talking to the walls

by Mark Burgess

Mark is an associate professor at Oslo College.

Mark.Burgess@iu.hio.no

A Meeting with Medusa

Throughout the passage of time we have talked to walls, in special rooms, and in private spaces, communing with deities and seeking guidance from spiritual powers. Today something else is happening: Our need for solace and comfort is more readily at hand in technological form. Our need for connection has become more rooted in the physical but has also expanded to become an addiction that veils a paradox. Are we all becoming possessed by distant voices – and thereby remote from our surroundings?

Imagine a chilly autumn day in downtown Oslo around 1999. The trams roll through the center of town; there are small flakes of snow in the air, and I am heading toward the Ibsen car park together with a visiting colleague at Oslo University College. (In Norway, we are careful to honor our important writers by naming parking lots after them.) The car park lies in the center of town, on the edge of the edge. It's a part of town called Grensen, literally "the edge," and it is populated by some of Oslo's more fantastic mythological beasts. In Oslo, as in most capital cities, a league of solvent abusers populates the city center, staggering around collecting coins and muttering to themselves in their own private reality. In this environment, it becomes natural to associate anyone muttering to themselves with some form of chemical escapism.

As we enter the high-tech lobby to the car park, I hear a voice talking frantically to someone, as if face to face. It is a figure in a black Armani, with expensive attaché case, standing next to the pay machines, stepping back and forth, staring into thin air, and facing the wall. A little wire hangs from his ear, but at the time I don't understand the significance of it. As he sees us, he seems shocked as though we have invaded his personal bubble. Right here in the most public place imaginable. I realize that there is something going on here that is of the greatest importance to society.

Today we don't think twice about hands-free mobile telephones. As we walk about, people are talking to themselves all the time, usually with a hand glued to their head. But all this has a deeper meaning – not just for us, but for system administration. Let's backtrack a little.

Getting Rid of the Keyboard . . .

Soon computers will be everywhere: in the walls, in our domestic appliances, and even in our clothing. Mark Weiser, former chief of technology at Xerox PARC, said, "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."

The keyboard is a potent symbol that this has not happened with computers yet. Computers are both conspicuous and unreliable, but there are several projects around the world to change this: the smart home of Hewlett Packard, Microsoft's tablet PCs, embedded Linux and Windows, etc. Still, given the advances in technology, it is reasonable to ask when this dream of disappearance might happen. The promise of a technological future has not yet caught up with science fiction. Technology for computation, multimedia, and communications has not yet disappeared from view: we cannot yet talk to our walls in a technological sense. A recent article in the IEEE computer magazine presented what it called the good news and the bad news about voice recognition. The bad news is that *Star Trek* has raised our expectations about voice

The location of individuals is unlikely to remain a real secret for much longer – the devices we carry will position us and cameras and sensors will recognize us.

recognition so high that it will be very hard to live up to them. The good news, on the other hand, is that we have until the 23rd century to sort it out.

We have had the promise of smart devices for many years, though they have been surprisingly slow in coming. The smart room that can detect your presence or switch on the lights and turn up the heating before you arrive by learning your patterns of behavior has not yet found widespread acceptance. The smart toilet that analyzes the colonies of bacteria that we donate to nature each day and finds out if we are sick or need dietary modifications has not yet materialized.

Kitchen computers were supposed to keep running inventories of supplies, be able to watch out for new recipes on the Net, order food when stocks got low, and so on. The kitchen cooker is supposed to be connected to your personal manager so that it starts warming up your dinner while you are on the way home (after all, everyone will be single in the future, so no one will have a partner to do this for them) – more on this later.

At the larger scale, smart cities will be able to route traffic automatically to avoid congestion and regulate resources such as lighting and heating. Buildings will control and reprocess their waste and be more resource efficient with regard to regulation of temperature and humidity. The location of individuals is unlikely to remain a real secret for much longer – the devices we carry will position us and cameras and sensors will recognize us. Cities will be able to share resources with other neighboring cities and organize common sharable resource pools – an automated city council, extra buses ordered when the demand increases. Local and global government will be replaced, slowly but surely, with automated cooperation and resource scheduling.

