ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (476-482), Month: July - September 2014, Available at: www.researchpublish.com

ROBOT: THE FUTURE HOUSEHOLD

[1]Sumit Kumar, [2]Sumit Dalal, [3]Vivek Dixit

[1,2,3]Dept. of Computer Science Engineering, Dronacharya Collage of Engineering (Gurgaon) Haryana, India

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.**

I. 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.

Fig.1 iRobot Roomba 560 Vacuum Cleaner

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, 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.

Fig.2 Willow Garage PR2, Robot for Research and Innovation

II. 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:*** The WowWee Rovio is a mobile webcam robot that is marketed towards adults 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 passwordprotected. The Rovio was introduced in late 2008.

- ***Erector Spykee:*** The Erector Spykee 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. 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.

- ***WowWee RoboSapien V2:*** The WowWee RoboSapien V2 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.

Fig.3

III. REQUIREMENTS FOR SECURED ROBOT IDENTITY

The author of 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.

Fig.4

IV. ADDITIONAL ATTACKS

Many of our attacks could have beenmitigated 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.

V. BRAINPOWER AND UTILITY

Though dispiriting to artificial-intelligence experts, the huge deficit does not mean that the goal of a humanlike artificial brain is unreachable. Computer power for a given price doubled each year in the 1990s, after doubling every 18 months in the 1980s and every two years before that. Prior to 1990 this progress made possible a great decrease in the cost and size of robot-controlling computers. Cost went from many millions of dollars to a few thousand, and size went from room-filling to handheld. Power, meanwhile, held steady at about 1 MIPS. Since 1990 cost and size reductions have abated, but power has risen to about 10,000 MIPS for a home computer. At the present pace, only about 20 or 30 years will be needed to close the gap. Better yet, useful robots don't need full human-scale brainpower.

Commercial and research experiences convince me that the mental power of a guppy—about 10,000 MIPS—will suffice to guide mobile utility robots reliably through unfamiliar surroundings, suiting them for jobs in hundreds of thousands of industrial locations and eventually hundreds of millions of homes. A few machines with 10,000 MIPS are here already, but most industrial robots still use processors with less than 1,000 MIPS.

Commercial mobile robots have found few jobs. A paltry 10,000 work worldwide, and the companies that made them are struggling or defunct. (Makers of robot manipulators are not doing much better.) The largest class of commercial mobile robots, known as automatic guided vehicles (AGVs), transport materials in factories and warehouses. Most follow buried signal-emitting wires and detect end points and collisions with switches, a technique developed in the 1960s.

It costs hundreds of thousands of dollars to install guide wires under concrete floors, and the routes are then fixed, making the robots economical only for large, exceptionally stable factories. Some robots made possible by the advent of microprocessors in the 1980s track softer cues, like magnets or optical patterns in tiled floors, and use ultrasonics and infrared proximity sensors to detect and negotiate their way around obstacles.

The most advanced industrial mobile robots, developed since the late 1980s, are guided by occasional navigational markers—for instance, laser-sensed bar codes—and by preexisting features such as walls, corners and doorways. The costly labor of laying guide wires is replaced by custom software that is carefully tuned for each route segment. The small companies that developed the robots discovered many industrial customers eager to automate transport, floor cleaning, security patrol and other routine jobs. Alas, most buyers lost interest as they realized that installation and route changing required time-consuming and expensive work by experienced route programmers of inconsistent availability. Technically successful, the robots fizzled commercially.

In failure, however, they revealed the essentials for success. First, the physical vehicles for various jobs must be reasonably priced. Fortunately, existing AGVs, forklift trucks, floor scrubbers and other industrial machines designed for accommodating human riders or for following guide wires can be adapted for autonomy. Second, the customer should not have to call in specialists to put a robot to work or to change its routine; floor cleaning and other mundane tasks cannot bear the cost, time and uncertainty of expert installation. Third, the robots must work reliably for at least six months before encountering a problem or a situation requiring downtime for reprogramming or other alterations. Customers routinely rejected robots that after a month of flawless operation wedged themselves in corners, wandered away lost, rolled over employees' feet or fell down stairs. Six months, though, earned the machines a sick day.

