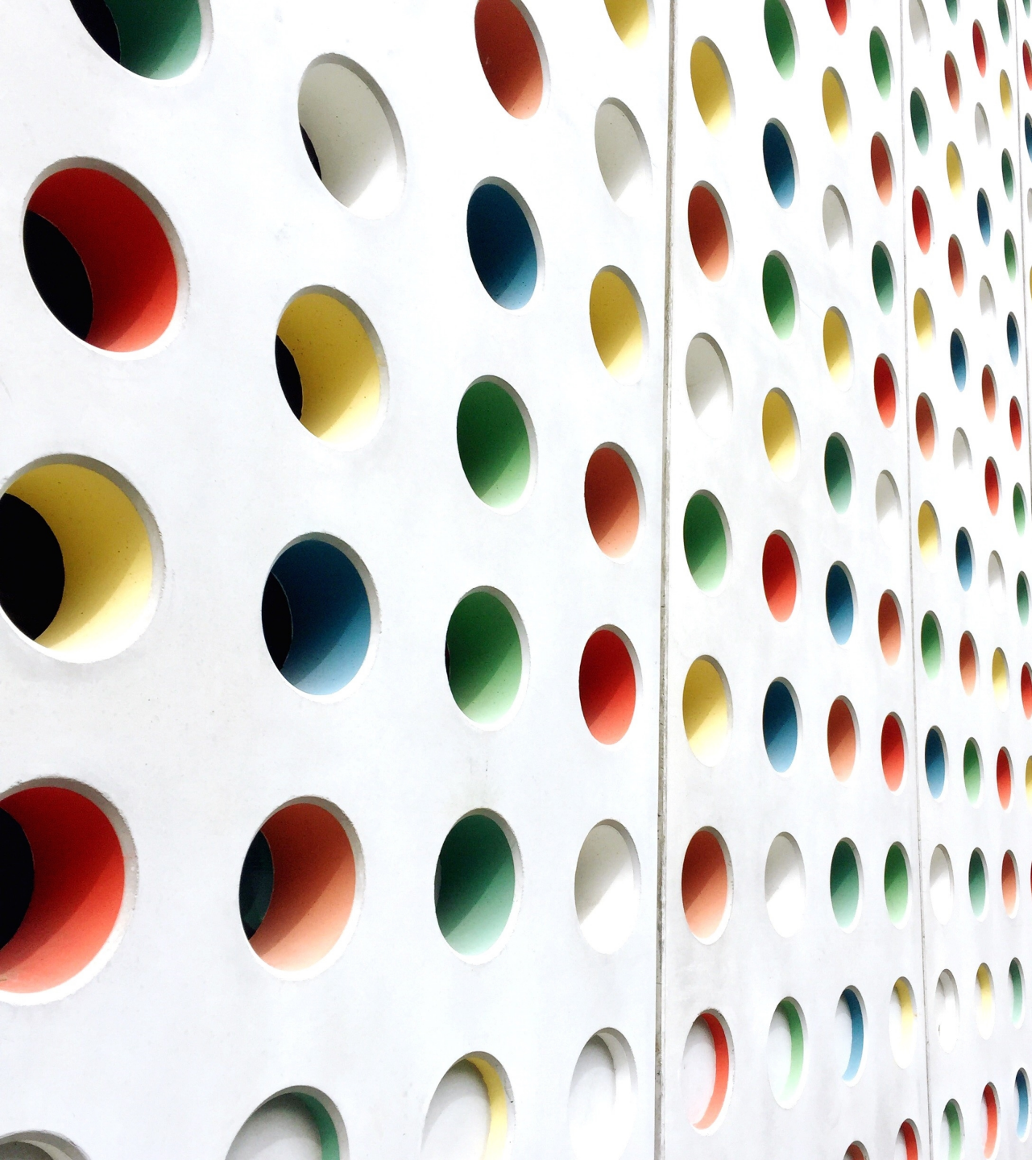


Responsible IoT Design

MS.T.KAVITHA

ASSISTANT PROFESSOR

CSE, KITS

Agenda

- The challenges of securing the Internet of Things
- The challenges of protecting users' privacy
- The risk that designing technology involves social engineering
- The environmental impact of IoT

