DOI:10.1145/2398356.2398377

**A framework for evaluating security risks associated with technologies used at home.**

BY TAMARA DENNING, TADAYOSHI KOHNO, AND HENRY M. LEVY

# Computer Security and the Modern Home

COMPUTATION IS EMBEDDED throughout our homes. Some devices are obvious: desktops, laptops, wireless routers, televisions, and gaming consoles. Increasingly, however, computational capabilities are appearing in our appliances, healthcare devices, children's toys, and the home's infrastructure. These devices are incorporating new sensors, actuators, and network capabilities: a Barbie with a video camera[1]; a lock for your front door controlled by your cell phone; or a bathroom scale that reports readings over your wireless network.[26] Many of these devices are also subject to control by servers external to the home, or are mobile technologies that regularly leave the home's perimeter and interact with other networks. These trends, which we expect to accelerate in the coming years, create emergent threats to people's possessions, well-being, and privacy. We seek to survey the security and privacy landscape for devices in the home and provide a strategy for reasoning about their relative computer security needs.

Many human assets—whether electronic, physical, or nontangible items of value to end users—can be accessed or influenced from computing devices within the home; unsurprisingly, these assets are also potentially attractive targets to adversaries. The capabilities of new electronics and their presence in

## » key insights

- **Homes are becoming increasingly computerized, filled with devices ranging from the traditional (laptops and desktops) to TVs, toys, appliances, and home automation systems.**
- **We survey potential computer security attacks against in-home technologies and their impact on residents; some of the attacks are familiar, but the new capabilities of home technologies enable novel attacks and allow some traditional attacks to have new consequences.**
- **We present a framework for articulating key risks associated with particular devices in the home, which includes identifying human assets, security goals, and device features that may increase the risk posed by individual technologies.**

PHOTOGRAPH FROM GETTY IMAGES/PANORAMIC IMAGES

the home facilitate traditional crimes and allow new classes of attacks. Technically savvy burglars, for example, may use technology both to identify houses with expensive, easily resold items and to better plan and execute their crimes. Adversaries can also target technologies with a wide range of new capabilities, with the goal of accessing video and audio feeds,[25] unlocking doors or disabling home security,[27] tampering with home healthcare devices,[13,26] or interfering with home appliances and utilities.[22,24]

Fortunately, there have been few "high tech" crimes to date exploiting these new capabilities. Now is the right time to develop a foundation for securing the myriad devices within the home: before these technologies become more ubiquitous, communicative, and capable, and before real adversarial pressures emerge. While progress has been made in understanding security concerns for specific home technologies or categories of technologies,[3,14] there is currently a lack of unified vision for evaluating security threats posed by the assortment of consumer devices within the home. There are trade-offs in the design of any security system, but without a cohesive strategy for reasoning about home device security, product manufacturers will be left to determine the appropriate trade-offs for themselves without best-practice references.

Our goal is first to survey the landscape of potential attacks, then to provide structure and guidance for reasoning about the differing security needs of home technologies. While many of these elements will be familiar from security for traditional computers, their implications are worth reassessing in the context of the home ecosystem. This article is also complementary to an existing body of research on security for home technologies, including work on the security needs and behaviors of users[4,8,10,18,19] and work on centralized security technology solutions.[28]

Table 1 presents an overview of the topics covered by this article. We begin by presenting an overview of how the ecosystem of home technologies can enable a range of attacks with electronic and physical consequences. Building on this discussion, we present the two key components of our strategy for evaluating the potential risks with home technologies: a taxonomy of security goals for home technologies; and a set of device characteristics that can be used to estimate a device's potential risk to users. We apply our approach to three home technologies: a webcam toy, a networked scale, and a home automation device. Our framework is not intended to be definitive, but rather informative: our intent is that this approach will provide a useful starting point for home technology stakeholders ranging from product manufacturers to consumer advocacy groups to the research community. Moreover, by focusing on the entire home technology ecosystem, our hope is that this work will strengthen the foundations for developing secure home technologies—with the ultimate goal of creating a trustworthy home environment for users.

## The Big Picture: Challenges and Attacks

The home technology space is interesting and unique from other domains. In a nutshell, the new home landscape takes four challenges—challenges that are not unique in and of themselves—and combines them to create a new problem space: (1) an extremely personal, asset-filled environment where there is (2) no dedicated, professional administrator to maintain a (3) heterogeneous collection of consumer technologies that (4) are increasingly cyber-physical and sensor-rich. The combination of these factors leads to an array of attacks and complicates the design of defenses for home devices. From a technical perspective,

