Empowering Consumer Electronic Security and Privacy Choices: Navigating the Modern Home

Tamara Denning and Tadayoshi Kohno
Computer Science and Engineering
University of Washington
{tdenning, yoshi}@cs.washington.edu

ABSTRACT
Currently, the casual consumer has few available resources on product security and privacy with which to inform purchasing decisions. This absence of coherent information becomes increasingly important as we incorporate an increasing level of sensors, actuators, and connectivity into the technologies in our homes. We wish to initiate a discussion on the potential utility of an organized entity which provides understandable, coherent security reviews and ratings of a large range of consumer technologies. In this paper, we first provide a background of our stance on security and privacy for consumer technologies in the modern home. We then sketch out a proposed resource for security and privacy information on consumer technologies. We discuss some of the potential benefits, obstacles to implementation, and propose potential areas of research that would improve the design of such a resource.

Categories and Subject Descriptors
K.4 [**Computers and Society**]

General Terms
Security, Human Factors.

Keywords
Computer security, consumer electronics, consumer information, consumer resources, privacy, security.

1. INTRODUCTION
Under the current status quo, the typical consumer has little power when it comes to making security- and privacy-conscious purchasing decisions. If diligent consumers wish to factor the security and privacy properties of a product into their decision process, they have little recourse. A "power-user" might browse forums for scuttlebutt regarding particular products or manufacturers, and a particularly dedicated consumer might peruse technology magazines for opinions or editorials; in general, however, these methods are time-consuming and more likely to yield security information on operating systems or enterprise-level routers than on refrigerators or garage door openers. And while some products may boast "ultra-secure encryption" or "ironclad dual-layer security," in the end these are unverified claims that provide little useful information to the end user.

As we bring a multitude of wireless-enabled technologies into our homes, the security and privacy properties of consumer technologies becomes increasingly important; these technologies enable new large-scale attacks, attacks with physical consequences, and unprecedented vulnerabilities to privacy at a rate which outpaces users' understanding of the risks. Consumers need to have reliable, easy sources of information available to help them make purchasing decisions and to implicitly inform them of risks involved with using various technologies.

We propose that consumers would benefit from the availability of an organized, cohesive set of reviews on the security and privacy properties of a broad range of consumer technologies, and we invite discussion in this space.

In this paper, we:

- Position our stance on the security and privacy of consumer technologies in the modern home;
- Propose an organized entity which serves as a resource on the security and privacy properties of a broad range of consumer technologies;
- Discuss the potential benefits of such a resource, as well as obstacles that it might encounter in its deployment;
- Discuss potential research questions that would help inform the design of such a resource.

While much of our discussions are focused on the modern home, the entity that we propose could also serve as a resource for consumers wishing to purchase other computational devices, ranging from automobiles to mobile phone apps.

2. COMPUTER SECURITY AND THE MODERN HOME
Before discussing the opportunities and challenges provided by a consumer resource on security and privacy, we provide background information on our stance on electronic security and privacy in the modern home.

The authors of this paper previously published an article sketching some of the new threats that emerge when we incorporate a multitude of consumer technologies into the home environment; the article included a rough framework by which to evaluate the risk presented by these [3]. Table 1 presents a

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

Infection Pathways	Human Assets	Defensive Goals	Device Risk Axes
Physical	The Biosphere	Device Privacy	Potential Exposure to Attack
In-person	Emotional Wellbeing	Device Availability	Communication Capabilities
Secondhand via Infected Device	Financial Wellbeing	Device Operability	Communication Behavior
Found	Personal Data	Command Authenticity	The Cloud
Gift	Physical Wellbeing	Execution Integrity	Software Updates
Infected from Manufacture	Relationships	Data Privacy	Configuration Defaults, User Interfaces, and Users
Lent	Societal Wellbeing	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	

Table 1. An overview of the topics discussed in Denning et al. [3]. The first column gives a casual taxonomy of some of the ways that an infection can be introduced into the home. The second column lists human assets that can be impacted by compromises of technology within the home. The third column articulates some variations of the traditional confidentiality, integrity, and availability defensive goals, as adapted for home consumer technologies. The fourth column lists some of the axes by which a device's overall risk to users may be approximated.

summary of some of the topics discussed in the article, including: potential vectors for infection; human assets within the home; defensive goals for technologies within the home; and properties by which to assess a technology's overall potential risk to the home and its inhabitants.

Our interest in the home as a security environment is due to its unique integration of technologies, assets, and users. The home is a hodgepodge of heterogeneous technologies, each of which is increasingly more likely to integrate sensors, actuators, and wireless connectivity. These properties amplify the convenience and impact of existing attacks and enable new attacks on physical properties of the home and its inhabitants; while not all attacks are novel, the overall risk assessment of even traditional attacks may change. Table 2 lists some examples of attacks in the home broken down into low-level mechanisms, intermediate goals, and the high-level goals that they enable; the article provides descriptive examples of potential attacks.

