This paper will be presented at the first

Workshop on Home Usable Privacy and Security

(HUPS)

at

SOUPS 2013

July 24-26, 2013

Newcastle, UK

The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button!

The Security and Privacy Impacts of Children and Childhood on Technology for the Home

Stuart Schechter
Microsoft Research
stuart.schechter@microsoft.com

ABSTRACT

Children represent a unique challenge to the security and privacy considerations of the home and technology deployed within it. While these challenges posed by children have long been researched, there is a gaping chasm between the traditional approaches technologists apply to problems of security and privacy and the approaches used by those who deal with this adversary on a regular basis. Indeed, addressing adversarial threats from children via traditional approaches to computer and information security would be a recipe for disaster: it is rarely appropriate to remove a child's access to the home or its essential systems; children require flexibility; children are often threats to themselves; and children may use the home as a theater of conflict with each other. Further, the goals of security and privacy must be adjusted to account for the needs of childhood development. A home with perfect security – one that prevented all inappropriate behavior or at least ensured that it was recorded so that the adversary could be held accountable – could severely stunt children's moral and personal growth. We discuss the challenges posed by children and childhood on technologies for the home, the philosophical gap between parenting and security technologists, and design approaches that technology designers could borrow when building systems to be deployed within homes containing this special class of user/adversary.

1. INTRODUCTION

...and I would have gotten away with it, too,
if it hadn't been for you meddling kids
—just about every villain on *Scooby Doo*

Much recent work on security in technologically-enhanced homes has focused on the dangers of outside threats, such as malicious visitors and remote attackers who might exploit the increasing connectedness of home automation systems. For example, visitors are the primary threat of Kim *et al*.'s investigation into access rights for secure home networks [6]. Denning *et al*.'s investigation of security for the home envisions such outsider-attack scenarios as the remote unlocking of doors, the causing washing machines to flood, and the adjustment of furnaces to waste heat [2]. Both Denning et al. and Kim et al. address children only as potential *victims* of attack, at risk from burglars who might trick them into opening a door, from stalkers who might discover they are home alone and spy on them, and from devices that might violate their privacy.

Yet children's role in home security and privacy goes beyond that of hapless victim, as they often have a surprising knack for mischief of their own. Children exploit door locks to isolate themselves or others, sometimes locking parents out of the parents' own rooms or even the entire house. Children find innovative and potentially-damaging applications for household objects, such as using crayons to write on walls or using the antennas of wireless routers as goalposts in games of miniaturized football. They adjust thermostats to extremes. They knowingly and intentionally invite into the household guests that would not be welcomed by their parents, not all of which may be human and some of which may carry contagion, filth, or other sources of environmental contamination. They escape the household and assist in the escape of both pets and of objects intended for indoor-only use. Many children perform surveillance operations which are invasive to the privacy of parents, siblings, or other members of the household.

In short, children are both users of household technologies and adversaries against which these technologies must be protected. An entire industry already subsists on parents' need to prevent their children from harming their homes, their siblings, and themselves.

Alas, approaches familiar to security technologists may not work, or may even be harmful, when blindly applied to the threats posed by children. Least privilege may be among the most sacred and respected principles of information security, but starting a conversation on appropriate use of household resources by informing children that their privileges are restricted to a prescribed set of allowable behaviors is a sure way to incite or escalate a conflict. Similarly, enforcing a fixed quota on screen-time at the dramatic climax of a movie or video game would likely make a child more adversarial and less trusting than a policy that was more flexible and more respectful of the child's agency. Unrestricted monitoring of the household as a system (e.g. using cameras), and the power asymmetry that access to such data would both exploit and highlight, could harm the trust built up between child and parent. Finally, evicting children guilty of adversarial behavior from the household would likely result in state-imposed eviction for those responsible for doing so (likely to an even higher-security living environment).

In this paper, we discuss the threat posed by children (Section 2) and the properties of children that make them different from traditional adversaries (Section 3). We argue that security technologies for the home should borrow more heavily from the existing body of knowledge on techniques for managing the adversary potential and special needs of child users (Section 4).

