Domestic robots: a case study on security in ubiquitous computing

Ubiquitous computing seminar FS2014
Student report

Thomas Knell
ETH Zurich
knellt@student.ethz.ch

ABSTRACT

The purpose of this essay is to look at the existing publications about domestic robots. Specifically those which are about security and privacy concerns and find possible reasons for the lack of papers in this research area.

INTRODUCTION

The industry as well as the academic world seem so agree that robots will become an integral part of our daily lives in the near future. Much of the early work on robotics focused on building industrial robots where robots helped automate parts of the manufacturing process. A more recent trend is that robots start appearing in households performing tasks such as cleaning windows, mowing lawns or cleaning floors (Figure 1).

Figure 1: iRobot Roomba 560 Vacuum Cleaner [14].

Robots like these have very specific tasks and can perform those tasks well, but generally don't offer a great set of interfaces to control/access them. Due to that fact, these kinds of robots are not very likely to be targets of potential attacks.

We can assume that more sophisticated robots like the PR2 robot (Figure 2), which for example can be told via web-interface to go grab a beer in the fridge and bring it to a certain location, will be used in household at some point in the future. An unauthorized entity being able to take over control of such a robot with its multiple sensors, actuators and mobility could cause serious harm. For this reason it is imperative to take security and privacy consideration into account when building such systems.

Figure 2: Willow Garage PR2, Robot for Research and Innovation [15].

Two papers addressing security and privacy in the context of robots, i.e. [1, 2] both from 2009, mention in their respective introductions that, according to them, there is a surprising lack of research done in this area. Five years later and there are still very little research papers devoted to this specific area of research.

BACKGROUND

In this section we introduce some general concepts needed for the later parts of this essay.

Domestic Robots

There exists no single definition of "robot" that satisfies everyone. Joseph Engelberger, a pioneer in industrial robotics, once made the remark: ”I can’t define a robot, but i know one when I see one.” A bit more concrete is the definition of the Encyclopaedia Britannica a robot is ”any automatically operated machine that replaces human effort, though it may not resemble human beings in appearance or perform functions in a humanlike manner.” And as a last example the definition used by [2], a robot is ”a cyber-physical system with sensors, actuators, and mobility.”

Network Security

Some contemporary robots are already able to join or create networks to communicate with other entities. This capability will only gain in importance in the future as robots in the home will become increasingly sophisticated, capable and ubiquitous. To understand certain risks and possible vulnerabilities caused by robots joining/creating networks to communicate, some terms and knowledge about network security is required. In this section we give a brief introduction to this subject.

The following three basic security goals are discussed and referred to as ”CIA”: [6]

- **Confidentiality.** Information should be accessible only to those authorized to see it. For example, the goal of a network sniffing attack is to violate confidentiality.
- **Integrity.** Information should not be modified without appropriate authorization. For example, the state of a database or an on-line banking system should be changed only by legitimate transactions.
- **Availability.** Information and systems should be available when needed. For example, the goal of a denial-of-service attack is to violate availability.

While useful as a guideline, this classification is quite simplistic, as it does not cover a number of security goals discussed below.

- **Authenticity.** Typically used in the sense that a message or other piece of information originates from the claimed (or believed) entity.
- **Non-repudiation.** Impossibility to inappropriately deny a transaction or having sent a message.
- **Auditability.** Ability to reconstruct (certain aspects of) earlier states of a system.
- **Accountability.** Ability to hold an entity accountable for its actions. This is related to non-repudiation and auditability.
- **Privacy.** There is no clear definition of the term privacy, but it basically refers to the security of personal information. Privacy means that a person has appropriate control over which information on him or her is generated, stored, processed, and deleted, and by whom.
- **Anonymity.** The identity of an entity is hidden. Anonymity is an aspect of privacy.

