of security and trust, and thereby design such that technology facilitates domestication. This research is obviously at an early stage but what clearly emerges from the work so far is the importance of an interdisciplinary approach to the topic of security, since getting a useful understanding of user fears and expectations requires the deployment and appreciation of social scientific methodologies and analytic frameworks.

In this fashion, traditional approaches to design that focus only on the relative importance of particular functionalities and their relative cost can be supplemented, supported or challenged by reference to user concerns and interests. So, for example, initially, and perhaps unsurprisingly, we focused on identity theft as an assumed focus of concern for residents within Wray, but the initial focus group has shown little indication of people having any great fear in that area. In a similar fashion we quickly realized the importance of providing some form of explanation of security in the WMN since it is evident that people in the village are not completely aware of the organization and security of the Wray network as it currently stands. There is a general lack of understanding regarding precisely how secure the network is (or is not). In such a setting any 'improvements' to security need to be

carefully introduced and explained if they are going to be appreciated. A number of people in the focus group requested a Q&A or FAQ sheet to outline and explain basic security information, whilst others mentioned the need for some form of security education over the WMN, either to help allay people's fears or to raise awareness of security issues. Finally, the focus group suggested ways in which a number of group concerns could be addressed by introducing security measures on the Wray network through; increased security for identifying the Wray mesh boxes to the clients; increased security for authenticating clients on the network; and IDS or anomaly detection systems identifying when people's computers are behaving in a suspicious manner and may be compromised.

In the context of a community we were interested initially in teasing out, in explicating, people's particular ideas and concerns about security—together with a method to accomplish this—alongside understanding the various complex technical challenges before commencing the extremely difficult task of somehow meshing these very different aspects together: developing a technology that is sensitive to user concerns and a user community sensitive to the requirements and limitations of the technology. What we are seeing here are the social processes of trust production [20] for it is in just such a fashion that a technology becomes trusted' as Silverstone [26] (even if he was talking about a different trusted technology, television) suggests: *"For most of us, most of the time, our natural attitude in the taken-for-granted world is one which enables us to maintain our sanity in our passage through life and the daily round. Routines, habits …and the consistencies with which our interactions with each other conform to expectations, together provide the infrastructure for a moral universe in which we, its citizens, can go about our daily business. Through learning to trust others we learn, one way or another, to trust things. And likewise, through learning to trust material things we learn to trust abstract things. Trust is therefore achieved and sustained through the ordinariness of everyday life and the consistencies of both language and experience."*

We freely admit that we are not the first (nor likely the last) to try and understand the social and cultural aspects of security. Like Dourish and Anderson [11], we agree that the dominant model of security is overly abstract and neglects social practices. In their formulation, our emphasis has been on security as a practical accomplishment. Consequently we agree that formulations of security are relatively unpredictable products of myriad social and cultural encounters; that an emphasis on use and on an understanding of trust in relation to flows of information is important and that we may be able to engage in more effective design interventions by looking at collective information practice. Like Dourish and Anderson, we have *'attempted to place technological privacy and security concerns within social and cultural contexts'* intending that any design or technical application reflects and incorporates the understandings achieved. We have done this through a structured research method—OCTAVE—which provides a way of understanding the social and cultural practices that underpin technical specifications of security. The method and the approach carries with it a range of important implications—and problems. Some of the problems concern exactly how we might go about understanding these issues and documenting them in a fashion that may prove useful to design, given that the end-product of our understanding is to improve design in some way. We believe that many of these problems in understanding social and cultural practices and then designing them into a technology are not well understood.

Our approach differs from previous attempts [11, 12] in that our emphasis is on community life, practices, values and associated issues of boundaries relationships and change that may be different from those found either individually or in workplace settings. Our interests therefore extend beyond detailing existing individual security practices, practices that people are likely to implement, to uncovering aspects of social, communal life that people think are worth keeping secured. We suggest that these may be key to understanding the ways in which technologies may become mundane. In attempting to apply and develop a structured methodological approach to understanding community security requirements, we document communal sets of values and practices held in common, the very things, some might say that security policies and protocols are designed to defend, and the very things that are likely to contribute most to a technology 'becoming mundane'.

Acknowledgments Paul Smith's research was supported by Telekom Austria AG. The authors are grateful to the members of the Wray village community that took part in this research.

