A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons

Tamara Denning, Cynthia Matuszek, Karl Koscher,
Joshua R. Smith, and Tadayoshi Kohno
Computer Science and Engineering, University of Washington
Paul G. Allen Center Box 352350
Seattle, WA 98195
{tdenning, cynthia, supersat, jrs, yoshi}@cs.washington.edu

ABSTRACT

Future homes will be populated with large numbers of robots with diverse functionalities, ranging from chore robots to elder care robots to entertainment robots. While household robots will offer numerous benefits, they also have the potential to introduce new security and privacy vulnerabilities into the home. Our research consists of three parts. First, to serve as a foundation for our study, we experimentally analyze three of today's household robots for security and privacy vulnerabilities: the WowWee Rovio, the Erector Spykee, and the WowWee RoboSapien V2. Second, we synthesize the results of our experimental analyses and identify key lessons and challenges for securing future household robots. Finally, we use our experiments and lessons learned to construct a set of design questions aimed at facilitating the future development of household robots that are secure and preserve their users' privacy.

Author Keywords

Cyber-physical systems, domestic robots, household robots, multi-robot attack, privacy, robots, security, single-robot attack, ubiquitous robots.

ACM Classification Keywords

I.m. Computing Methodologies: Miscellaneous.

General Terms

Design, Human Factors, Security.

INTRODUCTION

The robotics industry is blossoming, with numerous academic and industrial endeavors focused on integrating robots into the home. The potential benefits are clear. Robots in the home could assist with chores, provide sources of entertainment, enhance telepresence, provide companionship, and assist with health and elder care. To the best of our knowledge, however, there is currently a marked void in the consideration of the security and privacy risks associated with household robotics. The need for such considerations is clear: future robots in the home could introduce new or amplify existing security and privacy risks for homeowners and other occupants. In many cases it may not be obvious how to overcome these security and privacy risks.

The purpose of this paper is to explore these potential security and privacy risks, identify the associated challenges, and present suggestions for overcoming these challenges. We argue that now is the ideal time to conduct such research, while the field of household robotics is comparatively young and before robots with serious and fundamental security flaws become ubiquitous.

Our exploratory research takes an approach common to other security and privacy papers that seek to provide foundations for new problem domains, e.g., [2, 16, 17, 20]. Specifically, we begin by experimentally analyzing the security and privacy properties of three representative examples of today's household robots. Our experiments inform our discussions regarding future robots. The robots we study are the WowWee Rovio, the Erector Spykee, and the WowWee RoboSapien V2. We obtained one of each robot in October 2008 and an additional RoboSapien V2 before December 2006.

Our experiments uncovered a number of vulnerabilities—some of which we deem to be quite serious, such as the possibility of an attacker compromising a Rovio or a Spykee and leveraging the built-in video camera to spy on a child in her bedroom. We synthesize these results into a survey of potential implications, lessons, and challenges for current and future robot owners. We then use the results of our experiments and the corresponding synthesis to develop a set of key questions for household robot manufacturers and researchers. We believe that these questions can aid in the informed design of future household robots that are secure and respect their users' privacy.

BACKGROUND

Household Robots: Today and Tomorrow

There is no universally accepted definition of what exactly constitutes a "robot." For this study, a *robot* is a cyber-physical system with sensors, actuators, and mobility. This definition excludes a class of cyber-physical systems whose environmental actuators are strictly electronic, such as an oven with electronically controlled heating elements. *Household (domestic) robots* are designed and priced for use within a home or other domestic environment.

Numerous approaches exist for categorizing current robots, such as the work done by Steinfeld *et al.* [25]. For our purposes, we classify the robots currently available for purchase in the U.S. market as belonging to one or more of the following categories: chore robots, communication robots, entertainment robots, and companion robots. These robots range from the well-known Roomba vacuum cleaner and the popular RoboSapien toy to the newly introduced Spykee and Rovio telepresence robots.

These robots exhibit a diversity in capabilities, although the capabilities of today's robots pale in comparison to the likely capabilities of household robots in 5 to 10 years. The axes of variations in robot capability include degree of mobility within the environment, dexterity, sensing capabilities (including audio and video), autonomy, and wireless communications (i.e., method and range).

Robots in the home will become increasingly sophisticated, capable, and ubiquitous, due in part to active innovation in both industry and academia and in part because of consumer demand. There is also rapid innovation in robotics outside of the home in industrial [9], medical [10], commercial [12], military [30, 31], and vehicular [6, 29] settings. As with other technologies, innovations developed for these settings will likely transfer to the home.

Additional Related Work

Some of the vulnerabilities and challenges that we discuss in this paper are instantiations of the general issues brought up by Edwards and Grinter [13]. Specifically, the problems introduced by household robots—both those that we encountered and those that we foresee—can be attributed partly to the fact that the home is becoming "accidentally" smart and that there is no dedicated, trained system administrator for the home environment.

Aside from the challenge of making them secure and privacy-respecting, household robots pose other unique challenges to robot manufacturers and researchers. For example, Young *et al.* consider the sociological challenges associated with integrating robots into domestic environments [34]. One such challenge is the perception of safety, which is related to security but is evaluated in a non-adversarial context. Indeed, safety has long been a critical concern in robotics [8]. In military environments, robotics researchers have considered systems for preventing unethical behavior in autonomous military robots capable of lethal force [4].

No discussion of robotic safety would be complete without a discussion of Asimov's seminal Three Laws of Robotics, which were introduced in [5] and explored in several subsequent collections and novels; however, researchers have since stated that these laws alone are not sufficient to govern robot behavior [1, 3, 11].

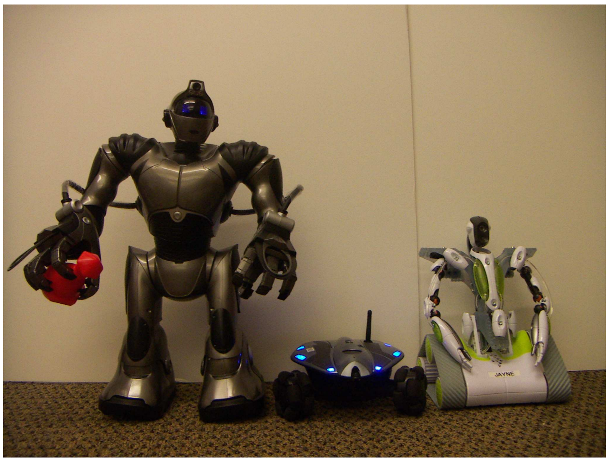


Figure 1. The WowWee RoboSapien V2 holding a toy bowling pin that came in its packaging (left), the WowWee Rovio (middle), and the Erector Spykee (right).