Embedded devices will eventually be found everywhere – and not just those left by the FBI! In restaurants we will have smart menus, with adaptive pricing and Amazon-style recommendations for your order based on what you ordered recently. Outside, attentive billboards will look back at you and gather information about sex, age, race, the clothes you wear, height, and weight. Walls will even monitor criminal activity for the police. Humans will be wearing the devices as they move around within this circus. The increase in surveillance devices has already been prolific in the last 10 years, especially in countries like the UK.

What Might It Mean?

What do these developments mean for those of us involved in the deployment and running of the technologies? We might expect to see tens of devices per room – a fairly complex network of devices linked probably by a Bluetooth type of wireless broadcast network.

There are management and security implications to living in such a density of information driven devices. The future of system management will not be a simple task like installing a package for Windows or GNU/Linux with some simple defaults, it will be a question of determining an increasingly complex policy that deals with how to exchange information with others, gives others access to our data, and protects ourselves from theirs. As we move from room to room in the house, the policy requirements will change. We will not want violent or explicit material transmitted to the children's den; we will not want telephone calls routed to the children after bedtime. Will we be able to cope with all of these constraints?

Today we use the term "trusted environment" quite often to describe a little island that we have made comfortable. But when computing becomes ubiquitous, the boundaries of our island have to break down, because we cannot sustain the illusion that we are all alone there. We cannot keep track of the pathways, the possibilities, or the interactions. There are people ballooning onto our island and digging tunnels to it. Others want to use it as a stepping-stone to get to somewhere else.

If computers are going to be running so-called intelligent software, then they cannot be isolated. How will they receive updates and instructions? We don't know exactly what operating systems embedded devices will use in the future, but they are bound to be complex adaptable operating systems (probably either Linux or Windows). If they are networked, it makes sense for them to receive updates and policy changes via the Net. But even after 10 years of developing management protocols for distributed devices, like SNMP, we are not much closer to finding a way to achieve this that is both efficient and non-intensive for humans.

Another problem is consistency and standardization. All of the pervasive devices listed above will eventually emerge, but not in any coordinated way. I am convinced that it is completely unrealistic to expect to be able to "manage" the resulting level of complexity using control protocols, as we shall see below.

The key to understanding pervasive computing lies very much in understanding people! We are the ones who will select or reject the technologies – by market forces. All we have to do today is to look around us. According to the dreams after the Second World War, everyone was going to be the proud owner of their own robot and personal spaceship by the year 2000. But, in reality, we were more interested in the immediate freedoms of cars and refrigerators.

Domestic Embedded Networks (DENs) will grow product by product, each with a different manufacturer using different standards. First it will be a Japanese or Korean microwave oven with an Internet connection. Then Microsoft will release the new X box that heats up a pizza while you're playing your favorite game so that you never have to remove the goggles and visit the real world. Then Sun will introduce a Java-enabled Open Sandwich toaster that produces more healthy food, and finally there will be a fight for standardization post-factum, and we will end up with the usual evolutionary gene pool of technologies that cannot be ignored. It won't be a neatly standardized set of controllable devices: After all, commerce is just warfare without politics.

If you are an evolutionist, then a broad technological gene pool is good for development. But if you are a system administrator control freak, or even the owner of one of these devices, then it is usually a nightmare. If technology is going to disappear, then it has to really disappear and not merely lurk in the shadows moaning for attention. All of this makes the problem of trust much harder – and therefore the problem of security a radically different one than before.

Eventually, simplicity tends to return as mass extinctions delete most of the competition and we learn to shift the boundaries of trust, and our little Cold War conspiracies dissolve toward more openness – if for no other reason than that it is really hard work distrusting people all the time. But before simplicity converges over this, we shall have to deal with the complexity of it. And here is a good reason why. Maybe smart rooms, smart walls, smart toilets are not what we want. What about smart people?

Maybe smart rooms, smart walls, smart toilets are not what we want. What about smart people?

Technology has never developed in the way we thought.

Mobility and Social Behavior

Steve Mann calls the smart room a "retrograde concept that empowers structure over the individual, imbuing our houses and public spaces with the right to constantly observe and monitor us." Mann wants us to be mobile devices – cyborgs. Others have argued that we already are! Take a look in the mirror.

The one aspect of ubiquitous computing that was never really envisioned (but which has flourished first) is mobile computing. Like the Internet, mobile services took off because they were at the root of a social phenomenon. In Japan, the under-25s call themselves the Thumb Generation, or the Thumb Tribe, because they live by their mobile phones, texting away with their thumbs – like touch typing.