VULNERABILITIES IN CONTEMPORARY ROBOTS

In this section we look at some results from [2], where the authors investigated the security levels of some of the at that time ”state of the art” consumer household robots, including the WowWee Rovio and the Erector Spykee. The authors describe the two robots as follows:

(a) WowWee Rovio [16]

(b) Erector Spykee [17]

Figure 3: Examples of contemporary robots

- **WowWee Rovio.** The WowWee Rovio (Figure 3a) is a mobile webcam robot that is marketed towards adults for the purpose of remote communication and home surveillance. It has a visual camera, a microphone, and a speaker. The Rovio can raise and lower its visual 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.** The Erector Spykee (Figure 3b) is a toy ”spy” telepresence robot. It has a visual 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`. Like the Rovio, the Spykee 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 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. The Spykee was introduced in late 2008.

The authors did not explore all possible attack vectors but rather focused on two instances of attacks, *remote identification and discovery* and *passive and active eavesdropping*,

	Rovio	Spykee
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	–	✓[‡]

Table 1: Summary of 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.

each of them in three different scenarios. First the robots are in their default (ad hoc network) modes, in the second scenario the robots are connected to the user's home wireless network (not password protected) and finally when connecting to the robots over the internet. The results are summarized in Table 1 and discussed in more details in the following subsections.

Remote Identification and Discovery

For an adversary it is possible to determine the presence of a Rovio or Spykee with relative ease.

If the Rovio or the Spykee are in the ad hoc network mode, an attacker has to be in range of the network. If that is the case, remote identification is trivial, since the SSIDs advertised by the robots are distinctive.

In the second scenario where the robots joined the user's (unprotected) home wireless network, an attacker can observe the MAC addresses used in the network. MAC addresses leak information, i.e. the name of the company that manufactured the device's network card.

In the first two cases the same methods worked for both robots. In the case where the attacker is remote, the methods to identify the two robots are slightly different. In the case of the Rovio, a port scan will yield a distinctive result for port 80. A Spykee can be detect by its response to remote control request on TCP port 9001. Additionally, if a Spykee is set up to receive remote connections via `spykeeworld.com`, it sends identifying keepalive packets to `spykeeworld.com` periodically.

Remote discovery may not seem to be an overly concerning issue at first, even though it clearly violated the security goal of privacy. But in combination with the vulnerabilities described in the following subsection it is a major threat.

Passive and Active Eavesdropping

Both the Rovio and the Spykee do not encrypt any of their traffic in ad hoc network mode nor in the case where they are part of the user's home wireless network. The user credentials, the audio-visual stream and any commands sent to the robot are all sent in the clear.

This means that an adversary can eavesdrop on the communication between user and robot. If during that time the user credentials are sent, the attacker will be able to take over full control of the robot. But even if the attacker starts eavesdropping after the user has logged in, if the user is watching the audio-visual stream, the attacker can watch it as well. In the case of the Rovio the situation is even worse, since the audio-visual stream is accessible at a static URL without needing username and password.

Even if the Rovio is accessed over the Internet, the communication is not encrypted. In this case the Spykee is doing a better job of protecting the secret account information and actually encrypts the communication. However during connection initialization the Diffie-Hellman protocol – used for key exchange – is not authenticated and is therefore vulnerable to a man-in-the-middle (MITM) attack.

Combining remote discovery with the just described vulnerabilities, attackers could easily launch large scale attacks if such robots were more common is households. Looking at the list of network security goals, attackers would be able to violate every one of them. The authors of [2] then describe some possible attacks that are made possible by the vulnerabilities, including robot vandalism, spying on homes and psychological attacks.

While these attacks are worrisome and certainly real, as two incidents [9, 10] from 2013 and 2014 show, where in both cases a hacker took over control of a baby monitor, but the main goal has to be preventing attackers from getting access to such system

MECHATRONIC SECURITY AND ROBOT AUTHENTICATION

Whereas the previous section focused on a paper concerned with finding security related vulnerabilities in contemporary robots, this section is about a paper [1] on how to potentially improve security of future robots.

In particular robot identification and security mechanisms which fit to robot technologies and their operating environment are of interest. To secure transactions between robots, they have to be securely identified "as persons" with unique provable identities. This is achieved with a sort of "Electronic mutation" technology.

Requirements for Secured Robot Identity

The author of [1] proposes the following security requirements which should be considered for designing robot identification technology, though the catalog can be extended and reduced depending on the robot's nature and its operation environment.