**Table 1. An overview of topics discussed in this article.**

| Infection Pathways | Human Assets | Defensive Goals | Device Risk Axes |
|---|---|---|---|
| Physical | The Biosphere | Device Privacy | Potential Exposure to Attack |
| In-person | Emotional Well-being | Device Availability | Communication Capabilites |
| Secondhand via Infected Device | Financial Well-being | Device Operability | Communication Behavior |
| Found | Personal Data | Command Authenticity | The Cloud |
| Gift | Physical Well-being | Execution Integrity | Software Updates |
| Infected from Manufacture | Relationships | Data Privacy | Configuration Defaults, User Interfaces, and Users |
| Lent | Societal Well-being | Data Integrity | Attractiveness as a Target |
| Returned | | Data Availability | Technology Market Share |
| Used | | Environment Integrity | Intended Users and Usage |
| Technological | | Activity Pattern Privacy | Sensors |
| Remote or In-Network | | Presence Privacy | Actuators |
| Direct Compromise | | Occupant Identities | Power |
| Eavesdropping | | Sensed Data Privacy | Connectedness |
| Man-in-the-Middle | | Sensor Validity | Storage and Computation |
| Social Engineering | | Sensor Availability | |

the home is filled with a diverse range of technologies with varying levels of security, hybrid communication structures, and no centralized security management system. From a human perspective, the home contains private and semi-private spaces shared by children, parents, siblings, elderly, roommates, and guests. Interpersonal dynamics, varying levels of security expertise, and different social and technical preferences all contribute to complicating the home technology security landscape. In order to effectively create and evaluate defenses, it is important to first understand the threat landscape.

**Attack Scenarios.** One unique aspect of the new home technology space is the vast array of attacks that it enables—many of which differ in effect from Web or desktop attacks. The increasing presence of electronics in the home—controlling our houses and coordinating our lives—provides unique opportunities for the technically savvy criminal.

Table 2 breaks down attacks into three tiers: low-level mechanisms, intermediate goals, and high-level goals. The low-level mechanisms listed in Table 1—such as denial-of-service attacks, tampering with logs, or eavesdropping on network traffic—will be familiar to anyone who has experience with computer security. However, the additional focus on sensors and actuators is something that is not generally encountered with traditional computing devices. Similarly, the high-level goals behind the attacks (blackmail, extortion, theft, and vandalism, among others) are the same motivations that one encounters with all criminal activities. Arguably, the most novel aspects of attacks on the home ecosystem are the intermediate goals: the ways in which the unique capabilities of devices or the assets to which they have access enable criminal opportunities.

In order to highlight some of the unique properties of the home ecosystem, we list examples of attacks that are not viable with traditional computing platforms:

- Determining the locations of lucrative home burglary targets via camera feeds or the distinctive signatures of multiple, expensive devices;
- Providing access to homes that have cyber-physical locks that are vulnerable to electronic compromise;
- Checking whether or not a home is occupied (and by whom) via: cameras; microphones; motion sensors; logs for lights, thermostats, and door locks; or HVAC air pressure sensors;[23]
- Turning up the thermostat settings while the user is away in order to increase heating bills, thereby causing financial harm;
- Electronically manipulating a washing machine to cause flooding;
- Tampering with home healthcare technologies in order to change treatment, notifications, or perform a denial-of-service attack; and
- Targeting entire communities by coordinating their devices to overload the power grid.

*Attack targets.* For many types of attacks, an adversary could either attempt to target a particular person of interest or simply take advantage of known hardware and software flaws to indiscriminately attack any vulnerable victim. Attacks on a designated person require that the adversary identify useful exploits for the target's particular technology configuration. On the other hand, for attacks on "low-hanging" targets—attacks of exploitative opportunity—the adversary need only focus on a known exploit and locate victims who are vulnerable to that exploit.

*The physical and the electronic.* At a high level, it is interesting that the presence of actuators and sensors in the new home environment allows interactions between the physical and electronic states of devices. It is possible to perform electronic attacks with physical consequences, but it is also possible to perform physical attacks with electronic consequences, or attacks that have both physical and electronic components. As an example of a physical attack that has electronic (then physical) consequences, an adversary might apply a bright, directed light source to an external light sensor in order to trick outdoor flood lighting into turning off. Similarly, one can imagine an attack where physically tricking a system sensor causes the system to enter a fail-safe mode that is more easily compromised via electronic attack.

**Infection Pathways.** The challenges of the home environment—such as its

heterogeneous topology and the idiosyncrasies of its occupants—help enable novel or complex infection pathways. Mobile devices, infrastructure electronics, cyber-physical systems, guest devices, and machines brought home from work all commingle in one hodgepodge environment, increasing the exposure to compromise. Understanding the potential infection pathways—particularly nontraditional pathways—that malware might follow to compromise a device helps us understand its exposure to risk, which we use later in our characterization of device risk. The Infection Pathways column of Table 1 provides an overview of the kinds of pathways that malware can take to infect a device in the home.