References

1. Agre P (1999) Rethinking networks and communities in a wired society. American Society for Information Science, Pasadena, May 1999
2. Alberts C, Behrens S, Pethia R, Wilson W (1999) Operationally critical threat, asset, and vulnerability evaluation framework, version 1.0. Technical Report CMU/SEI-99-TR-017, Carnegie Mellon University, June 1999
3. Anderson J (2008) What is the LocustWorld Meshbox? http://www.locustworld.com/overview.php
4. Annison L (2006) JFDI Community broadband: Wennington. Digital Dales Ltd, November 2006
5. Bauman Z (2001) Community: seeking safety in an insecure world. Polity, London
6. Becker H (1953) Becoming a marihuana user'. J Sociol 59:235–242

7. Besnard D, Arief B (2004) Computer security impaired by legitimate users. Comput Secur 23(3):253–264
8. Borgmann A (1984) Technology and the character of contemporary life. University of Chicago Press, Chicago
9. Castells M (2000) The information age: economy, society and culture. Blackwell, Oxford
10. Castells M (2000) Materials for an exploratory theory of the network society. Br J Sociol 51(1):5–24
11. Dourish P, Anderson K (2006) Collective information practice: exploring privacy and security as social and cultural phenomena. Hum Comput Interact 21:319–342
12. Dourish P, Grinter R, Delgado de la Flor J, Jospeh M (2004) Security in the wild: user strategies for managing security as an everyday, practical problem. Pers Ubiquitous Comput 8(6):19–30
13. Edwards W, Poole E, Stoll J (2007) Security automation considered harmful? In: Proceedings of the IEEE new security paradigms workshop (NSPW 2007), White Mountain, New Hampshire, September 18–21, 2007
14. Fleck J (1988) Innofusion or diffusation? The nature of technological development in robotics. Edinburgh PICT working paper no. 7. Edinburgh University, Edinburgh
15. Fleck J (1988) Innofusion or diffusation: the nature of technological development in robotics. Edinburgh PICT working paper no. 4. Edinburgh University, Edinburgh
16. Friedman B, Hurley D, Howe DC, Felten E, Nissenbaum H (2002) Users' conceptions of web security: a comparative study. In: Proceedings of CHI 2002, Minneapolis, Minnesota, 2002, pp 746–747
17. Harrison S, Dourish P (1996) Re-place-ing space: the roles of place and space in collaborative systems. In: Proceedings of CSCW '96, pp 67–76
18. Kindberg T, Sellen A, Geelhoed E (2004) Security and trust in mobile interactions: a study of users' perceptions and reasoning UBICOMP 2004, Nottingham, UK, September 2004
19. Lash S, Urry J (1994) Economies of signs and space. Sage, London
20. Luhmann N (1990) Familiarity, confidence, trust: problems and Alternatives. In: Gambetta D (ed) Trust: making and breaking cooperative relations, electronic edition. Department of Sociology, University of Oxford, chap 6, pp 94–107. http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf
21. Mackenzie A (2008) Wirelessness as experience of convergence Fibreculture Issue 13 http://journal.fibreculture.org/issue13/issue13_mackenzie_print.html
22. Mynatt E, O'Day V, Adler A, Ito M (1998) Network communities: something old, something new, something borrowed …. Comput Support Coop Work 7(1–2):123–156
23. Petersen SM (2007) Mundane cyborg practice: material aspects of broadband Internet use. Convergence: Int J Res New Media Technol 13(1):79–91
24. Silverstone R, Haddon L (1996) Design and the domestication of information and communication technologies: technical change and everyday life. In: Silverstone R, Mansell R (eds) Communication by design: the politics of information and communication technologies. Oxford University Press, Oxford
25. Silverstone R, Hirsch E, Morley D (1992) Information and communication technologies and the moral economy of the household. In: Silverstone R, Hirsch E (eds) Consuming technologies. Media and information in domestic spaces. Routledge, London
26. Silverstone R (1994) Television and everyday life. Routledge, London
27. Stewart J, Williams R (2005) The wrong trousers? Beyond the design fallacy: social learning and the user. Reprinted in Howcroft et al (eds) Critical IT handbook. Edward Elgar, Cheltenham, pp 195–221
28. Taylor N, Cheverst K. Fitton D, Race N, Rouncefield M, Graham C (2007) 'Probing communities: study of a village photo display. In: Proceedings of OzCHI 2007, pp 17–24
29. Tönnies F (1988) Community & society: gemeinschaft and gesellschaft. Transaction Publishers, Edison
30. Wellman B (1999) From little boxes to loosely-bounded networks: the privatization and domestication of community. In: Abu-Lughod J (ed) Sociology for the 21st century: continuities and cutting edges. University of Chicago Press, Chicago
31. Wellman B, Haase AQ, Witte J, Hampton K (2001) Does the Internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment. Am Behav Sci 45(3):436–455