This chapter addresses the following issues:

- Why embedded devices are especially at risk from network security threats •
- What design requirements for usable IoT security might look like •
- How data that seems innocuous can be aggregated to create a privacy breach
- What good data protection for IoT might look like
- How technology that tries to be “smart” can end up reinforcing social stereotypes
- Understanding the environmental impact of a connected device across its entire lifecycle

Security

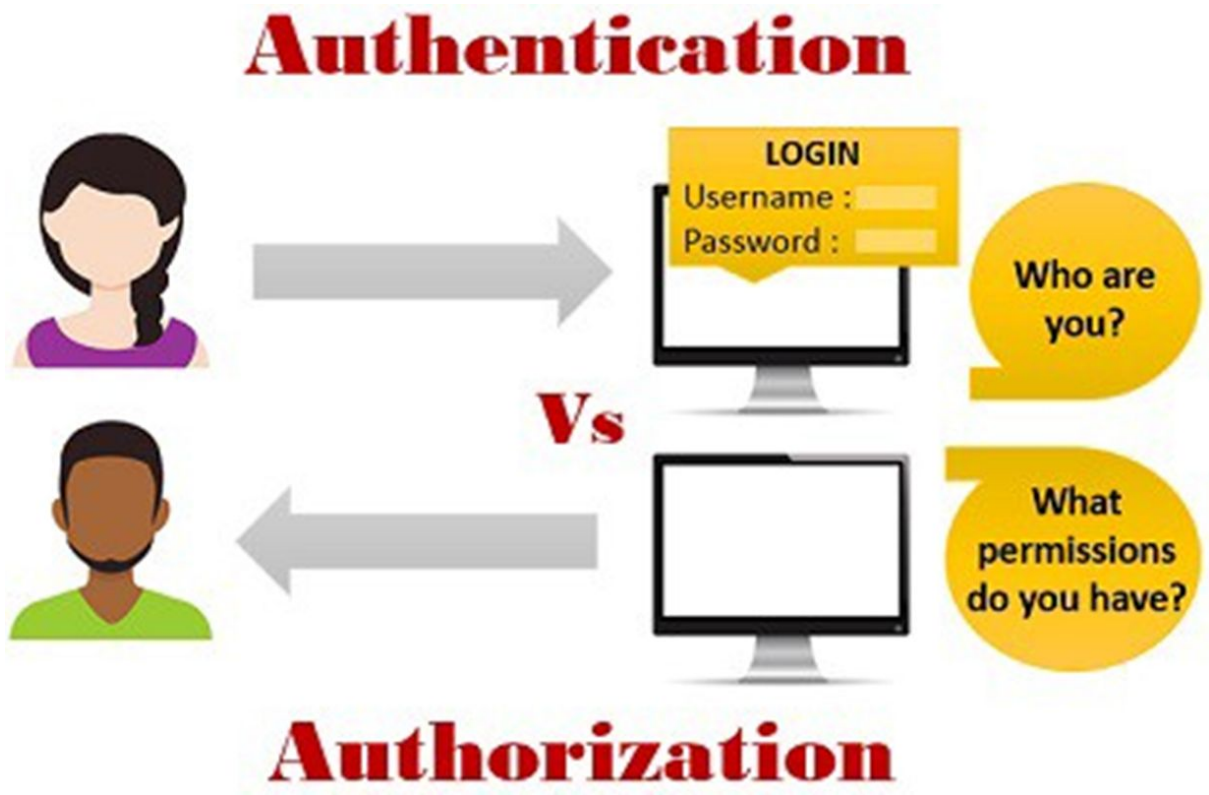
Computer security is the degree to which a system can protect the assets it contains from unauthorized access, modification, or destruction.

The “CIA triad” is a commonly used model of IT security, which defines three important aspects:

"CIA triad"

- **Confidentiality** Protecting information from unauthorized access—for example, through eavesdropping or spoofing (masquerading as a legitimate user). (This is related to privacy, which we'll discuss later.). Confidentiality ensures that only those individuals with the proper authority can access sensitive data.
- **Integrity** Protecting information from being modified or deleted by unauthorized parties (e.g., tampering with data or introducing viruses). Integrity ensures that data can only be changed by authorized individuals so that the accuracy, consistency, and trustworthiness of data are guaranteed.
- **Availability** Protecting the system from threats that would stop it working properly, resulting in loss of access to resources (e.g., loss of power, hardware failure, or a denial of service attack). Availability ensures that the data can be accessed when and where needed, including during times of both normal and disaster recovery.