VULNERABILITIES IN CONTEMPORARY ROBOTS

As part of our investigation, we set out to determine the security levels of some of today's "state of the art" consumer household robots. We specifically chose robots that span key points along the aforementioned axes of robot capabilities (mobility, dexterity, sensing capabilities, and wireless communication method). Table 1 presents a summary of the capabilities of our experimental robots. These three robots are:

- **WowWee Rovio.**[1] The WowWee Rovio (Figure 1) is a mobile webcam robot that is marketed towards adults[2] for the purpose of remote communication and home surveillance. It has a video camera, a microphone, and a speaker. The Rovio can raise and lower its video camera "arm" and move in the horizontal plane. The robot is controlled via a web interface. The Rovio can be controlled wirelessly in one of three ways: via the robot's ad hoc wireless network; via the user's home wireless network, with the user co-located with the robot; and remotely via the Internet, with the Rovio receiving commands via the home wireless network (the router must be set up to forward ports correctly). The default robot account is not password-protected. The Rovio was introduced in late 2008.
- **Erector Spykee.**[3] The Erector Spykee (Figure 1) is a toy "spy" telepresence robot. It has a video camera, a microphone, and a speaker. The Spykee can only move in the horizontal plane. The user controls the robot using a program available for download on `spykeeworld.com`.[4] Like the Rovio, the Spykee can be controlled wirelessly

[1] Our Rovio shipped with firmware version UI v3.94 / Evo v4.7b.201. We experimented using this firmware version.

[2] From the FAQ: "Rovio is fun to drive but it isn't a toy. Rovio is a sophisticated mobile webcam that makes telepresence a reality."

[3] Our Spykee shipped with firmware version 1.0.22. We experimented using this firmware version.

[4] We ran our experiments using the Windows console software version 1.0.10.

	Rovio	Spykee	RoboSapien V2
Primary Audience	Adults	Children	Children
Primary Communication Mode	802.11 wireless	802.11 wireless	Infrared
Mobility Control	✓	✓	✓
Audio-visual Streams	✓	✓	—
Sensing Capabilities	High (Audio / Video)	High (Audio / Video)	Low
Output Capabilities	High (Audio)	High (Audio)	High (Audio)
Physical Capabilities	Low (Mobility)	Low (Mobility)	High (Gripping)
Advertised Price	$349.99 (USD)	$299.99 (USD)	˜$250 (USD)

Table 1. Comparing the characteristics of the robots chosen for our experiments.

in one of three ways: via the robot's ad hoc wireless network; via the user's home wireless network, with the user co-located with the robot; and remotely via the Internet, with the Spykee receiving commands via the home wireless network. A remote user can connect directly to the Spykee by explicitly specifying a hostname, or can rendezvous with the Spykee via `spykeeworld.com`. In the first case, the robot must be connected to the user's home wireless network and be reachable by external hosts on the Internet. In the second case, the robot must be set up to accept remote connections and be registered with `spykeeworld.com`, which functions similarly to a dynamic DNS service. The Spykee's default user account has a non-distinct password (`admin`), but the software requires that the user change the password before allowing remote access when rendezvousing via `spykeeworld.com`. A key difference between the Rovio and the Spykee is the intended user base, with the former intended largely for adults and the latter intended largely for children.[5] The Spykee was introduced in late 2008.

- **WowWee RoboSapien V2.** The WowWee RoboSapien V2 (Figure 1) is a popular toy for children and hobbyists. It is controlled via infrared and, given current technology, has good manual dexterity for its price. The RoboSapien V2 has several sensors, including an embedded color camera that it uses for tracking objects. The RoboSapien V2 is capable of some autonomous movement, but is primarily controlled using a remote control. The RoboSapien V2 was introduced in 2005; the original RoboSapien sold 1.5 million units in the first 5 months after its launch [33].

We purchased our three robots in October 2008 and used another RoboSapien V2 unit obtained before December 2006. Our goal was to obtain a high-level understanding of the security and privacy properties of today's household robots in order to draw inferences for the future. We did not explore all possible attack vectors—such as buffer overflow attacks—because our intention was to understand the general capabilities afforded to attackers by these robots, and the weaknesses we uncovered sufficiently enable attackers to achieve attacks of value. We summarize our findings for each robot in Tables 2 and 3. The following subsections describe our findings in more detail.

Remote Identification and Discovery

An adversary can remotely identify the presence of a Rovio or a Spykee with relative ease. There are two scenarios for remote identification: an attacker within wireless range of the robot's network who has the ability to intercept or inject wireless packets; and an attacker who can intercept or inject packets remotely over the Internet.

Under the first scenario, if the Rovio or the Spykee are in their default (ad hoc network) modes, remote identification is trivial; the SSIDs advertised by the robots are distinctive. If the robots are using infrastructure 802.11 wireless (i.e., the robots are connected to the user's home network) the robots' MAC addresses also leak information about their presence to wireless attackers.[6] This information is leaked even if the network is encrypted is using WEP, WPA, or WPA2.

A remote attacker can also determine the presence of a Rovio or a Spykee by actively probing the robot's home network. For example, a query to port 80 on the Rovio yields distinctive results. A Spykee can be detected by its response to remote control requests on TCP port 9001. Additionally, if a Spykee is set up to receive remote connections via `spykeeworld.com`, it periodically sends identifying keep-alive packets to `spykeeworld.com`.

Finally, because of the predictable and unique title and content in the Rovio's HTTP interface, we conjecture that—as the Rovios achieve greater market penetration—it will become possible to use search engines to remotely discover some Rovios, as has been previously demonstrated for webcams [7].

