Domestic Robots

a case study on security in ubiquitous computing

Thomas Knell
Ubiquitous Computing Seminar
15.4.2014

Defining Robot

There exists no universally accepted definition of a robot

- Any automatically operated machine that replaces human effort, though it may not resemble human beings in appearance or perform functions in a humanlike manner.

  – Encyclopaedia Britannica

- A robot is a cyber-physical system with sensors, actuators and mobility.

  – A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons, T. Denning et al.

- I can't define a robot, but I know one when I see one.

  – Joseph Engelberger (pioneer in industrial robotics)

Example 1: Cleaning Robots

Roomba

MyWindoro

Example 2: PR2

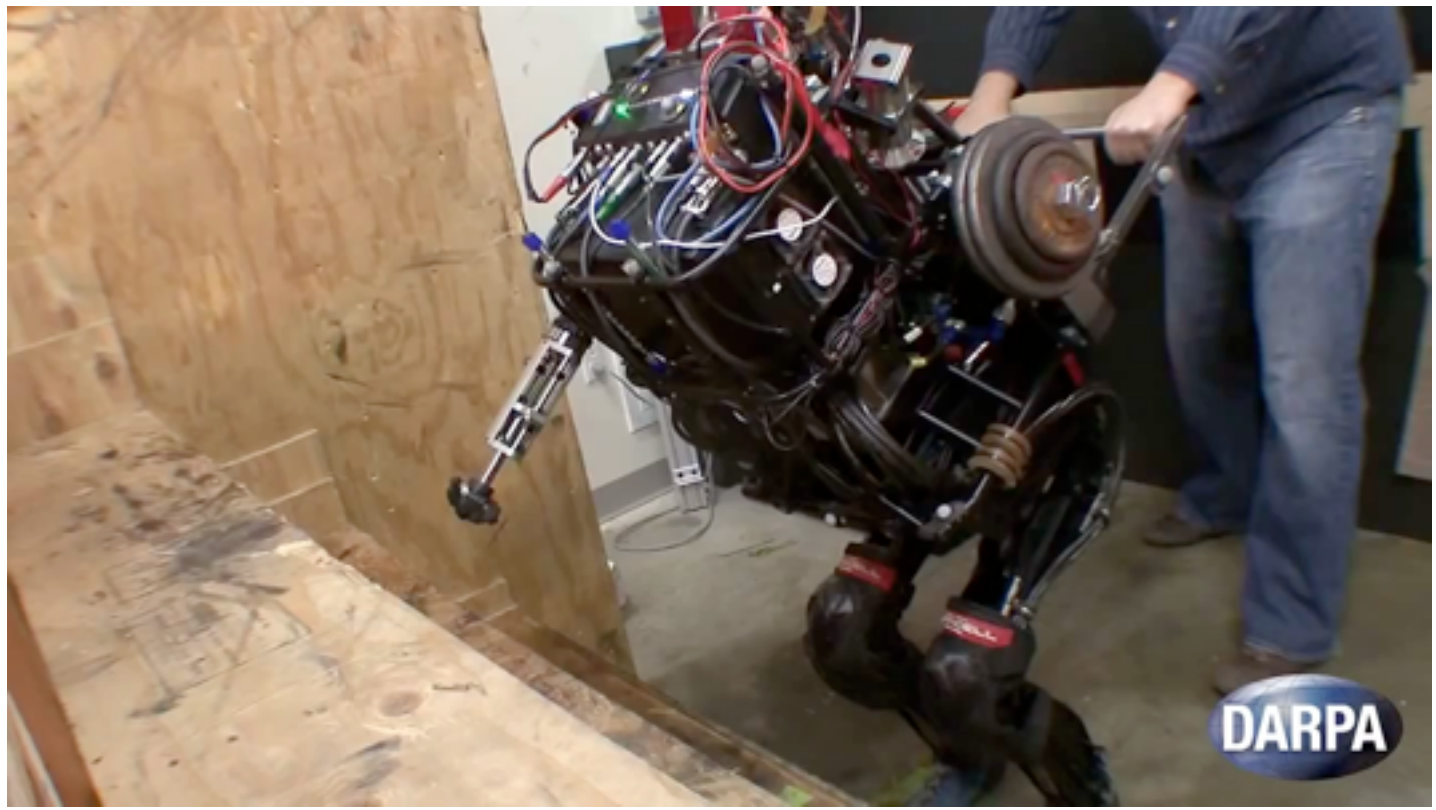
PR2 is a robotics research and development platform that lets you innovate right out of the box. No more building hardware and software from scratch.

http://www.willowgarage.com/pages/pr2/overview

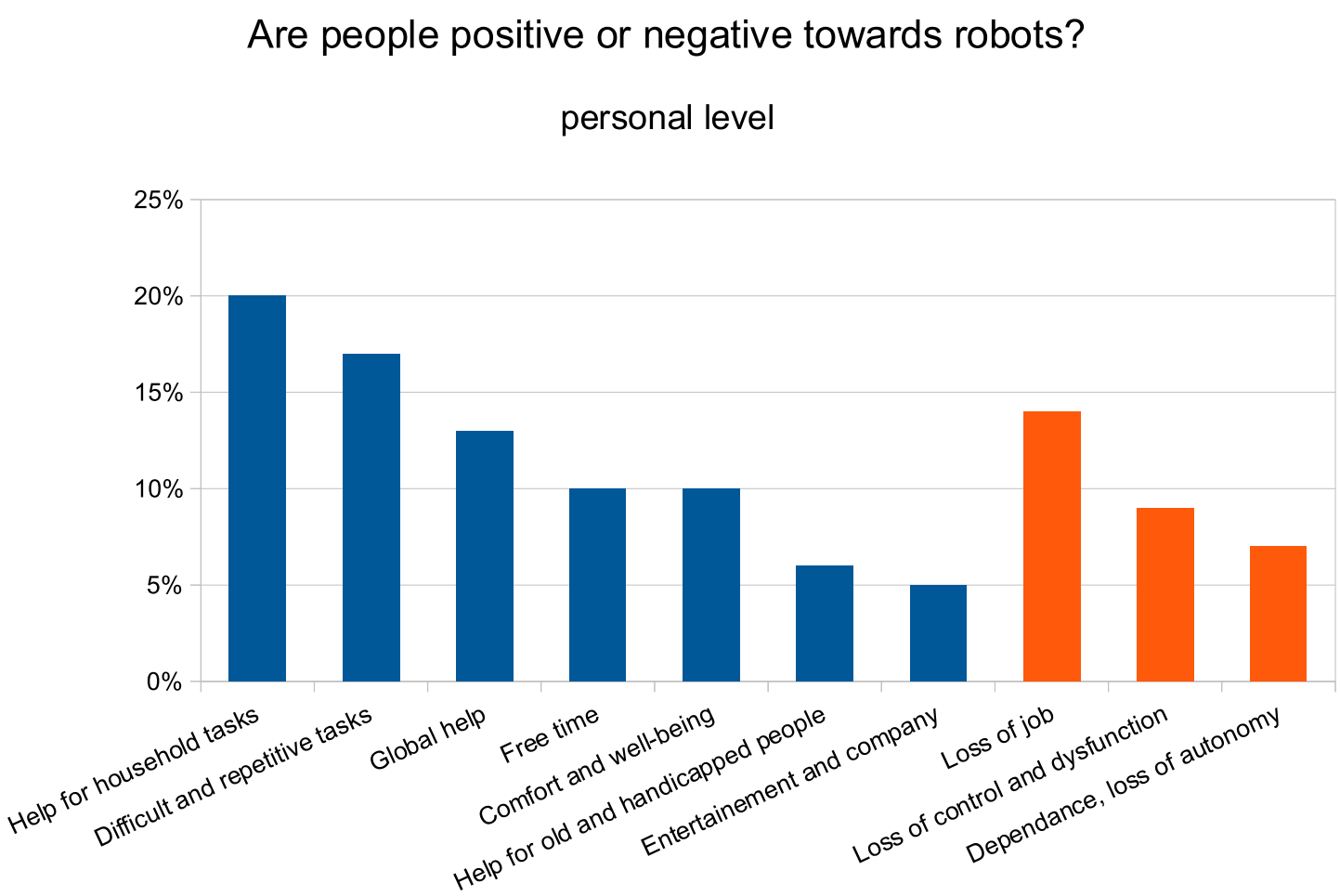
Example 3: Atlas

Atlas is a high mobility, humanoid robot designed to operate outdoors, even on extremely rough terrain.

http://www.bostondynamics.com/robot_Atlas.html



Perception of Robots



- Survey from 2007
- 240 Participants

What do people expect from robots?, C. Ray et al.

Stakeholder expectations

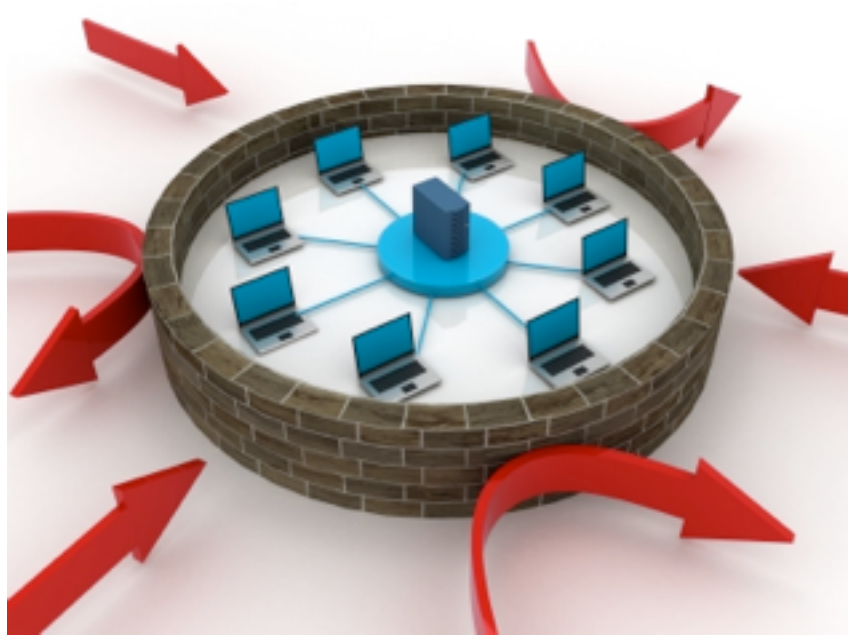
- New appliance: The household robot
- Users may have:
  - Incorrect preconceptions
  - No point of reference to understand the robot
- Designers will have to either:
  - Create very intuitive products, or
  - Integrate training course

What is Security?

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

Network Security Goals

- Confidentiality
  - Encryption
- Integrity
  - MAC, Digital Signature
- Availability
  - Redundancy, more Bandwidth