1. The robot identity should be unique and provable
2. Generating the same identity (cloning) should be technically impossible without great invasive attack. Even then the system should detect successful cloning attacks and resolve it. In other words the system security should be stable, robust and resilient.
3. Authenticity proof linked to robot identity should diffuse in each robot action when required.
4. Proof of identity should be scalable in a sense that many identification certainty levels and varieties can be deployed on demand similar to identifying persons in a living society.
5. The identity should exhibit and develop time variant components and evolutionary aspects as those of persons in real social environment.
6. Trust and identification proofs should allow building chains of testimony in a sense that if A trusts B and B trusts C then B can mediate a trust between A and C.
7. Identity based threshold secret sharing schemes using robot identity should be realizable.
8. Other scenarios similar to those of the human society can be implemented based on the robot identity

Bio-Inspired Robot Identity

Biological mutations are changes in the genetic sequence, and they are a main cause of diversity among organisms. These changes occur at many different levels, and they can have widely differing consequences. It is a permanent irremovable change in the genetic properties which reflects its effects on future behavior and properties.

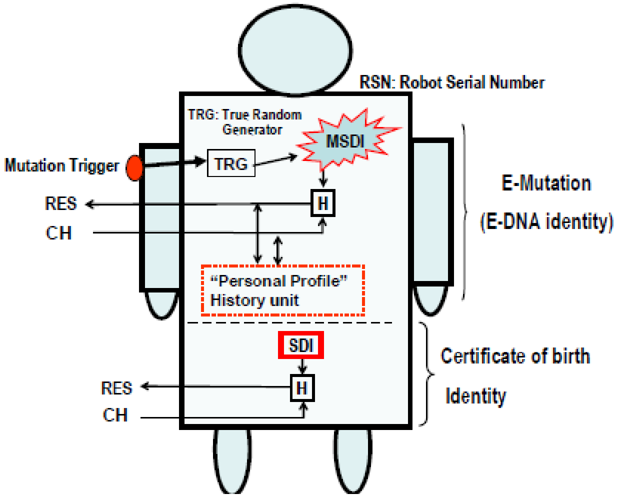

Figure 4: Robot e-Mutation and birth certificate [1].

The same idea holds for the "electronic mutation" e-mutation, where after a "mutation trigger" is activated as shown in Figure 4. The resulting self defined unknown identity MSDI (Mutated Secret Device Identity) together with a (possibly even unknown) hash function H should be provable but not clonable. The resulting "Mutated Identity" exhibits DNA-like properties as it is provable through challenge response traces of a hidden secret identity without the necessity to be revealed to anybody. This e-mutation can serve to generate a sort of electronic DNA (e-DNA) chain for a particular device.

Using the method presented in [1] it is possible to show that cloning a device would become practically equivalent to the difficulty of first cracking the mutated identity with its function H by some invasive attack and then seeking and copying all relevant robot transactions history. This is nearly impossible in most practical applications.

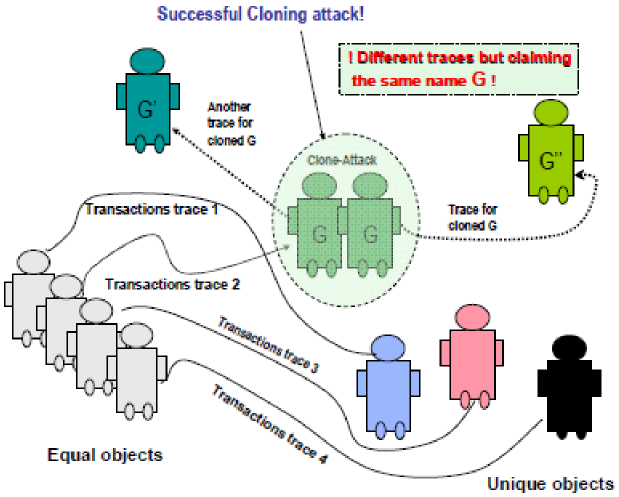

Figure 5: Traced-history and resolving cloning attack [1].