Passive and Active Eavesdropping

Rovio. A passive adversary able to intercept traffic to and from the Rovio is able to: (1) learn a username and password for accessing the Rovio when a user logs on (if set, which is not the default); and (2) intercept the RTSP audio-visual stream being transmitted to the user. The username and password are sent as unencrypted base-64 encoded values during authentication. Applying Wireshark and VLC to the RTSP audio-video stream, we learned that the audio uses (unencrypted) G.711 uncompressed audio and the video uses (unencrypted) MPEG4 or MJPEG encoding. We were able to capture a wireless trace from the Rovio's RTSP stream via

[5] The promotional video on the Spykee web site shows children using the product and the box shows a remote parent using the Spykee to talk to her children.

[6] Our Rovio has a MAC address beginning with `00:01:36` (CyberTAN) and our Spykee has a MAC address beginning with `00:1c:3d` (WaveStorm).

	Rovio	Spykee	RoboSapien V2
Wirelessly detectable by a local attacker	✓	✓	—
Detectable by a remote attacker	*	*	—
Wirelessly leaks login credentials on the home network			
In ad hoc mode	✓	✓	
In 802.11 infrastructure mode			
Accessed by local user	✓	✓	
Accessed by remote user	✓	—	
Acquire legitimate login credentials of a remote user with a MITM attack		✓	
Wirelessly leaks audio-visual stream on the home network			
In ad hoc mode	✓	✓	
In 802.11 infrastructure mode			
Accessed by local user	✓	✓	
Accessed by remote user	✓	—	
Eavesdrop on audio-visual stream of a remote user with a MITM attack		✓	
Audio-visual stream accessible if the robot is reachable			
With valid robot credentials	✓	✓	
Without valid robot credentials	✓	—	
Generates noise when moving	✓	✓	✓
Audible alert when users log on	—	✓[‡]	
Periodically generates noise when stationary	—	—	✓

Table 2. Summary of our findings on information leaked by the robot and other characteristics: yes/confirmed vulnerability (✓), under certain conditions (*), no/no found vulnerability (—). [‡]An attacker can interfere with the audio notification by lowering the robot's speaker volume immediately upon login.

Wireshark, reconstruct the video from that trace, and then view the video in VLC (see Figure 2). The login credentials and audio-visual stream of the robot were always unencrypted in our experiments, regardless of whether the robot is being accessed via its ad hoc network, locally via infrastructure 802.11, or remotely over the Internet.

Additionally, we found that the RTSP audio-visual stream of the Rovio does *not* require a username and password *even if* a password has been set on the Rovio interface. An attacker can use the following URI to access our Rovio's audio-visual stream, even when the user account is configured to "require" a password: `rtsp://our-rovio.cs.washington.edu/webcam`.

Spykee. The Spykee console software does a poor job of protecting the secrecy of account information in ad hoc mode and in local infrastructure 802.11 wireless mode (when the user is co-located with the robot); the software sends the login credentials to the robot in the clear. Furthermore, in these modes the video stream is encoded as an unencrypted MJPEG stream. To confirm this, we captured a trace of the video stream using Wireshark, reconstructed the video from the trace, and played the trace using VLC.

Intercepting data when the Spykee is being controlled by a remote user is more challenging because of the use of a Diffie-Hellman key exchange during connection initialization. However, the key exchange is unauthenticated and thus vulnerable to a man-in-the-middle (MITM) attack. We experimentally verified this vulnerability by opening the Spykee console application on one computer and (for experimental simplicity) initiating a connection from that computer to the hostname of our MITM attack machine. Our MITM attack machine then connected directly to the Spykee and emulated both ends of the Diffie-Hellman key exchange. Our attack program was able to extract sufficient login credentials to allow an attacker to subsequently initiate a new remote connection with the Spykee. The attack also allows an attacker to recover the session's audio-visual stream.

Operational Notifications

Rovio. The Rovio gives no auditory cue and only a minimal visual cue when a user logs on. The robot can broadcast an audio-visual stream any time it is on, including when docked on its home base. The Rovio has blue lights that indicate when it is powered on and the robot generates noticeable noise when moving.

Spykee. The Spykee does not broadcast an audio-visual stream when it is docked on its home base. The robot sounds chimes when someone logs on or when the robot is moved off of its base, although an attacker can quickly turn the robot's speaker volume down upon login to reduce the efficacy of this notification. There are minimal visual cues to indicate whether the Spykee is activated, but it generates noticeable noise when it moves.

RoboSapien V2. The RoboSapien V2 generates significant noise when it walks and makes occasional verbal exclamations.

Controlling the Robots

Rovio and Spykee. We were only able to control the Rovio and the Spykee using legitimate login credentials. As discussed in the subsection above on passive and active eavesdropping, an attacker can acquire legitimate login credentials in a number of ways, including: eavesdropping on the

	Rovio	Spykee	RoboSapien V2
Controllable			
By an attacker with line of sight and an off-the-shelf remote			✓
By a local attacker using an IR/RF repeater and an off-the-shelf remote			✓
By an attacker who can access the home network			
With valid robot credentials	✓	✓	
Without valid robot credentials	—	—	
By a remote attacker			
With valid robot credentials (if robot is configured for remote access)	✓	✓	
Without valid robot credentials	—	—	
Using remotely-accessible, compromised equipment (with an IR-transmitter) co-located with the robot			*
Can pick up and move small, lightweight objects	—	—	✓
Can push lightweight objects	✓	✓	✓

Table 3. Summary of our control capabilities: yes/confirmed (✓), not experimentally validated but conjectured possible (*), and not possible/no found vulnerability (—). See Table 2 for how to acquire valid robot credentials.

robot's ad hoc network; eavesdropping on a robot connected to infrastructure 802.11 wireless when the user is co-located with the robot; eavesdropping on a robot connected to infrastructure 802.11 wireless with a remote user (Rovio); and executing a MITM attack when a remote user attempts to connect to the robot (Spykee). If the robots or the network are configured to allow remote access, an attacker can control the robots from anywhere on the Internet. If the robots are in ad hoc mode or are not configured to allow remote Internet access an attacker can only control them if he has access to their home network.

Both the Rovio and the Spykee have limited physical capabilities, but can push light objects that are located on the floor.