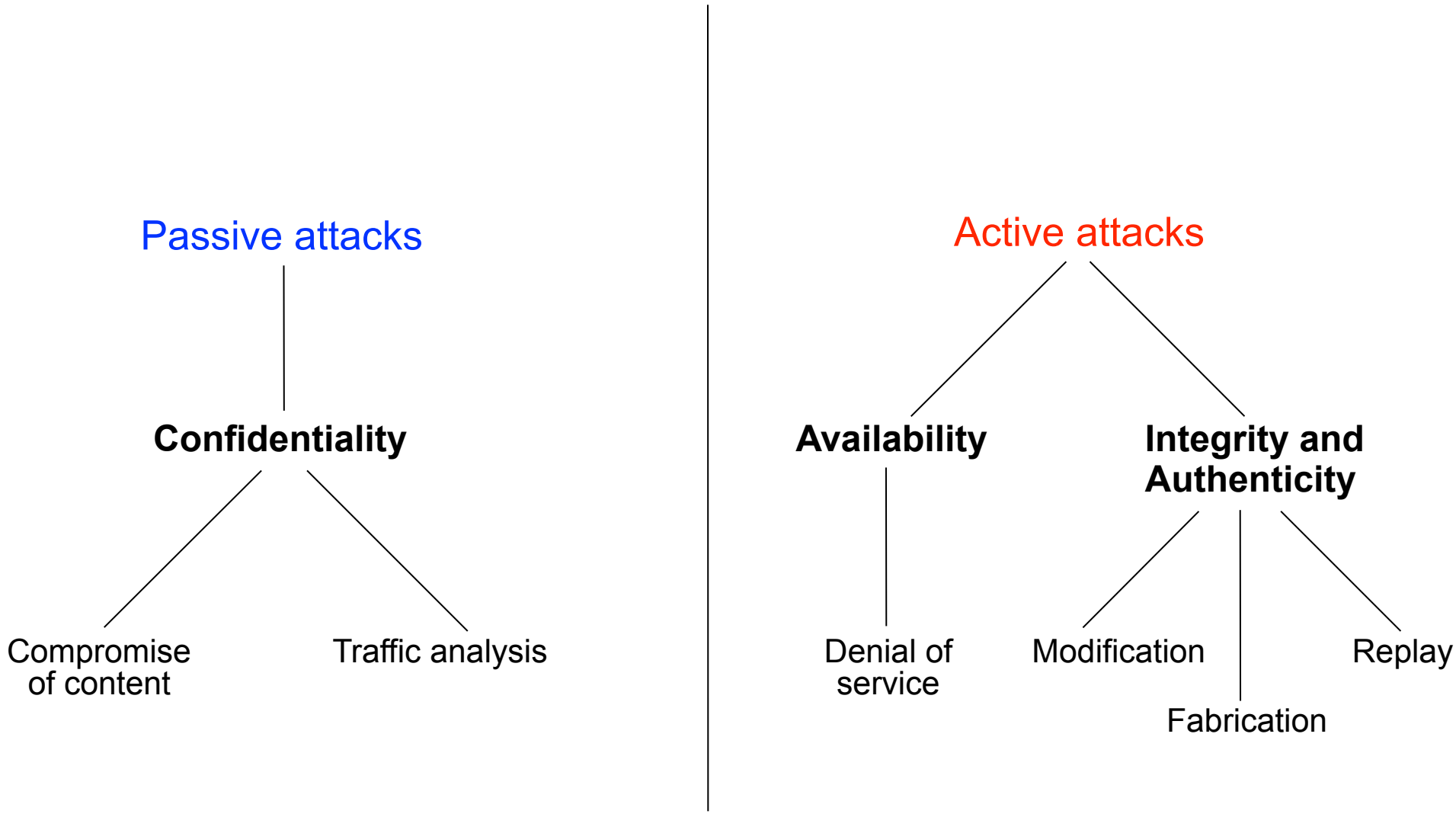
And More:

- Authentication
- Accountability
- Non-repudiation
- Privacy

Secure Communication Channel

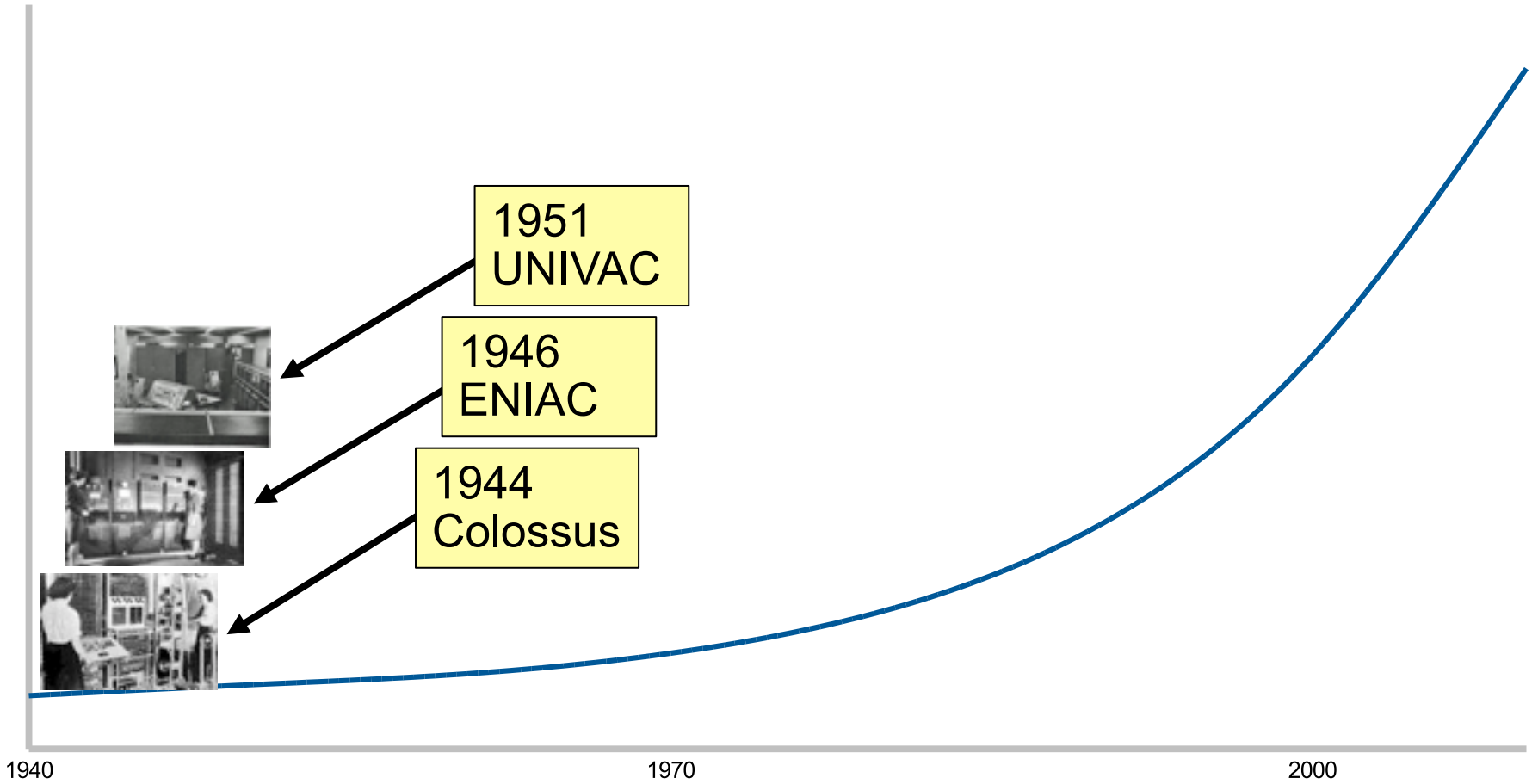
- Confidential channel
  - No eavesdropping possible on information sent
- Authentic channel
  - Sender is the one he claims to be and
  - Content is original
- Secure channel
  - Authentic and confidential channel