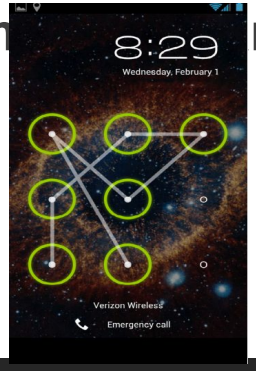
Authentication and Authorization

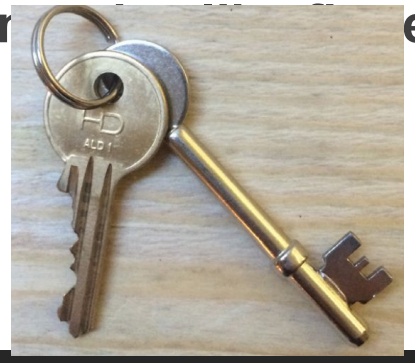


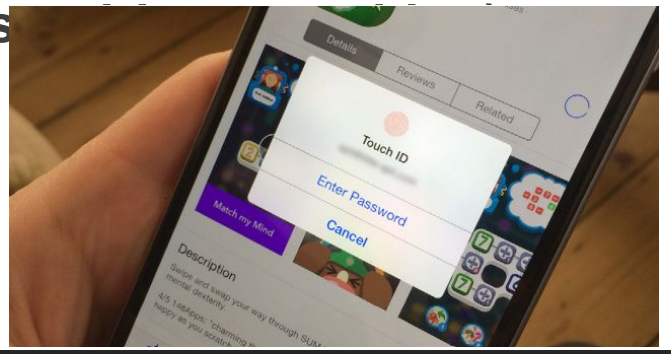
Authentication

The most important defense mechanism for a system that interacts with humans is generally authentication. This means ensuring that the system and user can be confident of each other's identity. This is often done through a shared secret. Shared secrets are often characterized as:

- **Something I know (e.g., text or graphical password)**
- **Something I have (e.g., smartcard or physical key)**
- **Som m (e.g., bior erprints**







Authorization

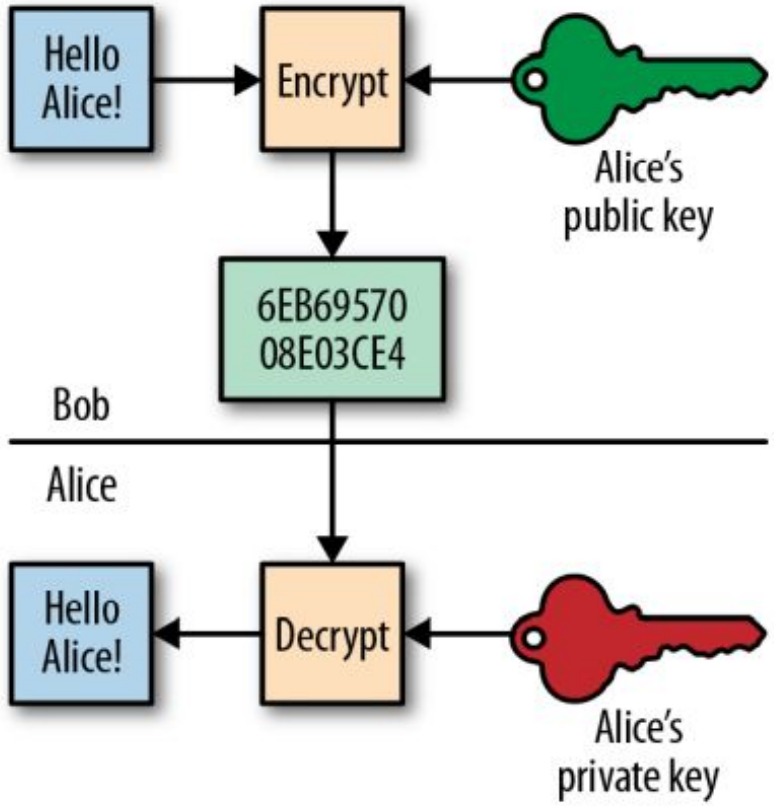
Following on from authentication is authorization. A user (or another system) may be permitted to access certain data or functionality on the system, but not others.