The home is an environment which incorporates a variety of direct and indirect stakeholders: adults, children, the elderly, siblings, friends, acquaintances, roommates, and pets. These stakeholders may have different goals and different levels of familiarity with technology. Furthermore, the home usually does not contain a dedicated, knowledgeable administrator who configures and maintains the technologies within the home. To top it off, the technologies within the home impact a wide range of human assets (see Table 1): our homes are our private spaces, and they are intertwined with our health, wealth, and happiness.

Consumers need to be empowered with the ability to make decisions about what kinds of technologies and which specific products they wish to bring into their homes.

3. SECURITY AND PRIVACY REPORTS

We propose an entity which provides understandable, coherent reviews and ratings detailing the security and privacy properties of a broad set of consumer technologies.

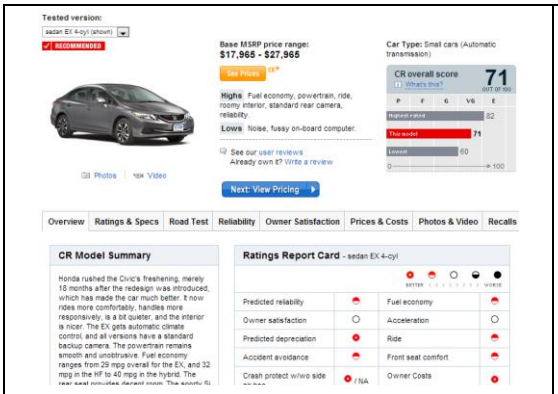
An analogous model—though not one in the security and privacy space—is *Consumer Reports* [2]. Consumer Reports offers access to reviews and ratings of a large number of consumer technologies. Reviews (see Figure 1a) include descriptive write-ups in addition to quantitative ratings on a set of relevant axes that are consistent across a product category. Consumers can review the high-level ratings (see Figure 1b) or investigate the ratings on more detailed level (see Figure 1c). Consumer Reports, which is published by a non-profit group, is available online and in print for a subscription fee, and as of 2010, had 7.3 million subscribers [1].

While the success of Consumer Reports cannot solely be attributed to its format, we propose this format as a starting point for discussions as to how best to present and deliver security and privacy information on products to consumers.

While an entity providing such a resource might do so via a

	Examples	
Low-level Mechanisms	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 false 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	

Table 2. Examples of some of potential components of attacks on the home, broken down into low-level mechanisms, intermediate goals, and high-level goals [3].



(a) a screenshot of a portion of the overall review, including part of the write-up;

Ratings Report Card - sedan EX 4-cyl

BETTER WORSE

Predicted reliability		Fuel economy	
Owner satisfaction		Acceleration	
Predicted depreciation		Ride	
Accident avoidance		Front seat comfort	
Crash protect w/wo side air bag	/ NA	Owner Costs	

See how this model did in more than 50 tests

(b) a table indicating a product's overall assessment on its major axes;

Safety			
Antilock brakes	Standard	Standard	Standard
Traction control	Standard	Standard	Standard
Stability control	Standard	Standard	Standard
Daytime running lights	Standard	Standard	Standard
Tire pressure monitor	Available	Available	Available
Safety belts			
Center-rear belt	3-point	3-point	3-point
Pretensioners, front/rear	Yes/no	Yes/no	Yes/no
Air bags			
Occupant-sensing system	Front and Side	Front and Side	Front and Side
Side bags, front/rear	Standard/no	Standard/no	Standard/no
Side curtain air bags	Standard	Standard	Standard
Accident alert system	Not available	Not available	Not available
Crash and rollover tests			
IIHS offset-crash test	Good	Good	Good
IIHS side-crash test with side airbags	Good	Good	Good
IIHS side-crash test without side air bags	NA	NA	NA
Gov't front-crash test, driver			
Gov't front-crash test, front pass.			
Gov't side-crash test, driver			
Gov't side-crash test, rear pass.			
Gov't rollover test, 2WD			
Gov't rollover test, 4WD	NA	NA	NA

(c) a breakdown of a major axis (Safety) into its detailed components.

Figure 1. Examples of evaluative tables Consumer Reports includes in its product review write-ups [2].

certification process with the manufacturer, such as with Common Criteria, we instead propose that ratings and reviews are based on experimental evaluation of the products.

We now turn to discussing the potential benefits of such a resource, the feasibility of such a resource being successful, and some open research questions that would impact the design of such a system.

3.1 Benefits

Although these claims are unproven, and potentially idealistic, we imagine that such a resource might have a variety of benefits to offer consumers. For example:

- **Empowering consumers.** Supplying consumers with a trusted, impartial source of security and privacy information gives them the opportunity to make more informed decisions; not every decision will be made solely on the basis of security, but consumers should have the right to weigh such considerations when making their purchasing decisions, alongside more common considerations such as price, durability, and feature set.
- **Increased consumer awareness.** The very existence of a resource dedicated to providing security and privacy ratings might make consumers more aware of the potential importance of such properties; for every person who accesses such a resource, one or more people might be exposed to the idea that they might want to consider the security or privacy properties of their future purchases.
- **Incentivizing better industry security practices.** If consumers have an increased awareness of security and privacy issues, and are subsequently empowered to make decisions based on security and privacy criteria, there will be increased pressure on companies to proactively and conscientiously address potential security and privacy risks with their products.