*Entry points.* There are a number of entry points an adversary could use to attack home technologies. Electronically, a device on the home network might be compromised by a direct attack from a device external to the home, or compromised by an infected device within the home (whether stationary, mobile, or belonging to a guest). If a device is mobile and connects to an infected network, it might become infected. Physically, a device might be infected by a manual interface such as USB or CD.[5,9] Alternative physical attack vectors include: receiving an infected device as a gift; purchasing a used, compromised device from a source such as eBay or Craigslist; purchasing a "new" device that has previously been purchased, infected, then returned; or purchasing a device that was infected during its manufacture.[11] Additionally, an adversary has a number of opportunities to socially engineer a user into installing malware, such as via app stores.[15,21] As another vector, an adversary could take advantage of the increasing number of "prosumers"—consumers who jailbreak their devices or perform similar automated modifications—whose devices allow behaviors that go beyond the capabilities expected by the manufacturer's typical APIs and might not receive security software updates.

*Stepping back.* As this survey of the attack scenarios and infection pathways shows, the risks with computer security vulnerabilities in home technologies are quite varied and, in some cases, significant. Here, we present a framework for more methodically identifying and prioritizing the security risks within the home.

## Human Assets and Security Goals

To design a system for defending home technologies, it is necessary to understand the human assets that are at stake and the desired security goals. We present a casual taxonomy of goals for protecting human assets in the home (also shown in the Defensive Goals column in Table 1). The general goals of confidentiality, integrity, authenticity, and availability are familiar security concepts; we frame the goals for defending the home slightly differently in order to highlight the domain in which they are applied and the unusual consequences of security failures. This taxonomy is meant to approach security and privacy goals from a variety of perspectives, and as such items are not mutually exclusive.

Security failures can result in a variety of kinds of harm to users. It is common to consider harm to users in terms of financial assets; it is less typical to consider damaging users by, for example, wasting their time or causing them stress. We suggest considering the potential negative impact of attacks on the following assets (in the Human Assets column in Table 1): emotional well-being, financial well-being, personal data, physical well-being, and relationships. In addition to considering the assets of individuals, it can be beneficial to consider the broader assets of societal well-being and impact on the biosphere. The list is derived in part from Value Sensitive Design[12]—an area of human-computer interaction that focuses on what different individuals value—and in part from the discussion sections of papers on emerging technologies.[5,7,16]

**Device Goals.** These are security goals that pertain to the operation of traditional or embedded computing devices.

1. *Device privacy.* A device should avoid broadcasting or otherwise disclosing its presence (for example, a wireless electronic adult toy, a device to treat a stigmatized medical condition, or an expensive device that is attractive to thieves). Example harms include: emotional harm from shame or embarrassment; or financial or physical harm if a physical break-in occurs.

2. *Device availability.* A device should not suffer malicious service interruptions. In many cases, device unavailability might only cause irritation and result in wasted time; however, consequences can range from financial (for example, the user cannot perform some time-critical transaction) to physical (if the user is unable to properly use a medical device or if a non-functioning refrigerator spoils food).

▸ *Device operability.* A device should have protection against operating in a manner that could damage or destroy itself since the device is an investment of time and money.

3. *Command authenticity.* A device should only accept and send authentic commands that reflect the user's inten-

**Table 2. An overview of the structure of attacks to the home ecosystem.**

| | Examples | |
|---|---|---|
| **Low-level Mechanism** | Altering logs | Viewing data |
| | Altering or destroying data | Viewing or altering traffic |
| | DoS attacks | Viewing sensors |
| | Using actuators | |
| **Intermediate Goals** | Accessing financial data | Gathering incriminating data |
| | Causing device damage | Misinformation |
| | Causing environment damage | Planting fake evidence |
| | Causing physical harm | Viewing private data |
| | Enabling physical entry | |
| **High-level Goals** | Blackmail | Physical Theft |
| | Espionage | Resource Theft |
| | Exposure | Stalking |
| | Extortion | Terrorism |
| | Framing | Vandalism |
| | Fraud | Voyeurism |
| | Kidnapping | |

tion. This applies both to commands that elicit immediate reactions and commands that elicit delayed reactions (for example, turn on the sprinklers at 10 A.M.).

4. *Execution integrity.* A device should not deviate from its intended operating specification. More specifically, security vulnerabilities should not allow unintended behaviors that violate other security goals.

**Digital Data Goals.** These are security goals that pertain to a user's digital data.

1. *Data privacy.* Defenses should protect the confidentiality of the user's data (for example, leaked data could result in embarrassment, loss of reputation, financial damage, or legal repercussions due to possession of information or evidence of activities incompatible with local laws).

2. *Data integrity.* Defenses should ensure that the user's data is not corrupted. Non-critical data can be an inconvenience if lost (such as minor corruption of address book), but critical or irreplaceable data can present major emotional or logistical challenges (such as losing photos of deceased family members). Alternatively, undetected, intentional changes to data or the addition of new data could have legal (for example, illicit materials), financial (for example, inaccurate tax paperwork), emotional (for example, SMSs or email messages being sent to unintended recipients), or physical (such as inaccurate medical logs) consequences.