RoboSapien V2. We experimentally analyzed the physical capabilities of the RoboSapien V2. The robot is able to reach objects on the floor and objects approximately 50 centimeters above the floor; this is sufficient to reach low objects on walls (such as electrical outlets) or on low surfaces such as coffee tables. The interior size of the RoboSapien's fist is approximately 1.5 centimeters when closed and 7.5 centimeters when open, suggesting rough upper and lower bounds on the size of graspable objects. It is difficult to achieve fine control with the robot, so lifting objects usually takes multiple trials. Additionally, the robot does not have enough manual dexterity to perform precise physical operations; for example, we were unable to successfully control the robot to light a match. We were able to have the robot pick up a set of keys; however, we were unable to use the RoboSapien to open door knobs. While the robot can grip the door knob and can lift a 250 gram object, its grip is not strong enough to open the door.

Network Security

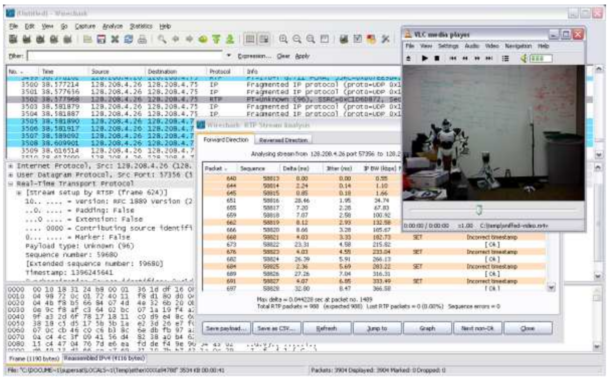
The Rovio and the Spykee can both connect to networks that are using WEP with 64-bit or 128-bit encryption. The Spykee can also connect to a network using WPA encryption, but the Rovio has no option to connect to a WPA network. We did not experiment with WPA2. A firmware update released by WowWee apparently adds support for WPA encryption, but we did not load this firmware onto our Rovio. We further note that networks using WEP encryption are vulnerable to cracking [14, 26], and weak WPA keys can be compromised via brute force attacks.

Additional Attacks

Many of our attacks could have been mitigated if these robots implemented conventional security best practices. Moreover, the majority of the vulnerabilities mentioned above become obsolete if the robot is connected to a wireless home network that is secure; however, we argue that it is still important to consider these robots as compromisable for two reasons. First, the supposition that the robot is secure is based upon the assumption that users will correctly configure and administer secure encryption on their networks. Additionally, while in one scenario the attacker is a stranger who does a "drive-by" on the neighborhood, in another scenario the attacker is a neighbor who has an extended period of time over which he can crack the user's wireless network. The second reason that we consider the robots' security to be suspect is that the technical directions we explore above are a subset of the full range of potential attacks. For example, we did not evaluate the vulnerability of the Rovio and Spykee to buffer overflow attacks. Such attacks would be more concerning—and more attractive to attackers—if the robots in question were not already vulnerable to more basic attacks. Anecdotal evidence in other contexts also suggests that such attacks are notoriously difficult to defend against in full. Experimenting with these additional attacks was not necessary for the purpose of drawing the overall conclusions that we present in the following sections.

SYNTHESIS AND IMPLICATIONS OF VULNERABILITIES

We now synthesize and reflect upon the results of our experimental analyses. Our goal is to identify key issues and challenges for developing secure and privacy-respecting household robots. The robots we studied, while sophisticated by today's standards, pale in comparison to the types of robots we may see deployed over the next 5 to 10 years. We therefore broaden our discussion to include potential implications for future household robots.


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
VLC media player
File View Settings Audio Video Navigation Help
Wireshark: RTP Stream Analysis
Forward Direction
Reversed Direction
Save payload...
Save as CSV...
Refresh
Jump to
Graph
Next non-Ok
Close
Frame (1190 bytes)
Reassembled IPv4 (4116 bytes)

```
No. -  Time        Source        Destination   Protocol  Info
3500 38.577214 128.208.4.26 128.208.4.75 IP   Fragmented IP protocol (proto=UDP 0x1
3501 38.577656 128.208.4.26 128.208.4.75 IP   Fragmented IP protocol (proto=UDP 0x1
3502 38.577968 128.208.4.26 128.208.4.75 RTP  PT=Unknown (96), SSRC=0xC1D6D872, Sec
3503 38.581879 128.208.4.26 128.208.4.75 IP   Fragmented IP protocol (proto=UDP 0x1
3504 38.581887 128.208.4.26 128.208.4.75 IP   Fragmented IP protocol (proto=UDP 0x1
3505 38.581890 128.208.4.26 128.208.4.7
3506 38.581917 128.208.4.26 128.208.4.7
3507 38.589092 128.208.4.26 128.208.4.7
3508 38.609901 128.208.4.26 128.208.4.7
3509 38.616514 128.208.4.26 128.208.4.7
```

```
⊞ Internet Protocol, Src: 128.208.4.26 (128.
⊞ User Datagram Protocol, Src Port: 57356 (5
⊟ Real-Time Transport Protocol
  ⊞ [Stream setup by RTSP (frame 624)]
    10.. .... = Version: RFC 1889 Version (2
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifi
    0... .... = Marker: False
    Payload type: Unknown (96)
    Sequence number: 59680
    [Extended sequence number: 59680]
    Timestamp: 1396245641
```

```
0000  00 10 18 31 24 b8 00 01  36 1d df 16 0
0010  04 98 72 0c 01 72 40 11  f8 d1 80 d0 0
0020  04 4b f8 b5 66 84 07 4d  4e 32 6b 20 0
0030  0e 9c f8 af c3 64 02 bc  07 1a 19 f4 a
0040  9f a3 2d 6f 78 17 18 11  c0 d9 e4 8c 0
0050  38 18 c5 d5 17 5b 5b 1a  e2 3d 26 e7 f
0060  07 0c cb 46 c0 c6 b3 8c  6e db fb 97 a
0070  0a c4 4c 3f 09 41 56 d4  82 38 a0 b4 6
0080  15 c4 47 04 76 7d e6 ea  fd de f4 9e 9
```