Companies have tried several times to define Mobile Services for us, to sell us services that they dream up – like the 3G effort, with streaming video that would be used for business-like applications. But these have not taken off. Instead, cheap SMS messages have flourished and now camera still-pictures are taking off better than streaming video, because these are more "fun." They are not very useful for important communication, but they give pleasure to their users – perhaps because they retain a level of non-realism that still makes it seem like a game.

Technology has never developed in the way we thought. In the future visions that followed the Second World War (a time of aircraft and missiles), we imagined that every household would have its own spacecraft and that we would be traveling around the galaxy in a rich utopian marshaling of the galaxy. But when it came down to it, more domestic pursuits that empowered the individual over its civilization took precedence. The Italians bought motor scooters to be like the Americans and their cars, and the refrigerator allowed people to eat better. Society was formed from individual wishes, rather than having families fall into line with a greater vision.

Mobile technology is a freedom-giving device that has changed the way a society works where it has taken off. Particularly in Japan and here in Scandinavia, we see a generation of teenagers in constant contact with friends, no matter where they are. People no longer worry about being late for a meeting, because they can just send a text message to excuse themselves and reschedule. Time is now fluid; life is constantly being re-planned and rescheduled. With one foot in the future, people live by the moment and plans change in real time.

Social Changes

Social attitudes to one another have changed considerably. I was brought up to believe that a newspaper at the dinner table is the height of bad manners. Today, mobile phones are placed firmly between the starter and the fish knife, and conversations to the wall have equal if not higher priority than the face-to-face social graces. People will interrupt face-to-face contact for the immediately demanding mobile message.

This leads to cognitive confusion and social fragmentation. In Oslo, women get out their phones and talk loudly about nothing for the duration of their bus or tram journey – quite incapable of being "alone" in public. Perhaps they are so afraid of missing out on something in their remote social network that they have to exclude the possibility of enjoying their immediate environment. Humans are wired to relate in social ways, but if one loses respect for those in one's immediate environment, conflict rather than tolerance tends to arise.

Only a few years previously, the idea of revealing anything of oneself in public would have been a matter of considerable embarrassment in many countries. Today, people broadcast information and demand that others ignore it, as if emulating the very wireless protocols that are invading the electromagnetic airwaves with sound. Mobile users are constantly trading privacy for convenience – and struggling to renegotiate the bounds of privacy for increasingly selfish purposes. There are good users and bad users – those who respect each other's social spaces and those who do not. But they also use mobile communications as a shield to push others away.

Mobile users are constantly trading privacy for convenience.

Smoke Screen

Some would say that we are becoming more selfish, that our own microcosm is all that matters. It is our right to a kind of technological telepathy, or to spurn casual listeners for their impudence if we intrude into their space. In Scandinavia, the mobile phone has increasingly replaced the cigarette as a way of blowing smoke in faces at crowded places, or in an awkward situation like an elevator where normally one would be forced to communicate. Checking for messages is so much easier than making eye contact with someone. As soon as a situation becomes awkward (in an elevator, for instance), out with the phone. Many are literally dependent on their mobile phones now to run their lives and to keep others at arm's length. Clearly we shall all be single in the future.

Scandinavia has always had the stigma of having a difficult time with interpersonal relations. Now we have a way of avoiding them altogether. But this has various consequences. By placing virtual relationships above real ones, we distance ourselves even further from actual interaction. This affects our attitudes in social encounters (we are "cozy" on the phone, but hostile in public) and thus our formulations of acceptable policy in such cases. Whether we retreat or fight, adapt or conquer depends very much on our tolerance of others in society. Mobile, remote communication eliminates vulnerability and commitment. We risk nothing and gain little. Of course this is exactly the reason why we explore Mars with a remote probe – to avoid the possible risks associated with the reality of actual presence. With safe mobile communication, we never again have to reveal when we are having a bad hair day.

In Isaac Asimov's novel *The Naked Sun*, he describes a world called Solaria in which people never meet physically. They have retreated into a virtual world where they are safe from their neighbors and their attendant germs and smells. Today, we see people putting fences around their property, staking out their territory in terms of material wealth, and retreating from direct contact. It is perhaps no accident that these cultures are emerging most rapidly in Japan and Scandinavia, where – for opposite reasons – the population is insistent on distancing itself from its neighbors.