3. *Data availability.* Defenses should ensure the user's data does not suffer from malicious access interruptions.

**Environment Goals.** We must also consider security goals that pertain to the home infrastructure and general environmental conditions.

1. *Environment integrity.* Defenses should protect against single or multiple cyber-physical devices accepting commands that maliciously change the home environment—particularly if those changes might harm the home or its occupants (for example, lowering the thermostat could result in poor sleep, increased susceptibility to illness, or damage to water pipes).

2. *Activity pattern privacy.* Defenses should protect against accidentally revealing information about the activities of home occupants. Such disclosure could be the direct result of one data source, or inference and cross-referencing from multiple sensors. Activity patterns could reveal information that is embarrassing (for example, intimate habits) or informative to a miscreant (for example, whether or not occupants are asleep). We consider two special cases:

▸ *Presence privacy.* Defenses should protect against accidentally revealing whether or not the home is occupied, as this can facilitate physical attacks on the home and enable cyber-physical attacks that might otherwise be detected and interrupted.

▸ *Occupant identities.* Defenses should protect against accidentally revealing the identities and number of occupants, thereby supporting freedom and privacy of association. As an example of privileged information, one may not wish to reveal that a young child is home alone.

3. *Sensed data privacy.* Defenses should protect against confidentiality leaks of sensor data (such as audio or video feeds) of shared and private home spaces.

4. *Sensor validity.* The readings from environmental sensors should be valid and immune to technical tampering. Sensor readings generally remain susceptible to tampering in the analog channel. Altered sensors might cause financial harm (for example, inaccurate power metering) and/or physical harm (for example, disabled home intrusion sensor facilitating a break-in). Alternatively, a miscreant who is unable to alter the function of a home system directly might instead tamper with sensor readings in an effort to alter the actions of the actuator in a feedback loop. In some scenarios, homeowners themselves may be considered the adversary (such as tampering with power meter readings to reduce billing[17] altering medical sensor readings for health insurance fraud).

5. *Sensor availability.* Sensor readings should be available without interruption according to their regular schedule. For example, the failure of a sensor can lead to physical harm or damage (such as the burglar alarm, the smoke detector, the temperature sensor in refrigerator).

Having explored human assets and security goals, we now explore a strategy for evaluating the potential risks with home technologies.

**If a device is mobile, then the chances are higher that it will come into contact with malicious or infected networks or devices.**

## Evaluating Potential Risks

The risk posed by a given home tech-

nology can be broken down into three components: the feasibility of an attack on the system; the attractiveness of the system as a compromised platform; and the damage caused by executing a successful attack. The first two factors, when combined, provide some indication of the likelihood that an adversary will compromise the device in question, while the third factor helps weight the overall risk. The human assets and security goals discussed previously provide a framework for reasoning about the impacts of potentially successful attacks. Here, we provide some guidelines for how to evaluate a device's exposure to attack and the likelihood of an attack attempt based upon the rough design characteristics of a technology (also summarized in the Device Risk Axes column of Table 1). Such a strategy for evaluation could be used by product designers, policymakers, or consumer advocacy groups.

**Potential Exposure to Attack.** In order to determine the risk posed by a home technology, it is necessary to evaluate how vulnerable the device is to an attack. It is difficult to make arbitrary evaluations of a technology's vulnerability without performing a hands-on study of the device in question; nonetheless, we provide some loose guidelines for design factors that tend to increase the likelihood that a device may be vulnerable to compromise. Those devices that are most likely to be vulnerable may deserve the most security consideration.

We stress that these guidelines indicate the likelihood of a potential vulnerability absent appropriate defenses, and are not an absolute measure of risk. Second, we stress that the list here is not exhaustive: instead, it focuses on some common issues that affect a device's attack surface. One would need to conduct a full security analysis of a product in order to more accurately gauge its level of security.

*Communication capabilities.* The more communication capabilities that a device possesses (for example, Wi-Fi, Ethernet, infrared, Bluetooth, ZigBee, cellular, powerline), the more media an adversary can use to attack the device. Manual communications capabilities such as USB or CD interfaces must also be considered.

*Communication behavior.* We consider three aspects of a device's communication behavior that affect its exposure to attack: initiated communications; receptiveness to incoming communications; and mobility. If a device is designed to communicate with a server or peer external to the home network, then a remotely located adversary has increased opportunities to attempt a range of passive and active attacks such as traffic eavesdropping, man-in-the-middle attacks, relay attacks, replay attacks, and spoofing. Additionally, a device's receptiveness to acting upon or replying to incoming network communications may also increase its exposure to attack.

If a device is mobile, then the chances are higher that it will come into contact with malicious or infected networks or devices.