2. THREATS

And I learned there are troubles of more than one kind.
Some come from ahead, and some come from behind.
—*Solla Sollew*, by Theodore Seuss Geisel (Dr. Seuss)

A number of real and demonstrable threats must be considered before introducing children into a household system. The threats include the possibility that one or more children may:

- Invade the privacy of other household members
- Misappropriate other household members' belongings
- Expropriate objects from the household system
- Grant household access to unauthorized individuals
- Cause damage to the objects, information resources, themselves, others or the household infrastructure itself
- Contaminate the household with filth, contagion, or noise
- Consume excessive household resources
- Consume content deemed inappropriate by parents
- Use the home as a theatre for interpersonal conflict (a danger which increases with the number of children introduced into the system)

These threats vary with the age, resolve, and resourcefulness of the child. Extensive anecdotal evidence from those who have engaged in field research suggest that the resolve and resourcefulness of children of a given age is often initially underestimated.

3. CHILDREN: A UNIQUE ADVERSARY

Teddy said it was a hat, so I put it on. Now dad is saying,
"where the heck's the toilet plunger gone?"
—Shel Silverstein

Children are *insiders*, as they are already trusted to use household systems, are familiar with them, and thus have a significant advantage in staging attacks over those who do not have this access and knowledge. Unlike other insiders, their role within the household also makes them harder to defend against.

Children are also natural hackers, because they live in a world designed for people with stronger muscles, better motor skills, keener senses, better communications skills, and other essential abilities and knowledge. Survival and development require them to tinker with their world in order to learn about it. Indeed, much of what child psychologists call *early learning* would be calling *hacking* by technologists. Younger children have little to do with their time but hack and, as children grow, the ones who retain their hacking skills will be the more formidable adversaries.

There are three features of children that make them truly unique among the adversaries we face…

3.1 Children Can Not be Banished

In an enterprise or small business, an employee or user who is revealed to be engaged in adversarial behavior can be banished from the system and, in some cases, prosecuted so as to discourage future treachery from others. Children can be punished, but only in the most extreme instances can they be banished from the home. More commonly, a child engaged in adversarial behavior will be forced to spend more time within the boundaries of the home.

To make matters worse, evolutionary forces have endowed children with emotive abilities designed to reduce the likelihood that they will be held to account for treachery. These *parental controls* may be looks, gestures, or phrases that lead victims to believe they are 'innocent by nature' or that their adversarial behaviors are 'cute'. These responses are not entirely irrational; children may engage in undesirable behavior without adversarial intent.

3.2 Children May be Threats to Themselves

Children often need to be protected from harms caused by their own actions. Protecting children from themselves is unlike protecting systems from external threats. Children cannot be re-architected or expected to operate under layers of physical protection. Restricting a child's access to dangerous tools or objects may negatively impact that child's sense of agency, competence, and self-sufficiency. Whereas most approaches to security do not concern themselves with the negative impact of protections on the adversary, understanding and limiting those impacts is essential when that adversary is also someone you are trying to protect.

3.3 Misbehavior is Necessary for Growth

A certain amount of misbehavior and lying may be essential to building maturity in children. A child who has never had the opportunity to secretly overdose on screen time, to the detriment of his or her homework, may not learn the consequences of failing to motivate himself or herself. A child raised in constant surveillance, who never gotten away with lying, may grow up not having felt the sense of guilt of having successfully deceived others. A child who has never taken the blame for another child's misdeed or been the victim of another child's deception may never develop a sense of injustice or empathy for those who suffer injustices. Unlike business environments, higher compliance rates in the home cannot be assumed to lead to better outcomes. Rather, compliance goals must be balanced against the need for children to develop and mature in a process that may include some amount of misbehavior.

4. DESIGN APPROACHES

A spoonful of sugar helps the medicine go down
—*Mary Poppins*, by Robert B. Sherman & Richard M. Sherman

Designing security with children in mind requires a more nuanced approach than simply restricting access. The following is a list of design approaches that, while neither original nor complete, may be a useful starting point for exploring the place of security in home environments with children.

4.1 Obviate Security When Possible

The best way to secure against risky actions is to remove the element of risk from the action. When risk cannot be eliminated, it can often be reduced.