Why am I talking about sociology? I want to paint a picture of how humans behave, because it is humans who deploy technology and make the management decisions. Eventually, this will be a new battleground for conflict between opposing interests.

Modern Perseus?

Perseus was the warrior who slew the Gorgon Medusa, thanks mainly to some gadgets that he got from Hermes the Telecom provider and Athena his security advisor.

Modern society is increasingly based on toys for communication. By giving everyone these tools, our modern warrior is supposed to slay the ugly face of loneliness and rejection in society, bringing us all together. But how does it do it? By giving us so

much body armor that we are never comfortable without it again? By giving us the ability to avoid each other in reality, while clinging to one another's reflections?

Ad hoc encounters are what make life interesting, but how much do we want to reveal? History reveals an interesting dichotomy – we are getting less formal as time goes on (more ad hoc), but we are putting up more barriers in order to protect ourselves from risk. The barriers are getting closer to the core – personal firewalls, rather than building trust. There is an increasing spiral of distrust – which, for now, might excite the security industry, but which is not sustainable in the end.

Techno-Challenges of Pervasion

What does this have to do with us as system administrators? The answer is complicated, I believe, but it has to do with several things:

- Technology changes our behavior and our expectations. We torture-test it in ways that have more to do with sociology than technology.
- The boundaries of trust are the key to our deployment and expectations of technology. These boundaries are determined by human behavior.
- It is the interaction between humans and technology that is problematical for system administrators.
- The type of infrastructure that we will be expected to support in the future will be different and will be governed by personal freedom, selfish desire, habit, and pop culture rather than by the dictates of an IETF.

What are the main challenges of this pervasive computing for system administration, and how can we address them? First of all, we do not fully know the extent of the challenges yet – but, for the most part, I believe that they will not be radically different from what we see today, except that the arrival of smart devices will be nothing like what we imagine. However, the increased diversity will increase the magnitude of the problem and the rate at which the details of policy evolve.

- Diversity – we shall have an even more market-driven economy, fueled by whim rather than a desire for well-designed technology. This will lead to lots of conflicting coexisting technology. (This is normal and we have always experienced this in a smaller way.)
- We shall have to seek stability in the face of the much greater environmental noise from neighboring devices.
- Sociology of interaction will play a much greater role, because we cannot cordon off areas and isolate them any more. One organization flows into the next, and users roam around like cyber-tourists in foreign policy zones.

Most people want devices and technologies to be predictable. If they are not, then they cannot perform a useful function. In fact, since I have often spoken about the need to relax our strict ideas about frozen device configurations in order to allow some noise, I often hear from system administrators that they believe that every device has a correct configuration that should never change.

The kind of absolute stability that can be approached for immobile workstations is not really commensurate with the level of interaction that mobile or pervasive devices undergo. The idea of accepting any kind of uncertainty is more than many system administrators are willing to swallow. Yet this is precisely what we are going to have to accept if we employ increasing numbers of smart devices. The boundaries of trust will have to shift.

One area where things will change is in the level of exposure to environment. Environment means changing conditions and policy about right and wrong. Security consultants often posit that encryption is the solution to all security issues, but encryption is unlikely to help us here. The problem is not one of privacy, when individuals are being empowered with devices that allow them to expose themselves entirely and eagerly to a public audience.

Local regions are likely to demand their own rules, like micro-cultures. Both humans and devices will have to be aware of a much wider range of policies, rules, and standards of behavior that change as they move around. Some uniformity will no doubt emerge, but there will always be local features. Our ability to interact at a distance is leading us increasingly to draw boundaries around our property and shield our interests.

We might want to build our private island, but when we are in such a highly connected environment, the number of points of contact is too great to view isolation as a realistic possibility.

Where Lies the Authority?

In a world with fluid boundaries and increasing connectivity and blind trust in technology, we must work ever harder to define our own acceptable limits – our *policy*. To put it another way: If humans are constantly retreating from face-to-face confrontation with one another, then the rules of engagement must be ever clearer. In a human-computer collaboration, both humans and machine are supposed to obey policy. Who gets to decide on what policy says?