Attack Classification

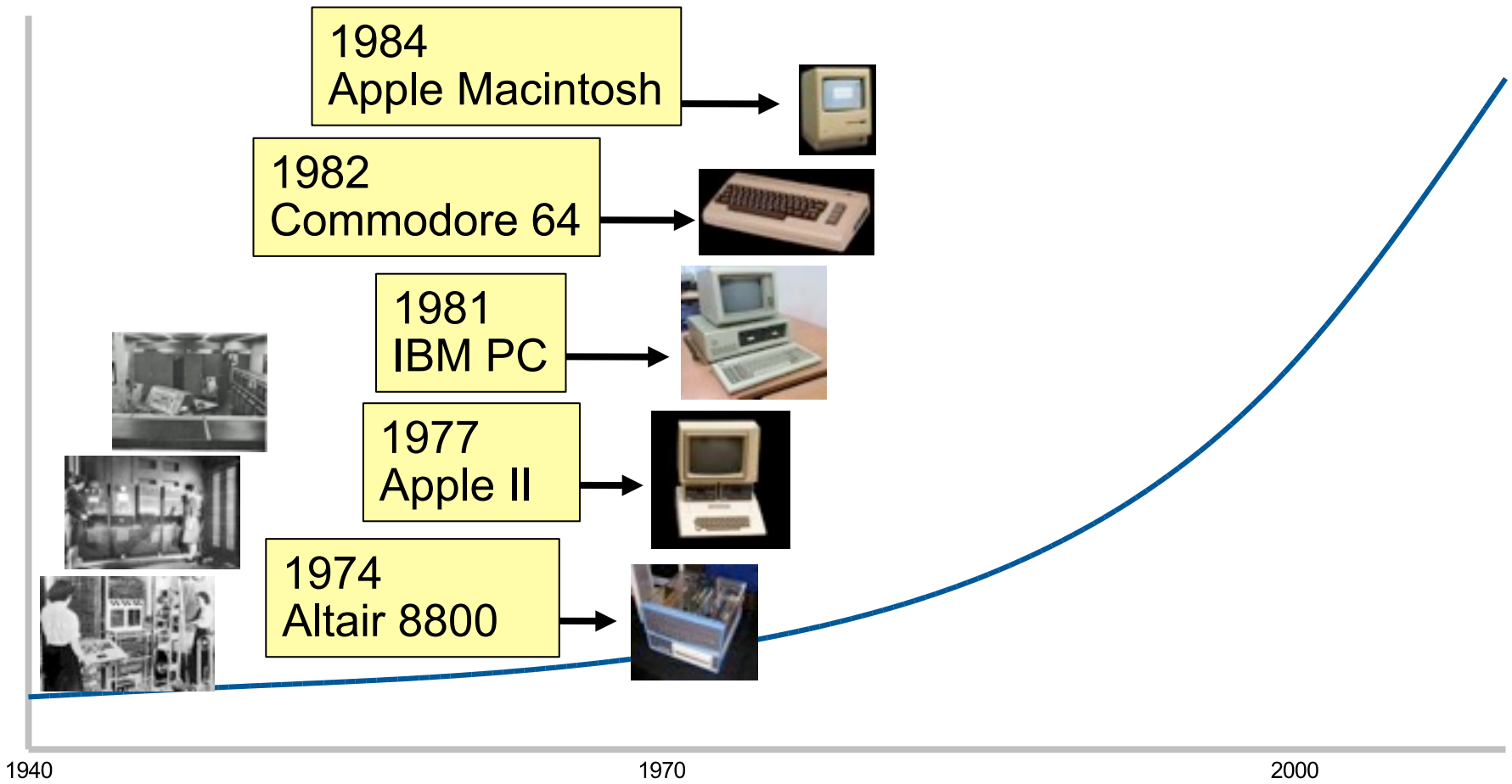


Classification due to Steve Kent, BBN Technologies

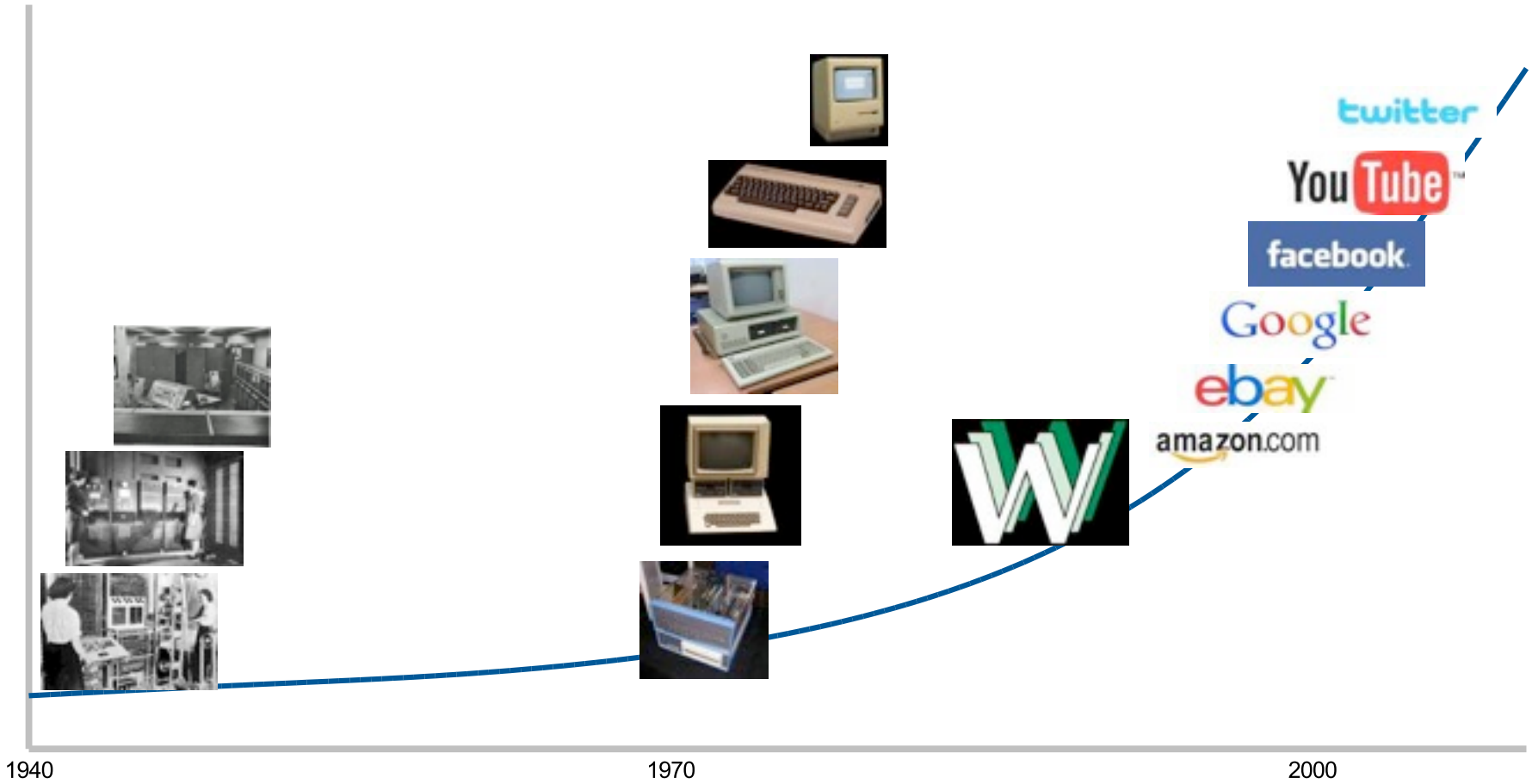
Timeline: Computers



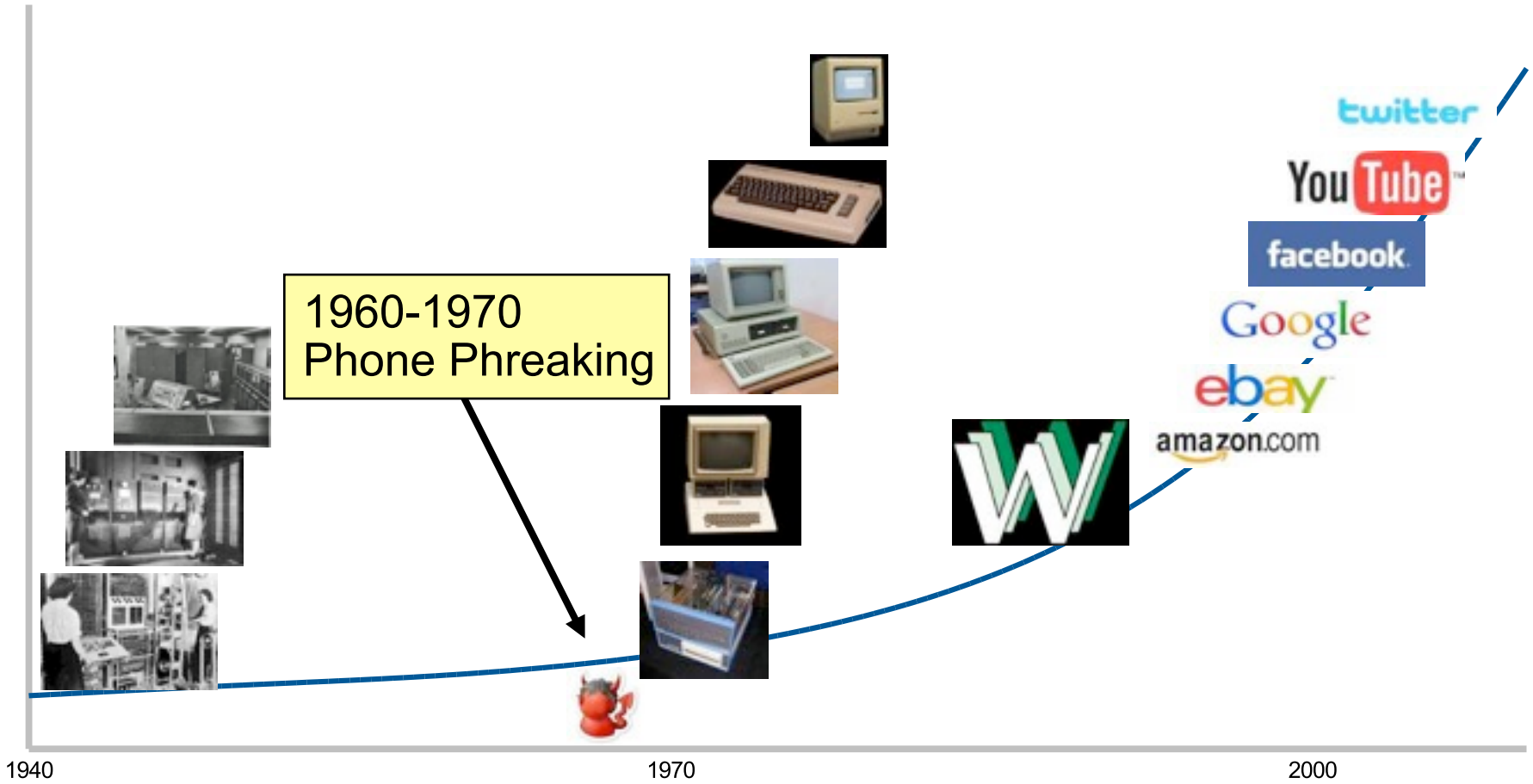
Timeline: Computers



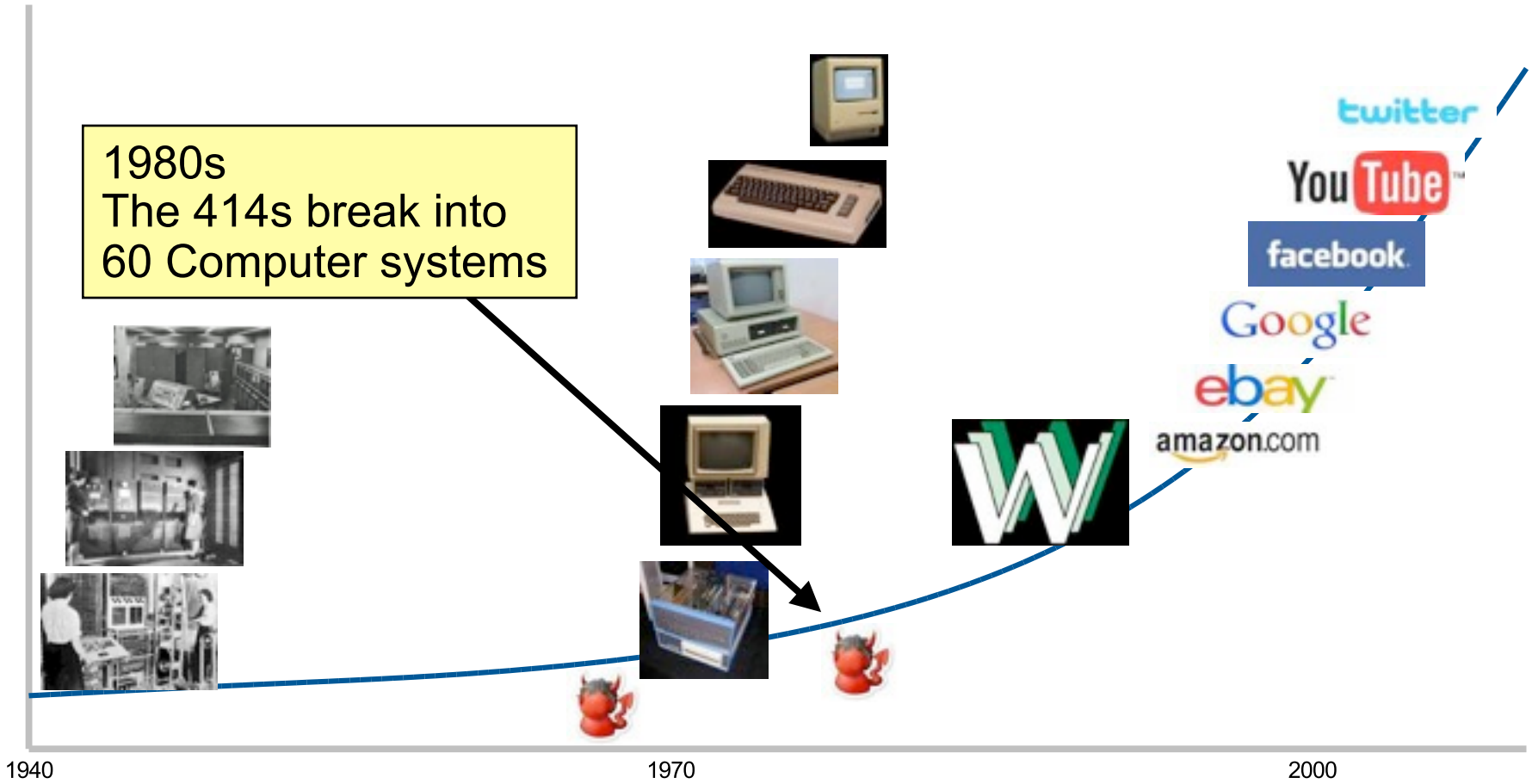
Timeline: Computers



