The Future of Household Robots: Ensuring the Safety and Privacy of Users

Tamara Denning
Cynthia Matuszek
Karl Koscher
Joshua R. Smith
Tadayoshi Kohno

Computer Science and Engineering
University of Washington
This talk is about two things:
- The future of robots in the home
- Computer security and privacy

To make sure we’re all on the same page, first:
- Brief background on robots
- Brief background on security and privacy
What is a Robot?

- Cyber-physical system with:
  - Mobility
  - Sensors
  - Actuators
  - Some reasoning capabilities (potentially)
What is a Robot?

- Cyber-physical system with:
  - Mobility
  - Sensors
  - Actuators
  - Some reasoning capabilities (potentially)

- Applications:
  - Elder care
  - Physically-enabled smart home
What is Security?

- **Security:**
  - Systems behave as intended even in the presence of an adversary
What is Security?

Security:
- Systems behave as intended even in the presence of an adversary

NOT Safety:
- Systems behave as intended even in the presence of accidental failures
To understand the importance of security for robots, we give context:

A brief history of computers and computer security.
Timeline: Computers

1940 1970 2000

11/24/2009
Timeline: Computers

1940
- Colossus

1946
- ENIAC

1951
- UNIVAC
Timeline: Computers

1940
1970
2000

1974 Altair 8800
1977 Apple II
1981 IBM Personal Computer
1982 Commodore 64
1984 Apple Macintosh
Timeline: Computers

- 1990 World Wide Web
Timeline: Computers

1940

1970

2000

11/24/2009
Now looking at computer security...
Timeline: Computer Security Attacks

1971
Phone Phreaking
1982
The 414s break into 60 computer systems
Timeline: Computer Security Attacks

1986
“The Brain” Virus
Timeline: Computer Security Attacks

1940
1970
2000

1988
Morris Worm
Timeline: Computer Security Attacks

1940

2000 DDoS Attack
Timeline: Computer Security Attacks

- Rootkits
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
- Keyloggers
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
- Keyloggers
- Cross-Site Scripting
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
- Keyloggers
- Cross-Site Scripting
- etc.
Timeline: Computer Security Attacks

Observations:
• The attack rate increases
• The attacks lag behind the technology
1979
Robotics Institute founded at Carnegie Mellon University
Timeline: Robots

1982
WABOT-2 accompanies people on a keyboard instrument
Timeline: Robots

1986
Honda founds Humanoid Robot Division

POWERED by HONDA™
Timeline: Robots

1999
AIBO

1960
2000
2020
Timeline: Robots

1960

2000
ASIMO

2020

11/24/2009
Timeline: Robots

2001
Paro therapeutic seal

1960
2000
2020

11/24/2009
Timeline: Robots

1960
1990
2000
2020

2002
Roomba
Timeline: Robots

2008
Okonomiyaki Robot
Timeline: Robots

2010 ?
HAL exoskeleton
Observation:
• No attacks on robot security yet

Recall (computer security):
• The attack rate increases
• The attacks lag behind the technology

What is the future of robot security?
Our focus: Robot security and privacy

- Evil people doing bad things with robots
- Most likely near term security and privacy threat
Our focus: Robot security and privacy
- Evil people doing bad things with robots
- Most likely near term security and privacy threat

Evil robots
- Popular topic of science fiction
- Unlikely near term security and privacy threat

Other challenges to mixing humans with robots
- Safety
- Human-robot interaction
Talk Outline

Part 1. Introduction

Part 2. Assessing the Risks: Today and Tomorrow

Part 3. Challenges and Next Steps
Understanding Current and Future Risks: The Computer Security Approach

- Identify representative examples of future tech
- Assess the security and privacy vulnerabilities of those examples
- Determine risks for today and extrapolate risks for tomorrow
There are many household robots for sale...

<table>
<thead>
<tr>
<th></th>
<th>Roomba (vacuum)</th>
<th>Scooba (mop)</th>
<th>Robomow (lawn mower)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pleo</td>
<td>Pleo (artificial lifeform toy)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lego Mindstorm NXT</td>
<td>Lego Mindstorm NXT (toy and learning kit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlyTech Bladestar</td>
<td>FlyTech Bladestar (flying toy)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to pick which robots to study?
Axes for Selecting Representatives Robots

- **Strategy:** Pick robots that span likely properties of future robots
  - Different Groups of Intended Users
  - Mobility
  - Actuators
  - Sensors
  - Communication Methods
Robots purchased for experimentation during or before October 2008.
RoboSapien V2

- Toy for children and hobbyists
- Mobile, bipedal
- Basic Dexterity
- Controlled by IR remote
- Some autonomous behavior
- Pre-programmed speech
Rovio

- For adults
- Telepresence
- Home surveillance
- Check up on relatives
- Follows pre-programmed IR beacons
Spykee

• Toy for children

• Assembled and configured by children

• Telepresence: Parent can tuck in kids when out of town

• “Spy” robot
So, what vulnerabilities did we find?
So, what vulnerabilities did we find?

Focusing on Spykee and Rovio for now (we’ll come back to RoboSapien V2 later)
Remote Discovery

(Artificial data -- not real locations of robots)
Other Vulnerabilities

- Eavesdrop on A/V streams sent to users
- Intercept valid login credentials
Physical Takeover

- With credentials: Drive the robot anywhere
- Access the AV stream at any time
What the vulnerabilities mean to people...

- We discussed some vulnerabilities...