Encryption

Encryption disguises information to keep it secret, on devices, servers, or in transit over the network. Network security methods often aim to verify that information has not been observed or modified in transit ("man in the middle" attacks).

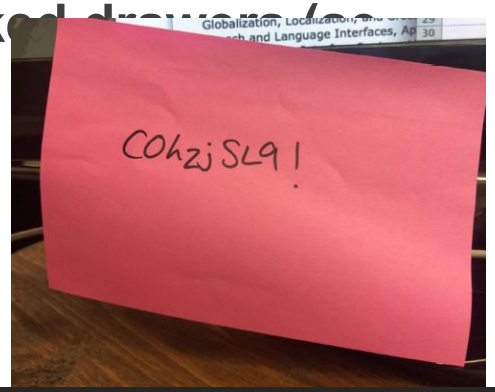
Each party has a public software key, which is published, and an associated private key known only to them. To ensure confidentiality, the sender encrypts the message using the recipient's public key. It can only be decrypted by the recipient, using their private key.

Diagram of public key encryption



THE UX OF SECURITY

- Usability seeks to make it easy for people to do things. Security measures often make it harder to do things.
- One of the big challenges in security is getting people to use it correctly. Security measures are often complex, often designed with highly trained users in mind.
- For example, truly random passwords are harder to break. But they are unmemorable to users, who write them down on notes stuck to computer monitors, or left in unlocked drawers/pa



WHY IOT SECURITY IS A BIG CHALLENGE?

Connecting up the physical world creates the potential for malicious hacking to have "real world" consequences.

- **In 2013, malicious hackers accessed a video baby monitor and verbally abused the child over the loudspeaker.**
- **A security breach could easily put lives in danger.**
- **Cars could be remotely hijacked to disable the brakes.**
- **Pacemakers could be compromised to kill cardiac patients.**

WHY IOT SECURITY IS A BIG CHALLENGE?

Devices with no UI, or very limited UIs, may be unable to tell us when they have been compromised. Eg.: A recent botnet attack co-opted 100,000 devices including WiFi routers, connected TVs, and at least one connected fridge into sending out hundreds of thousands of spam emails.

DESIGN REQUIREMENTS FOR USABLE IoT SECURITY

- **Building devices with more robust security models and securing network transmissions will solve some of these issues. But as far as the user's concerned, these improvements aren't visible in the system UX.**
- **<u>The most secure approach is not to connect a device to anything at all.</u> There's a lot to be said for not connecting things (either to each other or the Internet) without a strong case for doing so. But it would be a shame for IoT to be unnecessarily limited in this way.**

1. Limit the damage that can be caused

- **Limiting devices to a *very specific set of functionality* will help prevent them being roped into unintended activities.**
- **For example, a WiFi connected oven could be co-opted into sending spam email, sniffing the home WiFi network for sensitive details like bank account details, or compromising its functionality to endanger the user or environment (e.g., turning on the gas to cause a leak). It is safest to build it in such a way that it cannot support some of these behaviors.**

2.Keep devices secure

- **Security software needs to be kept up to date, ideally with as little user intervention as possible. This can be complicated to deliver when there are multiple business partners involved in supporting a system.**
- **For example, most current Android smartphones run out-of-date software and often have security vulnerabilities. *Google provides software updates to fix these issues* but they are not packaged up and pushed to consumers by the carriers or handset manufacturers.**