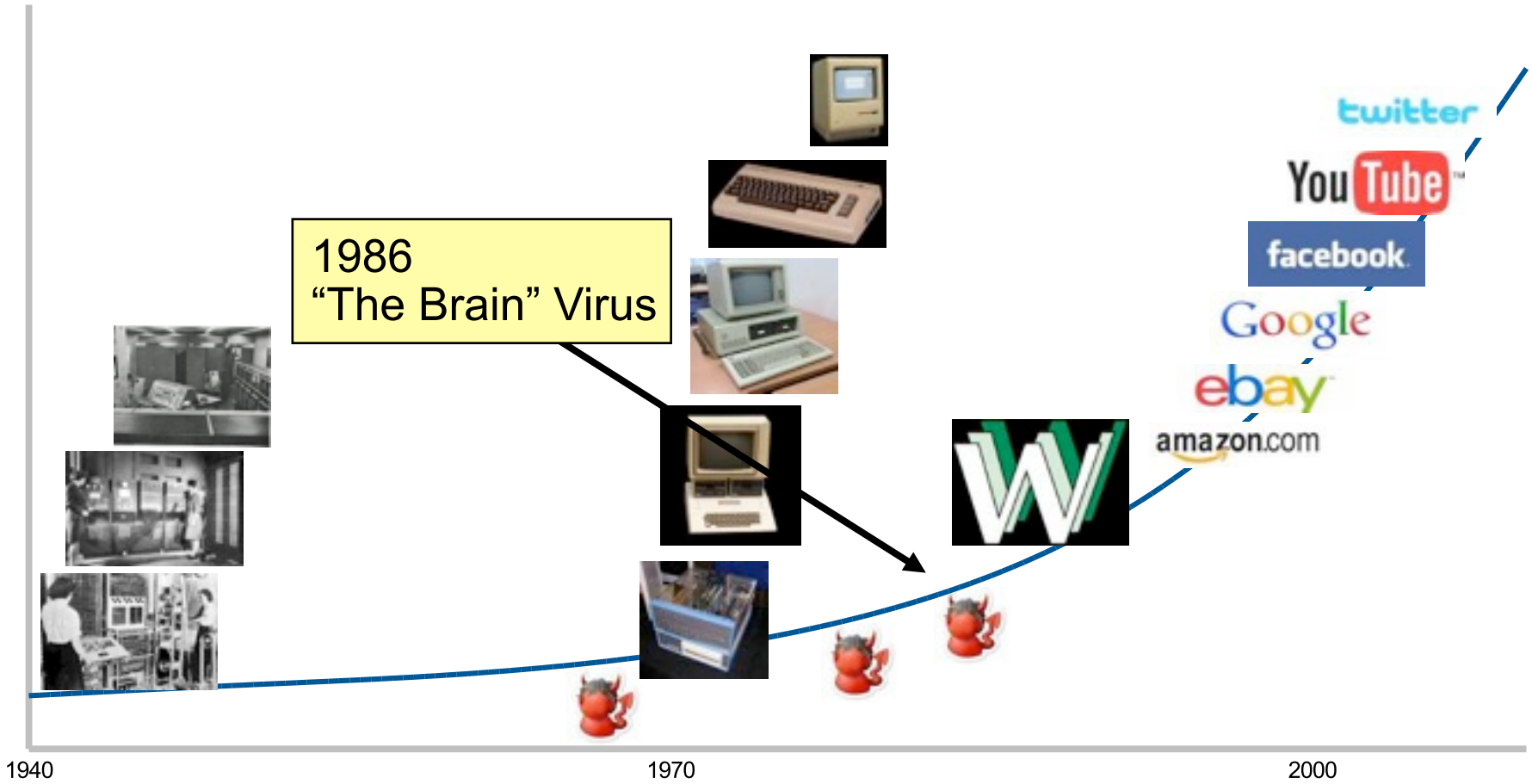
Timeline: Computer Security Attacks



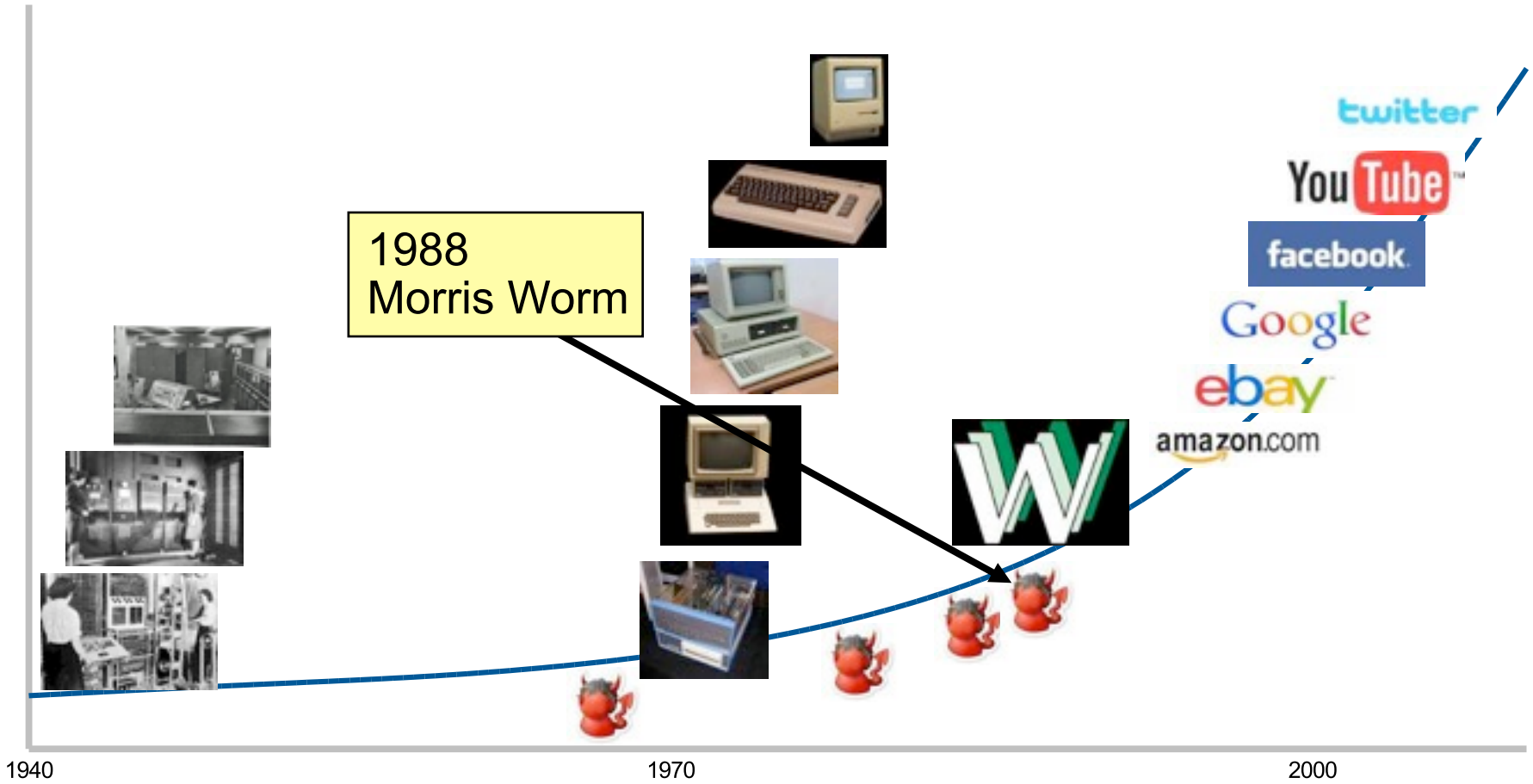
Timeline: Computer Security Attacks



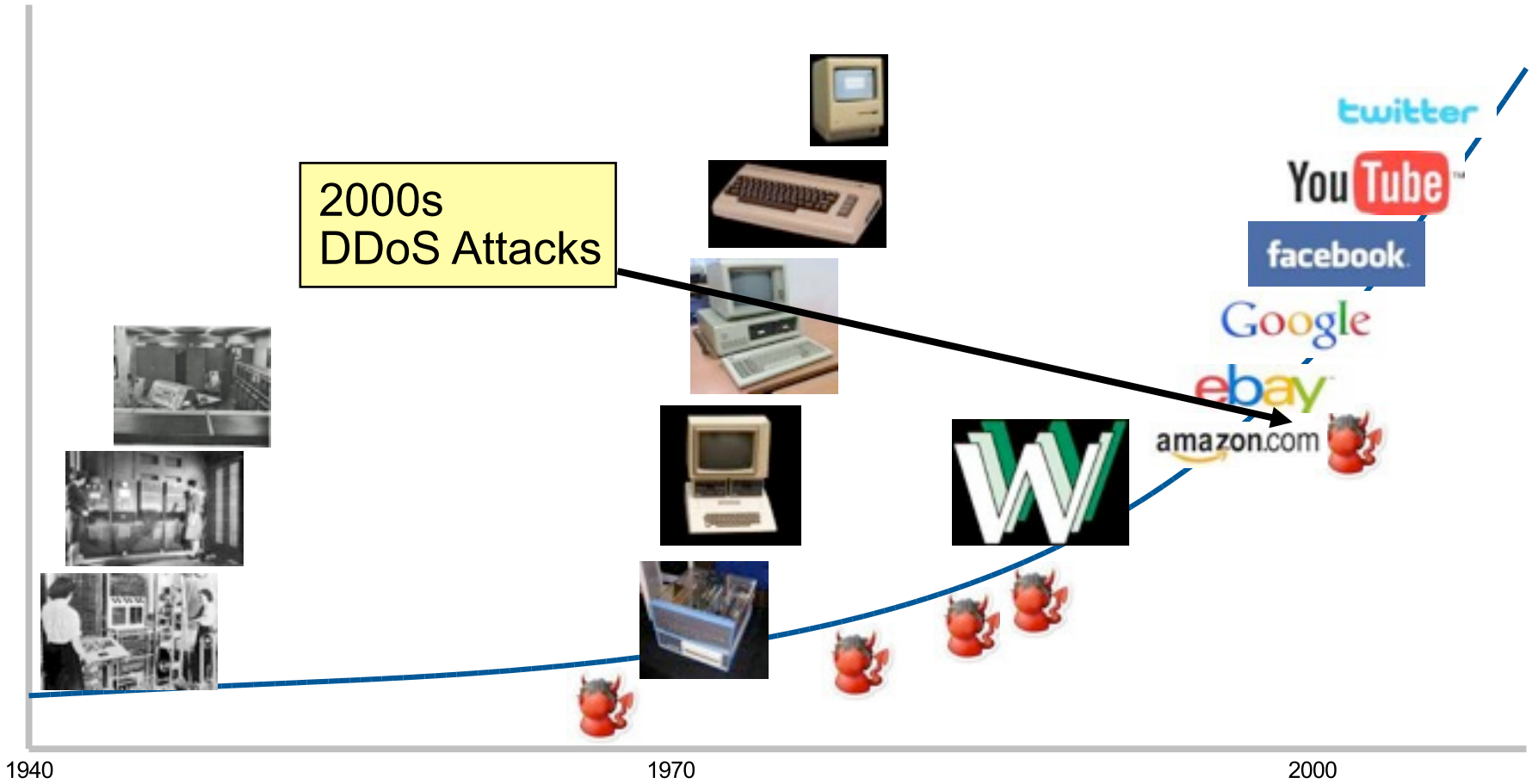
Timeline: Computer Security Attacks



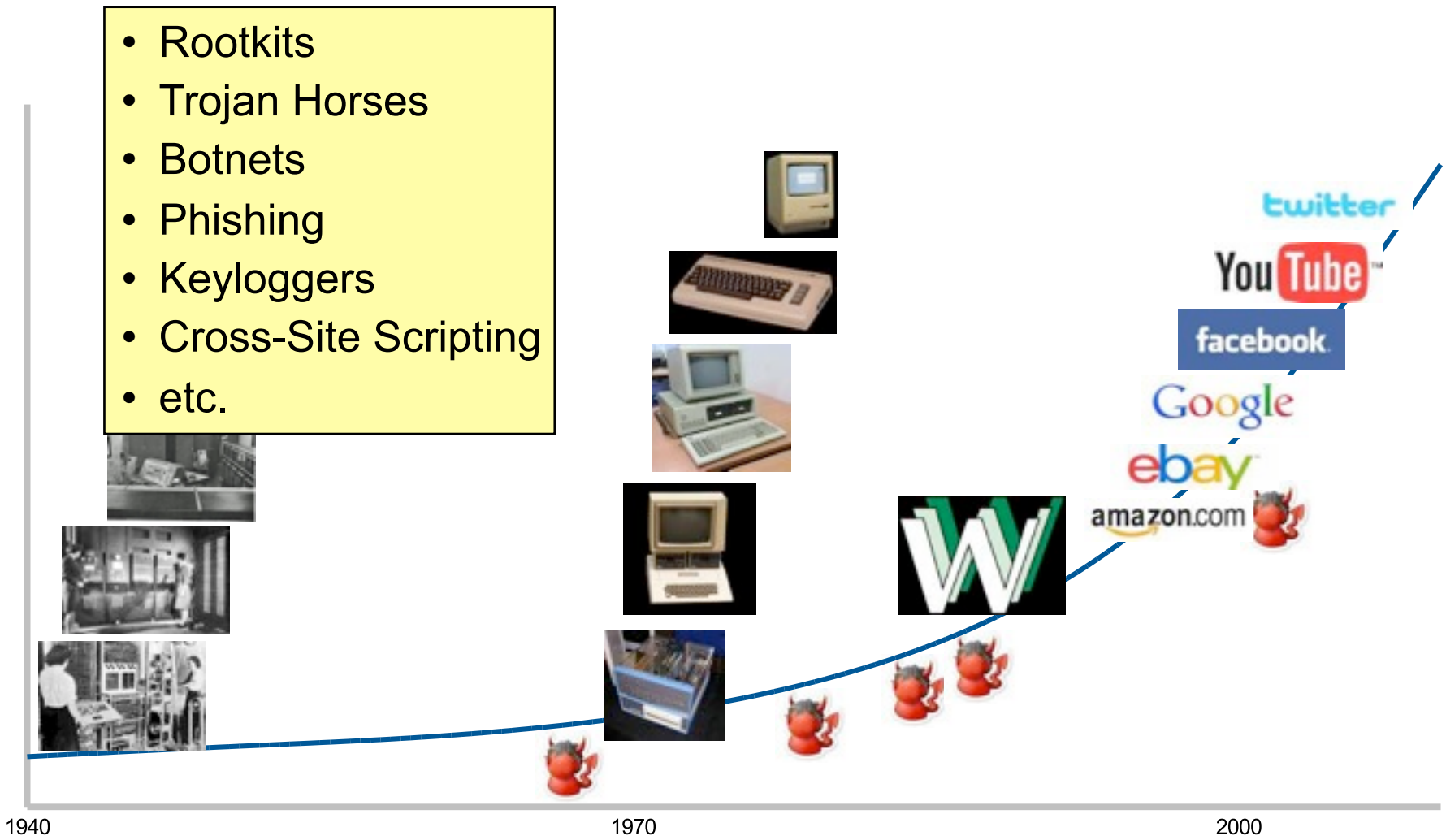