Analysing stream from 128.208.4.26 port 57356 to 128.2

Packet	Sequence	Delta (ms)	Jitter (ms)	IP BW (kbps)		
640	58813	0.00	0.00	0.55		
644	58814	2.24	0.14	1.10		
645	58815	0.85	0.18	1.66		
651	58816	28.46	1.95	34.74		
655	58817	7.20	2.28	67.83		
659	58818	7.07	2.58	100.92		
662	58819	8.12	2.93	132.58		
666	58820	8.66	3.28	165.67		
668	58821	4.03	3.33	182.73	SET	Incorrect timestamp
673	58822	23.31	4.58	215.82		[Ok]
676	58823	4.03	4.58	233.04	SET	Incorrect timestamp
682	58824	26.39	5.91	266.13		[Ok]
684	58825	2.36	5.69	283.22	SET	Incorrect timestamp
689	58826	27.26	7.04	316.31		[Ok]
691	58827	4.07	6.85	333.49	SET	Incorrect timestamp
697	58828	32.80	8.47	366.58		[Ok]

Max delta = 0.044228 sec at packet no. 1489
Total RTP packets = 988 (expected 988) Lost RTP packets = 0 (0.00%) Sequence errors = 0

0:00:00 / 0:00:00 x1.00 C:\temp\sniffed-video.m4v

File: "C:\DOCUME~1\supersat\LOCALS~1\Temp\ether0000a04788" 3534 KB 00:00:41 Packets: 3904 Displayed: 3904 Marked: 0 Dropped: 0

Figure 2. Reconstructing the Rovio's video stream by capturing packets in Wireshark.

Possible Attacks

To ground the subsequent discussions, we first survey a set of attacks that are made possible by the vulnerabilities discussed in the previous section. This list is not meant to be exhaustive, but rather illustrative of the diversity of attacks possible. We augment these attacks with additional attacks in the "multi-robot attacks" section below.

- *Robot vandalism.* An attacker can exploit the vulnerabilities of the Rovio or the Spykee to damage fragile objects in the surrounding environment. Previous work has demonstrated that owners can be concerned about potential property damage caused by the Roomba [15]. Since the Rovio and the Spykee are not autonomous, homeowners may not take the same precautions to remove fragile objects from the environment. While these robots do not have sufficient power to knock objects off of a table, similar robots in the future could have this strength; as a result, they could potentially create safety hazards in the environment. For example, if a robot knocks a bowl of grapes off of a coffee table, this presents a choking hazard for toddlers. Additionally, even a weak robot could push a fragile object down a flight of stairs, causing more damage than would be possible directly from its own actuation capabilities. Finally, damage to the robot itself is another special case of robot vandalism: depending on a robot's capabilities, an attacker could cause "robot suicide" by causing the robot to tumble down a flight of stairs or jump out a window.

  A robot with limited strength but some dexterity–such as the RoboSapien V2—could hide or otherwise move objects or throw objects into the trash or toilet.

- *Spying on homes (Rovio); spying on children (Spykee).* The Rovio and the Spykee both create privacy vulnerabilities within the home. The "always on" nature of the Rovio—due to its usage model as a home surveillance robot—means that there may be greater overall opportunities for an attacker to exploit the Rovio to spy on a home. Potential malicious uses of the Rovio could be to eavesdrop on private conversations, determine whether someone is home, or take embarrassing or compromising photographs.

  The Spykee's intended use as a toy for children creates a complementary set of concerns: compromising a Spykee allows an attacker to watch a child in potentially private locations, such as her bedroom. The problem with video cameras in children's rooms has been discussed before in the context of Nanny Cams [24]. A key difference here is that the Spykee is a mobile camera, which gives an attacker more flexibility than a traditional webcam. A second key difference is that the Spykee is designed to be administered by children, not their parents.

- *Eldercare.* The Rovio is partially aimed toward buyers who have responsibilities towards people who need special supervision.[7] This usage model provides insight into possible future attacks in the burgeoning field of robotic eldercare [23, 28, 35] and the associated area of childcare. The abilities that make the Rovio useful for "visiting elderly relatives" may also make it possible to harm those relatives. The Rovio could be used to trip an elder with limited stability and mobility, particularly if the elder has impaired hearing and cannot notice the Rovio approaching. Additionally, the Rovio could be used to play noises and speech that might confuse someone with dementia.

- *Psychological attacks.* Thinking further afield, we suggest some potential psychological attacks that could leverage compromised robots. Previous works have identified that humans can form an emotional bond with a robot [19, 27]. There have also been investigations into using robots to help children with conditions like autism [22]. An attacker, perhaps the mean kid down the block, can potentially exploit this bond and any vulnerabilities in a child's robot to cause psychological damage to the child.

  A related attack could take advantage of the Spykee's role as a telepresence robot. An attacker could hijack the audio capabilities to cause distress to a child.

  Other forms of psychological attacks are also possible, such as using a robot to arrange objects on the floor into a threatening or offensive symbol or constantly chasing the family dog during the day when the homeowner is away.

We view many of the above implications as serious considering the robots of today, and even more serious in the context of the household robots of tomorrow. Other threats, while arguably less likely to manifest today, highlight the diversity of attacks possible. In the following subsections we discuss broader lessons and challenges for securing household robots.

Multi-Robot Attacks

While we already view the above classes of single-robot attacks as serious, our experimental results uncover a separate set of issues which are even more challenging to overcome. Namely, even in the cases where a robot may operate safely and securely in isolation, it may facilitate attacks when used in conjunction with other robots.

[7] From `http://www.meetrovio.com/`: "Interact with your family, wherever they are"; "Check up on your office and speak with colleagues"; "Roam around your home to check on pets, etc."; and "Visit elderly relatives."

Consider, for example, the RoboSapien V2: we were unable to perpetrate any meaningful attacks using only the RoboSapien. Some of our difficulties were due to the limitations imposed on the robot's strength and dexterity by current technology. We can expect these barriers to be lowered as innovations make advanced actuators more affordable and more capable. Some of the obstacles that we encountered, however, are more central to the robot's design: for example, the RoboSapien is not designed to expose its camera interface to users and, indeed, has no way to transmit a visual stream without hardware modifications. Recall the comparison of our robots' capabilities given in Table 1: both the Spykee and the Rovio—neither of which have any manual dexterity—are capable of broadcasting audio-visual streams to remote viewers. We observe that an adversary may be able to take advantage of the selection of robots available in a household in order to acquire a complementary set of attack capabilities.