Robots exist that have worked faultlessly for years, perfected by an iterative process that fixes the most frequent failures, revealing successively rarer problems that are corrected in turn. Unfortunately, that kind of reliability has been achieved only for prearranged routes. An insectlike 10 MIPS is just enough to track a few handpicked landmarks on each segment of a robot's path. Such robots are easily confused by minor surprises such as shifted bar codes or blocked corridors (not unlike ants thrown off a scent trail or a moth that has mistaken a streetlight for the moon).

Fig.5

VI. 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.

The same idea holds for the ”electronic mutation” e-mutation, where after a ”mutation trigger” is activated. 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 DNAlike 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 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.

cessful it is be possible to detect the attack after at most onetransaction. 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.

VII. ROBOTICS RESEARCH

Much of the research in robotics focuses not on specific industrial tasks, but on investigations into new types of robots, alternative ways to think about or design robots, and new ways to manufacture them but other investigations, such as MIT'scyberflora project, are almost wholly academic.

A first particular new innovation in robot design is the opensourcing of robot-projects. To describe the level of advancement of a robot, the term "Generation Robots" can be used. This term is coined by Professor Hans Moravec, Principal Research Scientist at the Carnegie Mellon University Robotics Institute in describing the near future evolution of robot technology. *First generation* robots, Moravec predicted in 1997, should have an intellectual capacity comparable to perhaps a lizard and should become available by 2010. Because the *first generation* robot would be incapable of learning, however, Moravec predicts that the *second generation* robot would be an improvement over the *first* and become available by 2020, with the intelligence maybe comparable to that of a mouse. The *third generation* robot should have the intelligence comparable to that of a monkey. Though *fourth generation* robots, robots with human intelligence, professor Moravec predicts, would become possible, he does not predict this happening before around 2040 or 2050.[102]

The second is Evolutionary Robots. This is a methodology that uses evolutionary computation to help design robots, especially the body form, or motion and behavior controllers. In a similar way to natural evolution, a large population of robots is allowed to compete in some way, or their ability to perform a task is measured using a fitness function. Those that perform worst are removed from the population, and replaced by a new set, which have new behaviors based on those of the winners. Over time the population improves, and eventually a satisfactory robot may appear. This happens without any direct programming of the robots by the researchers. Researchers use this method both to create better robots,[103] and to explore the nature of evolution.[104] Because the process often requires many generations of robots to be simulated,[105] this technique may be run entirely or mostly in simulation, then tested on real robots once the evolved algorithms are good enough.[106] Currently, there are about 1 million industrial robots toiling around the world, and Japan is the top country having high density of utilizing robots in its manufacturing industry.

VIII. EDUCATION AND TRAINING

Robotics engineers design robots, maintain them, develop new applications for them, and conduct research to expand the potential of robotics. Robots have become a popular educational tool in some middle and high schools, as well as in numerous youth summer camps, raising interest in programming, artificial intelligence and robotics among students. First-year computer science courses at several universities now include programming of a robot in addition to traditional software engineering-based coursework.

Career Training

Universities offer bachelors, masters, and doctoral degrees in the field of robotics.[109]Vocational schools offer robotics training aimed at careers in robotics

Certification

The Robotics Certification Standards Alliance (RCSA) is an international robotics certification authority that confers various industry- and educational-related robotics certifications.

Summer Robotics Camp

Several national summer camp programs include robotics as part of their core curriculum, including Digital Media Academy, RoboTech, and Cybercamps. In addition, youth summer robotics programs are frequently offered by celebrated museums such as the American Museum of Natural History[110] and The Tech Museum of Innovation in Silicon Valley, CA, just to name a few. An educational robotics lab also exists at the IE & mgmnt Faculty of the Technion. It was created by Dr. Jacob Rubinovitz.

Robotics Afterschool Programs

Many schools across the country are beginning to add robotics programs to their after school curriculum. Two main programs for afterschool robotics are Botball and FIRST Robotics Competition.

IX. 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 nonexpert 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.

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] 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] 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/babymonitor- hacker-still-terrorizing-babies-and-theirparents/

[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/howa- creep-hacked-a-baby-monitor-to-say-lewd-things-toa-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-tipto-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/stephenhawking-transcendence-looks-at-the-implications-ofartificial-intelligence–but-are-we-taking-ai-seriouslyenough 9313474.html