Timeline: Computer Security Attacks



Timeline: Computer Security Attacks

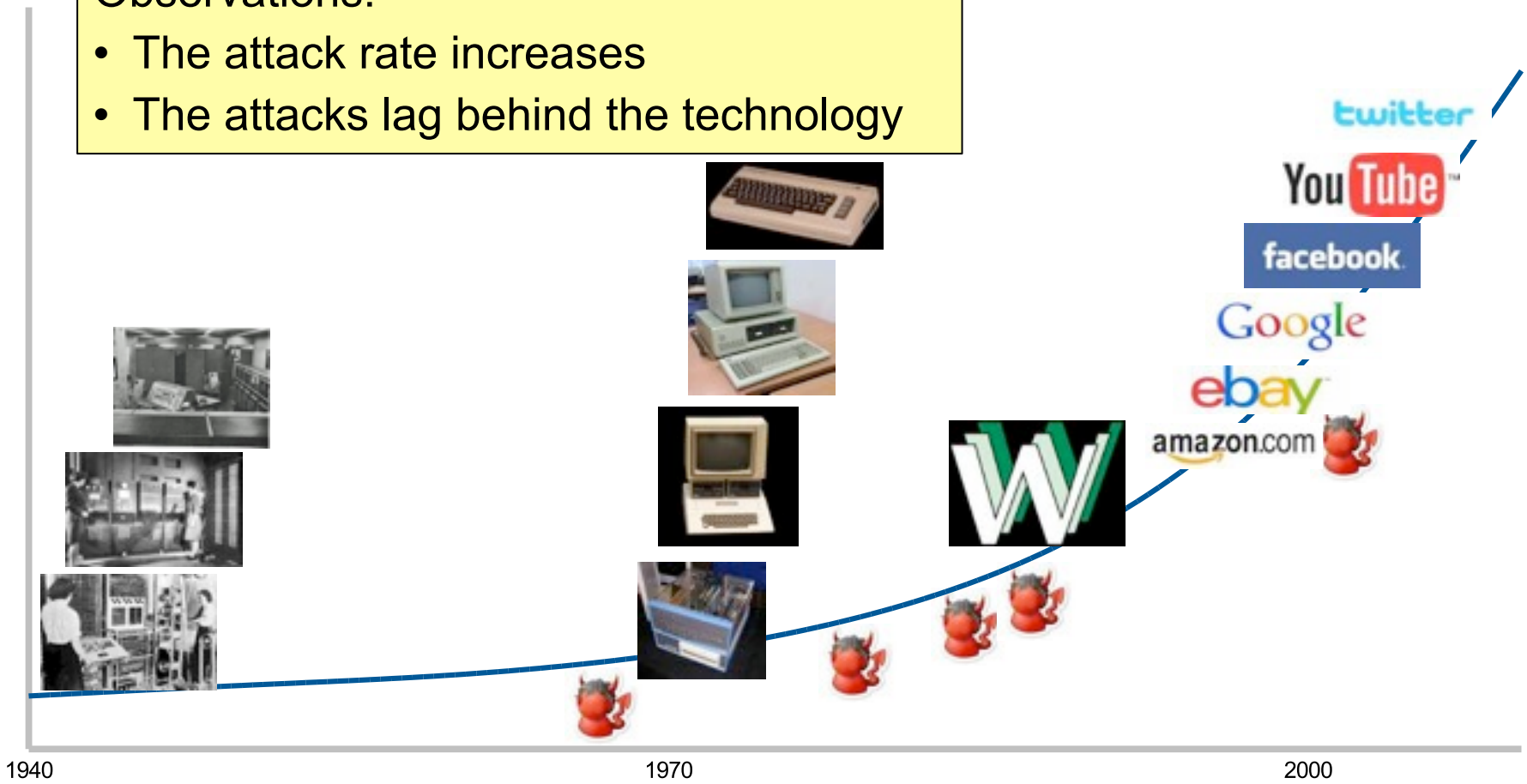


Timeline: Computer Security Attacks

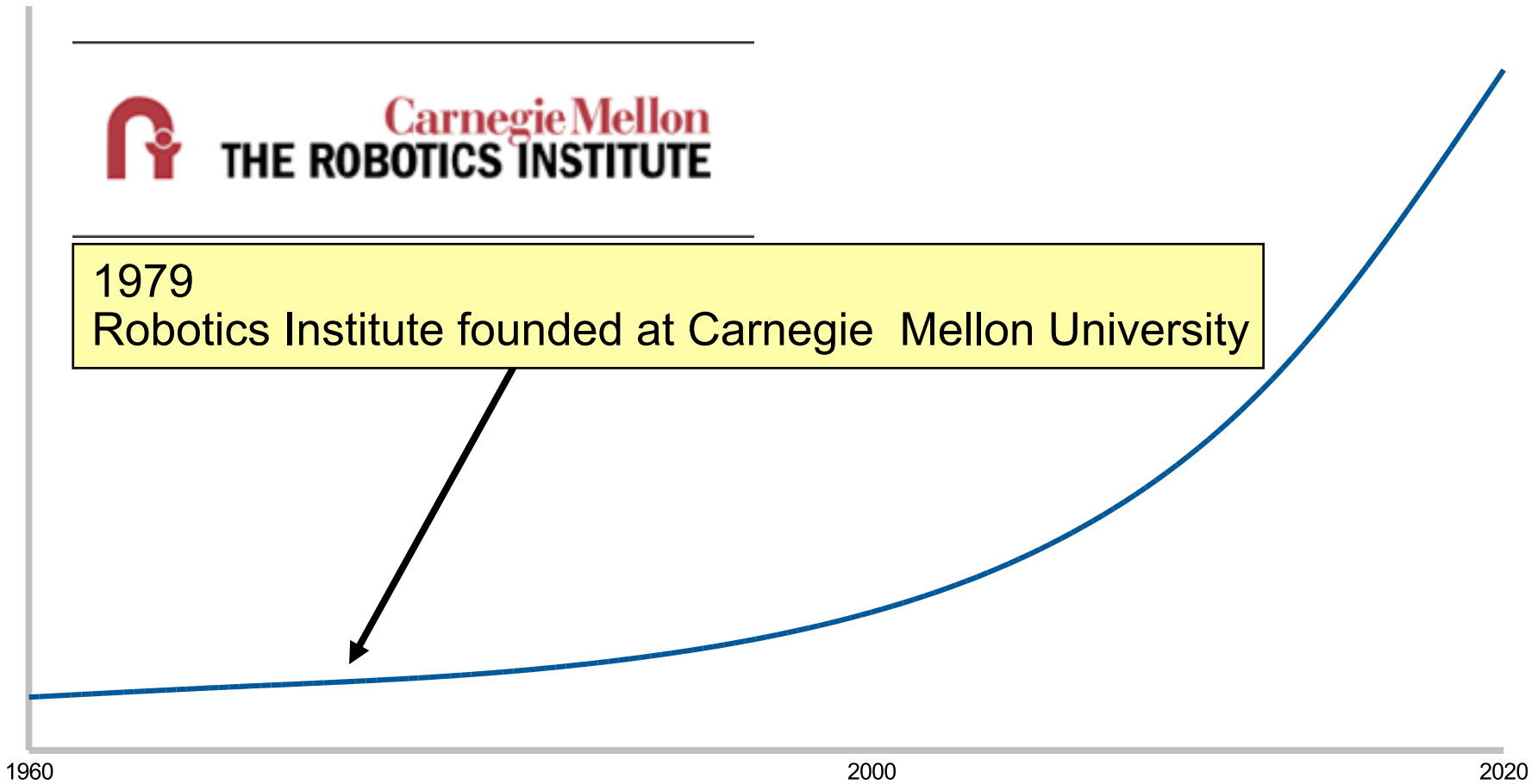


Timeline: Computer Security Attacks

Observations:
- The attack rate increases
- The attacks lag behind the technology