Example compound attack: Enabling duplication of physical keys. We used the Rovio and the RoboSapien to experimentally evaluate the feasibility of a multi-robot, compound attack. This example attack is targeted at enabling the reproduction of physical keys.

This attack is performed by coordinating four devices: a compromised Rovio, an uncompromised RoboSapien V2, the remote control for the RoboSapien V2, and an infrared repeater. The attacker uses the remote and repeater to issue commands to the RoboSapien from a distance. This allows him to control its movements, while the Rovio is maneuvered to provide a view of the RoboSapien and the environment. The RoboSapien can be used to pick up keys from the floor or a low table; they can held such that the Rovio can obtain a clear picture of one or more of the keys (our setup is shown in Figures 3 and 4). This picture can then be used to make physical copies of the keys [21]. We experimentally demonstrated the feasibility of this attack scenario in our lab, although we did not use the work of Laxton et *al.* to produce a key.

Given the capabilities of our robots, this attack would not be possible without using multiple robots in conjunction. Additional multi-robot attacks are possible, including attacks that leverage other compromised devices; for example, while our attack above can be executed using an infrared repeater that is positioned ahead of time, the attack would be much more flexible if it could exploit a compromised home computer with an infrared port, a universal remote control with 802.11 wireless, or another robot with the ability to transmit infrared.

Multi-robot attack scenarios are particularly challenging to thwart because they are outside the normal scope of security and safety considerations. Even if a robot manufacturer carefully considers the safety and security implications of its particular model and makes design decisions to mitigate those risks, the robot may still pose a security hazard when deployed in an environment with other robots.

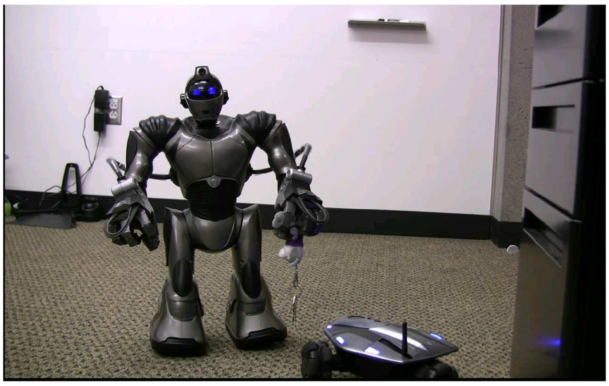


Figure 3. The RoboSapien holding a set of keys in front of the Rovio.

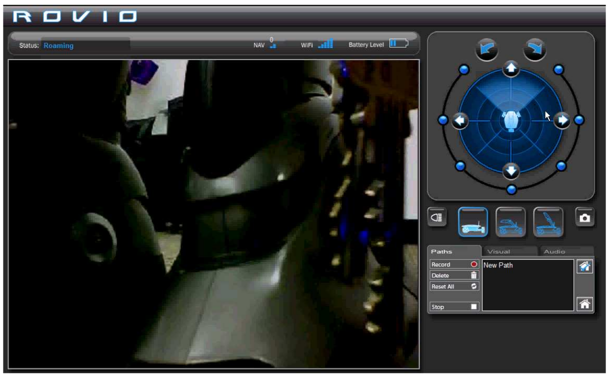


Figure 4. A screenshot of the Rovio's video stream from the same experimental trial as in Figure 3.

The People and the Environment

"Chaotic" environments; diverse stakeholders. We observe that household environments potentially contain a diverse group of stakeholders: residents, guests, parents, children, infants, the elderly, people with mental and physical impairments, and pets. This suggests that household robots may be deployed in chaotic environments, where a robot that is "misplaced" by an attacker might not be noticed. Even more fundamentally, manufacturers either need to design robotic systems with all of these potential stakeholders in mind or clearly indicate to consumers that these systems are not safe and secure in all environments. As a simple example, even if the Rovio provided auditory notifications to indicate when it is being accessed, those notifications might not suitably inform a person with impaired hearing.

Stakeholder perceptions and expectations. Another challenge with securing household robots is ensuring compatibility with users' expectations and mental models. Users have a basic understanding of the safety tradeoffs involved in the use of common household items such as vacuums, toasters, and ovens. The household robot is a new class of appliance, and as a result users will either have incorrect preconceptions about its security properties or they will have no convenient point of reference from which to understand the robot. Designers will either need to create products that coexist with users' (and indirect stakeholders') current mental models, create products that are so intuitive to use that a new (correct) mental model is easily formed, or integrate a "crash training course" into the robotic system. We note, however, that training users in the use of security technologies and concepts has traditionally been met with mixed success [32].

Metrics and Evaluation Criteria

Our investigations suggest that there may be some challenges to securing robots for the home environment and even greater obstacles to communicating security threats and tradeoffs to consumers. These two factors suggest the need to establish metrics and minimum criteria for household security and privacy, akin to the other classes of metrics already proposed for robots (e.g., [25]). Such systems will be useful both for manufacturers seeking to provide high-quality, security-conscious products, as well as for researchers developing new approaches for meeting these security goals. We contribute to this effort by providing a series of questions in the following section to guide the development and evaluation of secure household robots.

Along the same lines, we suggest that consumers could benefit from access to evaluations of household robots' security properties. For example, Consumer Reports publishes reviews and grades for a number of household products. In the case of automobiles, Consumer Reports also supplies a safety rating. A similar grading system could be applied to inform consumers of the security properties of robot products, particularly when those robots are likely to come into contact with children. Another potential direction is to introduce legislative oversight for the security and privacy of domestic cyber-physical systems. Such oversight, if well executed, could help prevent the introduction of high-risk robots and other cyber-physical systems into home environments.

SECURITY AND PRIVACY DESIGN QUESTIONS

We propose a set of questions that expose issues that designers and researchers should consider in the course of developing secure and privacy-respecting household robots. Our formulation of these questions is akin to the formulation of questions underpinning Hong *et al.*'s model for privacy in ubiquitous computing [18].