Smart devices are intrinsically bound to their environments. They must receive input and generate some output. If the exposure to environment increases, then a device will necessarily be more exposed to errors of configuration and random errors caused by misunderstandings and meddling.

I have claimed that we are becoming more mobile and connected, but also more suspicious of those who are not in our wired social networks. If we are roaming, do we have to adapt to the environment, or do we adapt the environment to us? Clearly the latter approach is a recipe for potential conflict. The likelihood for humans to cooperate is usually tied to the likelihood that they will see each other again. If we expect a long-term relationship in which reprisals for bad behavior are likely, then we are nice. All evidence shows that when humans believe that they will be long gone before anyone can catch them, they break rules and laws with alarming readiness.

Some imagine that mobile devices will always be rooted in a Virtual Private Network to home. How natural is it for a roaming device to maintain its ties to a home base? IPv6 allows and even encourages this, but I don't think that IETF has thought about an environment like Africa or Siberia, where connectivity will not be guaranteeable.

A more probable model will be for computing environments to supply cyber-tourists with services nearby. When the motor car was invented, it enabled freedom of movement because petrol/gas stations were available for refill wherever the individual decided to go. It was not necessary to stretch a cable from one's current location back to home base in order to fill up! This is why electric cars have had less success. Perhaps customers will be willing to pay the environment for a certain service (like a hotel) and guarantees on Quality of Environment will be the song of the day. Eventually, we will begin to accept local service provisions, because this is efficient. What this implies is

The likelihood for humans to cooperate is usually tied to the likelihood that they will see each other again.

that our environment is increasingly ad hoc. This has security as well as availability implications.

Trust in Clans and Societies

Who will make these decisions about what is acceptable? Will they occur top down or bottom up? By definition, administrators want to be on top, looking down. But down is not where users want to be. Clever users might resent this power structure and seek the freedom of their mobile phone or scooter to whisk them away from fascism.

We are increasingly empowering users toward autonomy. By giving them their own private communications bubble, we are also giving them the responsibility to find their own rules of engagement. Peer-to-peer networking shows this increasingly. It is an anti-authoritarian configuration. The only rule has to be mutual respect, or conflict. Human instincts will prevail here.

Perhaps a security policy based on mutual respect is more sustainable in the long term than one that is authoritarian. We shall have to discover the rules of society all over again. Mutual help and etiquette? Increased connectivity and mobility bring different cultures (social, racial, religious, or business), that is, different *policies*, closer together. Tolerance of others will be required.

In a ubiquitous computing environment everyone has roaming access to everything they need. That also means that the computers are exposed to a roaming environment — it usually works both ways: A greater contact area makes us more accessible and, therefore, more vulnerable. Even if we can apply access controls, there is a risk of configuration errors and possibly even the risk that persuasion might trick us into lowering defenses. Security does not depend only on technology.

The dynamics of cooperation and conflict are complex. Game theory is one way to analyze these issues. There are some basic results that characterize the interactions:

- The zero-sum game, where winner decides all.
- The prisoner's dilemma, bargaining for mutual gain, with tit-for-tat reprisals.
- Conditional consensus: I'll agree if everyone else agrees.

The results of games indicate that if we act in a purely selfish way, then a tit-for-tat strategy is best for protecting oneself from harm and for maximizing cooperation; that is, if one person is non-cooperative, non-cooperation is returned. If cooperation is offered, cooperation should be returned.

What about altruism and friendship (predictable agreement on policy)? What is it people get from investing in social relationships – even those with people they cannot see? We can call it social capital. Intimacy. A surrogate feeling of social acceptance that satisfies our genetic programming, like tofu for meat.

Game theory predicts that, if there is a reward from cooperation, then a reciprocal strategy is best. This forms a dynamical trust relationship, not merely a static one. Small groups are more likely to cooperate than large ones.

Cooperation takes us beyond zero-sum games, but when we have decided to cooperate conditionally, by voting, how do we arrive at consensus? In many cases, uncertainty leads to an overcautious strategy: we will vote if most other people do; we will flock with the others, if everyone is agreed. There is safety in numbers. These are the dynamics of consensus.

So, will there be discipline or anarchy in the world of pervasive computing? New alliances and allegiances are formed when roaming, but no stable consensus has to emerge. Humans make this even more difficult. In mathematics, if X=Y and X=Z, then Y=Z, but this is not true in human psychology. It is not impossible for X's policy to agree with Y's, but X and Y cannot agree, for other reasons. Humans are thus not easily predictable.