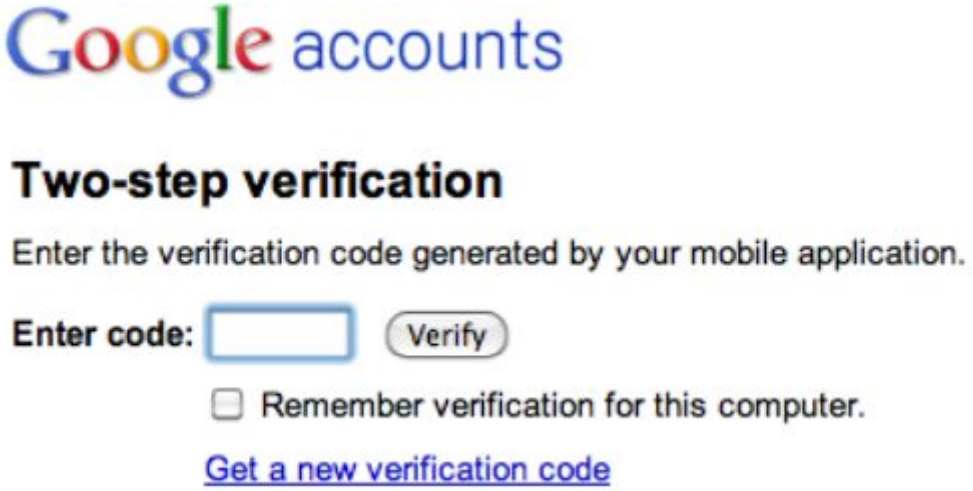
3.Make authentication easier

- **Users may need to authenticate themselves to devices and services. Devices and web services may also need to identify themselves to other devices and web services. User authentication often involves passwords *("something I know")*, but entering passwords to interact with many different devices would be onerous.**
- **In some cases, possession of a phone or smartcard *("something I have")* may be enough (e.g., my phone can control my home lights because it is my phone). But devices can fall into the wrong hands. Phones, keys, and smartcards can be stolen, copied, or cloned.**
- **Biometrics, a form of *"something I am"* (e.g., the iPhone's fingerprint recognition, iris recognition, or even heart rate or gait analysis), can be low-friction methods of user authentication.**
- **But they are not always reliable and can increase the personal risk to users. In 2005, a violent gang of carjackers in Malaysia chopped off a victim's finger to get around the car's fingerprint recognition system**

EXAMPLE

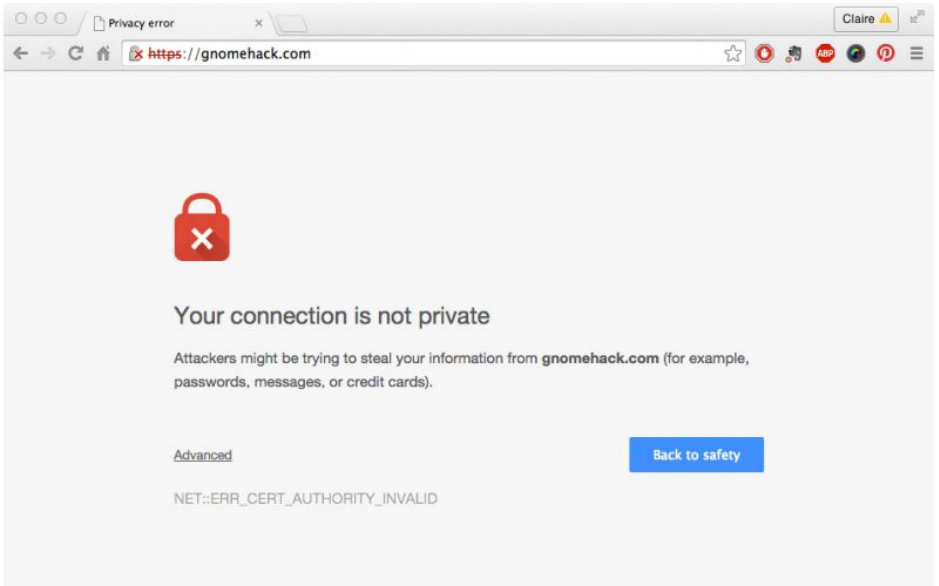
(e.g., Google's two factor authentication) is extra secure, but more hassle.

Google's two factor authentication requires the user to use a password and a one-time code sent to their mobile via SMS



EXAMPLE

If your browser cannot find a certificate proving that the website claiming to be mail.google.com really is mail. google.com, it will flag it up as a security risk. But users often simply click past such warnings.