Removing toxic metals from house paint from home reduced the risk that toddlers' low-altitude culinary explorations would lead to lead poisoning. The introduction of residual current devices (a.k.a. GFCI) [9] reduced the risk that a child's exploration of electrical outlets will lead to deadly shocks, though they do not eliminate the risk and the shocks that do remain are still dangerous and unpleasant. New home technologies could track toddlers' movements and turn off electricity to outlets when children get too close, or turn off stoves or ovens when detecting that pots are overheating or smoke is being emitted.

For information technologies, one way to reduce risk is to design functionality to reduce the risk that data will be deleted or corrupted. Research by Karlson et al. suggests isolating functions that permanently destroy or compromise the integrity of existing data, lessening the risk and corresponding security-requirements for the remaining functionality [5]. This design principle is reflected in the design of Windows phone's "kid's corner", which gives access to selected apps and games unfettered by the need to enter the owner's authentication code.

Storing data on remote services ("the cloud") rather on devices that live in the home may reduce the risk to these data.

Safety mechanisms can be put in place so that children can lock doors, but parents can override. This allows children to learn how locks work, and gain some sense of agency regarding the use of locks, without the risk that parents will be locked out in emergencies. (In the author's household, keys for interior door locks are placed on the molding above the outside of these doors.)

4.2 Decrease Device's Appeal to Children

The cool attention-drawing aesthetic that may help a device or technology sell well may also make it appealing for misappropriation by children.

The same has long been true for household products, such as cleaning solutions, which may be toxic to if ingested. Scary stickers containing such symbols as a skull and crossbones (the "Jolly Rodger") or "Mr. Yuk" have been used to discourage children from touching these hazards, though research has not demonstrated this approach to be effective [3],[11] . Using bittering agents to make poisons less attractive may be more effective [10].

One way to inhibit the abuse of devices, buttons, and interfaces is to make them unattractive to children. For example, moving the power light off of the power button may make the button less appealing to young children, reducing instances in which they use these buttons to turn computers off at inopportune times. Indeed, indicator lights may be unnecessary when a device is neither being configured or monitored. A master switch to turn off all of a device's indicator lights would not only make the device less attractive to children, but would also save energy and reduce indoor light pollution.

A further step would be to make such devices look as uninteresting as possible. Households with wiring that constrains the placement of wireless routers to locations reachable by young children may benefit from designs that resemble objects children are likely to be averse to: long small-print books (e.g. Russian novels) or bottles of shampoo.

4.3 Limit Discoverability

The first step in keeping children away from hazards or inappropriate content is to hide the fact that it is there in the first place. While computer and information security technologies usually offer ways to limit discoverability of the existence of data that users don't have access to, they are given short shrift because of the taboo against security through obscurity and an overconfidence in the efficacy of access control protections.

Consider that while traditional file systems enable users to limit who can read a directory, they do not make it possible to hide a directory. A directory can be placed within another directory that cannot be read, but if any directory within the ancestry is readable by the adversary, the adversary can learn that access to a descendent of that directory had being restricted.

Yet, obscurity may be quite valuable in the home. Children may be less likely to try to impersonate their parents or circumvent access controls if they are unaware that their parents' entertainment devices contain games, movies, or other content that their parents would not want them to have access to. They may be less likely to override limits on sound systems if they believe that the amplifiers are already capable of being turned up to eleven.

4.4 Signal Negative and Positive Feedback

Young children may be trained to avoid risks using negative feedback. A home-safety system designed to protect toddlers could include small speakers placed next to ovens, knife-holders, and other sources of danger that emit increasingly unpleasant sounds as youngsters approach them—not dissimilar to invisible fences for dogs (and related systems that take the unique approach of blending Internet technologies, videos, and cats [4]), but without harsh shocks. Refrigerators can be designed to emit unpleasant sounds if held open too long or closed improperly, just as elevators are designed to do so today.

Similarly, pleasant sounds may be emitted when a refrigerator door is closed properly or when a thermostat is adjusted to a setting that consumes less energy.