3.2 Feasibility

Having explored some potential benefits of a consumer-level security and privacy resource, we bring up potential obstacles to its implementation and adoption:

- **Economics.** In order for an entity providing security and privacy information to continue to exist, it ought to be self-sustaining. The profitability of such a venture is somewhat dependent upon consumer interest (below); however, the expenses behind such a venture are also a factor. One issue of interest might be how much analysis may be automated via static or dynamic analysis tools, versus how much analysis must be done by hand via experienced professionals.
- **Consumer interest.** Unless a security and privacy resource is provided solely as a public service, it needs to be financially self-sustaining. The profitability of such a venture is limited by consumers' interest in

paying for such information, and therefore limited by the general consumer level of interest in security and privacy; however, such an offering might attempt to piggyback an existing resource, thereby bypassing some overhead costs.

- **Evolving threats.** The security risks of a product do not remain fixed over time; as new threats emerge or as a technology is used in new ways, the security implications of a given product can change. For example, a new class of attacks might arise, or a product that is relatively secure in isolation—such as an automobile's internal communication network—might become commonly hooked up to wireless peripherals (e.g., [4]). It remains to be seen whether a security review of a product at launch time is sufficient to inform a consumer of its security performance over the course of its lifetime.
- **Psychology of security evaluations.** The organization conducting these evaluations—and the consumers who make use of these evaluations—must acknowledge that it is likely impossible for a security evaluation of a product to be "complete"; even with a thorough evaluation, undiscovered security vulnerabilities may exist. Unfortunately, if a product with a high security rating is a victim of new vulnerabilities or successful attacks, consumers may have decreased confidence in the system.

The practicality of resource on the security and privacy properties of consumer technologies is dependent upon the balance between its benefits and the obstacles which impact its feasibility. There remain, however, a number of open research questions—some of which ultimately affect this balance.

3.3 Open Questions

While many aspects of the success of a consumer-level security and privacy resource depend upon business practices, there remain a number of open research questions that could impact the development and deployment of such a system:

- **Areas of highest impact.** Given limited resources, it would make sense to concentrate human-hours and money upon product categories that would provide the most benefit to the largest number of consumers; this could either be due to large security and privacy discrepancies within the product category, or extremely common usage of products within the category. Similarly, product categories which people are most interested in reading about—and therefore categories that most contribute to continued readership—may not align with the product categories that have the highest security and privacy impact.
- **Rating axes.** Many open questions remain as to which axes on which it is most useful and appropriate to rate the security and privacy properties of consumer products. Certainly, it makes sense to determine the axes upon which consumers wish to evaluate their purchases; however, it is also valuable to ascertain the axes which experts deem most relevant to determining how successful a product is at preserving a user's security and privacy. While it is reasonable to assume that many product categories will have axes in common, further research could determine commonalities and differences among product categories.
- **User's mental models.** Common user mental models of security (e.g., [5]) affect how users perceive and react to the security settings and warnings of a system. Further research into user mental models of security and privacy—particularly in relation to the home environment—could have direct and appreciable effects upon the selection and presentation of information to users.
- **Level of detail.** In the Consumer Reports model, users can choose the level at which they browse information. For instance, a user can consider a high-level summary of information (see Figure 1b), or investigate information at a more detailed level (see Figure 1c). Further research could help differentiate between levels of detail where information is valuable versus levels of detail where information is excessive.
- **Resource model.** Although one avenue of research might be to investigate consumers' level of interest in a security review resource, a more interesting route might be to investigate the suitability of different dissemination structures for such an offering. Consider, for example, the issue of evolving threats raised in Section 3.2: one potential way to address this issue is to offer consumers a customized service which provides periodic new information and recommendation based on the risk landscape of the particular products within the consumer's own home. This potential model is one of many, and it remains to be seen what model would be the most effective, desired, and feasible.

4. CONCLUSION

In the course of this paper, we argued for the utility of a cohesive set of reviews on the security and privacy properties of consumer products, presented our stance on electronic security and privacy in the modern home, discussed the potential benefits and the feasibility of deploying such a system, and touched on open research questions for the design of such a resource. We invite further discussion on this topic, with the ultimate goal of increasing the status quo of security and privacy for consumer electronics, and empowering consumers with the ability to make informed decisions about the products that they bring into their homes and their lives.

5. ACKNOWLEDGMENTS

We thank Intel, Intel Trust Evidence Program, and the Intel Science and Technology Center for Pervasive Computing for supporting this work. This work was supported by an Intel PhD Fellowship.

6. REFERENCES

[1] G. Bounds. Meet the Sticklers: New Demands Test Consumer Reports; Flying in Cat Fur. *The Wall Street Journal*. May 5, 2010.

[2] Consumer Reports. http://www.consumerreports.org.

[3] T. Denning, T. Kohno, and Henry M. Levy. Computer Security and the Modern Home. *Communications of the ACM* 56(1) (January 2013), 94-103.

[4] Scosche. cellCONTROL: Safe Driving System for Cell Phones.

[5] R. Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10).