4.Keep users in control of permissions

- **Authenticating devices is one step, but users also have to be in control of how much those devices can do or what they can share.**
- **Authentication and authorization can to some extent be automated and happen without user interaction. But this *doesn't work if the user needs to determine what level of security is appropriate or how to use information appropriately.***

s.Make the invisible visible

- Devices with limited UIs can't always tell us when they have been compromised. Is your dishwasher trying to tell you it's been co-opted into a botnet or does it just need more rinse aid? Ways of making these invisible threats visible are needed, which requires both a way of detecting. and informing the user of these threats.
- For example, software agents might monitor system activity and inform the user about potential security threats and available countermeasures.

Design security measures to suit user and domain needs

- Security measures must be appropriate to user needs. There is no point requiring consumers to do something they are not capable of. Although not an IoT example, the One Laptop Per Child security principles are an interesting example here.
- These establish that the security measures on the computer must be suitable for users who cannot yet read, or choose and remember a password.
- Different domains (e.g., healthcare, banking, and home) may have unique requirements. The nature of the system and data, the context in which they are used, and the consequences of them being compromised may be different in each case.

Privacy

- If security is a network issue, privacy is a networked data issue. It is about collecting information about other people, and making it available, as opposed to the simple exploitation of weaknesses in the system.
- Privacy issues are less predictable than security issues, as what counts as privacy is neither universally agreed, nor static.
- Understanding the scope of privacy concerns helps in designing a system. It is possible to mitigate some of them, alert people where necessary, and generally choose options that make the flow of data more manageable. It is also worth noting that in some parts of the world, privacy legislation affects what it is possible to d

INFORMATION AND PRIVACY

- One important part of privacy is about controlling information: what is released and who sees what.
- The services in and out of homes, cars, and health devices carry enough information to embarrass and compromise their users repeatedly. It is possible to make many accurate— and inaccurate—inferences about what each user or group of users is doing and why.

Two types of privacy breach to consider.

- First, there are streams of information leaving connected devices for other destinations related to the service provider or made accessible on the journey. These streams may pass through the hands of hackers, advertisers, partner services and companies, other third parties, the NSA, and so on. We will return to these later.
- Second, there are the privacy breaches that the service commits locally among users sharing the same resources or space. As more data are stored, so there is more chance of revealing socially inappropriate details to other local users or doing something that makes them feel nervous. We might call these breaches tactless sharing.

Handling data with tact

The recent backlash against Google Glass has been tied to the insensitive handling of privacy in its design (among other things). Phone calls with a picture feed took more than 40 years to find their way into popular usage, partly because they threatened to give away too much about the person being phoned.

Google Glass can disconcert those on the other side of the camera

Collecting and distributing data

- As the designer of a connected product, some information will be necessary to you to provide a good service.
- The more that tools and products are expected to infer users' wishes from their behavior, the more information you will need to manipulate. Some of that information may also have to be given to third parties so that multiple services can interoperate.

Aggregation

One of the hardest things for people to understand is the way that innocuous information can be combined to give insight into beliefs, behavior, and choices. Connected product systems can use multiple data sources to make inferences about the world, especially where things are supposed to respond to context, hierarchies of user permissions, and contradictory inputs

Patterns of behaviour

- Privacy is mostly about information, though patterns of information flow are also relevant because these give access to patterns of behavior.
- A crude example would be turning off most of your network when you leave to go on holiday. Even the dip in energy consumption that your smart meter is picking up tells the story. That dip gives as much information as leaving a note for the milkman saying you don't need milk for the next week, as people used to do in more trusting times. It puts your home at risk by indicating you are absent, which is a security matter, but, taken over the year, it also reveals that you go away, when and for how long, how regularly you go, and so on.

LEGAL ISSUES, CONSENT, AND DATA PROTECTION

- Different parts of the world take different attitudes to this data management responsibility.
- In the United States, there is no single, comprehensive national law regulating the collection and use of personal data. There is piecemeal legislation, and security breaches in recent years have led to the field of privacy becoming one of the fastest growing areas of legal regulation.
- By contrast, Europe has long had a centralized approach to data protection. At the time of writing, a new regulation is being introduced into the European Union (EU) that will supersede the current Data Protection Directive, active since 1995. In Europe, privacy is a human right and data protection is upheld more stringently than in much of the world.