Timeline: Robots



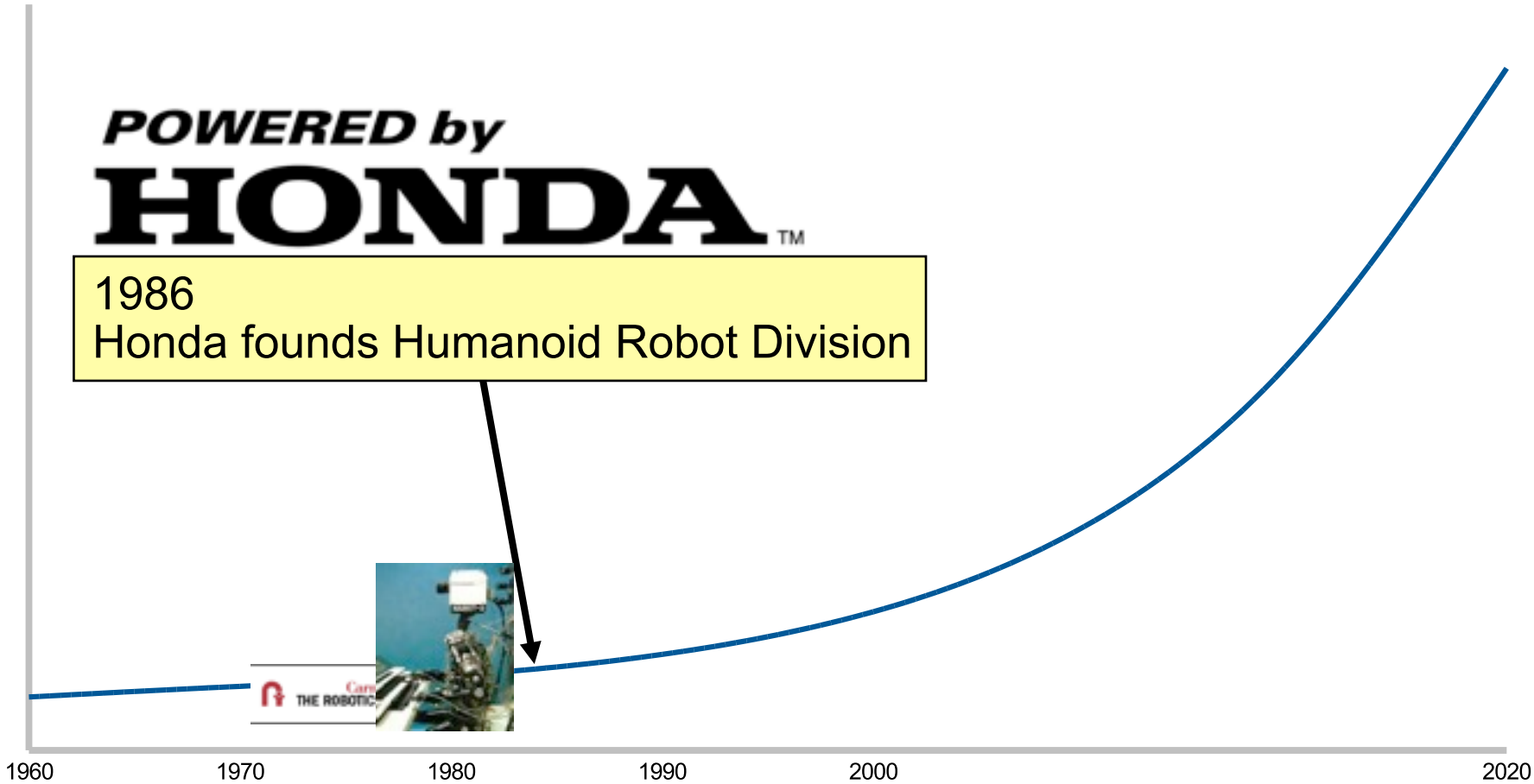
Timeline: Robots

1982
WABOT-2 accompanies people on a keyboard instrument

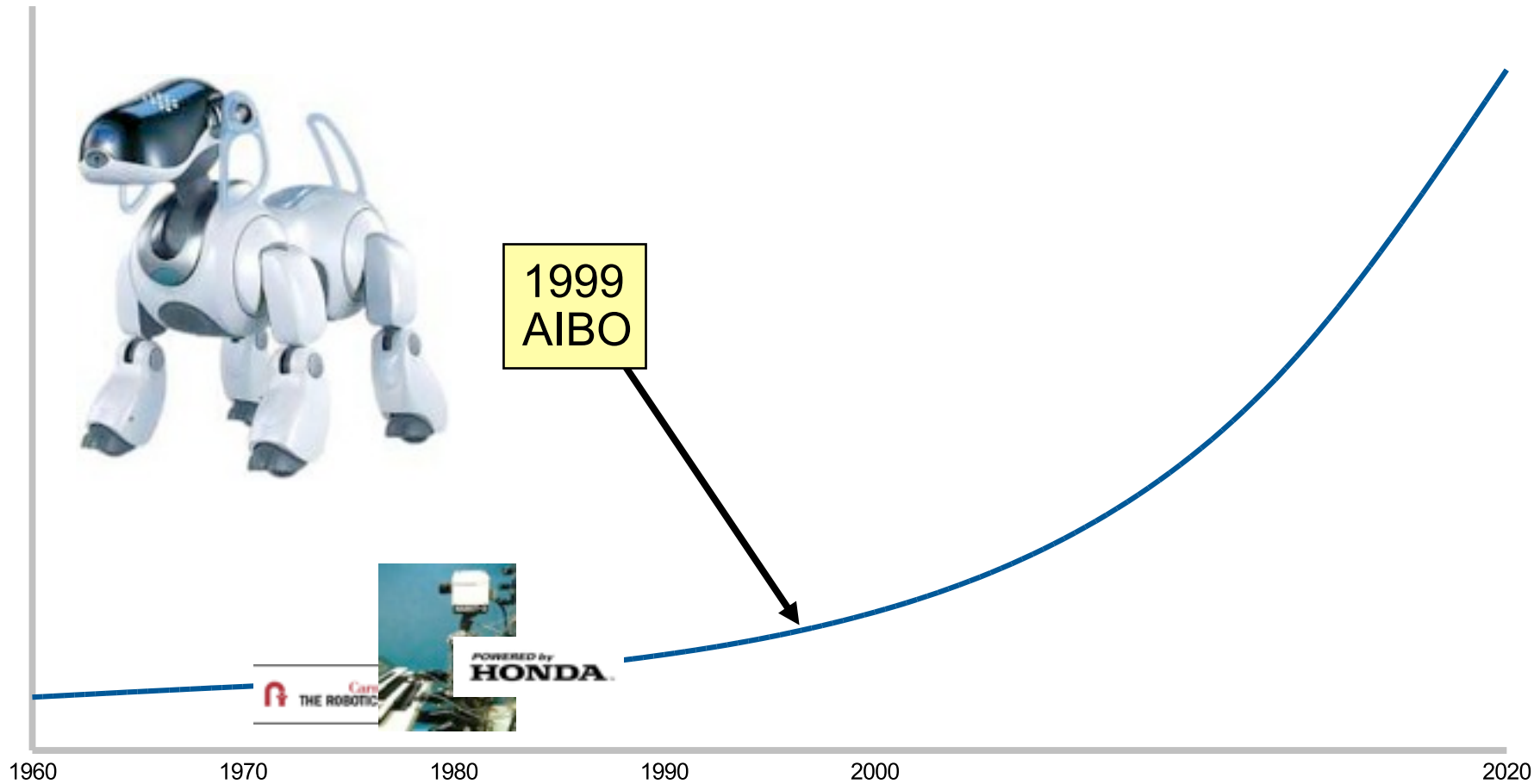
Carnegie Mellon
THE ROBOTICS INSTITUTE

1960 1970 1980 1990 2000 2020

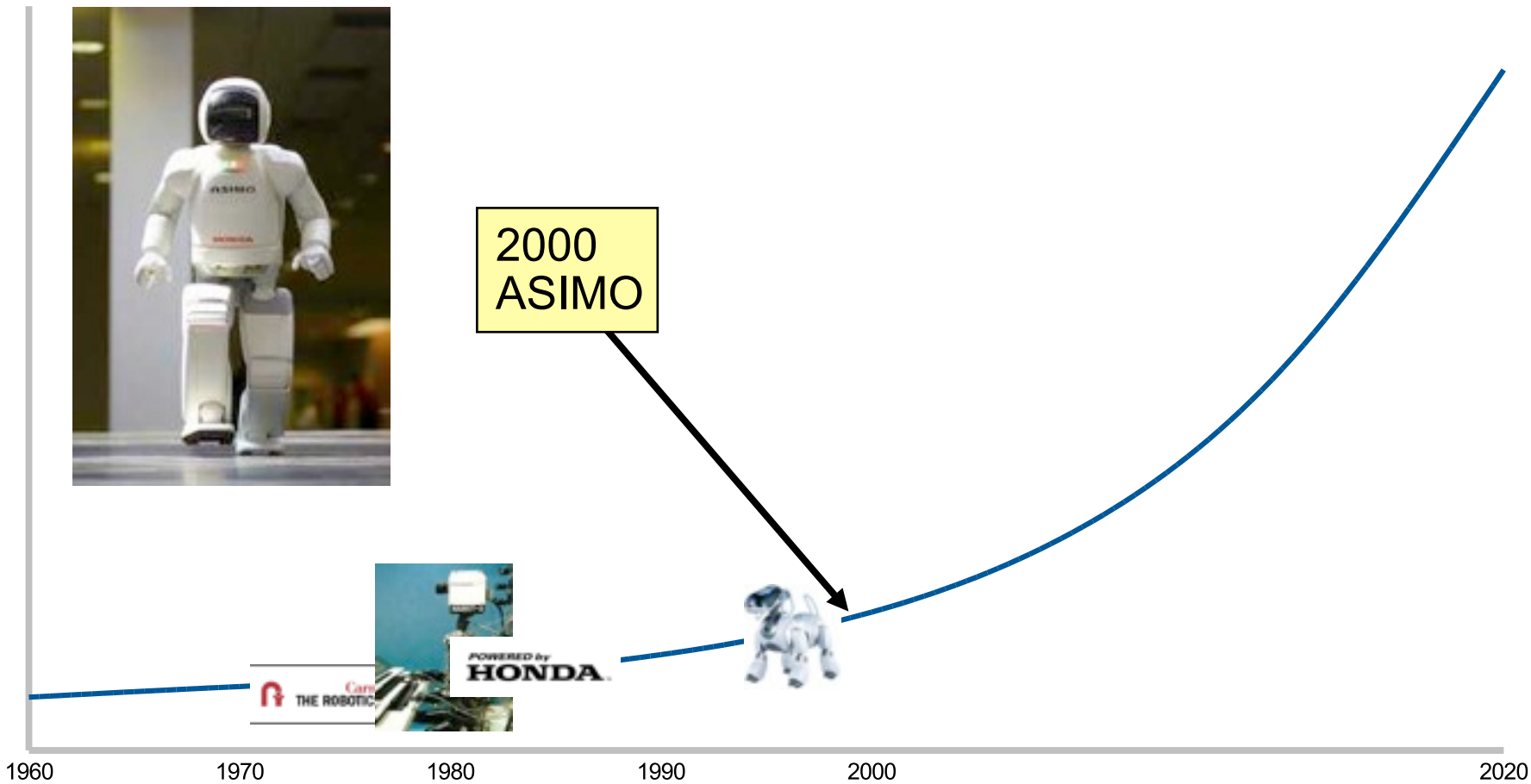
Timeline: Robots



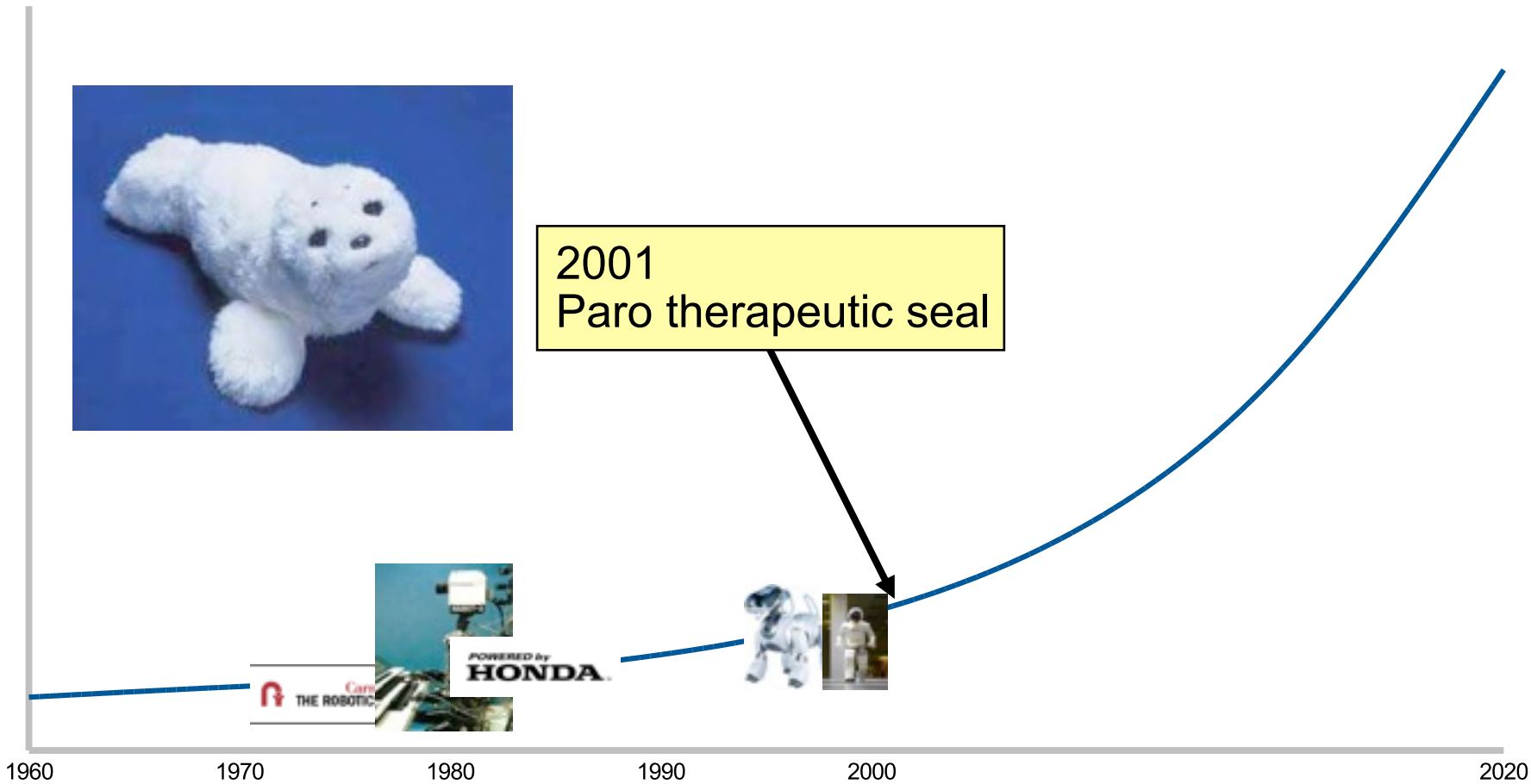
Timeline: Robots



Timeline: Robots



Timeline: Robots



Timeline: Robots

2002
Roomba

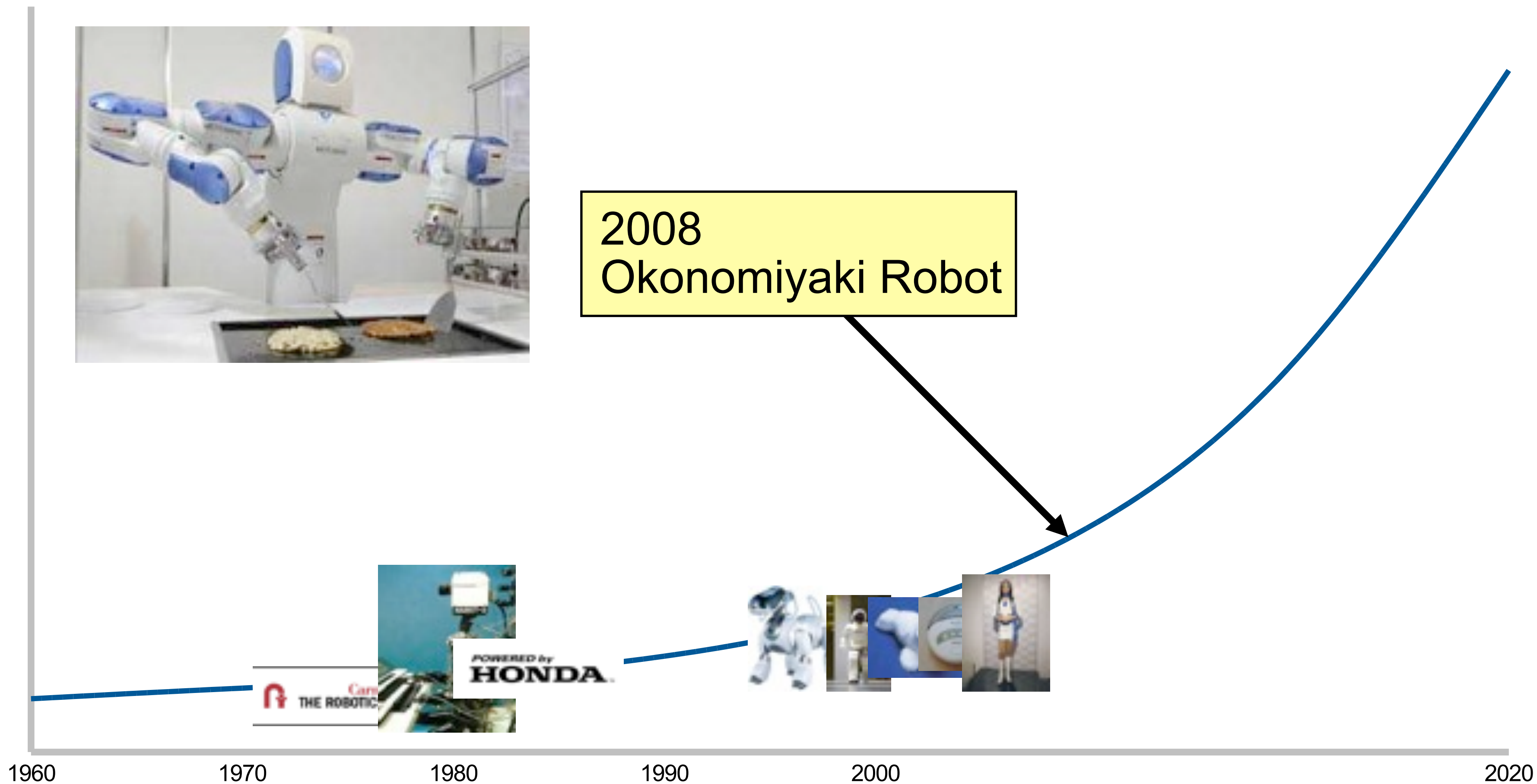
1960 1970 1980 1990 2000 2020

Timeline: Robots

2005
Actroid Android

1960 1970 1980 1990 2000 2020

Timeline: Robots



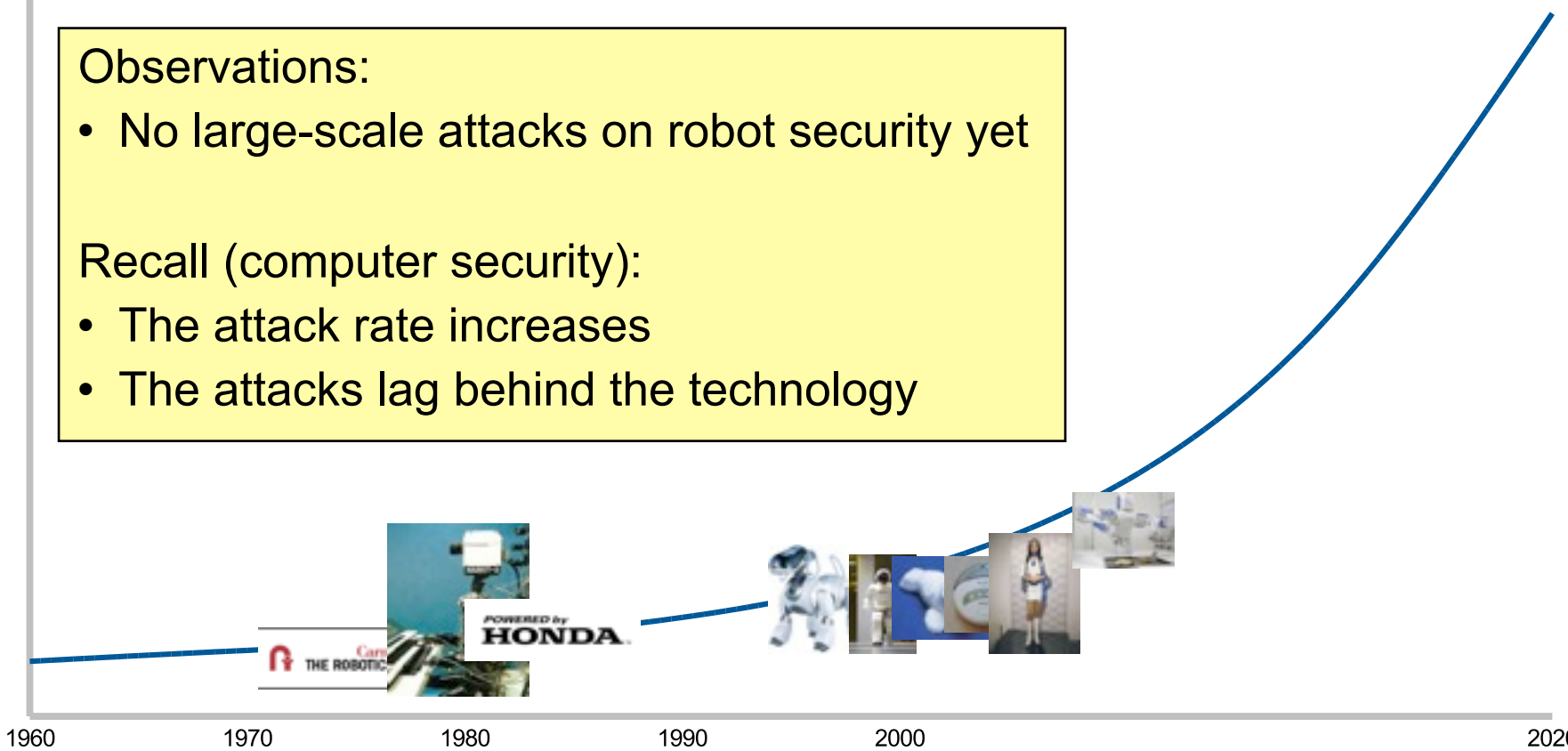
Timeline: Robots

Observations:

- No large-scale attacks on robot security yet

Recall (computer security):

- The attack rate increases
- The attacks lag behind the technology



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

Rovio

- For adults
- Telepresence
- Home surveillance
- Check up on relatives
- Follows pre-programmed IR beacons
- Controlled via web interface

Spykee

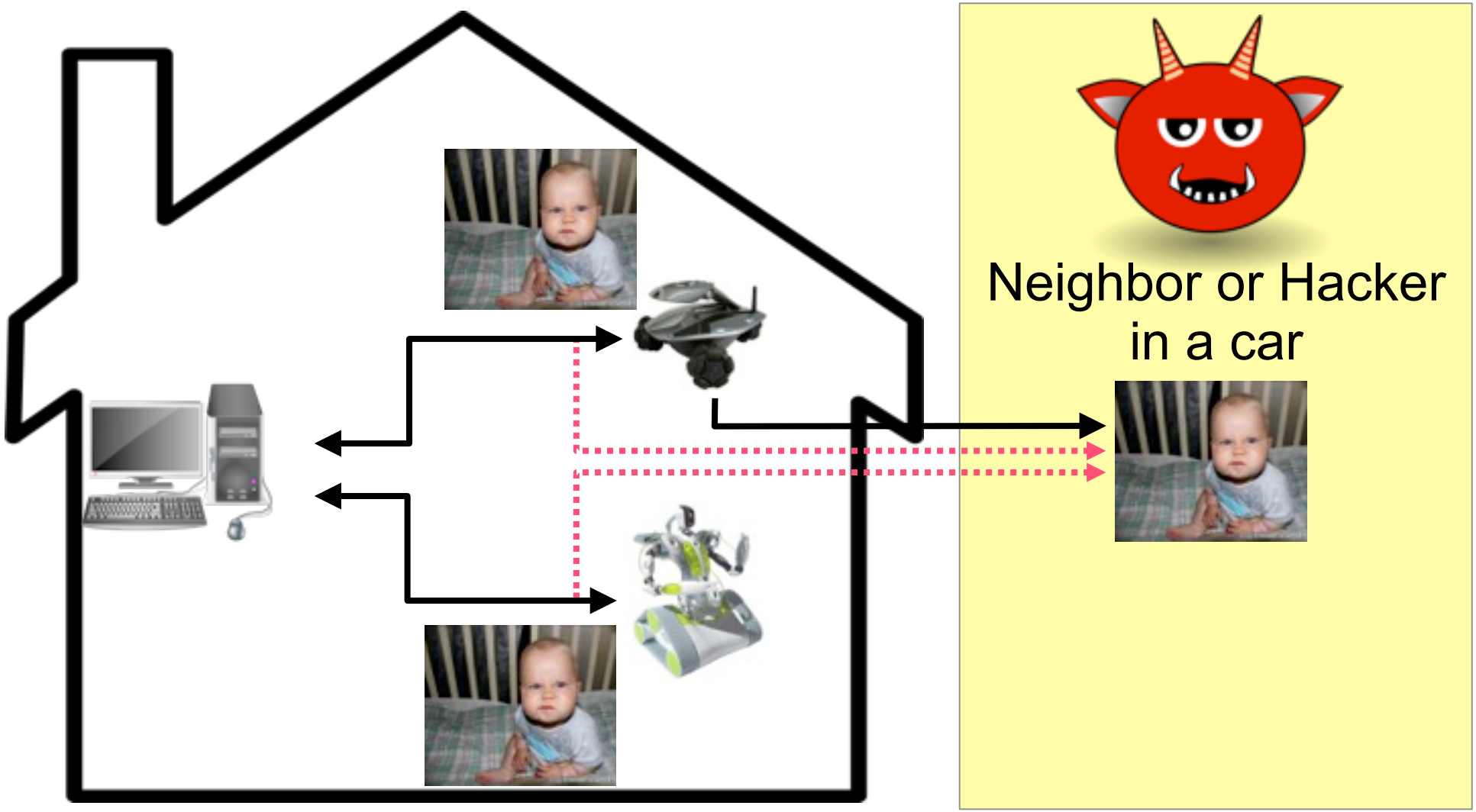
- Toy for children
- Assembled and configured by children
- Telepresence: Parent can tuck in kids when out of town
- “Spy” robot
- Controlled via program

Discovered Vulnerabilities

Remote Discovery

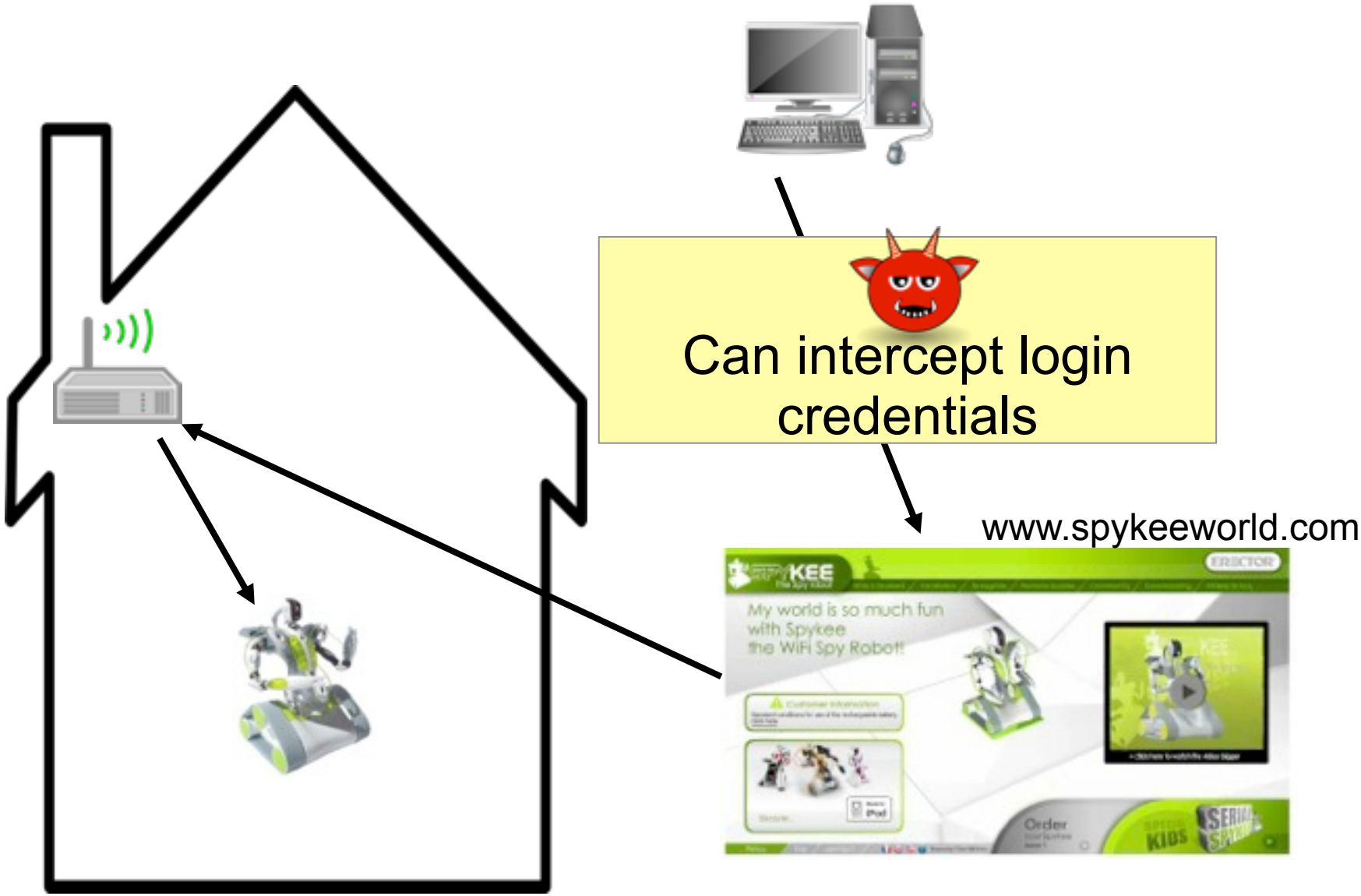
A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons, T. Denning et al.