Household technology may alert mature occupants to other hazards, small and large, such as when windows are open during a coming downpour or when those window are releasing the same air that heating or cooling systems are working to moderate.

4.5 Replace Denials with Redirects, Mediation

Enforcing access control restrictions with traditional denial messages may incite adversarial behavior in children.

Safety and security mechanisms may have more success by finding a more positive approach, such as suggesting alternatives to the prohibited behavior. For example, when enforcing a screen-time limit, a system could report that "You will have enough screen time built up to watch this video by 4:00PM tomorrow", could suggest a task or chore that could earn the child more of this resource, or could suggest watching a shorter video that would not exceed the child's screen-time quota.

Mediation may be improved by anticipating problems before they occur. If a child is about to start watching a 30-minute video but only has 25 minutes of screen time remaining, the disconnect may be negotiated at a time that is less disruptive than when the quota is reached.

In deterring a younger child from engaging in a task (s)he may not yet be equipped to perform safely on his/her own, a home safety system might ask "Would you like an adult to help you with that?"

4.6 Make Safety Easy, Fun, and Rewarding

Parents have long practiced social engineering in order to convince children that the parents' goals are actually their own. [Editor's note: For those pre-adolescent readers studying this paper to better your understanding of your adversary, we recommend Joshua *et al.'s* "The Quiet Game: The Only Winning Move is Not to Play."]

Children may be less likely to have an adversarial response to security technologies, and may even assist with security, if these technologies are presented as something a child would want. Good system designs would help parents to do this.

Consider, for example, surveillance systems designed with the primary purpose of providing the homeowner with a video record of every guest who enters the home. If the system were designed to provide functionality similar to that of a photo booth, giving children the opportunity to share photos from the stream with friends and record the visit an online scrapbook, those under surveillance might actively embrace such a system.

4.7 Align Incentives

As children grow to start thinking about managing limited resources of their own, incentive alignment becomes an increasingly more effective (and respectful) mechanism for protecting against resource-consumption concerns than strict access control. Variable-rate services and marketplaces, or the devices that access them, could be augmented to support billing children for some or all of the cost of the resources they consume. Further, children who want to adjust thermostats beyond the bounds their parents are willing to pay for could have the opportunity to pay some portion of the additional cost. Technology could reduce the barriers that prevent households today from accounting for the responsibility of each family member for such costs of such acts as leaving lights on and refrigerator doors opened.

However, accounting should not be taken to extremes, and children should not be billed for services essential to their survival. Even seemingly benign incentives may have unintended side effects. There will be some children who should not be given any additional incentive to avoid or shorten their use of hot water for showers. Others should not be given additional incentives to spend time away from the house, honing their adversarial skills and exchanging tricks of the trade with others of their kind.

Providing for some level of individual accounting for expenditures within the household would not only help to prepare children for a future in which they are responsible for paying their share of expenses, but could be beneficial to some service providers as well. Tracking the ownership of digital assets, such as music, videos, and software, would make the chain of ownership more clear when the child leaves the household.

4.8 Optimistic and Reactive Access Control

While children's' residence within the home makes access control harder, their reliance on the home makes it much easier to hold them to account for their actions than other adversaries. Children can be given more privileges than they may need and punished if they misuse them (optimistic security as defined by Povey [8]) or they may be given the ability to request additional permissions when necessary (reactive access control as defined by Mazurek *et al.* [7]).

Substituting accountability for access control requires an adversary who is old enough to consider the consequences of his or her actions. To use accountability as a deterrent it is necessary for a child to believe that parents will be able to identify him/her as the source of a misdeed. However, there are disadvantages to adding the surveillance that may be necessary to hold children accountable for their actions...

4.9 Just-Enough Audit & Surveillance

An employee of a corporation may accept auditing and surveillance because (s)he has some choice in where (s)he works, (s)he is being paid for the time during which (s)he is being monitored and because (s)he need not feel that (s)he is the object of distrust—corporations have many employees and presumably a few bad apples might have made it through the HR department.

Children react differently to surveillance because the decision to monitor them is personal: it reflects on their parents trust in them as individuals. Further, children do not have the choice to change households as employees can (at least in good economic times) change employers. Adding surveillance can breed distrust and cause adversarial behavior. (For an exploration of issues of mobile surveillance, see Czeskis *et al.* [1].)