Social, Environmental, and Technical Questions

We begin by identifying a set of questions capable of isolating key social, environmental, and technical properties of the robot in question.

What is the intended function of the robot? The intended function of the robot goes a long way towards identifying the robot's range of mobility, actuators, and sensors, as well as the environments in which the robot works and the people with whom the robot will interact. All these properties play a critical role in security since they indicate the range of assets that can be affected if an adversary compromises the robot.

How mobile is the robot? A robot's degree of mobility may give it access to new, unforeseen environment types with assets that are not sufficiently protected against the robot. Additionally, a robot's mobility enables it to bring together environmental elements that may be intentionally separated: for example, embers in the fireplace and flammable drapes.

What actuators does the robot possess? The actuators will dictate what physical assets the robot can affect and the ways that it can physically assist in an attack scenario. Does the robot have fine manual dexterity, allowing it to manipulate switches and open doors and cabinets? Do the robot's joints and motors allow it to throw projectiles? Does the robot have the proper leverage and generate enough force to move heavy objects? For example, our RoboSapien V2 was able to manipulate small, lightweight objects such as a set of keys, but was unable to open doors or light matches.

What sensors does the robot possess? The sensing capabilities of a robot dictate the kinds of information that the robot can gather. Audio-visual data in the home environment are frequently sensitive in nature. Both our Rovio and our Spykee have a microphone and a camera with which to perceive their environment, creating potential privacy leaks.

What communication protocols does the robot support? The communication protocols that the robot supports, such as infrared or 802.11 wireless, will dictate what other devices the robot can potentially control, what other devices can potentially control the robot, and the ways in which the robot can transmit information to an external agent. Our RoboSapien V2 was more resistant to external control than our other robots due to the fact that it is controlled via infrared.

Who are the intended users of the robot? Vulnerabilities may arise from unique interactions between the users' characteristics and the robot's usage model. For example, non-expert users may try to configure the robot's settings in an insecure fashion, so it is important to consider the training and prior experience users might have with the system. The physical and mental capabilities of users also require consideration, since they can introduce dangerous situations or diminish the user's ability to react to a potentially dangerous situation.

What is the robot's intended operational environment? The robot's intended environment will play a large role in dictating the assets to which the robot has access. Is the robot intended for use in the communal area of the home? A kitchen with knives? A bedroom? The answers to these questions may indicate valuable information, such as whether the robot operates in proximity to children or objects of personal and financial value.

Besides the intended users of the robot, what other people (and animals) will be in the the robot's environment? The robot's intended environment dictates the people and animals around which the robot will perform its tasks. The robot should respect the safety and privacy of these indirect stakeholders, regardless of whether or not these people intend to use the robot. The same questions that apply to users should apply to family members and visitors. As for animals, a designer should consider how they might react to the robot and whether their presence can introduce some new hazard.

What kind of development processes are in place? Do the overall development processes used in the robot's design and manufacture take security and privacy goals into consideration? Are any third-party software or hardware components used on the robot, and if so, how are they evaluated? Can software, hardware, or firmware upgrades disable security features or introduce unintended, malicious robot behaviors?

Security and Privacy Questions

We next provide a core set of questions to identify how the robot's properties might affect the security and privacy of users and their property. While some of the threats—such as breaches of privacy—are common to many ubiquitous computing applications, the remaining questions address threats that are more particular to robots positioned in the home environment.

Does the robot create new or amplify existing privacy vulnerabilities? Might an attacker be able to use the robot's audio-visual capabilities to obtain private data about a person or a location? The home is considered to be a private area; any information obtained from within the home—without the residents' knowledge or permission—is confidential information.

Does the robot create new or amplify existing physical integrity vulnerabilities? Can an attacker use the robot to target a user's valued possessions? Can an attacker use the robot to breach the physical perimeter of the building? Vandals might use a robot to cause direct physical damage to property, while a thief might use a robot to unlock a door or open a window to facilitate a burglary.

Does the robot create new or amplify existing physical safety vulnerabilities? Cyber-physical systems such as household robots have the potential to cause harm to people's health in several ways: by neglecting to perform an essential task, such as moving an impaired person or dispensing medication; by causing direct physical harm to a person; or by manipulating the environment to cause physical harm to a person, via either small actions like moving furniture to create a trip hazard or large actions like setting the house on fire. It is important to consider how the robot might be co-opted to cause physical harm to its surroundings.

Does the robot create new or amplify existing psychological vulnerabilities? Is there some way that the robot can be used to cause a person emotional harm? Prior works indicate that users can develop emotional bonds with robots [19, 27], which could potentially be exploited.

Can the robot be combined *with other robots or technologies to facilitate an attack?* Considering what other robots might be in the robot's deployment environment, can this robot participate in a multi-robot attack? How can those attacks be anticipated and addressed?

CONCLUSIONS

Commercial robots such as the Roomba already have a significant presence in residential homes. In the future we can expect a greater number of increasingly sophisticated robots to be used in the home for diverse tasks including chores, communication, entertainment, and companionship. We performed an experimental investigation of three current household robots—the WowWee Rovio, the Erector Spykee, and the WowWee RoboSapien V2—and found that robots already introduce security vulnerabilities into the home. Creating household robots that are secure is a challenging undertaking for several reasons: multi-robot homes may face increased security risks, since even a robot that is designed to be secure in isolation may be vulnerable to participating in a compound attack; the typical household is a dynamic environment that is filled with many entities, including non-expert users, children, elderly people, and pets; and it is difficult to deem systems secure without any standardized point of reference. The paper concludes with of a set of questions aimed at informing the future design and evaluation of secure and privacy-respecting household robots.

Acknowledgments

We thank Tim Kindberg for shepherding this paper. We thank Hal Perkins for loaning us equipment. We thank Shwetak Patel and the anonymous reviewers for their input and feedback. Joshua R. Smith is with Intel Labs Seattle. This work was supported in part by NSF Awards CNS-0722000, CNS-0722004, CNS-0846065, and an Alfred P. Sloan Research Fellowship.