Eavesdropping



A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons, T. Denning et al.

Intercepting Credentials (MITM)



Physical Takeover

- With credentials: Drive the robot anywhere
- Access the AV stream at any time

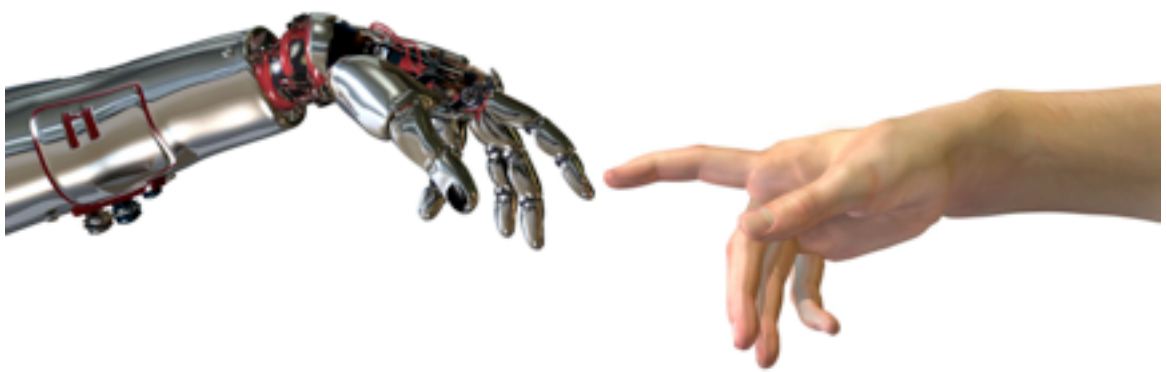
Possible Attacks

- Robot vandalism
  - Damage fragile object
  - Knock object off of a table
  - Damaging the robot itself (robot suicide)
- Manipulate Objects
  - Use mobility to locate (physical) key
    - Take image of a key
    - Pick up and hide key
- Eldercare
  - Robot used to trip an elder
  - Play noises and speech to confuse elder

Mechatronic Security
and
Robot Authentication

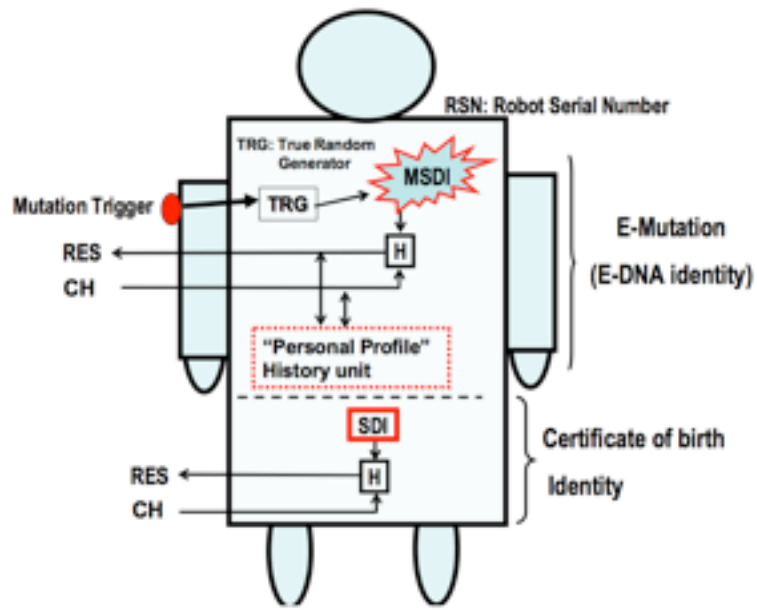
Robot as Living Individuals

- Born at some point
  - Has non-clonable DNA
  - Gets a birth certificate
- Starts usual transactions with its environment
  - Learning, developing its knowledge and capabilities
- Gets old
  - Has to be repaired, or
  - dies



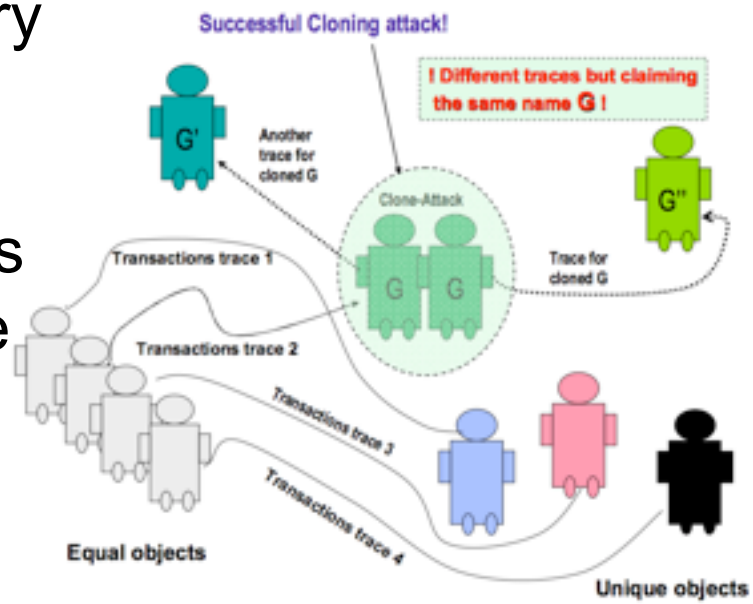
Bio-Inspired Robot Identity

- Biological mutation
  - Permanent irremovable change
- Electronic mutation
  - Simulated change
- e-DNA
  - Generate e-DNA chain from e-Mutation



Detecting Cloning Attack

- Cloning almost impossible
  - Crack mutated identity
  - Copy all robot transactions history
- Detect Cloning Attack
  - Two G units with same properties
  - Each unit G generates new trace
  - G' and G'' most likely different
  - Both systems claim to be G ↯
  - Identification process will fail



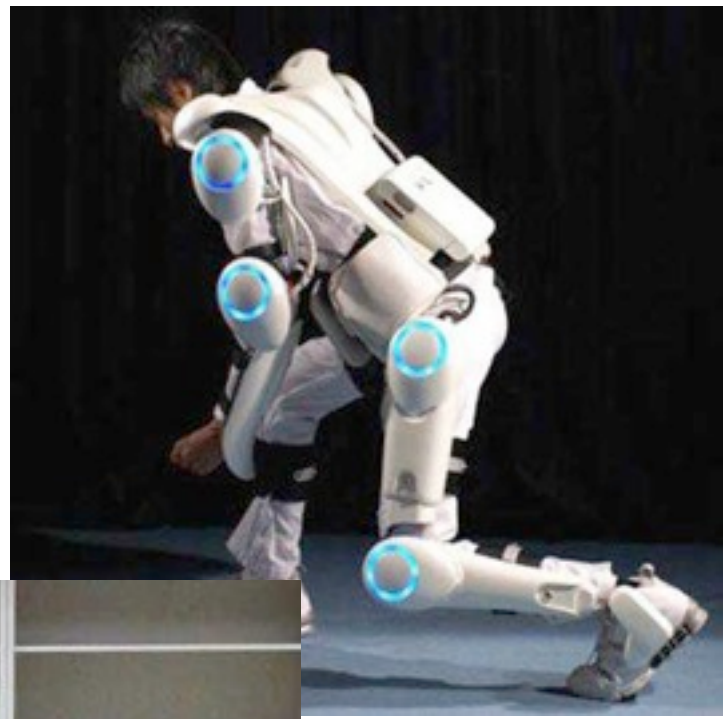
Mechatronic Security Goals

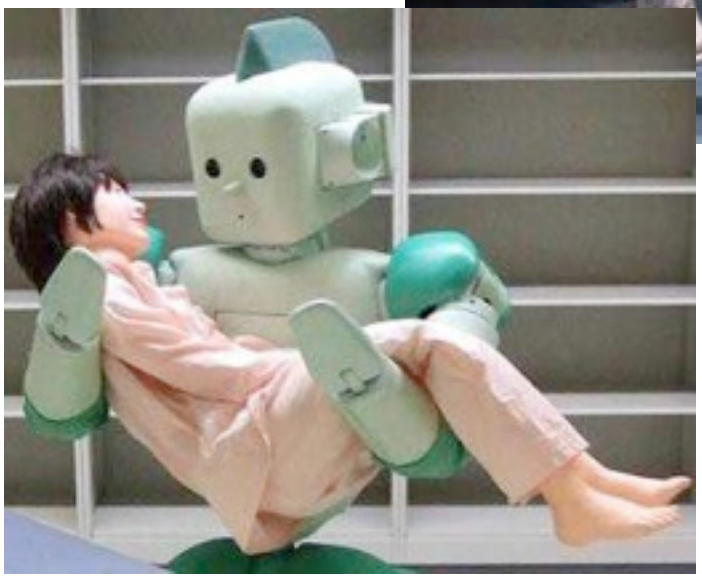
- Robot is provable witness of event
- Robot can prove having performed action
- Robot cannot falsly claim to have performed action

Risks of Tomorrow

Risks of Tomorrow

- Robots for elders
  - Exoskeleton for mobility
  - Lifting robot





Risks of Tomorrow

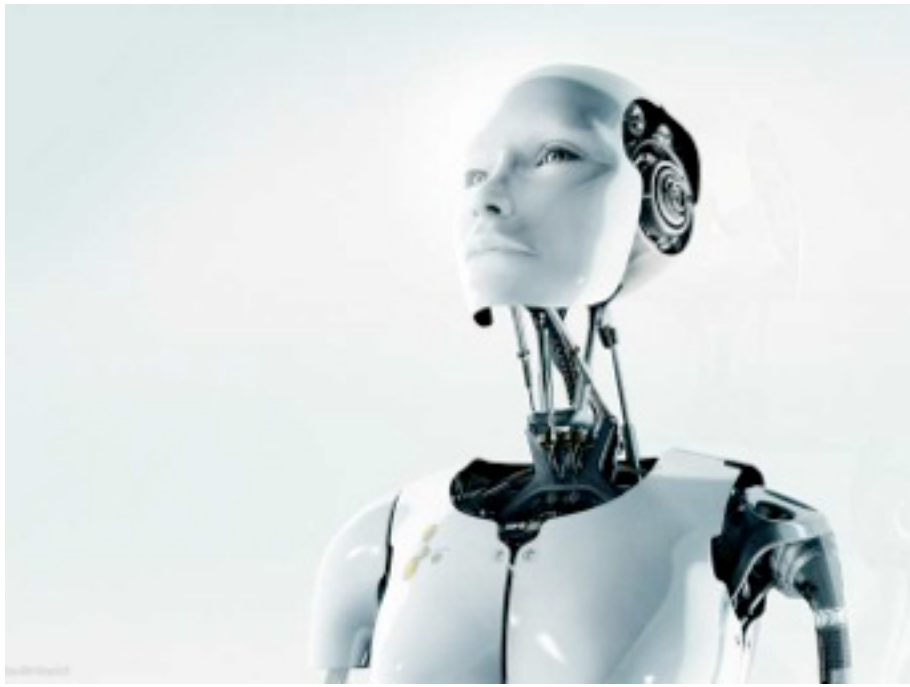
- Robots for elders
  - Exoskeleton for mobility
  - Lifting robot
- Robots for children
  - As companions or as therapy for unique emotional needs

Risks of 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

Risks of 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
- Robots with sophisticated A.I.



Are the Risks real?

Potential types of attackers

- Terrorists
- Competitor
- Acquaintance
- ID Thief
- Prankster
- Governments

Conclusion

- Spykee and Rovio robots are “only” toys
  - Security not first priority
  - Vulnerabilities not specific to robots
    - Can be easily fixed
- Future robots more complex
  - Even developers don't understand reasons for behavior
  - Difficult to detect an enemy's attack
  - How to prevent the robot from leaking information?
- Young area of research
  - Lack of detailed studies
  - Difficult to predict technology

Questions?