Swarm Intelligence: The Outcome of Weak Interaction

The new forms of pervasive computing and mobile communications lead to new social rules of engagement. If we do not understand those rules, some of us will disagree and the result will be conflict. Swarming or flocking is a way of capturing the equilibrium points of social conflicts and negotiations. On the one hand, isolationism creates little autonomous devices (insects), but mobile communications lead to involuntary clustering and flocking.

Swarms of insects and flocks of animals, for example, are assemblies of "devices" or "things" that communicate loosely but which spontaneously form quasi-stable structures that persist over long periods of time. Perhaps this is just what we are after for our devices (though perhaps not for our society).

The non-intelligent pieces have surprising properties when allowed to interact *weakly*. Do the pieces in a jigsaw puzzle know anything about the picture they form? Do any of the cells in our body have any idea about what they contribute to? These are emergent phenomena.

Swarm phenomena are already happening in humans as a result of mobile phone communication. Kids flock around like schools of fish with their mobile phones. They do not need to meet to be together, and final rendezvous can change even as they approach the moment! They are ad hoc social swarms – they change their behavior according to text messages and telephone conversations.

But can we harness swarming to secure a stable environment of pervasive devices? Conversely, once we release these devices, will be we able to prevent swarming phenomena from occurring? How do we guarantee that a swarm of ubiquitous computing devices will be a colony of helpful bacteria rather than a plague of harmful locusts?

One clue about the role of swarms is that socially developed swarms have many of the properties of social networks – quasi-hierarchies. Communication in swarms is by peer-to-peer transaction. This gives a robustness of form, combining trust in local neighbors with long-reaching connections ("strange connections") which occur in all social clusters. This is why no one on the planet is (on average) more than six degrees of separation from anyone else. Sometime, a central command might emerge spontaneously through centrality, but we should not be worried if it doesn't. Stability and security are not contingent on centralization or authoritarian control.

Conclusions

Do we want swarm behavior to emerge or not? In devices, in humans, or both? Can we stop it with judicious policies (i.e., "police" it away)? Sociology has a tendency to get its way; society has its own consciousness which usually trumps individuals. Does that mean that we are not safe? Security is about acceptable risk in relation to operating requirements. This should not be perceived as a problem, but we might need a change of philosophy in many system administrators.

Can we expect an ignorant tribe of technologically dependent, self-interested individuals to cooperate?

Society will not be threatened by its tendency to self-organize, but there are deeper ethical implications for society's use of technologies. We are constantly dumbing down human technology, taking responsibility away from the individual while simultaneously arming individuals with devices that allow them to be increasingly selfish. Soon we will have no burden of responsibility to learn about technology and we shall end up slaves to it – unable to understand, repair, or master it. As Arthur C. Clarke said, "Any sufficiently advanced technology is indistinguishable from magic." When it starts to seem like magic to us or when it truly disappears into the walls – out of sight and out of mind – we have a genuine cause for concern.

Can we expect an ignorant tribe of technologically dependent, self-interested individuals to cooperate? What kind of policy would they write? Is this a circuitous route back to nomadic anti-social behavior, in which individuals do battle rather than cooperate in meaningful society? Cold War isolationism is a slippery slope that leads to a downward spiral of trust.

To have our private boundaries penetrated is bad enough for our feeling of safety and well-being. To have our homes completely permeable to the outside world would be, for most of us, the ultimate breach of trust. Yet this is the potential vision we are concocting – will we fight it, or will we learn to embrace it? Not only in our homes, but in our clothes and in every aspect of our being. Pervasive computing is not only about making true cyborgs of us, but about weaving society together into a super swarm. How shall we behave then?

Society will always have a face that it cannot bear to look at. Our Medusa, the terrible face of loneliness, will probably always remain unbeheaded, but we must not be seduced into isolation-confrontation mode. Better to talk to smart neighbors than to end up talking only to our smart walls. Communication and cooperation are too complex to be entrusted to blunt electronic instruments. The way to solve our management and security problems is not by fueling an arms race, but by diplomatic conversation. That means that we must deploy technology along with education about the workings of both humans and machines, and we must preserve genuine close encounters between friends.