- What do these vulnerabilities mean to people and their environment?
What the vulnerabilities mean to people...

- We discussed some vulnerabilities...

- What do these vulnerabilities mean to people and their environment?
  - (We did not implement these attacks.)

Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Move around rooms of the house to facilitate spying and eavesdropping.

Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Rovio: Possible Threats

- Spy/eavesdrop in the home
- Move around rooms of the house to facilitate spying and eavesdropping
- Use weight to cause minor property damage
- Create hazards (e.g., for infants) by knocking things over

Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Rovio: Other Threats

- Drive underneath elder’s feet to trip them
- Make sounds to confuse people with dementia
- Displace objects to confuse people with dementia

Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.
Spykee: The Risks

- Same kinds of risks as the Rovio, but...
Same kinds of risks as the Rovio, but...

**Spykee meant to be:**
- Built by children (Erector set, 8+ years)
- Configured by children
- Connected to the Internet by children
Spykee: The Risks

• Same kinds of risks as the Rovio, but...

• Spykee meant to be:
  ○ Built by children (Erector set, 8+ years)
  ○ Configured by children
  ○ Connected to the Internet by children

• And most of all...played with by children
Spykee: The Risks

- Same kinds of risks as the Rovio, but...

- Built by children
- Configured by children
- Connected to the Internet by children

And most of all... played with by children.

We have not analyzed the robots shown. They may or may not have vulnerabilities and may or may not be used for attacks. We are using them as examples of future kinds of robots.
We have not analyzed the robots shown. They may or may not have vulnerabilities and may or may not be used for attacks. We are using them as examples of future kinds of robots.
The Risks Tomorrow

- Robots for elders
  - Exoskeleton for mobility
  - Lifting robot

- Robots for children
  - As companions or as therapy for unique emotional needs

We have not analyzed the robots shown. They may or may not have vulnerabilities and may or may not be used for attacks. We are using them as examples of future kinds of robots.
The Risks Tomorrow

- Robots for elders
  - Exoskeleton for mobility
  - Lifting robot

- Robots for children
  - As companions or as therapy for unique emotional needs

- Robots that use tools

We have not analyzed the robots shown. They and may or may not be used for attacks. We are using them as examples of future kinds of robots.

11/24/2009
Are the risks real?

- Our focus is on the future, when household robots might be ubiquitous and sophisticated

- Potential types of attackers
  - Terrorist
  - Competitor
  - Acquaintance
  - ID Thief
  - Prankster
Talk Outline

Part 1. Introduction

Part 2. Assessing the Risks: Today and Tomorrow

Part 3. Challenges and Next Steps
There are many ways to raise the bar...

- **Basic Steps (for the user)**
  - Encrypted home network
  - Don’t use ad hoc
  - Don’t connect robots to the Internet
  - Don’t allow the robots in “private” spaces

- **Basic Steps (for the manufacturers)**
  - Security evaluations
  - Use encryption (properly!)
  - Secure firmware updates
Standard Security Practices Are Not Sufficient

- Implementation vulnerabilities
  - No such thing as perfect security
  - Vulnerabilities often found even in modern desktop computing systems implementing best practices
  - Secure networks can be cracked

- Usage vulnerabilities
  - Users don’t always secure networks
  - Users can misconfigure security settings even when employing them
Robots Have Unique Properties

- Physicality
  - Mobility
  - Dexterity

- Interactive and in the middle of the home

- These lead to unique challenges...

CC image courtesy of: http://www.flickr.com/photos/eiriknewth/282273087/
No Longer a Desktop Computer: New Challenges

- Robots that connect to the Internet are not traditional vacuum cleaners or toasters
- Children as administrators
- Robot interface is minimal
No Longer a Desktop Computer: New Challenges

- **Heterogeneous environments**
  - Multiple direct and indirect users
  - Pets
  - Children
  - Elderly
  - Guests

- **Meaning...**
  - The people affected by robot security vulnerabilities may not be the robots’ administrators
  - May be difficult to notice a hijacked robot
Even if you secure one robot in isolation...
Multi-Robot

- Even if you secure one robot in isolation...

- What can *two* robots achieve?
  - Overcome each other’s safeguards?
  - Combine physical capabilities?
  - Combine sensorial capabilities?

- Manufacturers might not expect this!
Our Setup

- **Toy example**
  - Compromised Rovio (supplies camera)
  - IR/RF repeater positioned within line of sight of the RoboSapien V2
  - Remote for the RoboSapien V2

- **What can we do?**
## Multi-Robot: Our Setup

<table>
<thead>
<tr>
<th></th>
<th>Rovio</th>
<th>RoboSapien V2</th>
<th>IR/RF Repeater</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV Feed</td>
<td>✗</td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Grippers</td>
<td></td>
<td>✗</td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Communication</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Out of Line of Sight</td>
<td>✗</td>
<td></td>
<td></td>
<td>✗</td>
</tr>
</tbody>
</table>
Multi-Robot Attack: Demo
Security and Privacy for Users of Future Household Robots

- A near term threat: evil people using robots
  - Needs attention today before technology matures

- Identified security and privacy vulnerabilities in today’s robots. Implications:
  - For today: Mild to moderate risks
  - For future: More severe risks
  - Attacks: Spying/eavesdropping, damaging objects, tripping or confusing residents, emotional abuse

- Challenges to securing future robots:
  - Non-expert users may think of robots as appliances
  - Heterogeneous home environment
  - Multiple robots co-opted by an attacker to work together
Questions?