Principles of data management for privacy

The OECD, in 1980, produced seven principles that underpin the EU system. The OECD principles are:

Notice: Data subjects should be given notice when their data is being collected

Purpose: Data should only be used for the purpose stated and not for any other purposes

Consent: Data should not be disclosed without the data subject's consent

Security: Collected data should be kept secure from any potential abuses

Disclosure: Data subjects should be informed as to who is collecting their data

Access: Data subjects should be allowed to access their data and make corrections to any inaccurate data

Accountability: Data subjects should have a way to hold data collectors accountable for not following these principles

Privacy settings and informed consent

- There is no legal breach of privacy if consent for the use of the information in the way that it is being used has been given.
- At the time, control still seemed plausible. Ethically, it is now debateable whether people are capable of giving informed consent in many of the cases we discuss here, as we have shown how hard it is to understand possible uses of data.

"PRIVACY BY DESIGN AND PRIVACY BY DEFAULT"

- One way of overcoming the problem of consent and data privacy is to store all data in the local system, where it belongs to the user, and only take the minimum of processed and anonymized information back into the service to provide necessary functionality.
- "The Struggle for the Internet of Things" relates how centralized IoT information could become if the big five super-companies he identifies start to manage every interaction users have with all their devices.
- If this is the future of the Internet of Things, then mass surveillance is a critical part of the plan. But even monetizing every interaction (as they may hope to do) does not require that precise knowledge of who is doing what is centrally stored and mined for individuals' details, even while it is being analyzed for trends, relationships, and patterns.

Social Engineering

In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.

“Social engineering scams are based on how people think and act.”

Examples of Social Engineering Attack Scenarios

Savvy cyber criminals know that social engineering works best when focusing on human emotion and risk. Taking advantage of human emotion is much easier than hacking a network or looking for security vulnerabilities.

The following are some familiar notes successful social engineering attacks hit again and again.

Fear
You receive a voicemail saying you're under investigation for tax fraud and must call immediately to prevent arrest and criminal investigation. This social engineering attack happens during tax season when people are already stressed about their taxes. Cyber criminals prey on the stress and anxiety of filing taxes and use these fear emotions to trick people into complying with the voicemail.

Examples of Social Engineering Attack Scenarios

Greed
Imagine if you could transfer $10 to an investor and see this grow into $10,000 without any effort on your behalf. Cyber criminals use the basic human emotions of trust and greed to convince victims that they really can get something for nothing. A carefully worded baiting email tells victims to provide their bank account information, and the funds will be transferred the same day.

Curiosity
Cyber criminals pay attention to events capturing a lot of news coverage and then take advantage of human curiosity to trick social engineering victims into acting. For example, after the second Boeing MAX8 plane crash, cyber criminals sent emails with attachments that claimed to include leaked data about the crash. The attachment installed a version of the Hworm RAT on the victim's computer.

Examples of Social Engineering Attack Scenarios

Helpfulness
Humans want to trust and help one another. After researching a company, cyber criminals target two or three employees with an email that looks like it comes from the targeted individuals' manager. The email asks them to send the manager the password for the accounting database – stressing that the manager needs it to ensure everyone gets paid on time. The email tone is urgent, tricking the victims into believing they are helping their manager by acting quickly.

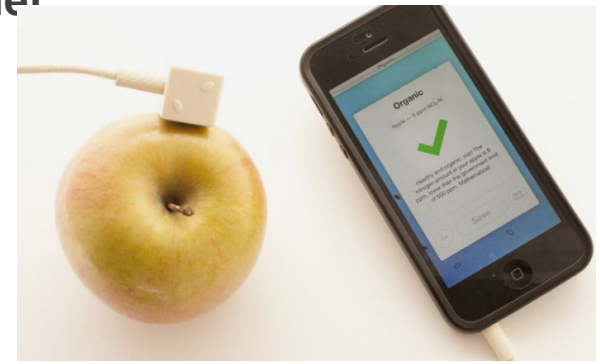
Urgency
You receive an email from customer support at an online shopping website that you frequently buy from, telling you they need to confirm your credit card information to protect your account. The email language urges you to respond quickly to ensure that criminals don't steal your credit card information. Without thinking twice, you send the information, which results in the recipient using your details to make thousands of dollars of fraudulent purchases.