REFERENCES

1. R. Aiken and R. Epstein. Ethical Guidelines for AI in Education: Starting a Conversation. *Intl. Journal of AI in Education*, 11, 2000.

2. R. Anderson, P. Street, and M. Kuhn. Tamper Resistance – a Cautionary Note. In *Proc. 2nd USENIX Workshop on Electronic Commerce*, 1996.

3. S. Anderson. Asimov's "Three Laws of Robotics" and Machine Metaethics. *AI & Society*, 22(4), 2008.

4. R. Arkin. Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. In *Proc. of the 3rd Intl. Conf. on Human Robot Interaction,* 2008.

5. I. Asimov. *I, Robot*. Gnome Press, 1950.

6. A. Bacha, C. Bauman, R. Faruque, M. Fleming, C. Terwelp, C. Reinholtz, D. Hong, T. Alberi, D. Anderson, S. Cacciola, et al. Odin: Team VictorTango's entry in the DARPA Urban Challenge. *Journal of Field Robotics*, 25(8), 2008.

7. J. Billig, Y. Danilchenko, and C. Frank. Evaluation of Google Hacking. In *Proc. of the 5th Conf. on Information Security Curriculum Development*. ACM New York, NY, USA, 2008.

8. M. Bonney and Y. Yung. *Robot Safety*. IFS Publications, Springer-Verlag, Berlin, 1985.

9. D. R. Butcher. Invasion of the Robots in (Factory) Space, August 2006. `http://news.thomasnet.com/IMT/archives/2006/08/state_of_industrial_robots_in_plants_factories_forcast_trend.html`.

10. Y. Choi, J. Gordon, and N. Schweighofer. ADAPT – Adaptive Automated Robotic Task Practice System for Stroke Rehabilitation. In *IEEE Intl. on Conf. Robotics and Automation (ICRA)*, 2008.

11. R. Clarke. Asimov's Laws of Robotics: Implications for Information Technology, Parts 1 and 2. *IEEE Computer*, 1993.

12. Digital Chosun. 'Thinking' Robot Breaks Barriers but not Eggs, 2007. `http://english.chosun.com/w21data/html/news/200511/200511150007.html`.

13. W. Edwards and R. Grinter. At Home with Ubiquitous Computing: Seven Challenges. In *Proc. of the 3rd International Conference on Ubiquitous Computing (Ubicomp 2001)*, pages 256–272, 2001.

14. S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key schedule algorithm of RC4. In *Proc. 4th Workshop on Selected Areas of Cryptography*, 2001.

15. J. Forlizzi. How Robotic Products Become Social Products: an Ethnographic Study of Cleaning in the Home. *ACM SIGCHI/SIGART Human-Robot Interaction*, 2007.

16. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proc. of the IEEE Symposium on Security and Privacy*, 2008.

17. T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. Ohare. Vulnerabilities in First-Generation RFID-enabled Credit Cards. In *Proc. of Eleventh Intl. Conf. on Financial Cryptography and Data Security*, February 2007.

18. J. Hong, J. Ng, S. Lederer, and J. Landay. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In *DIS '04: Proc. of the 5th Conf. on Designing Interactive Systems*, Cambridge, MA, USA, 2004. ACM.

19. C. Kidd and C. Breazeal. Designing a Sociable Robot System for Weight Maintenance. In *IEEE Consumer Communications and Networking Conference. Las Vegas, NV: IEEE*, 2006.

20. T. Kohno, A. Stubblefield, A. Rubin, and D. Wallach. Analysis of an Electronic Voting System. In *IEEE Symposium on Security and Privacy*, 2004.

21. B. Laxton, K. Wang, and S. Savage. Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding, October 2008.

22. C. Liu, K. Conn, N. Sarkar, and W. Stone. Affect Recognition in Robot Assisted Rehabilitation of Children with Autism Spectrum Disorder. In *Proc. of the 15th IEEE Intl. Conf. on Robotics and Automation*, 2006.

23. T. Mukai, M. Onishi, T. Odashima, S. Hirano, and Z. Luo. Development of the Tactile Sensor System of a Human-Interactive Robot "RI-MAN". *IEEE Transactions on Robotics*, 24(2), 2008.

24. J. Schwartz. Nanny-Cam May Leave a Home Exposed. *The New York Times*, April 2002.

25. A. Steinfeld, T. Fong, D. Kaber, M. Lewis, J. Scholtz, A. Schultz, and M. Goodrich. Common Metrics for Human-Robot Interaction. In *Proc. of the 1st ACM SIGCHI/SIGART Conf. on Human-Robot Interaction*. ACM New York, NY, USA, 2006.

26. A. Stubblefield, J. Ioannidis, and A. Rubin. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In *Proc. of the 2002 Network and Distributed Systems Security Symposium*, volume 1722, 2002.

27. J. Sung, L. Guo, R. Grinter, and H. Christensen. "My Roomba Is Rambo": Intimate Home Appliances. *Proc. of UbiComp 2007*, 2007.

28. A. Tapus, M. Mataric, and B. Scassellati. The Grand Challenges in Socially Assistive Robotics. *IEEE Robotics and Automation Magazine*, 14(1), 2007.

29. S. Thrun, M. Montemerlo, H. Dahlkamp, D. Stavens, A. Aron, J. Diebel, P. Fong, J. Gale, M. Halpenny, G. Hoffmann, et al. Stanley: The robot that won the DARPA Grand Challenge. *Journal of Field Robotics*, 23(9), 2006.

30. D. Voth. A new Generation of Military Robots. *IEEE Intelligent Systems*, 19(1), 2004.

31. P. Warren. Launching a New Kind of Warfare. *The Guardian*, October 2006.

32. A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium*, 1999.

33. Wikipedia. WowWee Robotics home page. `http://en.wikipedia.org/wiki/Wowwee`.

34. J. Young, R. Hawkins, E. Sharlin, and T. Igarashi. Toward Acceptable Domestic Robots: Applying Insights from Social Psychology. *Intl. Journal of Social Robotics*, 2008.

35. Yuri Kageyama. Invention that may have far-reaching benefits for the disabled and elderly. Associated Press, 2009. `http://www.msnbc.msn.com/id/27066773/`.