*The cloud.* The flexibility and affordability of storage and computation in the cloud (such as software-as-a-service, platform-as-a-service, infrastructure-as-a-service) are causing more manufacturers to rely on the cloud for storage, backup, remote access, or configuration. If data is stored on those remote servers, then we must consider the risks to users if that data is exposed, altered, rendered inaccessible, or otherwise misused. By facilitating online configuration or remote access, manufacturers expose a different surface to attack—one that should not be overlooked even though it lies outside the physical boundaries of the home.

*Software updates.* The ability or inability to perform software updates can have positive or negative implications in a security context.[2] A device that connects to a manufacturer's server regularly to download updates may receive patches that remove vulnerabilities; however, if the update system does not properly verify that an update is legitimate or if that verification process is flawed, then an adversary has a convenient mechanism with which to modify a device's behavior.

*Configuration defaults, user interfaces, and users.* Defaults, user interfaces, and intended users all affect a device's security configuration (for example, sharing settings, account passwords, or update settings) and therefore its ultimate vulnerability to attack. A device with more secure default settings has an advantage over devices with less secure defaults, as some users never modify default configurations. Entire research venues are dedicated to tackling issues surrounding configuration models and defaults.

Some user interfaces are rich whereas others are minimal. There are advantages and disadvantages with each. Rich interfaces have the potential to be confusing but can allow greater control over security settings. Rich interfaces can also inform users of security compromises and give them the ability to respond.

Similarly, it is important to consider the characteristics of the people who are most likely to administer the device. Different users might have different levels of security caution, different levels of familiarity with computers, or different priorities. For example, if a device resembles a toy or is meant to be used by children, then parents might give it to their children to administer, despite the child's likely lack of experience with computer security and different stance on privacy issues.

**Attractiveness as a Target.** To understand the risk posed by a home technology, it is also necessary to consider how much value the device holds for an adversary. A device's attractiveness to an adversary is relevant for two reasons: first, it affects the likelihood that an adversary will attempt to compromise the device. Second, the properties that cause a device to be of interest to an adversary are most likely the same properties that make the device a potential risk to users: after all, an adversary has some goal in attacking the device, and most of those goals cause direct or indirect harm to the user. We articulate here some of the capabilities and usage scenarios that make a device more attractive as an attack target.

*Technology market share.* If an adversary is intending to perform attacks of exploitative opportunity—attacks targeted at nonspecific vulnerable people rather than specific victims—then it is most efficient for the adversary to attack a technology that is deployed in many homes. Conversely, targeted attacks may better succeed with devices that have received less scrutiny due to a smaller market share.

*Intended users and usage.* Understanding a technology's most likely usage scenario helps indicate how valuable it would be to an adversary, since it dictates the assets with which the tech-

nology will interact. For example, a nanny cam would allow an adversary to spy on children; a networked storage server might hold backups of tax records or other financial data; and an electronically controlled door lock might allow full access to a home, whereas an electronic garage door opener would only allow access to the garage. While one cannot always anticipate how a device might be repurposed, it is important to consider future usage scenarios.

*Sensors.* If a device has sensors that record data then it might be a target of increased interest. The value of a sensor depends upon how much interest the raw or mined data holds for the adversary: for example, microphones and cameras have obvious value for voyeurs, blackmailers, or even private investigators or industrial spies; accelerometers might indicate whether or not a person is awake; and devices with GPS or Wi-Fi can be used to track an individual.

*Actuators.* A device holds increased value for an adversary if it can be used to effect changes in the physical world, since cyber-physical systems are both more efficient and less risky to use than physically traveling to a home. Cyber-physical effects of interest might include: locking or unlocking doors, cutting off electricity or water, changing thermostat temperatures, controlling lights, and turning appliances such as fireplaces on or off.

*Power.* The power reserves and power schedule of a device affects its utility to an adversary. A device with limited battery life, such as a mobile phone or a universal Wi-Fi remote, has constraints on its usefulness. Alternatively, devices that are regularly unplugged or powered off by their users are not dependably accessible to the adversary.

*Connectedness.* A target might have value for an adversary either because it is likely to interact with many devices in the future—due to mobility or high network traffic—or because it will interact with a device of particular interest to the attacker; for example, an adversary might target a mobile device with the intention that it will later be able to infect networked-attached storage that houses financial data.

*Storage and computation.* Devices with large storage capabilities might be targeted to store illegal materials. Devices with smaller storage capabilities are less useful on their own, but could be used as part of a distributed storage botnet. Devices with large computational capabilities might also be attractive to adversaries with heavy computational tasks, such as farming Bitcoins or cracking passwords. While there are additional properties that might affect a device's potential exposure to attack or its attractiveness as a target for attack, we chose to list the characteristics that we judged most significant and relevant for home technologies.

## Tying Things Together

We tie together our framework with an example of how one might use it to analyze or compare the potential risks posed by different technology designs. We present a conceptual investigation of three technologies: a mobile webcam toy, a wireless scale, and a siren for a home security system. These technologies are not meant to be specific products, but rather amalgamations of products or exemplars of product categories. They represent a range of target audiences, technical capabilities, and application scenarios.