To reduce distrust, systems could record information that is less personal or to give children greater control over how records are used.

Children may be less offended when parents track the locations of means of transport (bicycles and cars) than the children themselves. In a household with one child, it may be possible to eschew the use of video and record only the timing of doors opening to detect a curfew violation. Rather than recording what children watch, a system might only record the amount of time watched and the maturity rating of the content.

In a house with children who have regular arguments about the assignment of blame, the choice to turn surveillance on could be left to the children. Homes could monitor who enters and who leaves, but not necessarily what goes on inside.

Alternatively, always-on surveillance could be used more judiciously by only allowing video to be monitored if both the child and parent agree. Children could then use surveillance feeds as evidence of their innocence, but not have the video used against them. However, such an arrangement would still be problematic from the child's perspective, as, similar to defendants in U.S. courts who assert their fifth amendment rights, the refusal to allow evidence to be presented may be interpreted as evidence of guilt in and of itself.

5. CONCLUSION

Children are a formidable adversary unlike any other. Technologies for the home should make opportunities for misuse less discoverable, less appealing, and less dangerous. As children grow, technologies that seek to enforce policies upon them, or to help adults monitor children or their environment, need to be designed in a manner that is respectful, allow for natural negotiation, and that do not stunt children's personal maturation.

ACKNOWLEDGMENTS

The author would like to thank those who provided comments on earlier drafts of this paper: A. J. Brush, Lorrie Cranor, Jaeyeon Jung, Ratul Mahajan, James Scott, and Blase Ur, and the anonymous reviewers (especially the one who found and detailed over twenty typos that made it into the submission draft).

The author would also like to thank his playpen-etration testers, Leia and Ahna Jung, for their contributions to the threat model. However, he would also to remind them that his gratitude has its limits. No matter how much my research might benefit from exposure to non-human adversaries, and no matter how sincerely you promise to do the required walking and cleansing, we are not – I repeat we are not – getting a fuzz tester.

REFERENCES

[1] Alexei Czeskis, Ivayla Dermendjievay, Hussein Yapity, Alan Borningy, Batya Friedmanz, Brian Gill, and Tadayoshi Kohno. *Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety*. Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2010

[2] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy, *Computer Security and the Modern Home*. Communications of the ACM, Vol. 56 No. 1, Pages 94-103

[3] D. M. Fergusson, L. J. Horwood, A.L. Beautrais, and F. T. Shannon. *A controlled field trial of a poisoning prevention method*. Pediatrics, 1982; 69(5): 515-520.

[4] Brian Gaut. *Blender Defender*. 2008 http://www.plasma2002.com/blenderdefender/

[5] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter, *Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones*. Proceedings of the SIGCHI Conference on Human Factors in Computing System. May, 2009. 1647-1650

[6] Tiffany Hyun-Jin Kim, Lujo Bauer, James Newsome, Adrian Perrig, and Jesse Walker. *Challenges in Access Right Assignment for Secure Home Networks.* In Proceedings of the 5th USENIX Workshop on Hot Topics in Security (HotSec'10) August 10, 2010, Washington, DC.

[7] Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. *Exploring reactive access control*. In CHI 2011: Conference on Human Factors in Computing Systems, May 2011.

[8] Dean Povey. *Optimistic security: a new access control paradigm.* Proceedings of the 1999 workshop on New security paradigms. Pages 40 - 45 ACM New York, NY, USA

[9] Residual Current Device, http://en.wikipedia.org/wiki/Residual-current_device

[10] J R Sibert and N Frude, *Bittering agents in the prevention of accidental poisoning: children's reactions to denatonium benzoate (Bitrex)*. Archives of Emergency Medicine. 1991 March; 8(1): 1–7

[11] K Vernberg, P Culver-Dickinson, and DA. Spyker, *The deterrent effect of poison-warning stickers*. American Journal of Diseases of Children 1984 Nov;138(11):1018-20. http://www.ncbi.nlm.nih.gov/pubmed/6496418