Figure 5 shows that even if such a cloning-attack was successful it is be possible to detect the attack after at most one transaction. Suppose that the unit G was successfully cloned at some time and two G units were created having exactly the same properties at the cloning time point. After a mutation trigger (transaction) both G units would independently generate together with the system new traces/properties caused by two independent processes which are most likely different. The result is two different identities G' and G", where both claim to be G and therefore the cloning-attack was detected and the identification process will fail.

CONCLUSION

Looking at Google's robot-buying binge [11] it is safe to assume that it won't be too long until sophisticated robots will become available to the consumer market. While this is exciting it is important to note that security considerations have to be an integral part of developing such robots. As seen in the section about vulnerabilities in contemporary robots, neglecting such aspects results in very unsatisfying products from a security point-of-view.

Even though a paper [4] on robot security has been published as early as 1985, there is still a lack of detailed studies in this area. Indeed I would argue that the vulnerabilities seen in contemporary robots have very little to do with robot specific problems and could be easily avoided if some basic best-practices would have been followed.

There are efforts being made to explore privacy concerns around robots at Oxford University's Cyber Security Center [13], but generally speaking it seems like until we are able to create significantly more powerful artificial intelligence (AI) robots face similar security challenges as do other systems.

Of course AI will not only have an impact on robot security, but Stephen Hawking goes as far as to say: "Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last." [12]

REFERENCES

1. Wael Adi. Mechatronic Security and Robot Authentication. Proceedings of the BLISS 2009.

2. Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R. Smith, Tadayoshi Kohno. A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons. Proceedings of the ACM Ubicomp 2009.

3. Keith Edwards, Rebecca Grinter. At Home with Ubiquitous Computing: Seven Challenges. Proceedings of the ACM Ubicomp 2001.

4. Douglas W. Gage. Security Considerations for Autonomous Robots. Proceedings of Symposium on Security and Privacy 1985.

5. Kheng Lee Koay, Dag Sverre Syrdal, Michael L. Walters, and Kerstin Dautenhahn. Five Weeks in the Robot House - Exploratory Human-Robot Interaction Trials in a Domestic Setting. Proceedings of the ACHI 2009.

6. Ueli Maurer. Information Security (Part I). Script for the "Information Security" lecture taught at ETH Zurich 2013.

7. JaYoung Sung, Henrik Christensen, Rebecca Grinter. Sketching the Future: Assessing User Needs for Domestic Robot. Proceedings of the IEEE International Symposium on Robot and Human Interactive Communication 2009.

8. Céline Ray, Francesco Mondada, Roland Siegwart. What do people expect from robots? Proceedings of the IROS 2008.

9. Kashmir Hill. How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old. Forbes online article 2013. *http://www.forbes.com/sites/kashmirhill/2014/04/29/baby-monitor-hacker-still-terrorizing-babies-and-their-parents/*

10. Kashmir Hill. Baby Monitor Hacker Still Terrorizing Babies And Their Parents. Forbes online article 2014. *http://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/*

11. Steven Hill. With Google's Robot-Buying Binge, A Hat Tip To The Future. NPR online article 2014. *http://www.npr.org/blogs/alltechconsidered/2014/03/17/290888529/with-googles-robot-buying-binge-a-hat-tip-to-the-future*

12. Stephen Hawking: 'Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough?'. Independent online article 2014. *http://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence–but-are-we-taking-ai-seriously-enough-9313474.html*

13. Designing robots that can keep secrets. Oxford University online article 2014. *http://www.ox.ac.uk/media/news_stories/2014/140305.html*

14. *http://yuppiecrap.com/content/uploads/2010/05/irobot-roomba-560-working.jpg*

15. *http://www.youtube.com/watch?v=c3Cq0sy4TBs*

16. *http://www.foroiphone.com/attachments/barra-iphone-off-topic/18446d1322318917t-rovio-robot-con-wifi-webcam-y-mas-rb-wow-23-rovio-elevated.jpg*

17. *http://www.hack4fun.eu/wp-content/uploads/2010/09/spykee-robot1.jpg*