▸ *Mobile webcam toy.* Consider a mobile robotic webcam designed as a telecommunications toy for children. The toy can be used to drive around the house, chat with a friend, or communicate with a parent away on business. The toy broadcasts an ad hoc Wi-Fi wireless network to which a client computer can connect to view the webcam or drive the robot; alternatively, port forwarding can

**Table 3. An approximate risk evaluation of the three example technologies via potential exposure to attack and attractiveness of the attack target. The cells are color-coded to indicate the approximate severity of the concern: dark orange (serious), light orange (moderate), and light blue (minor).**

| | Communication Capabilities | Communication Behavior | Software Updates | Configuration Defaults, User Interfaces, and Users | Market Share |
|---|---|---|---|---|---|
| Mobile Webcam Toy | Long-range (Internet), short-range (Wi-Fi), USB (physical) | Communication with external server; Low inter-home mobility; Accepts incoming connections | Manual via USB | Global default password; Minimal UI inputs[1]; Minimal notification of connection (LED); Children admins | Marginal |
| Wireless Scale | Long-range (Internet), short-range (Wi-Fi), USB (physical) | With external server; Low inter-home mobility; Rejects incoming connections | No | No default data protection; Minimal UI inputs[1]; No visual cue when data is accessed; Adult admin | Marginal |
| Security Siren | Short-range (Z-wave) | Low inter-home mobility; Highly connected to other automation devices | No | Manual reset required to join automation network; No UI inputs[2]; No UI feedback; Adult admins | Marginal |

1. Configured with PC via USB. 2. Programmed over short-wave.

be set up on the home router to allow the toy to be accessed from the Internet.

▸ *Wireless scale.* The second example technology we consider is a scale that wirelessly connects to an access point to send users' measurements over the Internet to their accounts on a server. Users can access their data, graphs, and trends via an online Web site or a smartphone application.

▸ *Security siren.* The third technology is a siren that is part of a home automation or security system. The siren receives notification from entry sensors if a suspected break-in occurs and sounds an alarm. The various components in the home automation system communicate over short-range wireless.

Tables 3 and 4 present a high-level view of how our framework might be used to evaluate the approximate risk posed by these device designs. Interpretations and rankings of different risk levels are subjective and depend upon perspective. Table 3 considers the technologies according to the characteristics presented in the section "Evaluating Potential Risks." Table 4 summarizes the consequences that can result if the security goals discussed in the section "Human Assets and Security Goals" are not met. Color-coding provides an overview of the comparative risk patterns of the different devices.

Our goal is not to be exhaustive or predictive. Rather, our goal is to facilitate an informed discussion about the potential risks with a technology if security is not sufficiently addressed in its design. To clarify, this framework only provides a skeleton for characterizing risks; individuals not accustomed to considering attack scenarios might require additional guidance.

*Mobile webcam.* Having populated the tables, we can now quickly assess the potential security risks with each technology. With its communications capabilities, communication behaviors, and user interface design, the mobile webcam toy clearly has significant potential exposure to attack (Table 3). Furthermore, with its proximity to children and its significant sensing capabilities (camera and microphone), the webcam toy appears to be a potentially attractive target to some adversaries (Table 3); more particularly, this device might be an attractive target to adversaries seeking to compromise the privacy of home occupants (Table 4). Given the high potential exposure to compromise, the attractiveness of the target, and the importance of the corresponding security goals, we would identify the mobile toy robot as a technology that merits significant security review by product designers before the device enters the market. Similarly, based on the data in these tables, consumer advocacy groups would likely identify this device as one deserving post-market security auditing.

Fortunately, security best practices—if deployed—could significantly harden this device against attack: for example, the ability to perform authenticated software updates could allow the manufacturer to quickly address vulnerabilities once uncovered and strong audit logs could help further dissuade attack.

*Wireless scale.* Turning to the wireless scale, we see that although it does have some technical features that increase its potential exposure to attacks (Table 3)—particularly the inclusion of Wi-Fi capabilities—it is not a particularly attractive attack target and the associated security goals are not critical (Table 4). While there are arguments for trying to harden all devices against all possible attacks, that strategy is not feasible in practice. First, increasing security may impact the usability, desirability, or utility of the product. Second, companies do not have unlimited budgets to spend on security. These tables suggest that if a single manufacturer produced both the mobile webcam toy and the scale, the company would be well advised to focus

| Intended Users and Usage | Sensors | Actuators | Power | Connectedness | Storage and Computation |
|---|---|---|---|---|---|
| Webcam used in the proximity of children | Video camera, microphone | Wheels, speaker | Several hours continuous operation before recharge | High (externally addressable) | Medium |
| Used by adults to weigh themselves | Pressure sensor | None | AA batteries | Medium (not externally addressable) | Low |
| Used to alert home owners and neighbors of burglaries | None | Speaker | Continuous (plugged in) | Medium (connects with automation devices) | Low |

its security efforts on the webcam toy over the wireless scale; nevertheless, given the scale's potential effects on emotional well-being, eating, or exercise activities, the integrity of sensor readings might become a security priority if the product were being marketed toward users with eating disorders (Table 4).