Mitigating the dangers of social engineering?

- Implementing security awareness training that changes behavior and reduces risk is an increasingly important part of many organizational cultural and cyber security metrics.
- One way of avoiding the worst of these scenarios is to use methods that mean you design with your users as well as for them, listening to them and mitigating their concerns.
- The long-term trajectory for connected products is one that impacts on the local control of ordinary people, and eventually, on identity and self-determination.

Environment

Sensors monitoring air and water quality and radiation can help us better understand our impact on the planet



The Lapka organic matter sensor detects levels of nitrates in fruit and vegetables

But it's hard to understand what the true positive or negative environmental impact may be of the systems we create.

In this section, we look at factors that may affect the impact of IoT systems, and what designers' responsibilities may be.

WHAT'S THE ENVIRONMENTAL IMPACT OF AN IOT PRODUCT?

Ethically, we should ask ourselves how our systems may be doing both good and harm. Standards and certification bodies provide limited information and legal controls on some aspects of products. But assessing this accurately requires us to look at the environmental impact of a product over its entire lifetime. For that, no complete picture is available.

1. Manufacturing

- **The first impact of manufacturing is in resources. Electronic devices tend to contain more precious and rare earth metals (e.g., copper, gold, palladium, and platinum). These are valuable resources yet often lost when old products are not recycled (only 1% of cellphones in the United.**
- ***Mining them consumes a considerable amount of energy and has environmental consequences.* For example, radioactive waste *(thorium)* is a by-product of rare earth metal mining. In some cases, such as tantalum (mined from coltan and used in capacitors), ethical questions have been raised about the corporate responsibility of the mining companies. Tantalum is even classified as a conflict resource due to links between coltan smuggling and warfare in the Democratic Republic of Congo.**

2.Usage

During usage, the device should make efficient use of energy (for many embedded devices that *run on batteries*, this is not just an environmental concern but essential to the normal functioning of the system). Energy Star, a program of the US Environmental Protection Agency, sets globally used standards for energy efficiency in consumer product specifications.

3. Maintenance and upgradeability

- In theory, providing a device with Internet connectivity ought to extend its lifespan. It should be relatively easy to deliver software or firmware updates that improve the device's functionality and performance and keep it in service for longer.
- You could even charge for software updates in lieu of new hardware. However, in practice, increases in functionality tend to make ever-increasing demands on hardware, which is usually manufactured to a tight budget and may not have the additional processing power, memory, or UI capabilities to handle very many future upgrades.
- At some point, ***the old devices may no longer be powerful enough to support the latest and greatest software.*** It can also become uneconomic for manufacturers or service providers to continue to support software updates and security patches to a large number of older versions of devices out in the field

Disposal

- Finally, there is disposal: retiring devices at the end of their lives. This creates waste, some of which is highly toxic.
- Electronic waste represents 2% of America's waste in landfills, but is responsible for 70% the heavy metals in that waste. 39 Chemicals from landfill leach into the groundwater. Very few PCs and smartphones are currently recycled.
- According to the US Environmental Protection Agency, fewer than 10% of the 141 million mobile phones discarded in the United States in 2009 were recycled.

Disposal

In the European Union, the Waste Electrical and Electronic Equipment Directive (WEEE) mandates that it is the responsibility of the producer or distributor to make provision for the collection and recycling of electronic equipment placed on the market after 2005

E-waste waiting for recycling at a specialist processing facility in Kent, UK

WHAT CAN DESIGNERS DO?

- IoT products may offer the promise of reduced energy consumption, better understanding of the world, and more efficient use of resources. But if we approach creating connected products the way we've approached everything else, we're at risk of accelerating the destruction of our environment through burning resources making disposable junk. We need to reduce the impact of the systems we create and not add to the damage.
- We can choose responsible hosting companies who try to conserve energy and inves wer. We can design for upgradeability and longevity throu s

The Fairphone smartphone uses conflict-free minerals and is designed for repairability and upgradeability