*Security siren.* Finally, we turn to the security siren. Table 4 suggests the primary security goals for the siren are related to device operability and command authenticity. If an attacker can disable the siren, then the attacker might be able to enter a home without alerting those nearby, thereby rendering the short-term benefits of the home alarm system ineffective; the home security system might still automatically call the police, but the police will not arrive immediately. Since the market share is listed as small in Table 3, the likelihood of an attacker choosing to target this system today seems small; however, the market share may increase over time. Having identified device operability as a particularly pertinent security goal, the device manufacturer can once again implement techniques to harden the device. For example, the device could issue a distinctive alert if a denial-of-service attack renders the siren unavailable to the rest of the home automation network. The continuous sounding of an alarm could also cause a service interruption by tempting the user into turning off or ignoring the system; therefore, it is also important for the manufacturer to deploy defenses such as transmitting logs and incident reports to a monitoring agency.

*Stepping back.* As these examples illustrate, our framework can guide the analysis of potential security risks with technologies in the home. Devices in the home will likely incorporate varying degrees of security defenses, due in part to oversights by designers and developers, but also due to the costs associated with implementing security measures. By methodically evaluating a device's potential exposure to attack and its attractiveness to adversaries (Table 3), as well as the potential impacts on security goals and human assets if the device is compromised (Table 4), one can assess the degree to which security might be important for a given device, as well as which security goals are the most important to address. This information can help developers focus their energies on the most significant risks of a design and help consumer advocacy groups direct their attention toward the computer security properties of the most concerning home technologies.

## Conclusion

Our homes are increasingly becoming hubs for technologies with a wide variety of capabilities. While it would be ideal to strive for "perfect" security on all consumer devices, the reality is that resources such as time and money constrain these efforts. In the coming years, it will become increasingly important to improve the efficacy, interoperability, and usability of computer security solutions for the home. It remains to be seen what such a security solution would look like. It might take the form of a centralized security console that displays and controls device permissions and traffic.[28] The security system could incorporate trusted hardware, network intrusion detection systems, tiered security,[6,20] or cryptographic trust evidence of past transactions or device state.

We need a strategy for how to secure devices in the home. We need to understand the potential risks: risks that are a function of a device's potential exposure to attack, its attractiveness as an attack target, and the potential impacts on human assets if the device is compromised. In this article, we explored the landscape of technological attacks on the home and provided a strategy for thinking about security in the home. In particular, we have identified human

**Table 4. An approximate risk evaluation of the three example technologies considering how human assets might be impacted if defensive goals are not met. The cells are color-coded to indicate the approximate severity of the concern: dark orange (serious), light orange (moderate), and light blue (minor).**

| | Device Privacy | Device Operability | Device Availability | Command Authenticity | Data Privacy | Data Integrity | Data Availability |
|---|---|---|---|---|---|---|---|
| Mobile Webcam Toy | Device is interesting target | Replaceable but not cheap; Non-essential device | Non-essential | Potential minor property damage; Could send spam or launch similar attacks | Videos of household, including children | Could add disturbing images or sounds into stream | Non-essential |
| Wireless Scale | Device is not sensitive; Not a theft target | Replaceable but not cheap; Non-essential device | Non-essential | Could send spam or launch similar attacks | Weights are private; Online account credentials | Inaccurate weights could cause shame, affect eating and exercise | Non-essential |
| Security Siren | Device is interesting target, may indicate affluent household | Replaceable; Destruction would disable security siren | If unavailable weakens home security | Continuous alarm an annoyance, could cause user to disable or ignore alarm | N/A—does not store data | N/A—does not store data | N/A—does not store data |

assets at stake within the home and security goals for computational home devices. We then identified key features of devices that, in general, make them more vulnerable to attack or more attractive as attack targets. Together, these axes can be used to evaluate the level and type of security attention appropriate for different home technologies. We applied our approach to three example technologies: a wireless webcam toy, a wireless scale, and a home automation siren. With further research, we conjecture that our risk framework could be distilled into a decision tree-like structure with questions that would allow those without security expertise to deterministically assign a device to a risk category. By seeking to understand the risks posed by home technologies as a cohesive whole, our hope is that this work will strengthen the foundations for developing secure home technologies—with the ultimate goal of creating a more trustworthy home environment for users.

## Acknowledgments

We thank Intel and the Intel Trust Evidence Program for supporting this work. We thank Dan Halperin, Greg Piper, Jesse Walker, and Meiyuan Zhao for feedback on earlier versions of this article.

**References**

1. Barbie Video Girl; http://www.barbie.com/videogirl/
2. Bellissimo, A., Burgess, J. and Fu, K. Secure software updates: Disappointments and new challenges. In *Proceedings of USENIX Hot Topics in Security*, (July 2006).
3. Bojinov, H., Bursztein, E. and Boneh, D. Xcs: Cross channel scripting and its impact on Web applications. In CCS '09.
4. Brush, A.J.B. and Inkpen, K.M. Yours, mine and ours? Sharing and use of technology in domestic environments. In *Proceedings of UbiComp '07*.
5. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of USENIX Security '11*.
6. Cisco NAC; http://www.cisco.com/en/US/products/ps6128/index.html.
7. Denning, T., Matuszek, C., Koscher, K., Smith, J.R. and Kohno, T. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceeding of Ubicomp '09*.
8. Dixon, C., Mahajan, R., Agarwal, S., Brush, A.J., Lee, B., Saroiu, S. and Bahl, V. The home needs an operating system (and an app store). In *Proceedings of Hotnets '10*.
9. Edwards, C., Kharif, O. and Rile, M. Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy (June 27, 2011); http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html
10. Edwards, W.K., Grinter, R.E., Mahajan, R. and Wetherall, D. Advancing the state of home networking. *Commun. ACM 54*, 6 (June 2011).
11. Fisher, D. Samsung Handsets Distributed With Malware-Infected Memory Cards (June 4, 2010); http://threatpost.com/en_us/blogs/samsung-handsets-distributed-malware-infected-memory-cards-060410
12. Friedman, B., Kahn Jr., P.H. and Borning, A. Value sensitive eesign and information systems: Three case studies. In *Human-Computer Interaction and Management Information Systems: Foundations*.
13. GlowCaps; http://www.rxvitality.com/glowcaps.html.
14. Gourdin, B., Soman, C., Bojinov, H. and Bursztein, E. Toward secure embedded Web interfaces. In *Proceedings of USENIX Security '11*.
15. Greenberg, A. iPhone Security Bug Lets Innocent-Looking Apps Go Bad (Nov. 7, 2011); http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/
16. Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T. and Maisel, W.H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. IEEE 2008.
17. Khurana, H., Hadley, M., Lu, N. and Frincke, D.A. Smart-grid security issues. *IEEE Security and Privacy 8* (2010), 81–85.
18. Kim, T-H.J., Bauer, L., Newsome, J., Perrig, A. and Walker, J. Challenges in access right assignment for secure home networks. In *Proceedings for HotSec'10*.
19. Mazurek, M.L., Arsenault, J.P., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., Shay, R., Vaniea, K., Bauer, L., Cranor, L.F., Ganger, G.R. and Reiter, M.K. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of CHI '10*.
20. Microsoft NAP; http://technet.microsoft.com/en-us/network/bb545879.
21. Mills, E. More malware targeting Android (July 11, 2011); http: //news.cnet.com/8301-27080_3-20078606-245/more-malware-targeting-android/
22. Nest; http://www.nest.com/.
23. Patel, S.N., Reynolds, M.S. and Abowd, G.D. Detecting human movement by differential air pressure sensing in HVAC system ductwork: An exploration in infrastructure mediated sensing. In *Proceedings of Pervasive '08*.
24. Rock Star in your kitchen; (Aug. 29, 2008); http://www.gorenjegroup.com/en/news?aid=933
25. Spykee; http://www.spykeeworld.com/.
26. Withings WiFi Body Scale; http://www.withings.com/en/bodyscale.
27. XFINITY Home Security; http://www.comcast.com/homesecurity/.
28. Yang, J., Edwards, W.K. and Haslem, D. Eden: Supporting home network management through interactive visual tools. In *Proceedings of UIST '10*.

**Tamara Denning** (tdenning@cs.washington.edu) is a Ph.D student at the University of Washington, Seattle.

**Tadayoshi Kohno** (yoshi@cs.washington.edu) is an associate professor at the University of Washington, Seattle.

**Henry M. Levy** (levy@cs.washington.edu) is Wissner-Slivka Chair of Computer Science and Engineering at the University of Washington, Seattle.



| Environment Integrity | Activity Pattern Privacy | Presence Privacy | Occupant Identities | Sensed Data Privacy | Sensor Validity | Sensor Availability |
|---|---|---|---|---|---|---|
| Toy can cause minor physical property damage (for example, fragile objects) | Activities easily deduced from A/V feed | Could reveal whether house is occupied and the presence of children | Occupants easily identifiable | Home can be very private | Could add disturbing images or sounds into stream | Non-essential |
| N/A | Weighing times might indicate when occupants wake up | Could potentially reveal whether occupants are on vacation | Could reveal profile information (for example, name, age) | Weights are private | Inaccurate weights could cause shame, affect eating and exercise | Non-essential |
| Continuous alarm an annoyance, user might disable or ignore alarm | Siren may indicate unauthorized entry | Siren may indicate unauthorized entry | N/A | N/A | N/A | N/A |